NAME: BINYANYA DEBORAH NYATICHI

CS NO: ADC-CSS02-25051.

DESCRIPTION: Week 3 Assignment 5

ASSIGNMENT: Lab on Describe the capabilities of Microsoft Security Solutions

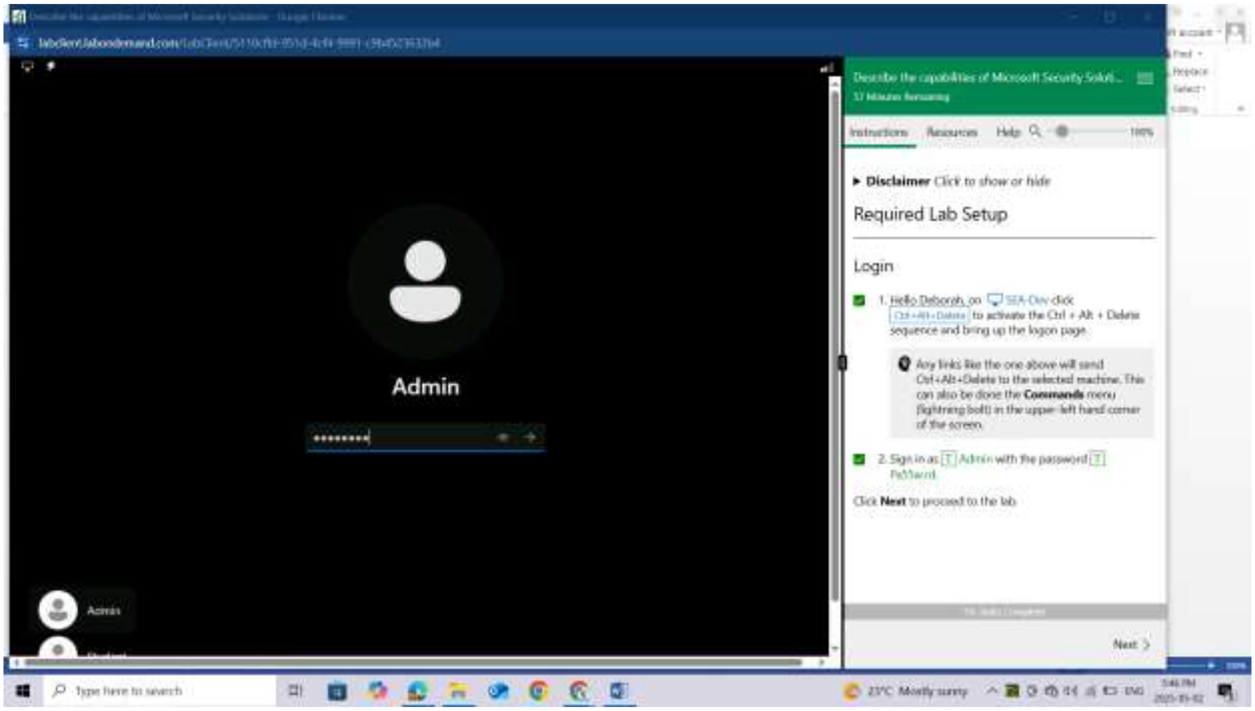
DATE: 02/05/2025

INTRODUCTION

This week, I will be working on a series of labs designed to help me explore the capabilities of Microsoft Security Solutions. I will begin by setting up a Microsoft 365 tenant, which will provide the foundation for testing and configuring various security features. I will then explore tools such as Azure Network Security Groups (NSGs), Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Defender for Cloud Apps, and the Microsoft Defender portal. Through these labs, I aim to gain hands-on experience in managing cloud security, monitoring threats, and understanding how Microsoft's integrated tools work together to protect enterprise environments.

REQUIRED LAB SETUP

Login to your virtual machine



Describe the capabilities of Microsoft Security Soluti...
57 Minutes Remaining

▸ Disclaimer Click to show or hide

Required Lab Setup

Login

1. Hello Deborah, on SEA-Dev click Ctrl+Alt+Delete to activate the Ctrl + Alt + Delete sequence and bring up the logon page.

Any links like the one above will send Ctrl+Alt+Delete to the selected machine. This can also be done the **Commands** menu (lightning bolt) in the upper-left hand corner of the screen.

2. Sign in as Admin with the password Pa55w.rd

Click **Next** to proceed to the lab.

LAB: SETUP OF THE MICROSOFT 365 TENANT

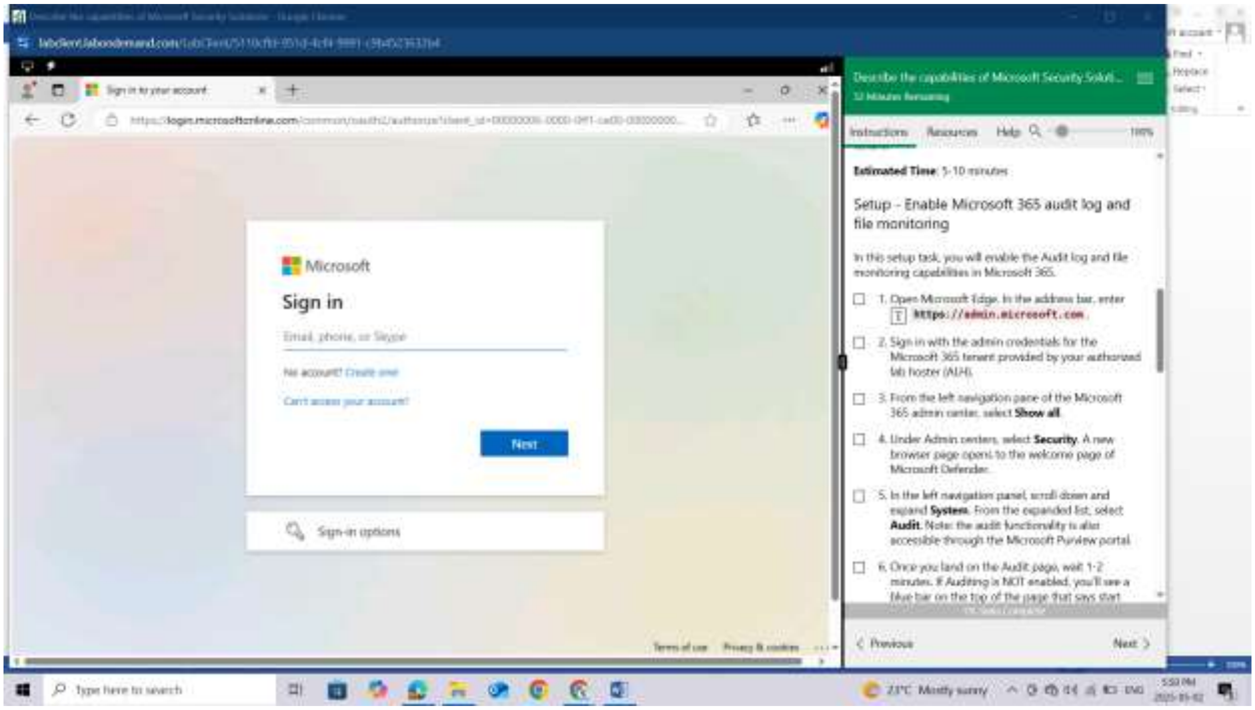
Lab scenario

This setup lab consists of enabling the Microsoft Audit Log and file monitoring capabilities in the Microsoft 365 tenant.

Setup - Enable Microsoft 365 audit log and file monitoring

In this setup task, you will enable the Audit log and file monitoring capabilities in Microsoft 365.

Open Microsoft Edge. In the address bar, enter https://admin.microsoft.com.



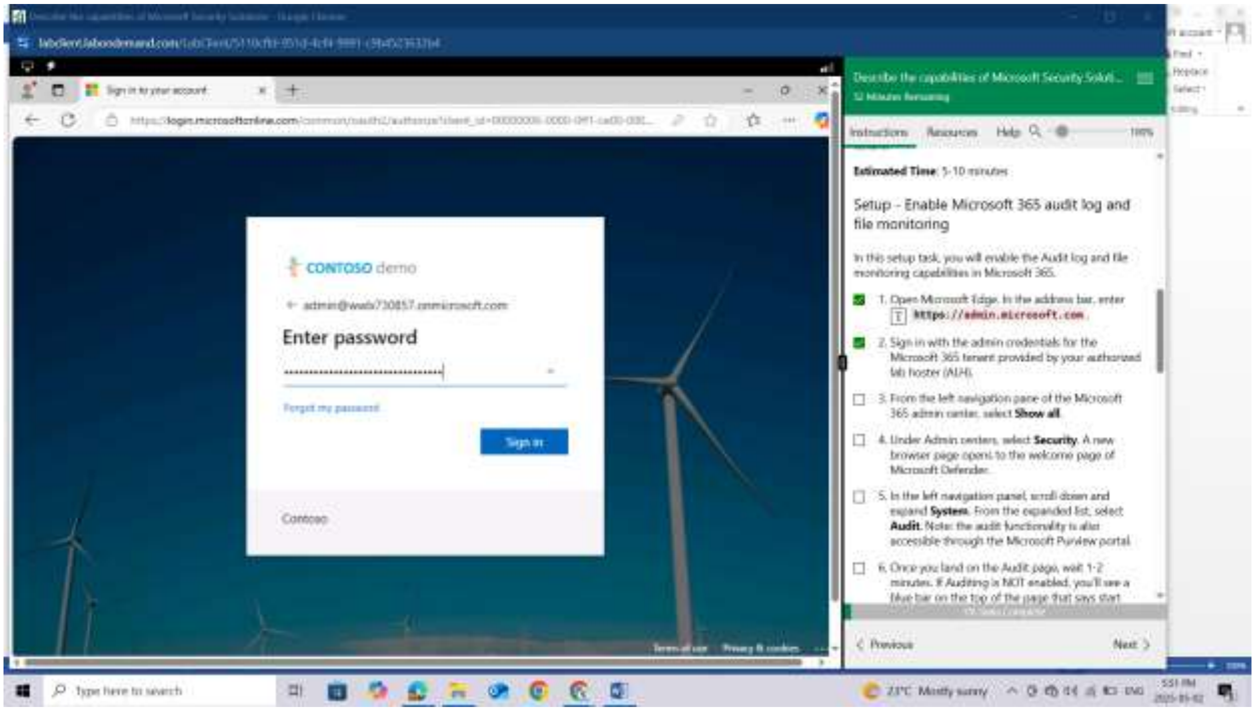
Estimated Time: 5-10 minutes

Setup - Enable Microsoft 365 audit log and file monitoring

In this setup task, you will enable the Audit log and file monitoring capabilities in Microsoft 365.

- ☐ 1. Open Microsoft Edge. In the address bar, enter `https://admin.microsoft.com`.
- ☐ 2. Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).
- ☐ 3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.
- ☐ 4. Under Admin centers, select **Security**. A new browser page opens to the welcome page of Microsoft Defender.
- ☐ 5. In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note: the audit functionality is also accessible through the Microsoft Purview portal.
- ☐ 6. Once you land on the Audit page, wait 1-2 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start

Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).



admin@wads730857.onmicrosoft.com

Enter password

••••••••••••••••••••••••••••••••

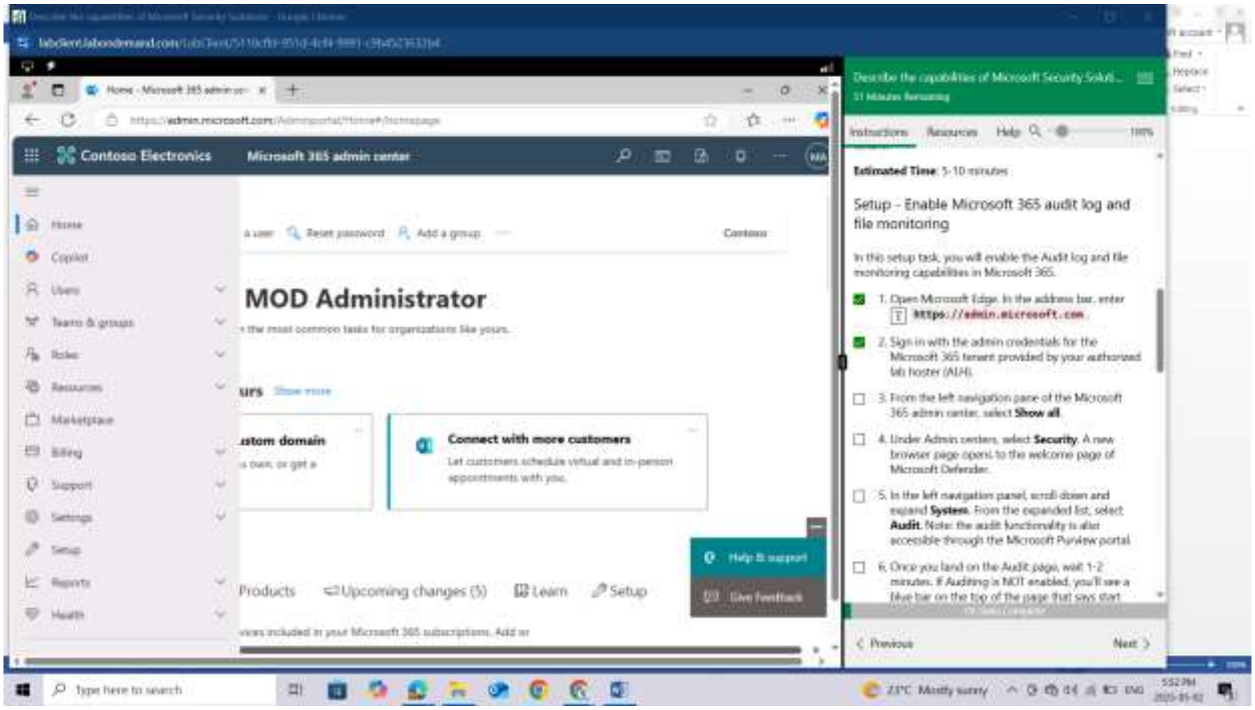
Estimated Time: 5-10 minutes

Setup - Enable Microsoft 365 audit log and file monitoring

In this setup task, you will enable the Audit log and file monitoring capabilities in Microsoft 365.

- ☑ 1. Open Microsoft Edge. In the address bar, enter `https://admin.microsoft.com`.
- ☑ 2. Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).
- ☐ 3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.
- ☐ 4. Under Admin centers, select **Security**. A new browser page opens to the welcome page of Microsoft Defender.
- ☐ 5. In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note: the audit functionality is also accessible through the Microsoft Purview portal.
- ☐ 6. Once you land on the Audit page, wait 1-2 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start

From the left navigation pane of the Microsoft 365 admin center, select **Show all.**



MOD Administrator

Connect with more customers

Let customers schedule virtual and in-person appointments with you.

Describe the capabilities of Microsoft Security Soluti...

51 Minutes Remaining

Estimated Time: 5-10 minutes

Setup - Enable Microsoft 365 audit log and file monitoring

In this setup task, you will enable the Audit log and file monitoring capabilities in Microsoft 365.

☑ 1. Open Microsoft Edge. In the address bar, enter `https://admin.microsoft.com`.

☑ 2. Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).

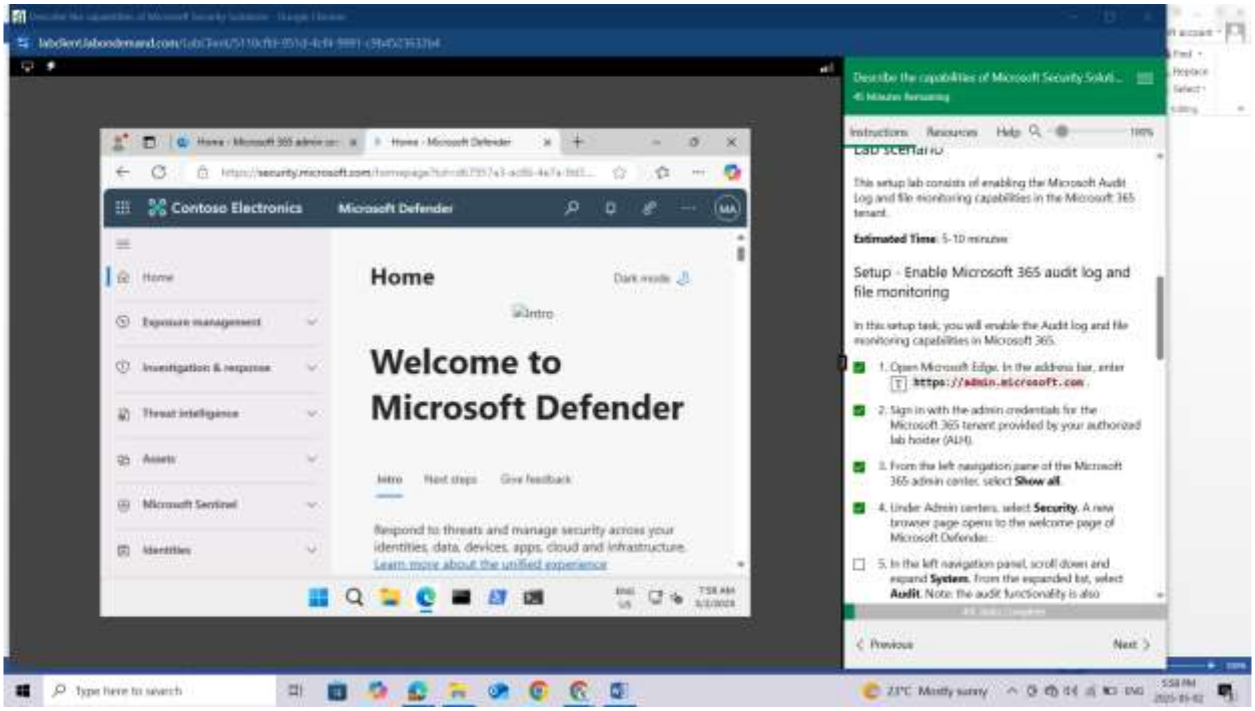
□ 3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.

□ 4. Under Admin centers, select **Security**. A new browser page opens to the welcome page of Microsoft Defender.

□ 5. In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note: the audit functionality is also accessible through the Microsoft Purview portal.

□ 6. Once you land on the Audit page, wait 1-2 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start

Under Admin centers, select **Security**. A new browser page opens to the welcome page of Microsoft Defender.



Home

Welcome to Microsoft Defender

Respond to threats and manage security across your identities, data, devices, apps, cloud and infrastructure.

Learn more about the unified experience

Describe the capabilities of Microsoft Security Soluti...

45 Minutes Remaining

Lab scenario

This setup lab consists of enabling the Microsoft Audit Log and file monitoring capabilities in the Microsoft 365 tenant.

Estimated Time: 5-10 minutes

Setup - Enable Microsoft 365 audit log and file monitoring

In this setup task, you will enable the Audit log and file monitoring capabilities in Microsoft 365.

☑ 1. Open Microsoft Edge. In the address bar, enter `https://admin.microsoft.com`.

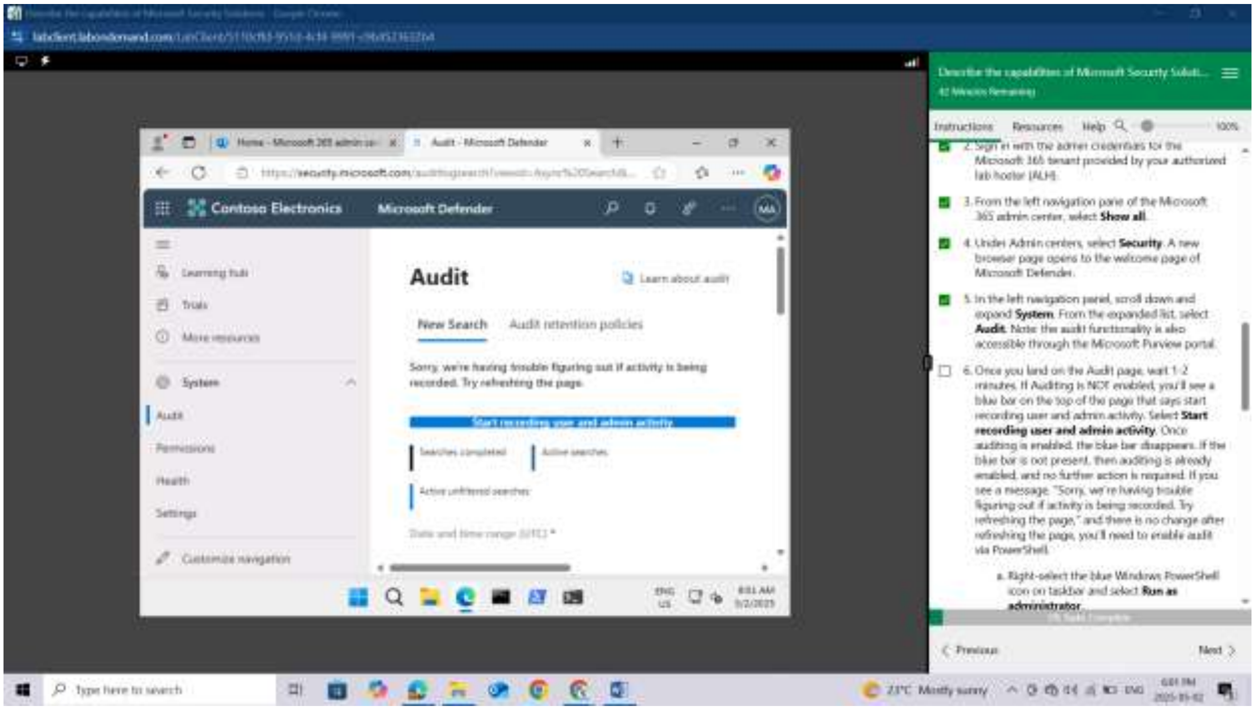
☑ 2. Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).

☑ 3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.

☑ 4. Under Admin centers, select **Security**. A new browser page opens to the welcome page of Microsoft Defender.

□ 5. In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note: the audit functionality is also

In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note: the audit functionality is also accessible through the Microsoft Purview portal.



Audit

Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page.

☑ 2. Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).

☑ 3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.

☑ 4. Under Admin centers, select **Security**. A new browser page opens to the welcome page of Microsoft Defender.

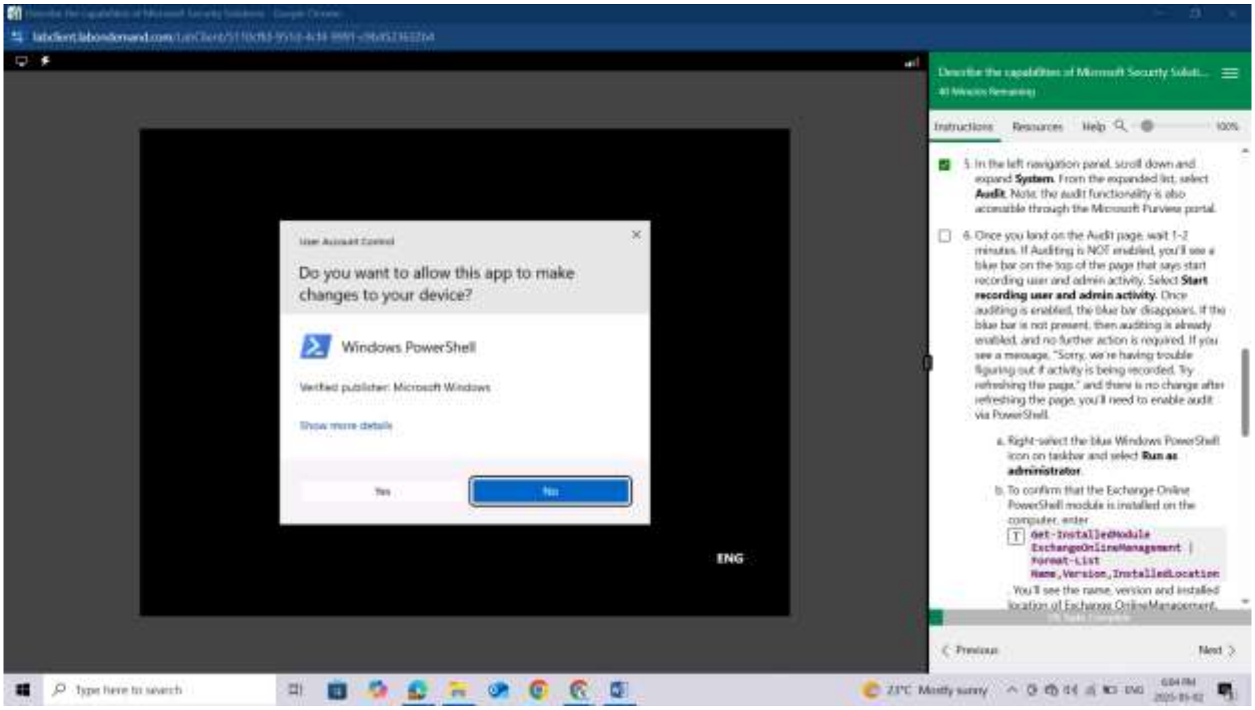
☑ 5. In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note the audit functionality is also accessible through the Microsoft Purview portal.

□ 6. Once you land on the Audit page, wait 1-2 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start recording user and admin activity. Select **Start recording user and admin activity**. Once auditing is enabled, the blue bar disappears. If the blue bar is not present, then auditing is already enabled, and no further action is required. If you see a message, "Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page," and there is no change after refreshing the page, you'll need to enable audit via PowerShell.

a. Right-select the blue Windows PowerShell icon on taskbar and select **Run as administrator**.

Once you land on the Audit page, wait 1-2 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says **start recording user and admin activity**. Select Start recording user and admin activity. Once auditing is enabled, the blue bar disappears. If the blue bar is not present, then auditing is already enabled, and no further action is required. If you see a message, "Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page," and there is no change after refreshing the page, you'll need to enable audit via PowerShell.

Right-select the blue Windows PowerShell icon on taskbar and select **Run as administrator.**



User Account Control

Do you want to allow this app to make changes to your device?

Windows PowerShell

Verified publisher: Microsoft Windows

Show more details

Yes No

Describe the capabilities of Microsoft Security Soluti...

Instructions Resources Help 100%

☑ 5. In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note: the audit functionality is also accessible through the Microsoft Purview portal.

□ 6. Once you land on the Audit page, wait 1-2 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start recording user and admin activity. Select **Start recording user and admin activity**. Once auditing is enabled, the blue bar disappears. If the blue bar is not present, then auditing is already enabled, and no further action is required. If you see a message, "Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page," and there is no change after refreshing the page, you'll need to enable audit via PowerShell.

a. Right-select the blue Windows PowerShell icon on taskbar and select **Run as administrator**.

b. To confirm that the Exchange Online PowerShell module is installed on the computer, enter

```
Get-InstalledModule ExchangeOnlineManagement | Format-List Name,Version,InstalledLocation
```

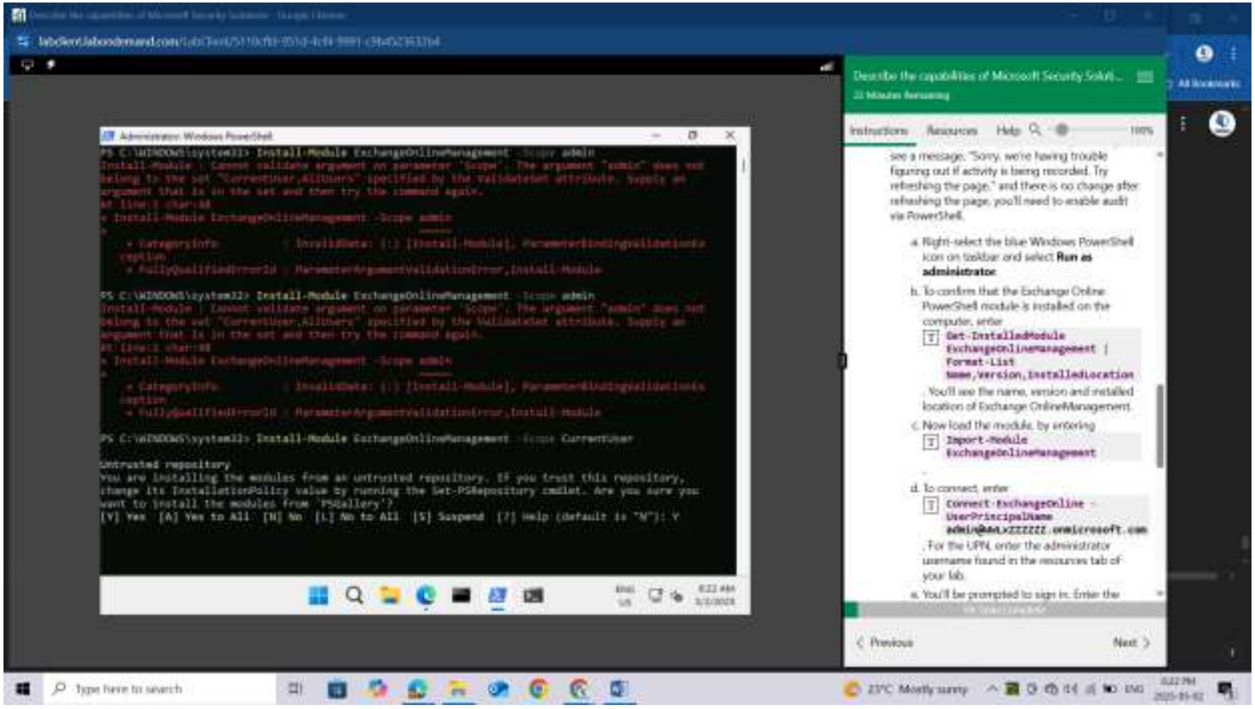
. You'll see the name, version and installed location of Exchange OnlineManagement.

Previous Next

To confirm that the Exchange Online PowerShell module is installed on the computer, enter

Get-InstalledModule ExchangeOnlineManagement | Format-List Name,Version,InstalledLocation. You'll see the name, version and installed location of Exchange OnlineManagement.

If its not yet install you can install using the command: **Install-Module ExchangeOnlineManagement -Scope CurrentUser**



Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> Install-Module ExchangeOnlineManagement -Scope admin
Install-Module : Cannot validate argument on parameter 'Scope'. The argument "admin" does not
belong to the set "CurrentUser,AllUsers" specified by the ValidateSet attribute. Supply an
argument that is in the set and then try the command again.
At line:1 char:48
+ Install-Module ExchangeOnlineManagement -Scope admin
+                                                ~~~~~
    + CategoryInfo          : InvalidData: (:) [Install-Module], ParameterBindingValidationEx
   ception
    + FullyQualifiedErrorId : ParameterArgumentValidationError,Install-Module

PS C:\WINDOWS\system32> Install-Module ExchangeOnlineManagement -Scope admin
Install-Module : Cannot validate argument on parameter 'Scope'. The argument "admin" does not
belong to the set "CurrentUser,AllUsers" specified by the ValidateSet attribute. Supply an
argument that is in the set and then try the command again.
At line:1 char:48
+ Install-Module ExchangeOnlineManagement -Scope admin
+                                                ~~~~~
    + CategoryInfo          : InvalidData: (:) [Install-Module], ParameterBindingValidationEx
   ception
    + FullyQualifiedErrorId : ParameterArgumentValidationError,Install-Module

PS C:\WINDOWS\system32> Install-Module ExchangeOnlineManagement -Scope CurrentUser

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository,
change its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you
want to install the modules from 'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
```

Describe the capabilities of Microsoft Security Soluti...

Instructions Resources Help 100%

see a message, "Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page," and there is no change after refreshing the page, you'll need to enable audit via PowerShell.

a. Right-select the blue Windows PowerShell icon on taskbar and select **Run as administrator**.

b. To confirm that the Exchange Online PowerShell module is installed on the computer, enter

```
Get-InstalledModule ExchangeOnlineManagement | Format-List Name,Version,InstalledLocation
```

. You'll see the name, version and installed location of Exchange OnlineManagement.

c. Now load the module, by entering

```
Import-Module ExchangeOnlineManagement
```

d. To connect, enter

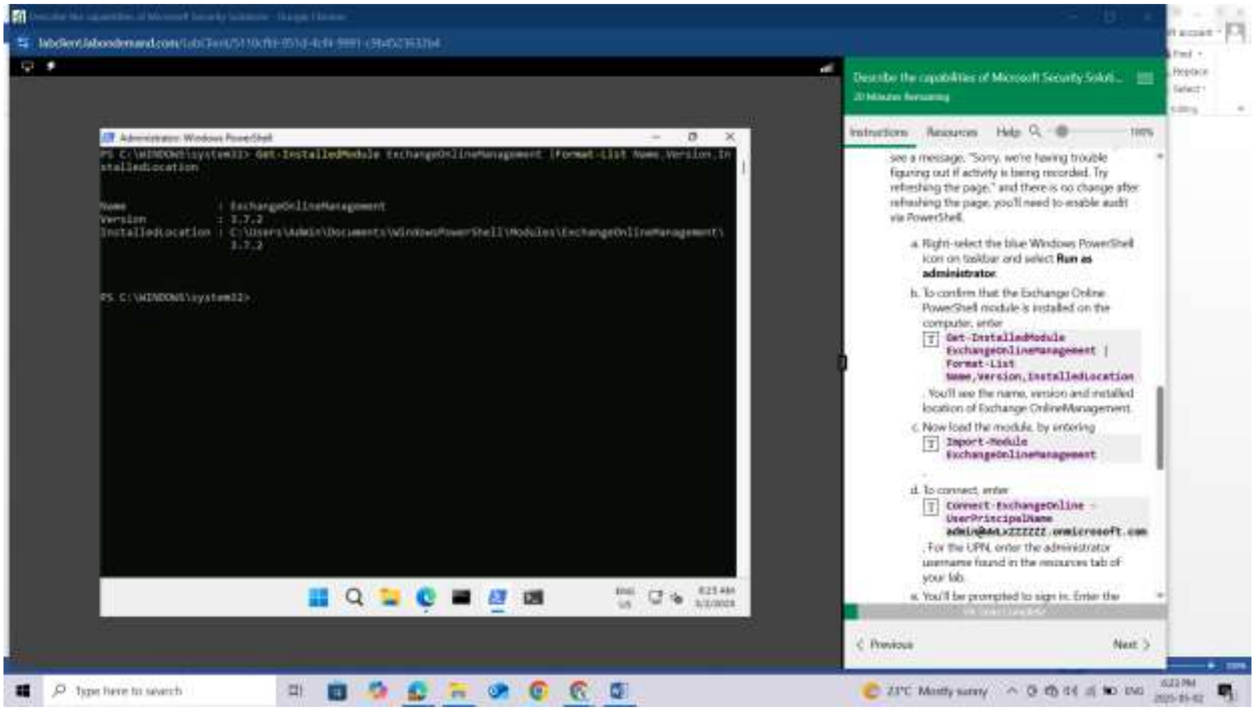
```
Connect-ExchangeOnline -UserPrincipalName admin@xxxZZZZZZ.onmicrosoft.com
```

. For the UPN, enter the administrator username found in the resources tab of your lab.

e. You'll be prompted to sign in. Enter the

Previous Next

Confirm installation with: **Get-InstalledModule ExchangeOnlineManagement | Format-List Name,Version,InstalledLocation**



```
PS C:\WINDOWS\system32> Get-InstalledModule ExchangeOnlineManagement |Format-List Name,Version,In
stalledLocation


Name              : ExchangeOnlineManagement
Version           : 3.7.2
InstalledLocation : C:\Users\Admin\Documents\WindowsPowerShell\Modules\ExchangeOnlineManagement\
                    3.7.2



PS C:\WINDOWS\system32>
```

Describe the capabilities of Microsoft Security Soluti...

20 Minutes Remaining

see a message. "Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page." and there is no change after refreshing the page, you'll need to enable audit via PowerShell.

a. Right-select the blue Windows PowerShell icon on taskbar and select **Run as administrator**.

b. To confirm that the Exchange Online PowerShell module is installed on the computer, enter

```
Get-InstalledModule ExchangeOnlineManagement | Format-List Name,Version,InstalledLocation
```

. You'll see the name, version and installed location of Exchange OnlineManagement.

c. Now load the module, by entering

```
Import-Module ExchangeOnlineManagement
```

.

d. To connect, enter

```
Connect-ExchangeOnline -UserPrincipalName admin@WWLxZZZZZZ.onmicrosoft.com
```

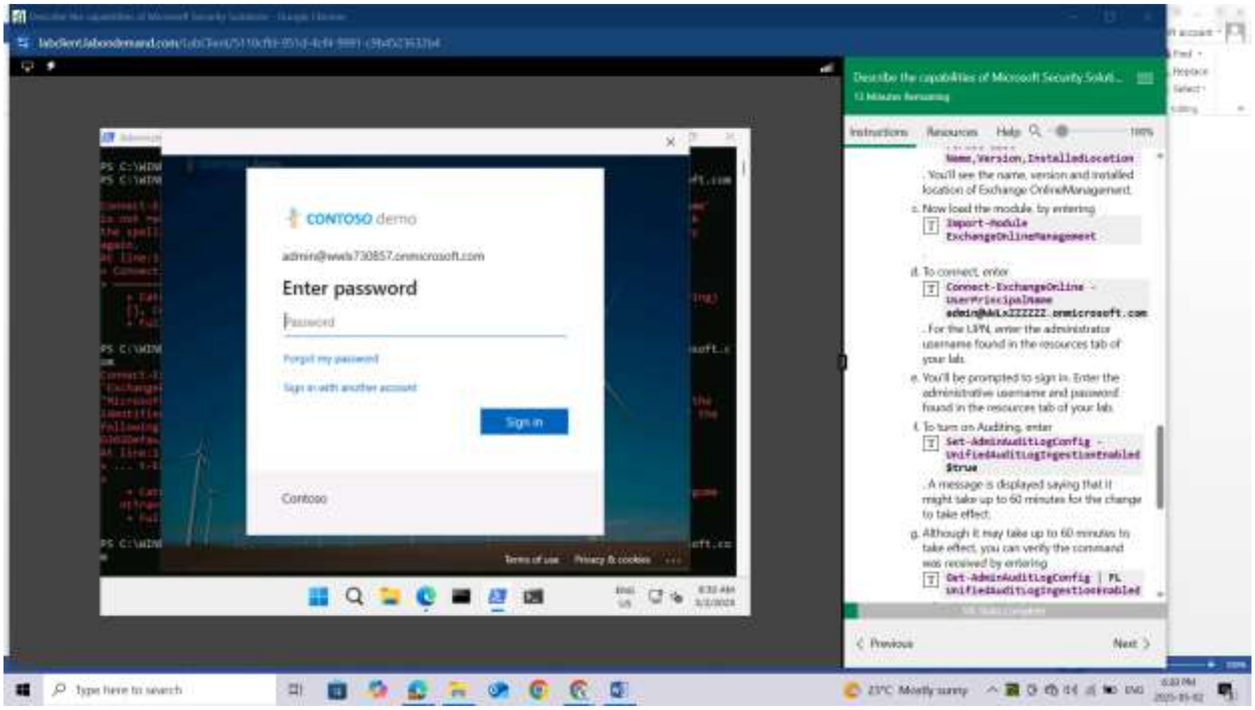
. For the UPN, enter the administrator username found in the resources tab of your lab.

e. You'll be prompted to sign in. Enter the

Now load the module, by entering **Import-Module ExchangeOnlineManagement**.

To connect, enter **Connect-ExchangeOnline -UserPrincipalName admin@WWLxZZZZZZ.onmicrosoft.com.** For the UPN, enter the administrator username found in the resources tab of your lab.

You'll be prompted to sign in. Enter the administrative username and password found in the resources tab of your lab.



CONTOSO demo

admin@wwls730857.onmicrosoft.com

Enter password

Password

Forgot my password

Sign in with another account

Sign in

Contoso

Describe the capabilities of Microsoft Security Soluti...

12 Minutes Remaining

Name,Version,InstalledLocation

. You'll see the name, version and installed location of Exchange OnlineManagement.

c. Now load the module, by entering

```
Import-Module ExchangeOnlineManagement
```

d. To connect, enter

```
Connect-ExchangeOnline -UserPrincipalName admin@WWLx222222.onmicrosoft.com
```

. For the UPN, enter the administrator username found in the resources tab of your lab.

e. You'll be prompted to sign in. Enter the administrative username and password found in the resources tab of your lab.

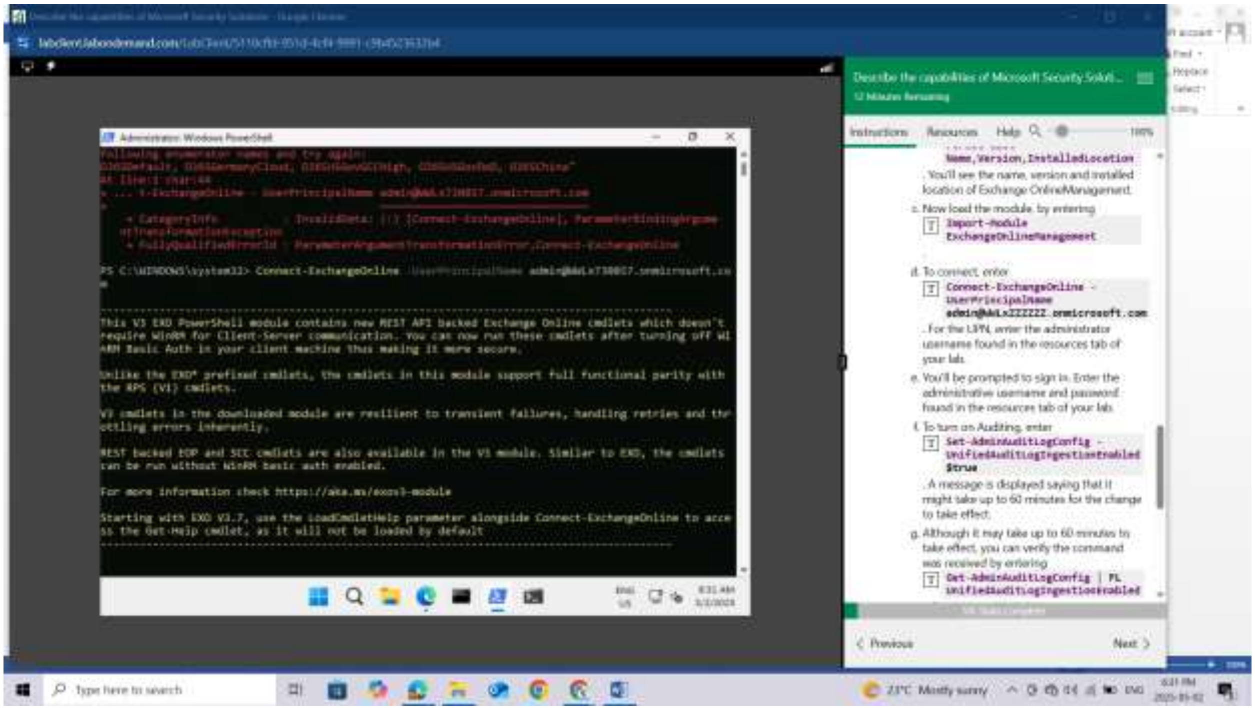
f. To turn on Auditing, enter

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

. A message is displayed saying that it might take up to 60 minutes for the change to take effect.

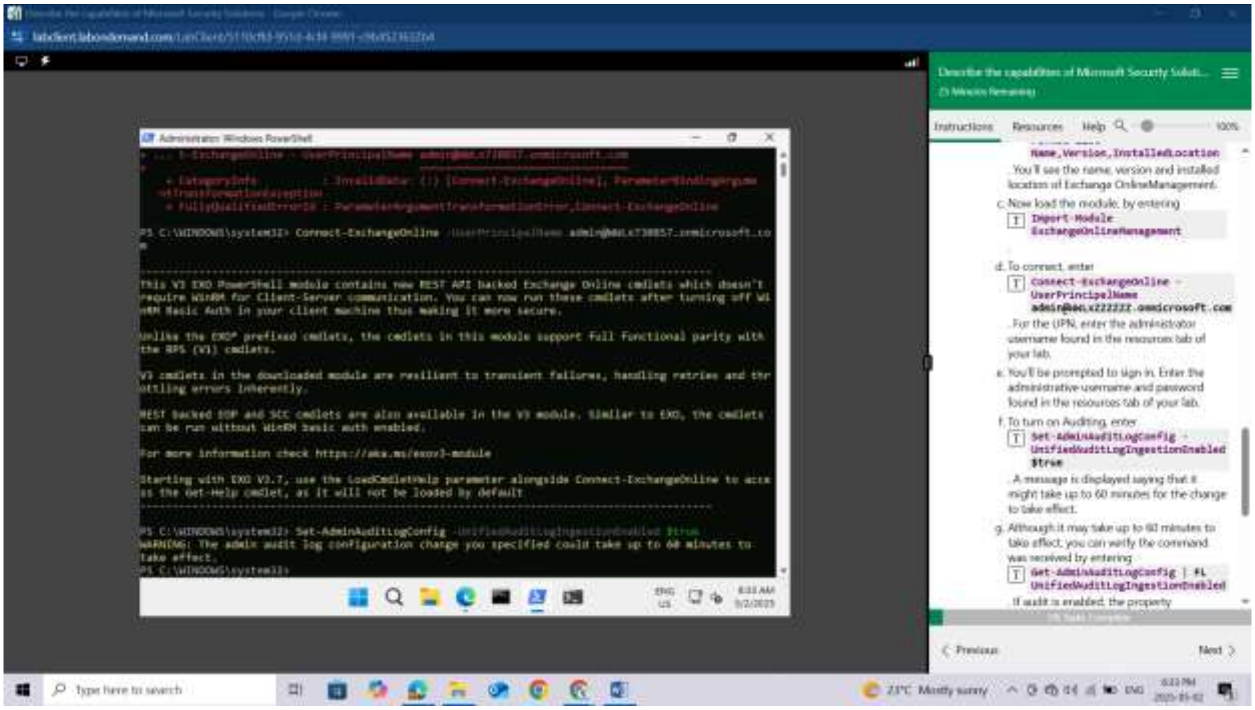
g. Although it may take up to 60 minutes to take effect, you can verify the command was received by entering

```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```



```
following enumerator names and try again:
O365Default, O365GermanyCloud, O365USGovGCCHigh, O365USGovDoD, O365China"
At line:1 char:44
+ ... t-ExchangeOnline -UserPrincipalName admin@WWLx730857.onmicrosoft.com
+
    + CategoryInfo          : InvalidData: (:) [Connect-ExchangeOnline], ParameterBindingArgume
   ntTransformationException
    + FullyQualifiedErrorId : ParameterArgumentTransformationError,Connect-ExchangeOnline

PS C:\WINDOWS\system32> Connect-ExchangeOnline -UserPrincipalName admin@WWLx730857.onmicrosoft.co
m

----------------------------------------------------------------------------------------
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't
require WinRM for Client-Server communication. You can now run these cmdlets after turning off Wi
nRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with
the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and thr
ottling errors inherently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets
can be run without WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module

Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to acce
ss the Get-Help cmdlet, as it will not be loaded by default
----------------------------------------------------------------------------------------
```

To turn on Auditing, enter **Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true**. A message is displayed saying that it might take up to 60 minutes for the change to take effect.



```
+ ... t-ExchangeOnline -UserPrincipalName admin@M365x738857.onmicrosoft.com
+
    + CategoryInfo          : InvalidData: (:) [Connect-ExchangeOnline], ParameterBindingArgume
   ntTransformationException
    + FullyQualifiedErrorId : ParameterArgumentTransformationError,Connect-ExchangeOnline

PS C:\WINDOWS\system32> Connect-ExchangeOnline -UserPrincipalName admin@M365x738857.onmicrosoft.co
m

----------------------------------------------------------------------------------------
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't
require WinRM for Client-Server communication. You can now run these cmdlets after turning off Wi
nRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with
the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and thr
ottling errors inherently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets
can be run without WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module

Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to acce
ss the Get-Help cmdlet, as it will not be loaded by default
----------------------------------------------------------------------------------------

PS C:\WINDOWS\system32> Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
WARNING: The admin audit log configuration change you specified could take up to 60 minutes to
take effect.
PS C:\WINDOWS\system32>
```

Describe the capabilities of Microsoft Security Soluti...

Name,Version,InstalledLocation

. You'll see the name, version and installed location of Exchange OnlineManagement.

c. Now load the module, by entering

```
Import-Module ExchangeOnlineManagement
```

d. To connect, enter

```
Connect-ExchangeOnline -UserPrincipalName admin@M365x222222.onmicrosoft.com
```

. For the UPN, enter the administrator username found in the resources tab of your lab.

e. You'll be prompted to sign in. Enter the administrative username and password found in the resources tab of your lab.

f. To turn on Auditing, enter

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

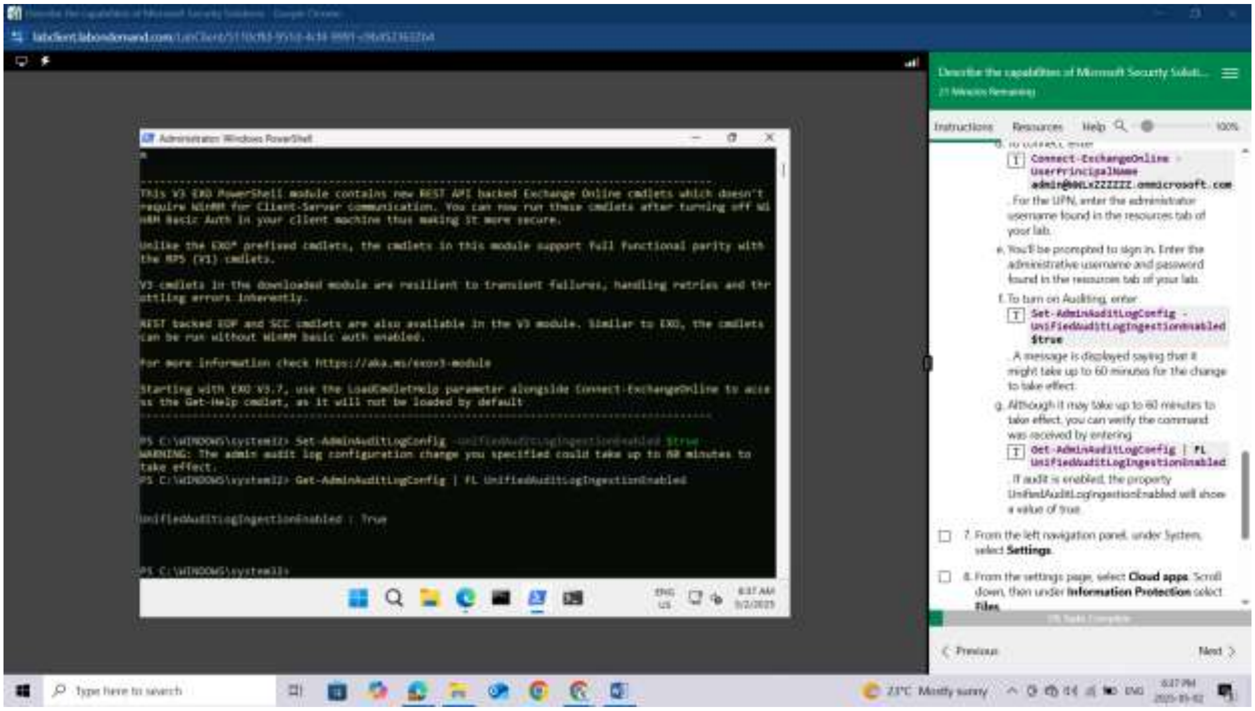
. A message is displayed saying that it might take up to 60 minutes for the change to take effect.

g. Although it may take up to 60 minutes to take effect, you can verify the command was received by entering

```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```

. If audit is enabled, the property

Although it may take up to 60 minutes to take effect, you can verify the command was received by entering **Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled**. If audit is enabled, the property **UnifiedAuditLogIngestionEnabled** will show a value of true.



```
m

----------------------------------------------------------------------------------------
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't
require WinRM for Client-Server communication. You can now run these cmdlets after turning off Wi
nRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with
the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and thr
ottling errors inherently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets
can be run without WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module

Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to acce
ss the Get-Help cmdlet, as it will not be loaded by default
----------------------------------------------------------------------------------------

PS C:\WINDOWS\system32> Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
WARNING: The admin audit log configuration change you specified could take up to 60 minutes to
take effect.
PS C:\WINDOWS\system32> Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled


UnifiedAuditLogIngestionEnabled : True



PS C:\WINDOWS\system32>
```

Describe the capabilities of Microsoft Security Soluti...

d. To connect, enter

```
Connect-ExchangeOnline -UserPrincipalName admin@M365x222222.onmicrosoft.com
```

. For the UPN, enter the administrator username found in the resources tab of your lab.

e. You'll be prompted to sign in. Enter the administrative username and password found in the resources tab of your lab.

f. To turn on Auditing, enter

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

. A message is displayed saying that it might take up to 60 minutes for the change to take effect.

g. Although it may take up to 60 minutes to take effect, you can verify the command was received by entering

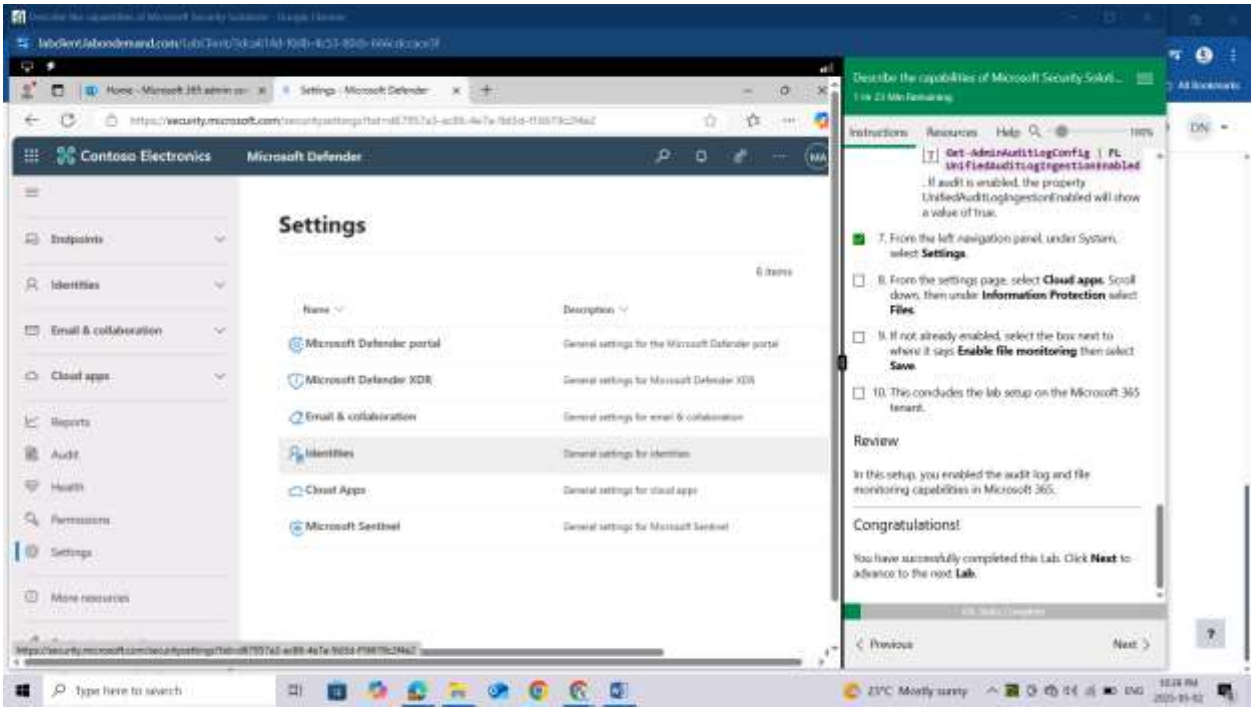
```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```

. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.

□ 7. From the left navigation panel, under System, select **Settings**.

□ 8. From the settings page, select **Cloud apps**. Scroll down, then under **Information Protection** select **Files**.

From the left navigation panel, under **System**, select **Settings**.



Settings

6 items

Name	Description
Microsoft Defender portal	General settings for the Microsoft Defender portal
Microsoft Defender XDR	General settings for Microsoft Defender XDR
Email & collaboration	General settings for email & collaboration
Identities	General settings for identities
Cloud Apps	General settings for cloud apps
Microsoft Sentinel	General settings for Microsoft Sentinel

Describe the capabilities of Microsoft Security Soluti...

```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```

. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.

☑ 7. From the left navigation panel, under System, select **Settings**.

□ 8. From the settings page, select **Cloud apps**. Scroll down, then under **Information Protection** select **Files**.

□ 9. If not already enabled, select the box next to where it says **Enable file monitoring** then select **Save**.

□ 10. This concludes the lab setup on the Microsoft 365 tenant.

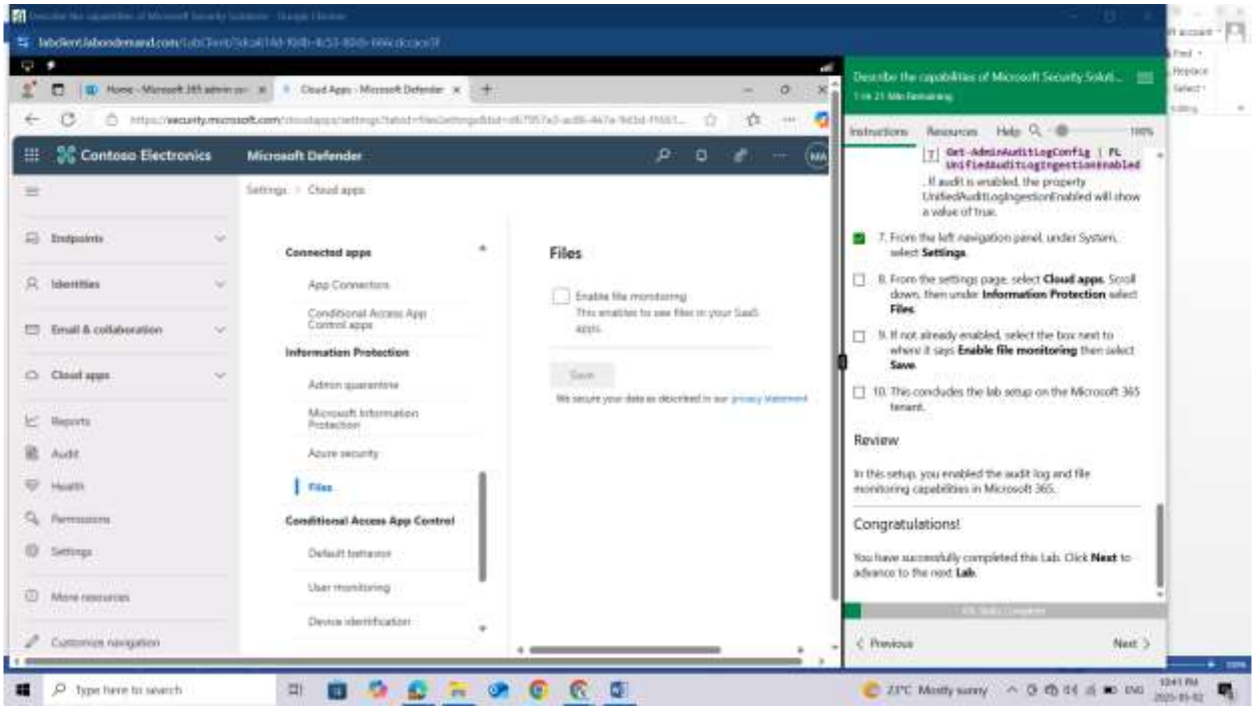
Review

In this setup, you enabled the audit log and file monitoring capabilities in Microsoft 365.

Congratulations!

You have successfully completed this Lab. Click **Next** to advance to the next **Lab**.

From the settings page, select **Cloud apps**. Scroll down, then under **Information Protection** select **Files**.



Files

□ Enable file monitoring
This enables to see files in your SaaS apps.

We secure your data as described in our privacy statement

Describe the capabilities of Microsoft Security Soluti...

☑ 7. From the left navigation panel, under System, select **Settings**.

□ 8. From the settings page, select **Cloud apps**. Scroll down, then under **Information Protection** select **Files**.

□ 9. If not already enabled, select the box next to where it says **Enable file monitoring** then select **Save**.

□ 10. This concludes the lab setup on the Microsoft 365 tenant.

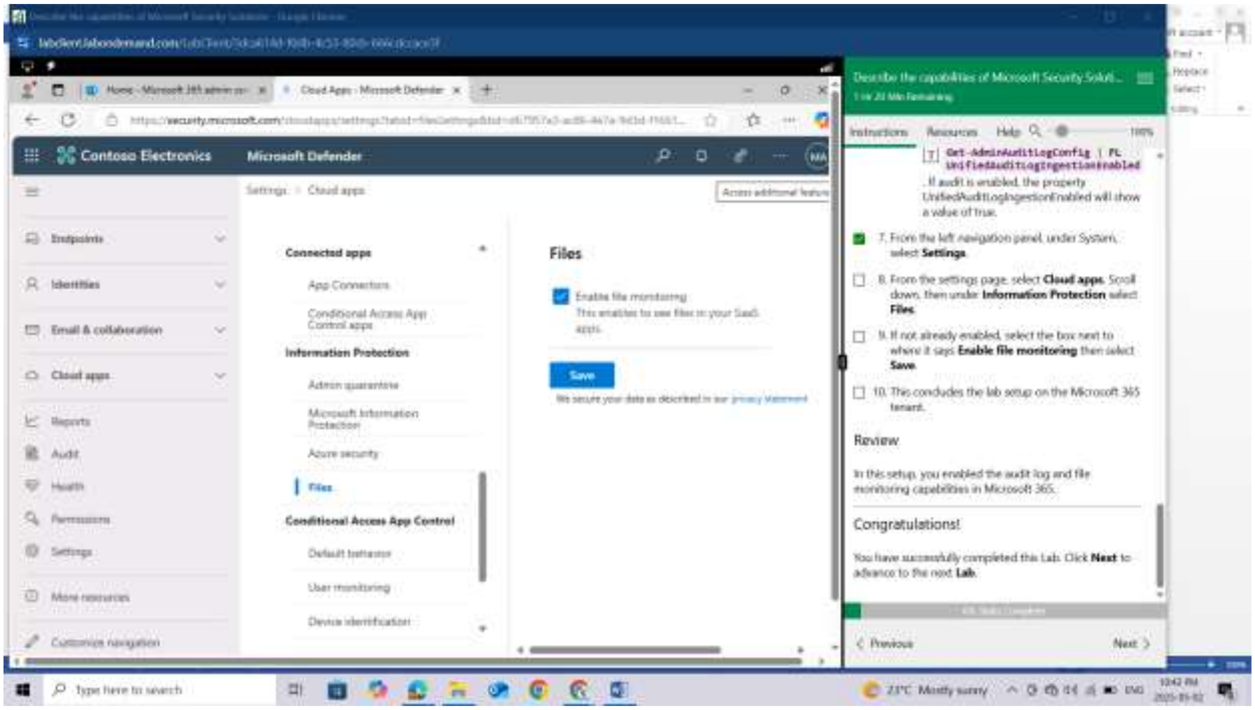
Review

In this setup, you enabled the audit log and file monitoring capabilities in Microsoft 365.

Congratulations!

You have successfully completed this Lab. Click **Next** to advance to the next **Lab**.

If not already enabled, select the box next to where it says **Enable file monitoring** then select **Save**.



☑ Enable file monitoring
This enables to see files in your SaaS apps.

Describe the capabilities of Microsoft Security Soluti...

```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```

. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.

☑ 7. From the left navigation panel, under System, select **Settings**.

☐ 8. From the settings page, select **Cloud apps**. Scroll down, then under **Information Protection** select **Files**.

☐ 9. If not already enabled, select the box next to where it says **Enable file monitoring** then select **Save**.

☐ 10. This concludes the lab setup on the Microsoft 365 tenant.

Review

In this setup, you enabled the audit log and file monitoring capabilities in Microsoft 365.

Congratulations!

You have successfully completed this Lab. Click **Next** to advance to the next **Lab**.

This concludes the lab setup on the Microsoft 365 tenant.

REVIEW

In this setup, you enabled the audit log and file monitoring capabilities in Microsoft 365.

LAB: EXPLORE AZURE NETWORK SECURITY GROUPS (NSGS)

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the basic security capabilities in Azure
- Unit: Describe Azure Network Security groups

LAB SCENARIO

In this lab, you'll explore the function of network security groups in Azure. You'll do this by creating a network security group (NSG) and assigning the NSG to the interface of a pre-existing virtual machine (VM). Once configured you'll observe the default inbound and outbound rules, create new rules, and test those rules. In this lab, the VM you'll use with the NSG is created for you, so you'll first view some of the information associated with that VM.

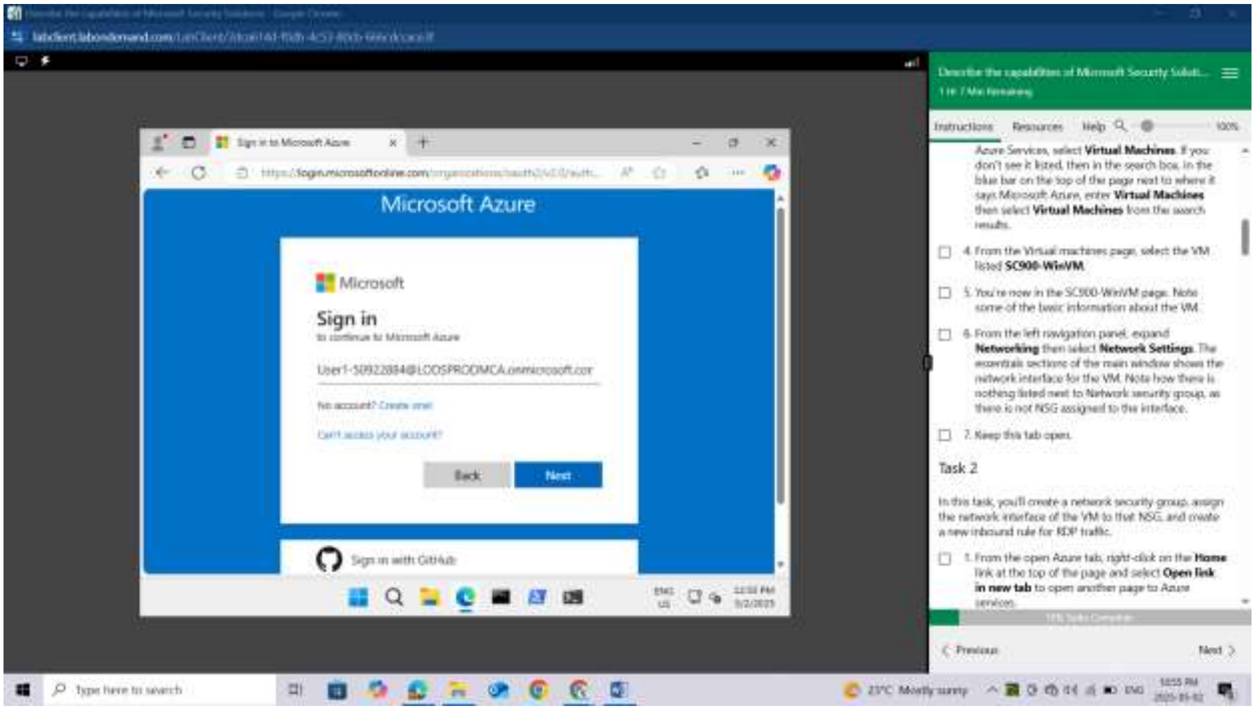
Task 1

In this task, you'll view some of the parameters associated with the VM that that was created for use with this lab.

Open Microsoft Edge. In the address bar, enter https://portal.azure.com.

Sign in with your Azure Portal admin credentials.

In the Sign-in window, enter the username provided by your lab hosting provider then select Next.



Sign in to Microsoft Azure

Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

User1-50922884@LODSPRODMCA.onmicrosoft.com

No account? Create one!

Can't access your account?

Back Next

Sign in with GitHub

Describe the capabilities of Microsoft Security Soluti...

Instructions Resources Help 100%

Azure Services, select **Virtual Machines**. If you don't see it listed, then in the search box, in the blue bar on the top of the page next to where it says Microsoft Azure, enter **Virtual Machines** then select **Virtual Machines** from the search results.

- □ 4. From the Virtual machines page, select the VM listed **SC900-WinVM**.
- □ 5. You're now in the SC900-WinVM page. Note some of the basic information about the VM.
- □ 6. From the left navigation panel, expand **Networking** then select **Network Settings**. The essentials sections of the main window shows the network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.
- □ 7. Keep this tab open.

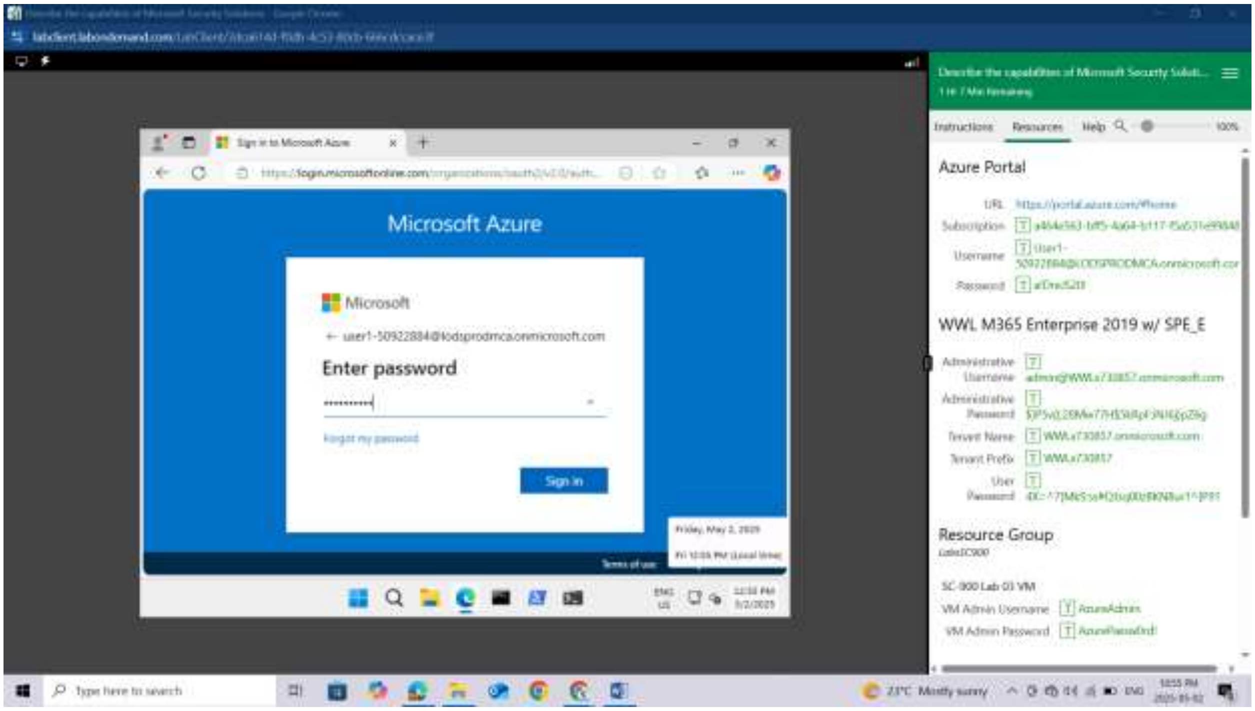
Task 2

In this task, you'll create a network security group, assign the network interface of the VM to that NSG, and create a new inbound rule for RDP traffic.

- □ 1. From the open Azure tab, right-click on the **Home** link at the top of the page and select **Open link in new tab** to open another page to Azure services.

Previous Next

Enter the admin password that should be provided by your lab hosting provider. Select Sign in.



Sign in to Microsoft Azure

Microsoft Azure

Microsoft

← user1-50922884@lodsprodmca.onmicrosoft.com

Enter password

••••••••••

Forgot my password

Sign in

Describe the capabilities of Microsoft Security Soluti...

Instructions Resources Help 100%

Azure Portal

URL	https://portal.azure.com/#home
Subscription	a464e563-[illegible]
Username	User1-50922884@LODSPRODMCA.onmicrosoft.com
Password	[illegible]

WWL M365 Enterprise 2019 w/ SPE_E

Administrative Username	admin@WWLx730857.onmicrosoft.com
Administrative Password	[illegible]
Tenant Name	WWLx730857.onmicrosoft.com
Tenant Prefix	WWLx730857
User Password	[illegible]

Resource Group

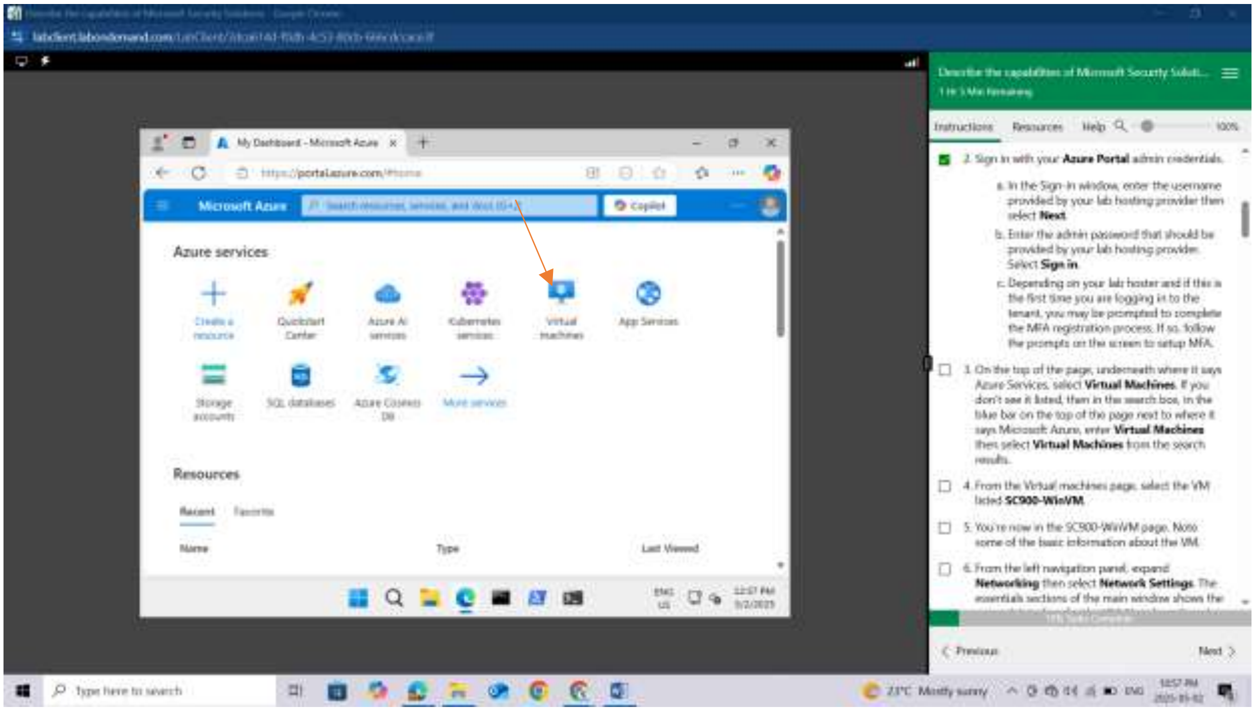
LabsSC900

SC-900 Lab 03 VM

VM Admin Username	AzureAdmin
VM Admin Password	[illegible]

Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

On the top of the page, underneath where it says Azure Services, select **Virtual Machines**. If you don't see it listed, then in the search box, in the blue bar on the top of the page next to where it says Microsoft Azure, enter **Virtual Machines** then select **Virtual Machines** from the search results.



☑ 2. Sign in with your **Azure Portal** admin credentials.

a. In the Sign-in window, enter the username provided by your lab hosting provider then select **Next**.

b. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

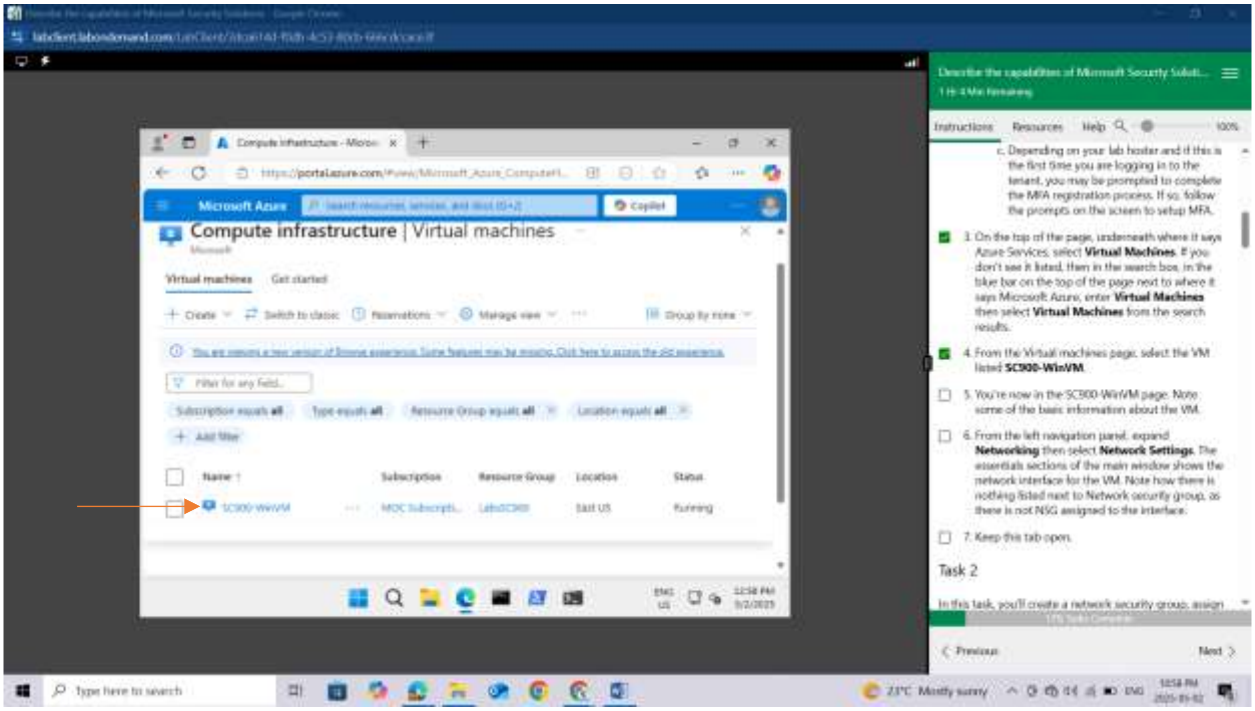
□ 3. On the top of the page, underneath where it says Azure Services, select **Virtual Machines**. If you don't see it listed, then in the search box, in the blue bar on the top of the page next to where it says Microsoft Azure, enter **Virtual Machines** then select **Virtual Machines** from the search results.

□ 4. From the Virtual machines page, select the VM listed **SC900-WinVM**.

□ 5. You're now in the SC900-WinVM page. Note some of the basic information about the VM.

□ 6. From the left navigation panel, expand **Networking** then select **Network Settings**. The essentials sections of the main window shows the

From the Virtual machines page, select the VM listed **SC900-WinVM.**



Name ↑	Subscription	Resource Group	Location	Status
SC900-WinVM	MOC Subscripti...	LabsSC900	East US	Running

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

☑ 3. On the top of the page, underneath where it says Azure Services, select **Virtual Machines**. If you don't see it listed, then in the search box, in the blue bar on the top of the page next to where it says Microsoft Azure, enter **Virtual Machines** then select **Virtual Machines** from the search results.

☑ 4. From the Virtual machines page, select the VM listed **SC900-WinVM**.

□ 5. You're now in the SC900-WinVM page. Note some of the basic information about the VM.

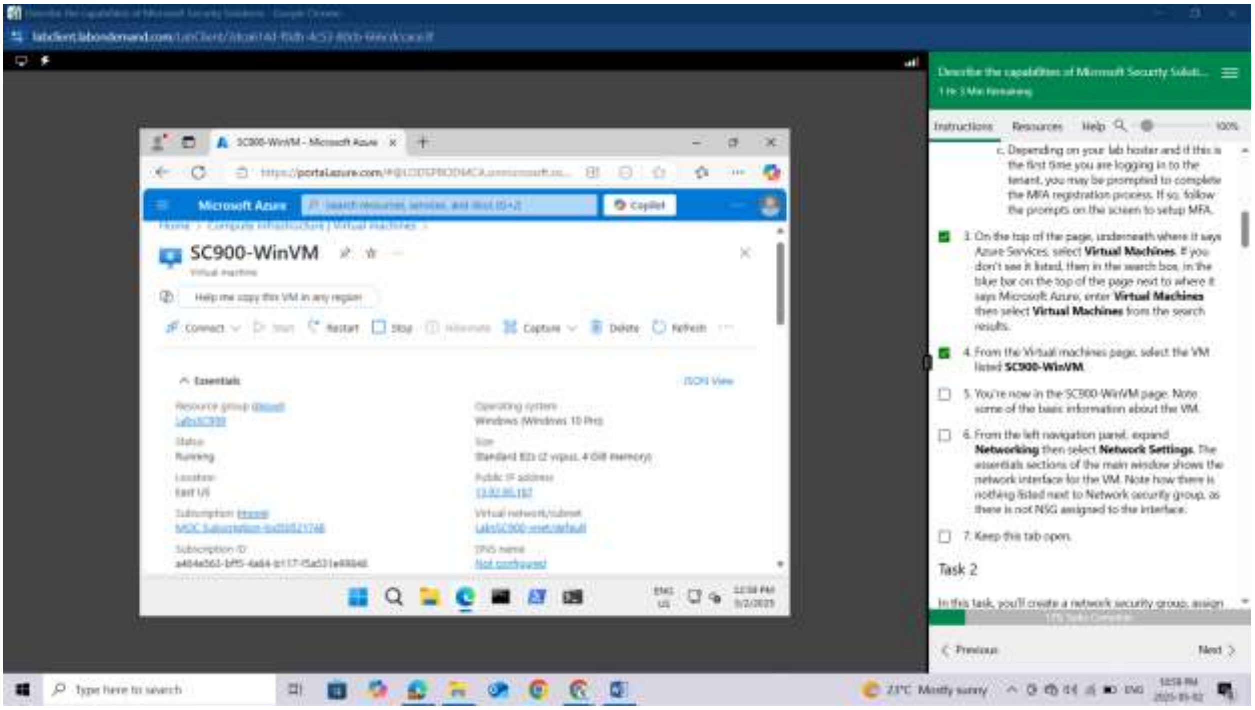
□ 6. From the left navigation panel, expand **Networking** then select **Network Settings**. The essentials sections of the main window shows the network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.

□ 7. Keep this tab open.

Task 2

In this task, you'll create a network security group, assign

You're now in the **SC900-WinVM page**. Note some of the basic information about the VM.



SC900-WinVM - Microsoft Azure

https://portal.azure.com/

Home > Compute infrastructure | Virtual machines >

SC900-WinVM

Virtual machine

Help me copy this VM in any region

Essentials

Resource group (move) LabsSC900	Operating system Windows (Windows 10 Pro)
Status Running	Size Standard B2s (2 vcpus, 4 GiB memory)
Location East US	Public IP address 13.92.85.187
Subscription (move) MOC Subscription-[illegible]	Virtual network/subnet LabsSC900-vnet/default
Subscription ID a484e563-bff5-4a84-b117-f5a531e88848	DNS name Not configured

Describe the capabilities of Microsoft Security Soluti...

1 Hr 3 Min Remaining

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

☑ 3. On the top of the page, underneath where it says Azure Services, select **Virtual Machines**. If you don't see it listed, then in the search box, in the blue bar on the top of the page next to where it says Microsoft Azure, enter **Virtual Machines** then select **Virtual Machines** from the search results.

☑ 4. From the Virtual machines page, select the VM listed **SC900-WinVM**.

☐ 5. You're now in the SC900-WinVM page. Note some of the basic information about the VM.

☐ 6. From the left navigation panel, expand **Networking** then select **Network Settings**. The essentials sections of the main window shows the network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.

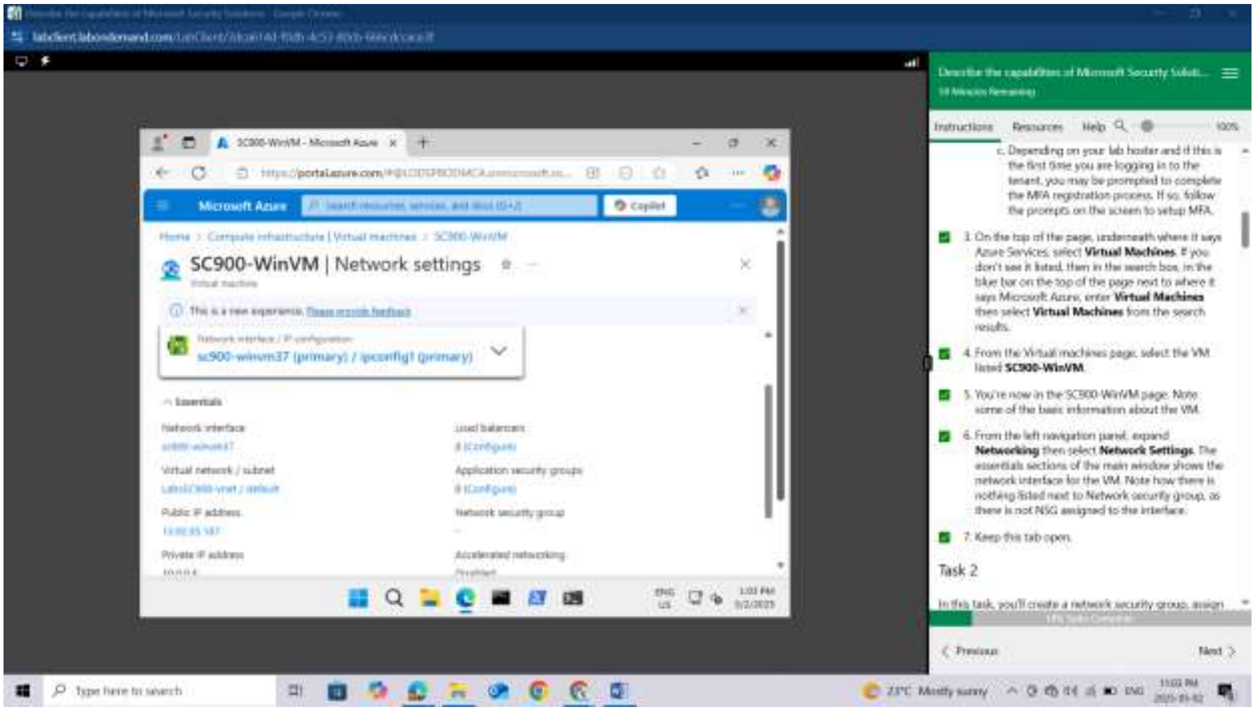
☐ 7. Keep this tab open.

Task 2

In this task, you'll create a network security group, assign

From the left navigation panel, expand **Networking** then select **Network Settings**. The essentials sections of the main window shows the network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.

Keep this tab open.



SC900-WinVM - Microsoft Azure

https://portal.azure.com/

Home > Compute infrastructure | Virtual machines > SC900-WinVM

SC900-WinVM | Network settings

Virtual machine

This is a new experience. Please provide feedback

Network interface / IP configuration
sc900-winvm37 (primary) / ipconfig1 (primary)

Essentials

Network interface sc900-winvm37	Load balancers 0 (Configure)
Virtual network / subnet LabsSC900-vnet / default	Application security groups 0 (Configure)
Public IP address 13.92.85.187	Network security group -
Private IP address 10.0.0.4	Accelerated networking Disabled

Describe the capabilities of Microsoft Security Soluti...

59 Minutes Remaining

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

☑ 3. On the top of the page, underneath where it says Azure Services, select **Virtual Machines**. If you don't see it listed, then in the search box, in the blue bar on the top of the page next to where it says Microsoft Azure, enter **Virtual Machines** then select **Virtual Machines** from the search results.

☑ 4. From the Virtual machines page, select the VM listed **SC900-WinVM**.

☑ 5. You're now in the SC900-WinVM page. Note some of the basic information about the VM.

☑ 6. From the left navigation panel, expand **Networking** then select **Network Settings**. The essentials sections of the main window shows the network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.

☑ 7. Keep this tab open.

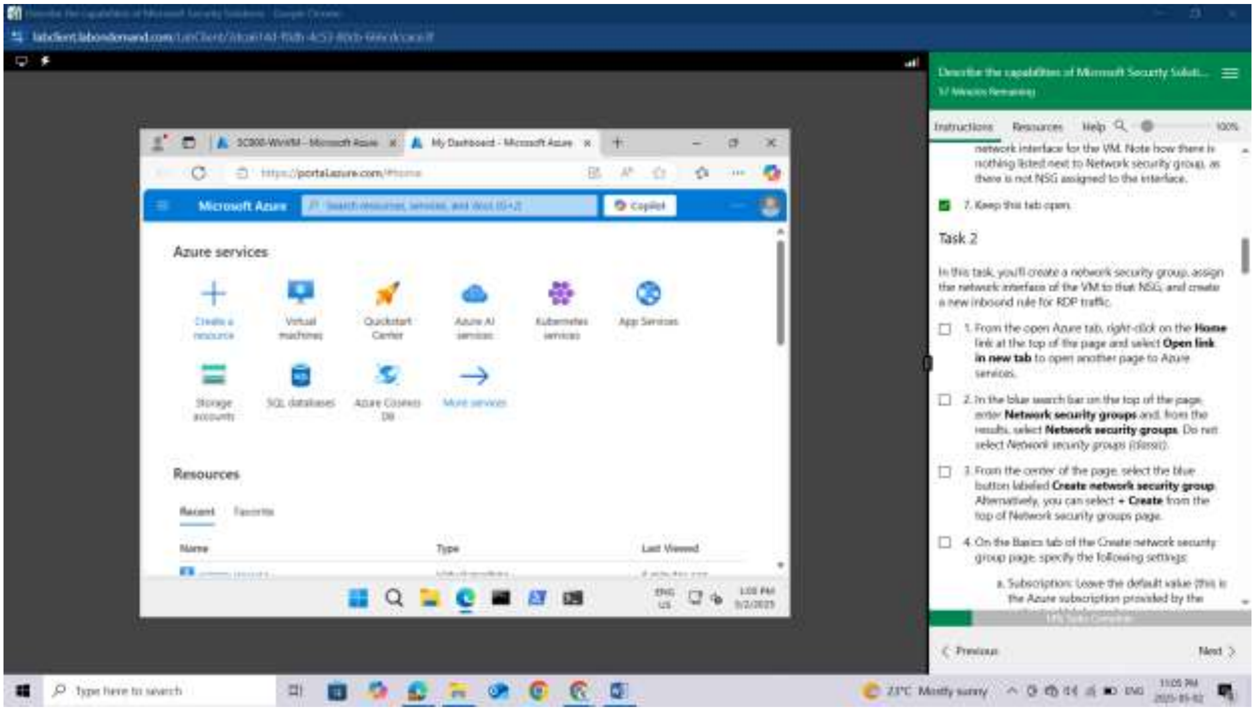
Task 2

In this task, you'll create a network security group, assign

Task 2

In this task, you'll create a network security group, assign the network interface of the VM to that NSG, and create a new inbound rule for RDP traffic.

From the open Azure tab, right-click on the **Home** link at the top of the page and select **Open link in new tab** to open another page to Azure services.



Describe the capabilities of Microsoft Security Soluti...

network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.

☑ 7. Keep this tab open.

Task 2

In this task, you'll create a network security group, assign the network interface of the VM to that NSG, and create a new inbound rule for RDP traffic.

☐ 1. From the open Azure tab, right-click on the **Home** link at the top of the page and select **Open link in new tab** to open another page to Azure services.

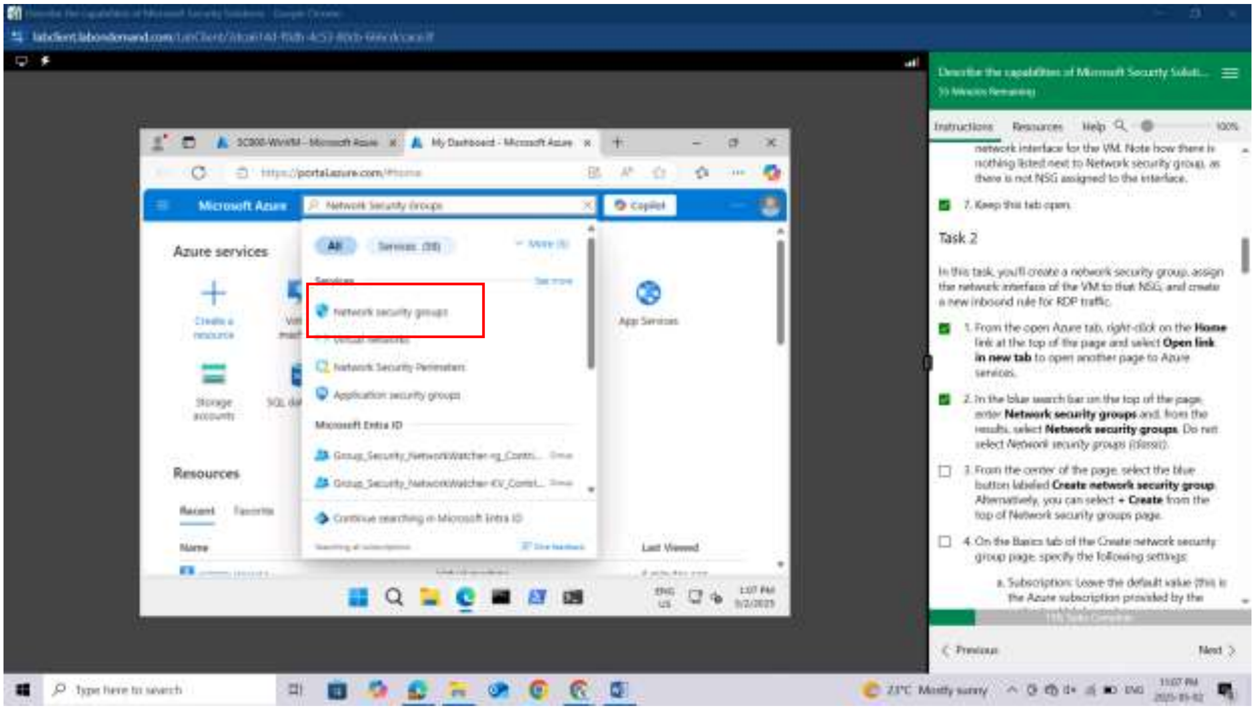
☐ 2. In the blue search bar on the top of the page, enter **Network security groups** and, from the results, select **Network security groups**. Do not select *Network security groups (classic)*.

☐ 3. From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.

☐ 4. On the Basics tab of the Create network security group page, specify the following settings:

a. Subscription: Leave the default value (this is the Azure subscription provided by the

In the blue search bar on the top of the page, enter **Network security groups** and, from the results, select **Network security groups**. Do not select **Network security groups (classic).**



Describe the capabilities of Microsoft Security Soluti...

network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.

☑ 7. Keep this tab open.

Task 2

In this task, you'll create a network security group, assign the network interface of the VM to that NSG, and create a new inbound rule for RDP traffic.

☑ 1. From the open Azure tab, right-click on the **Home** link at the top of the page and select **Open link in new tab** to open another page to Azure services.

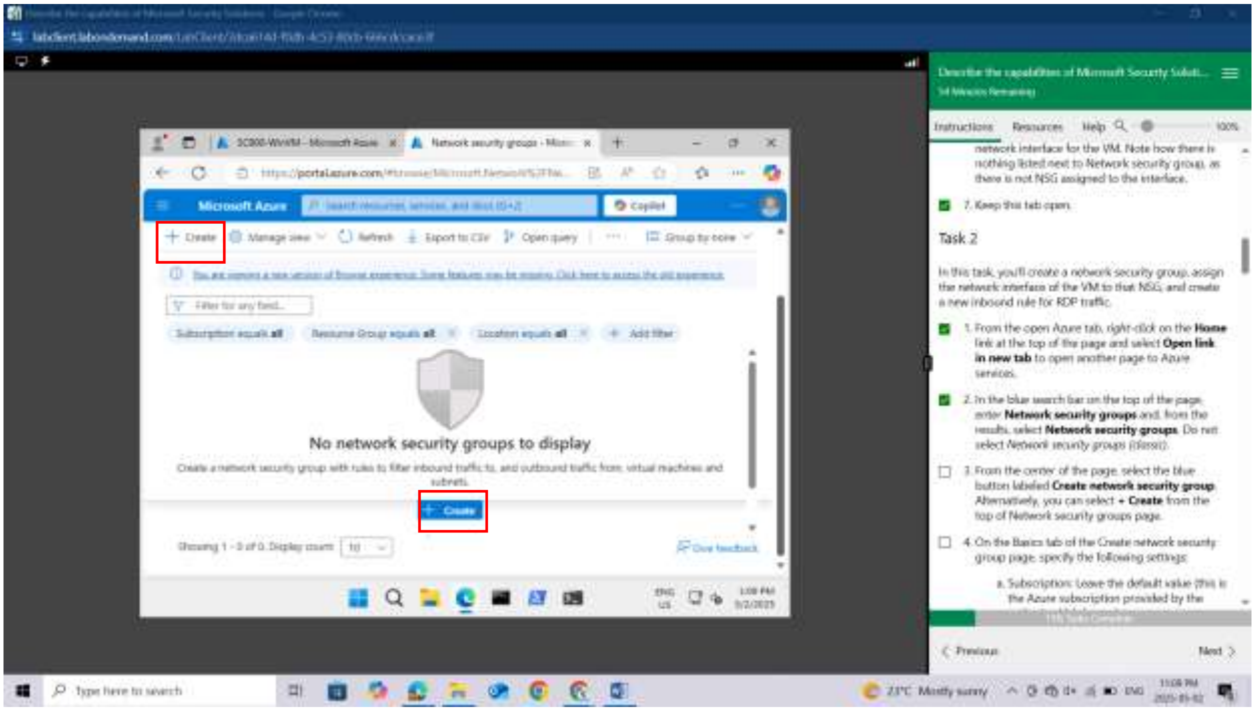
☑ 2. In the blue search bar on the top of the page, enter **Network security groups** and, from the results, select **Network security groups**. Do not select *Network security groups (classic)*.

□ 3. From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.

□ 4. On the Basics tab of the Create network security group page, specify the following settings:

a. Subscription: Leave the default value (this is the Azure subscription provided by the

From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.



No network security groups to display

Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and subnets.

Describe the capabilities of Microsoft Security Soluti...

network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.

☑ 7. Keep this tab open.

Task 2

In this task, you'll create a network security group, assign the network interface of the VM to that NSG, and create a new inbound rule for RDP traffic.

☑ 1. From the open Azure tab, right-click on the **Home** link at the top of the page and select **Open link in new tab** to open another page to Azure services.

☑ 2. In the blue search bar on the top of the page, enter **Network security groups** and, from the results, select **Network security groups**. Do not select *Network security groups (classic)*.

□ 3. From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.

□ 4. On the Basics tab of the Create network security group page, specify the following settings:

a. Subscription: Leave the default value (this is the Azure subscription provided by the

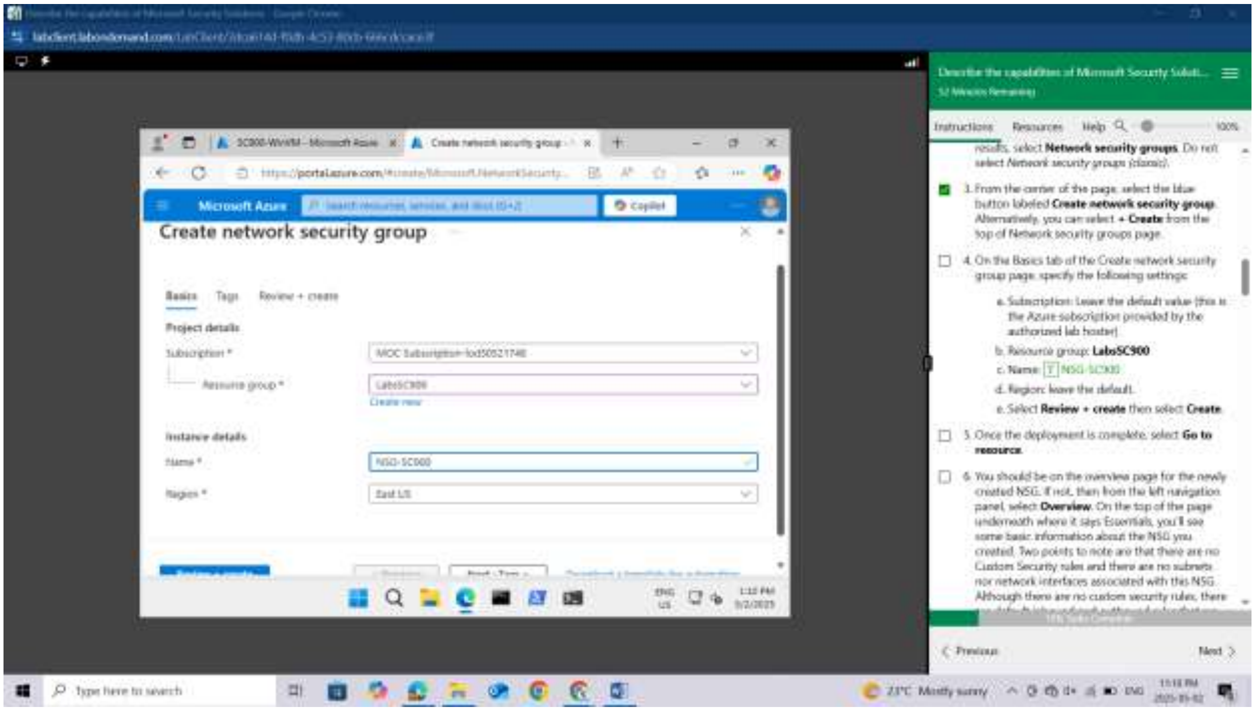
On the Basics tab of the Create network security group page, specify the following settings:

Subscription: Leave the default value (this is the Azure subscription provided by the authorized lab hoster)

Resource group: **LabsSC900**

Name: **NSG-SC900**

Region: leave the default.



Create network security group

Basics | Tags | Review + create

Project details

Subscription * : MOC Subscription-lod50521748

Resource group * : LabsSC900

Create new

Instance details

Name * : NSG-SC900

Region * : East US

Describe the capabilities of Microsoft Security Soluti...

52 Minutes Remaining

results, select **Network security groups**. Do not select *Network security groups (classic)*.

☑ 3. From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.

□ 4. On the Basics tab of the Create network security group page, specify the following settings:

a. Subscription: Leave the default value (this is the Azure subscription provided by the authorized lab hoster)

b. Resource group: **LabsSC900**

c. Name: NSG-SC900

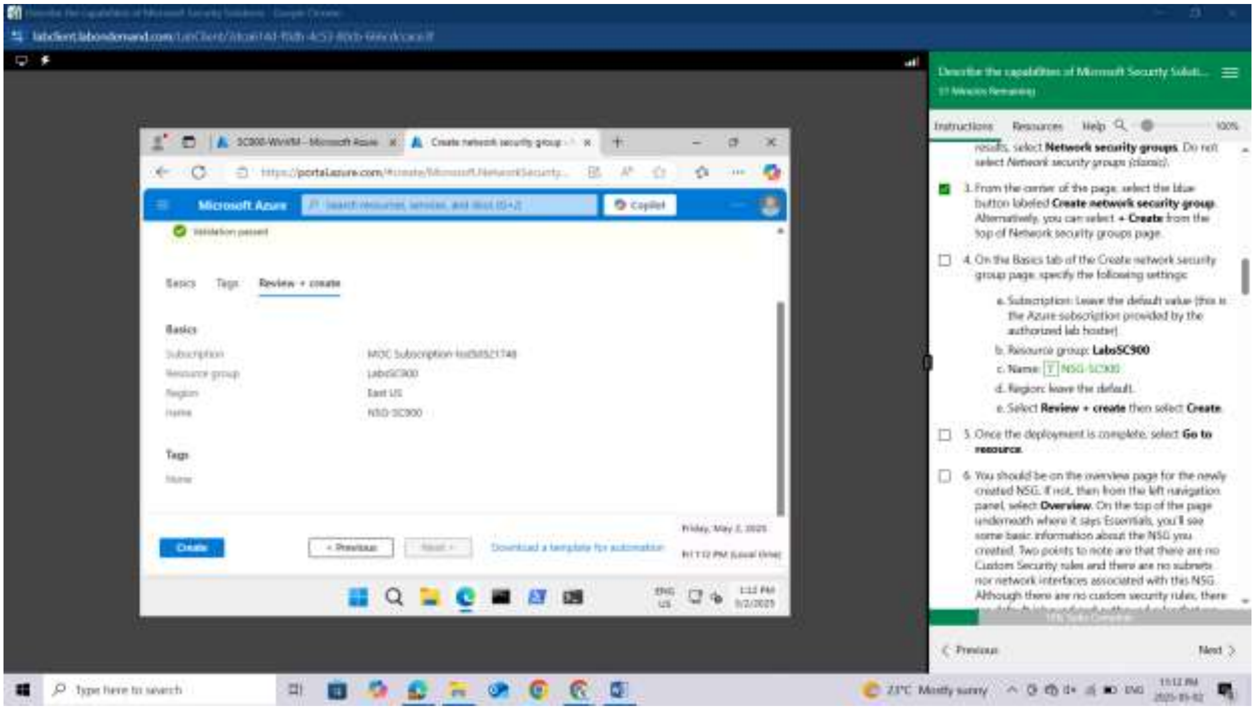
d. Region: leave the default.

e. Select **Review + create** then select **Create**.

□ 5. Once the deployment is complete, select **Go to resource**.

□ 6. You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there

Select **Review + create** then select **Create.**



Validation passed

Basics | Tags | Review + create

Basics

Subscription: MOC Subscription-lod50521748

Resource group: LabsSC900

Region: East US

Name: NSG-SC900

Tags

None

Describe the capabilities of Microsoft Security Soluti...

51 Minutes Remaining

results, select **Network security groups**. Do not select *Network security groups (classic)*.

☑ 3. From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.

□ 4. On the Basics tab of the Create network security group page, specify the following settings:

a. Subscription: Leave the default value (this is the Azure subscription provided by the authorized lab hoster)

b. Resource group: **LabsSC900**

c. Name: NSG-SC900

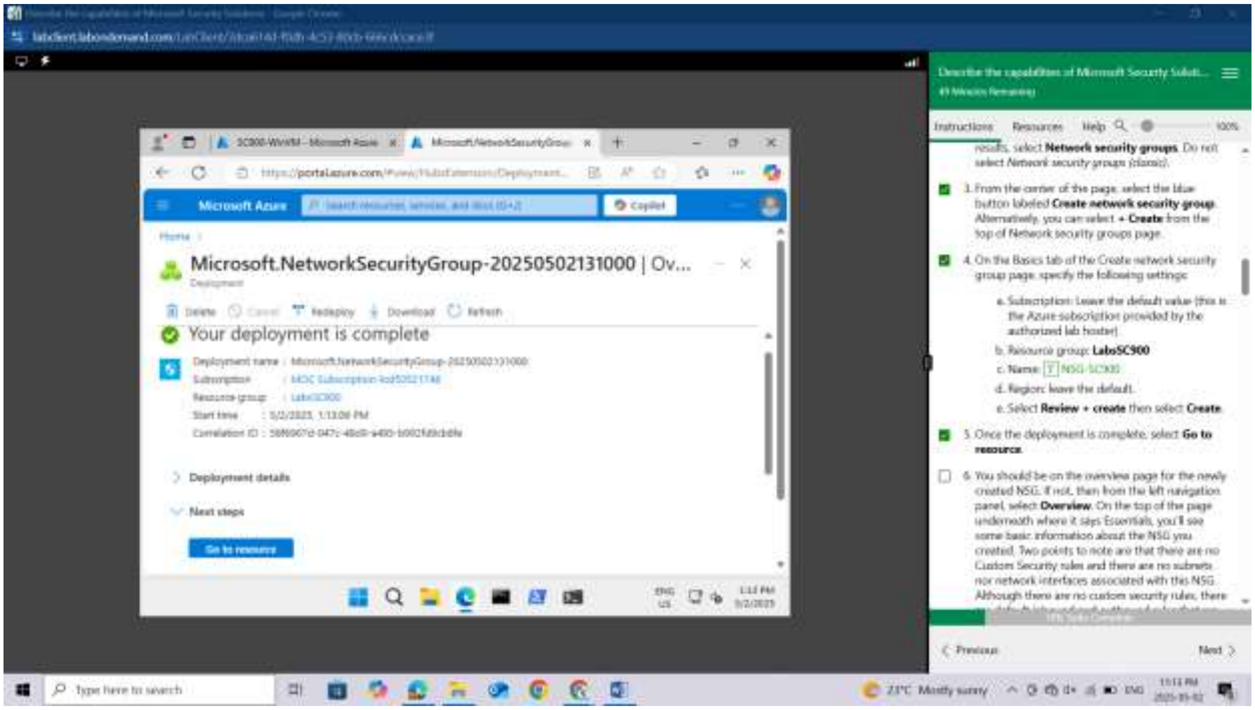
d. Region: leave the default.

e. Select **Review + create** then select **Create**.

□ 5. Once the deployment is complete, select **Go to resource**.

□ 6. You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there

Once the deployment is complete, select **Go to resource**.



Microsoft.NetworkSecurityGroup-20250502131000 | Ov...

Deployment

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGroup-20250502131000
Subscription : MOC Subscription-lod50521748
Resource group : LabsSC900
Start time : 5/2/2025, 1:13:08 PM

Deployment details

Next steps

Go to resource

Describe the capabilities of Microsoft Security Soluti...

results, select **Network security groups**. Do not select *Network security groups (classic)*.

☑ 3. From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.

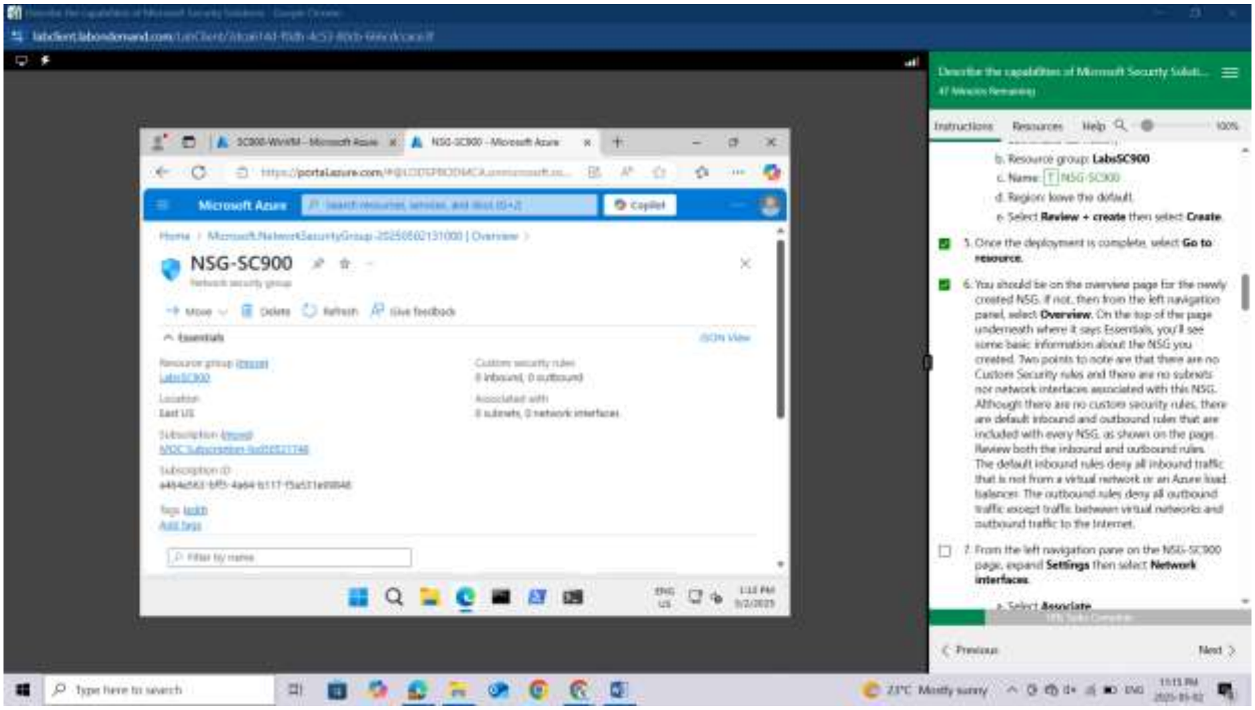
☑ 4. On the Basics tab of the Create network security group page, specify the following settings:

a. Subscription: Leave the default value (this is the Azure subscription provided by the authorized lab hoster)
b. Resource group: **LabsSC900**
c. Name: NSG-SC900
d. Region: leave the default.
e. Select **Review + create** then select **Create**.

☑ 5. Once the deployment is complete, select **Go to resource**.

□ 6. You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there

You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG.



Home > Microsoft.NetworkSecurityGroup-20250502131000 | Overview >

NSG-SC900

Network security group

Essentials

Resource group (move): LabsSC900
Location: East US
Subscription (move): MOC Subscription-lod50521748
Custom security rules: 0 inbound, 0 outbound
Associated with: 0 subnets, 0 network interfaces

Describe the capabilities of Microsoft Security Soluti...

b. Resource group: **LabsSC900**
c. Name: NSG-SC900
d. Region: leave the default.
e. Select **Review + create** then select **Create**.

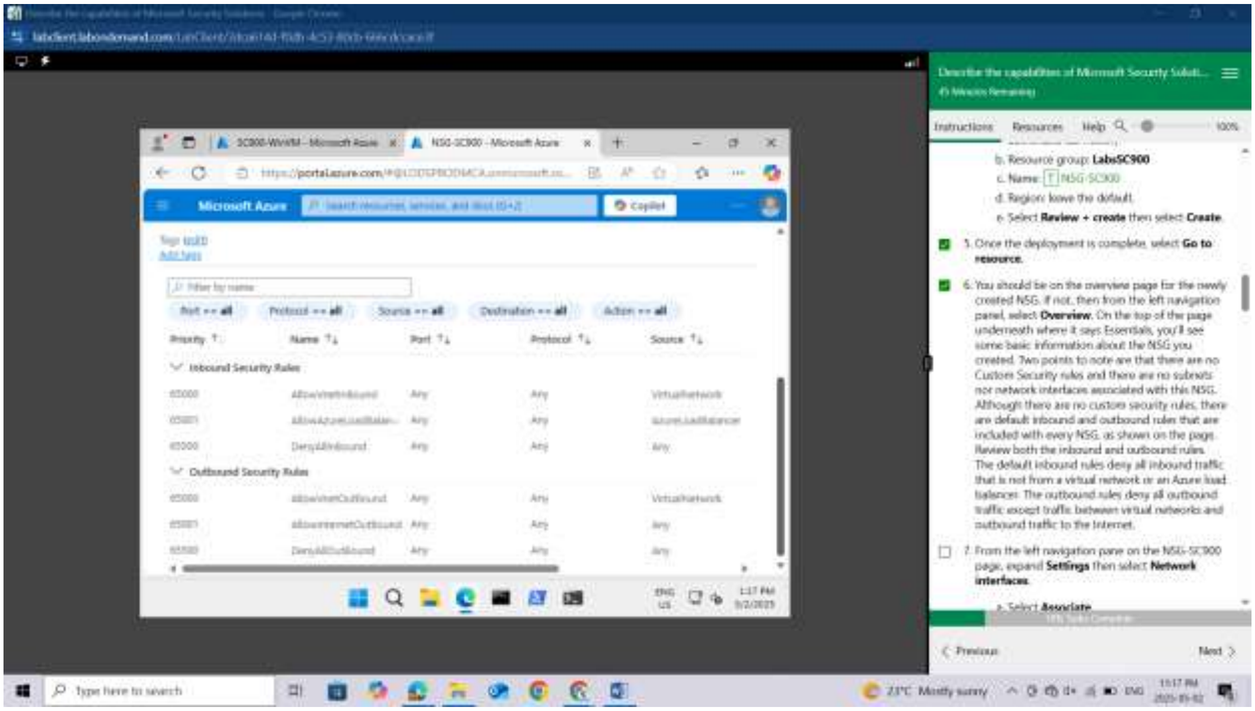
☑ 5. Once the deployment is complete, select **Go to resource**.

☑ 6. You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there are default inbound and outbound rules that are included with every NSG, as shown on the page. Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.

□ 7. From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces**.

a. Select **Associate**.

Although there are no custom security rules, there are default inbound and outbound rules that are included with every NSG, as shown on the page. Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.



Priority	Name	Port	Protocol	Source
Inbound Security Rules				
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer
65500	DenyAllInbound	Any	Any	Any
Outbound Security Rules				
65000	AllowVnetOutBound	Any	Any	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any
65500	DenyAllOutBound	Any	Any	Any

b. Resource group: **LabsSC900**
c. Name: NSG-SC900
d. Region: leave the default.
e. Select **Review + create** then select **Create**.

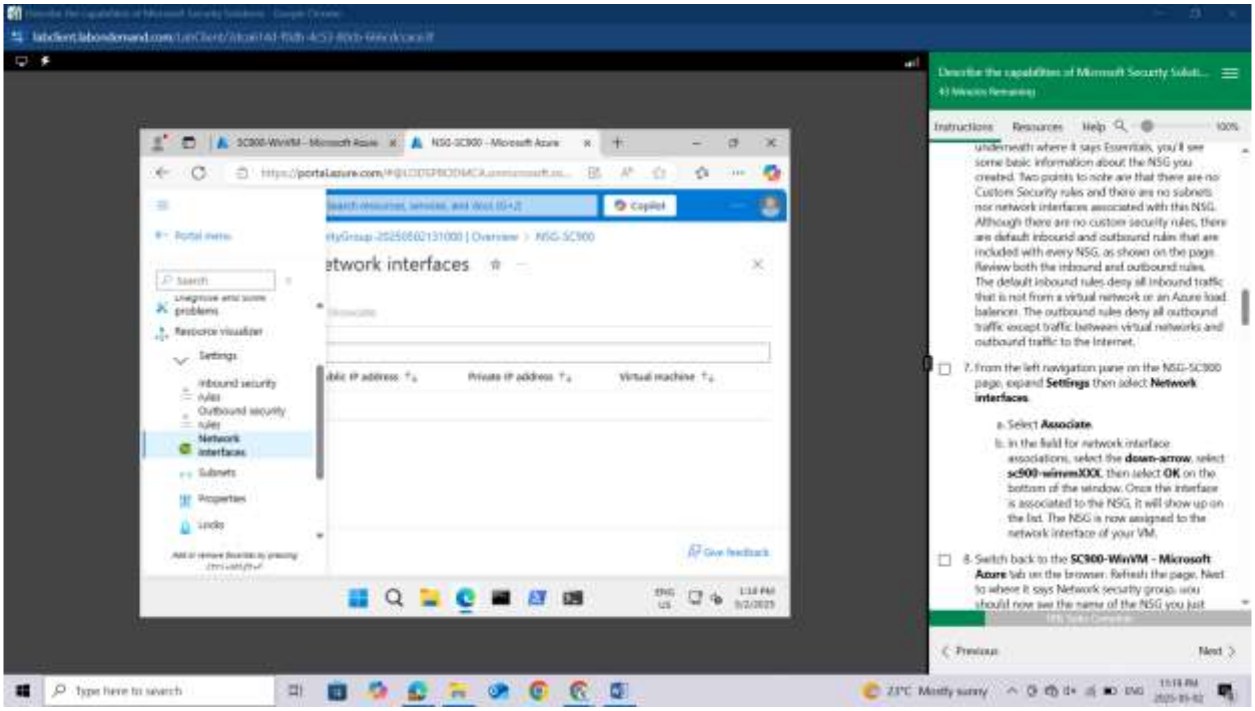
☑ 5. Once the deployment is complete, select **Go to resource**.

☑ 6. You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there are default inbound and outbound rules that are included with every NSG, as shown on the page. Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.

☐ 7. From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces**.

a. Select **Associate**.

From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces.**



underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there are default inbound and outbound rules that are included with every NSG, as shown on the page. Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.

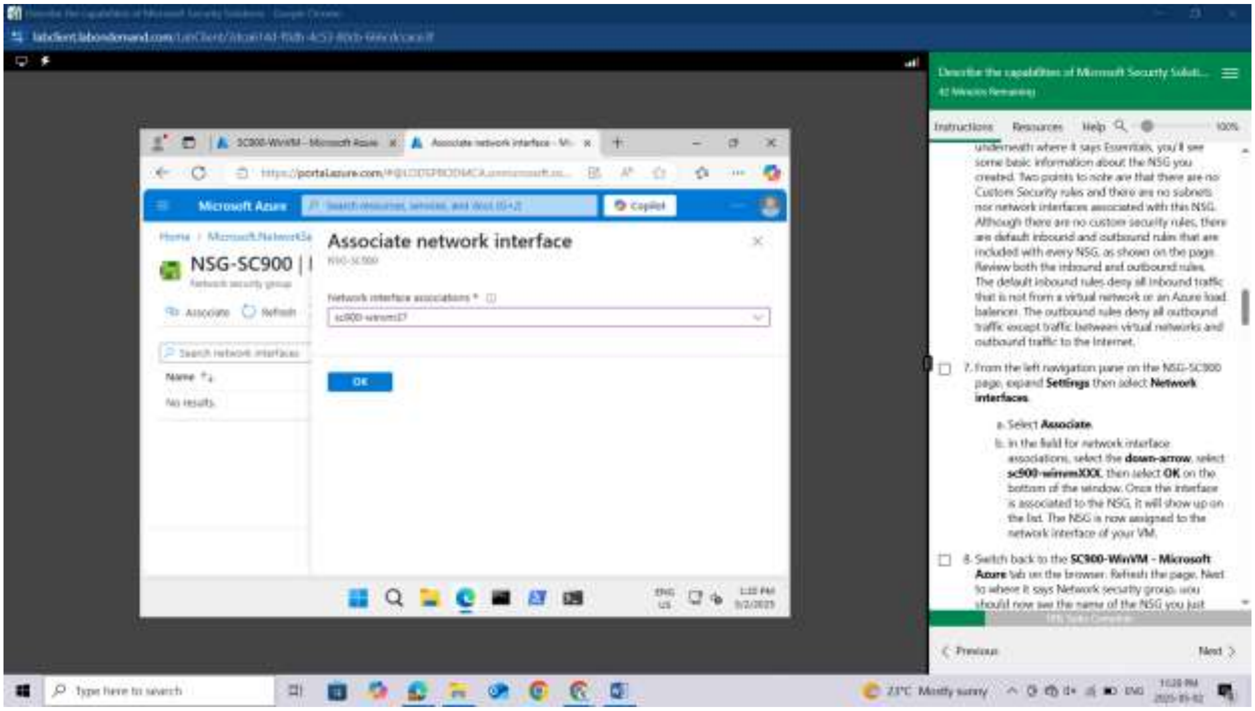
☐ 7. From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces**.

a. Select **Associate**.
b. In the field for network interface associations, select the **down-arrow**, select **sc900-winvmXXX**, then select **OK** on the bottom of the window. Once the interface is associated to the NSG, it will show up on the list. The NSG is now assigned to the network interface of your VM.

☐ 8. Switch back to the **SC900-WinVM - Microsoft Azure** tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just

Select **Associate**.

In the field for network interface associations, select the **down-arrow**, select **sc900-winvmXXX**, then select **OK** on the bottom of the window. Once the interface is associated to the NSG, it will show up on the list.



Associate network interface

NSG-SC900

Network interface associations * sc900-winvm17

OK

NSG-SC900 | Network security group

Name

No results.

Describe the capabilities of Microsoft Security Soluti...

underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there are default inbound and outbound rules that are included with every NSG, as shown on the page. Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.

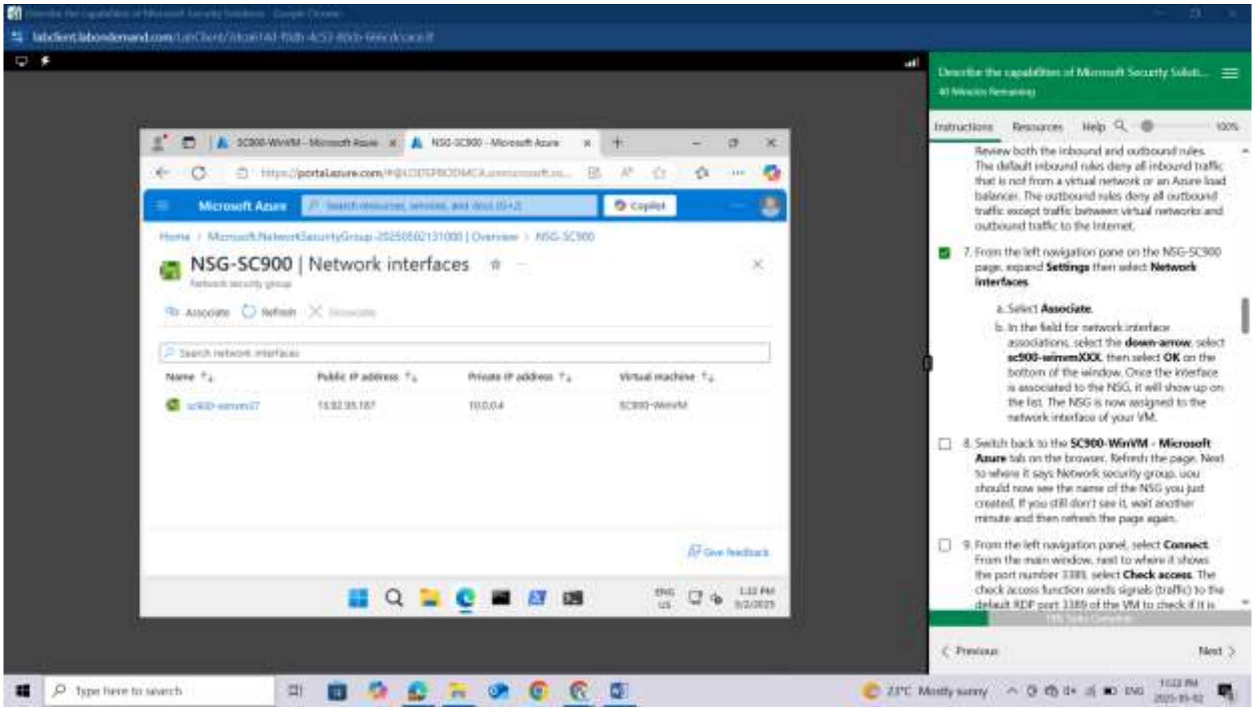
□ 7. From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces**.

a. Select **Associate**.

b. In the field for network interface associations, select the **down-arrow**, select **sc900-winvmXXX**, then select **OK** on the bottom of the window. Once the interface is associated to the NSG, it will show up on the list. The NSG is now assigned to the network interface of your VM.

□ 8. Switch back to the **SC900-WinVM - Microsoft Azure** tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just

The NSG is now assigned to the network interface of your VM.



Home > Microsoft.NetworkSecurityGroup-20250502131000 | Overview > NSG-SC900

NSG-SC900 | Network interfaces

Network security group

Name	Public IP address	Private IP address	Virtual machine
sc900-winvm17	13.92.95.187	10.0.0.4	SC900-WinVM

Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.

☑ 7. From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces**.

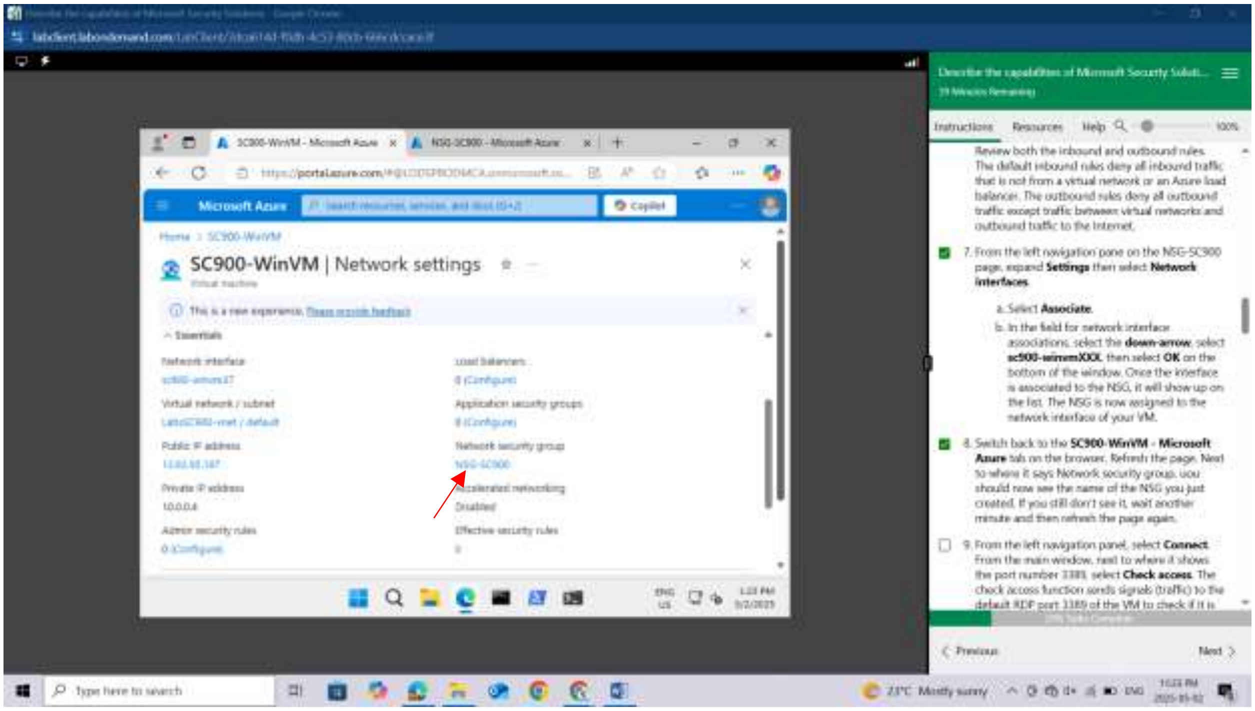
a. Select **Associate**.

b. In the field for network interface associations, select the **down-arrow**, select **sc900-winvmXXX**, then select **OK** on the bottom of the window. Once the interface is associated to the NSG, it will show up on the list. The NSG is now assigned to the network interface of your VM.

□ 8. Switch back to the **SC900-WinVM - Microsoft Azure** tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just created. If you still don't see it, wait another minute and then refresh the page again.

□ 9. From the left navigation panel, select **Connect**. From the main window, next to where it shows the port number 3389, select **Check access**. The check access function sends signals (traffic) to the default RDP port 3389 of the VM to check if it is

Switch back to the **SC900-WinVM - Microsoft Azure** tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just created. If you still don't see it, wait another minute and then refresh the page again.



SC900-WinVM | Network settings

Virtual machine

This is a new experience. Please provide feedback

Essentials

Network interface: sc900-winvm137

Virtual network / subnet: LabsSC900-vnet / default

Public IP address: 13.93.55.187

Private IP address: 10.0.0.4

Admin security rules: 0 (Configure)

Load balancers: 0 (Configure)

Application security groups: 0 (Configure)

Network security group: NSG-SC900

Accelerated networking: Disabled

Effective security rules: 0

Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.

☑ 7. From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces**.

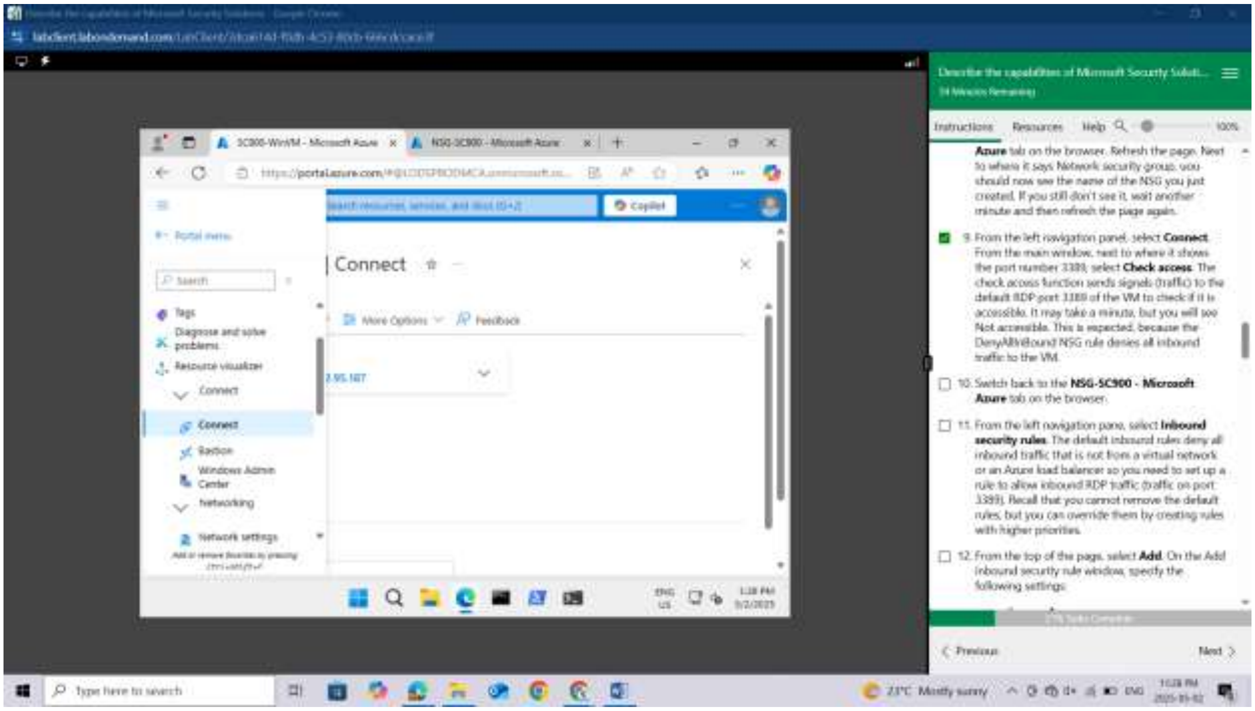
a. Select **Associate**.

b. In the field for network interface associations, select the **down-arrow**, select **sc900-winvmXXX**, then select **OK** on the bottom of the window. Once the interface is associated to the NSG, it will show up on the list. The NSG is now assigned to the network interface of your VM.

☑ 8. Switch back to the **SC900-WinVM - Microsoft Azure** tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just created. If you still don't see it, wait another minute and then refresh the page again.

□ 9. From the left navigation panel, select **Connect**. From the main window, next to where it shows the port number 3389, select **Check access**. The check access function sends signals (traffic) to the default RDP port 3389 of the VM to check if it is

From the left navigation panel, select **Connect**.



Azure tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just created. If you still don't see it, wait another minute and then refresh the page again.

☑ 9. From the left navigation panel, select **Connect**. From the main window, next to where it shows the port number 3389, select **Check access**. The check access function sends signals (traffic) to the default RDP port 3389 of the VM to check if it is accessible. It may take a minute, but you will see Not accessible. This is expected, because the DenyAllInBound NSG rule denies all inbound traffic to the VM.

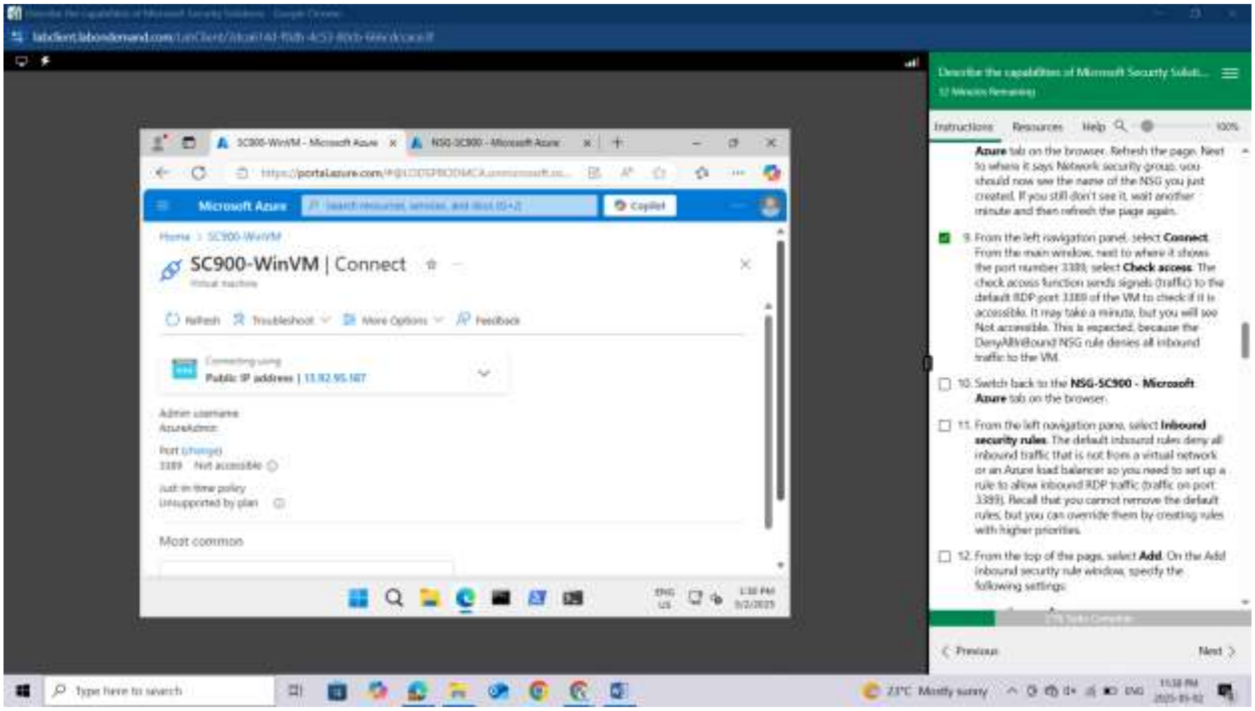
□ 10. Switch back to the **NSG-SC900 - Microsoft Azure** tab on the browser.

□ 11. From the left navigation pane, select **Inbound security rules**. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.

□ 12. From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:

From the main window, next to where it shows the port number **3389**, select **Check access.** The check access function sends signals (traffic) to the default RDP port 3389 of the VM to check if it is accessible.

It may take a minute, but you will see **Not accessible**. This is expected, because the DenyAllInBound NSG rule denies all inbound traffic to the VM.



SC900-WinVM | Connect

Virtual machine

Connecting using
Public IP address | 13.92.95.107

Admin username
AzureAdmin

Port (change)
3389 Not accessible

Just-in-time policy
Unsupported by plan

Most common

Describe the capabilities of Microsoft Security Soluti...

Azure tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just created. If you still don't see it, wait another minute and then refresh the page again.

☑ 9. From the left navigation panel, select **Connect**. From the main window, next to where it shows the port number 3389, select **Check access**. The check access function sends signals (traffic) to the default RDP port 3389 of the VM to check if it is accessible. It may take a minute, but you will see Not accessible. This is expected, because the DenyAllInBound NSG rule denies all inbound traffic to the VM.

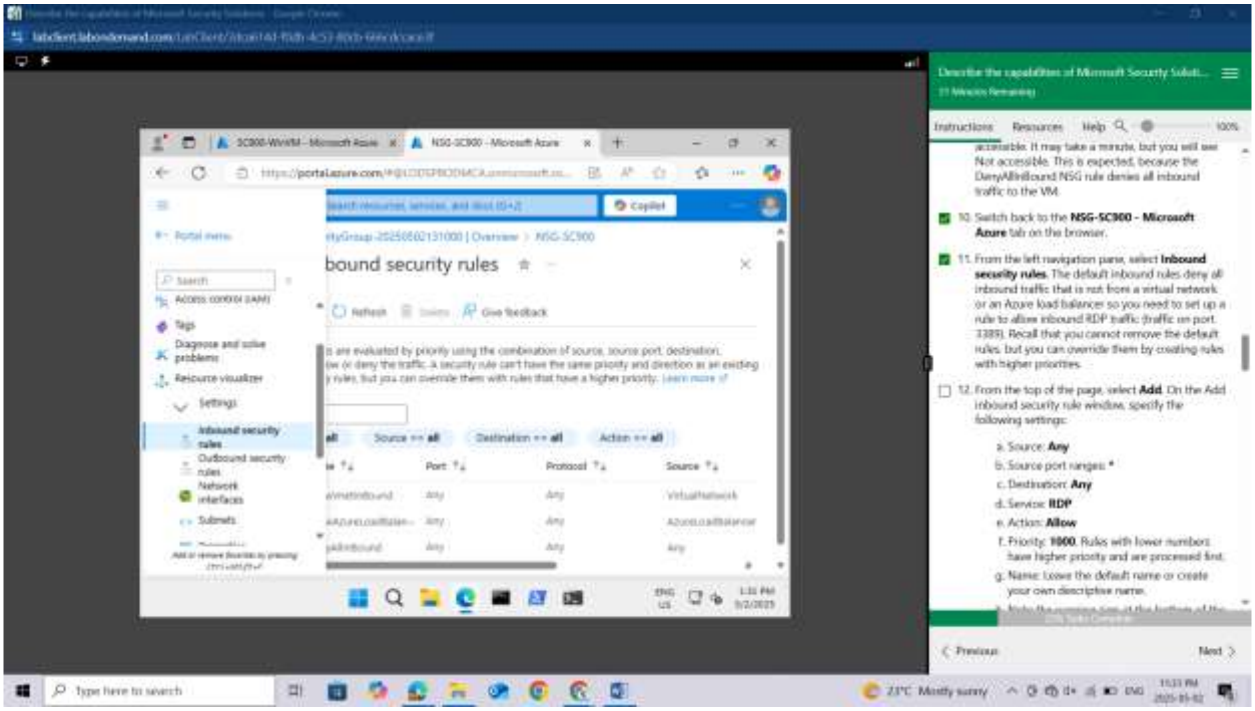
☐ 10. Switch back to the **NSG-SC900 - Microsoft Azure** tab on the browser.

☐ 11. From the left navigation pane, select **Inbound security rules**. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.

☐ 12. From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:

Switch back to the **NSG-SC900 -** Microsoft Azure tab on the browser.

From the left navigation pane, select **Inbound security rules**.



Inbound security rules

...s are evaluated by priority using the combination of source, source port, destination, ...ow or deny the traffic. A security rule can't have the same priority and direction as an existing ...y rules, but you can override them with rules that have a higher priority. Learn more

...e	Port	Protocol	Source
...VnetInBound	Any	Any	VirtualNetwork
...AzureLoadBalan...	Any	Any	AzureLoadBalancer
...yAllInBound	Any	Any	Any

Describe the capabilities of Microsoft Security Soluti...

accessible. It may take a minute, but you will see Not accessible. This is expected, because the DenyAllInBound NSG rule denies all inbound traffic to the VM.

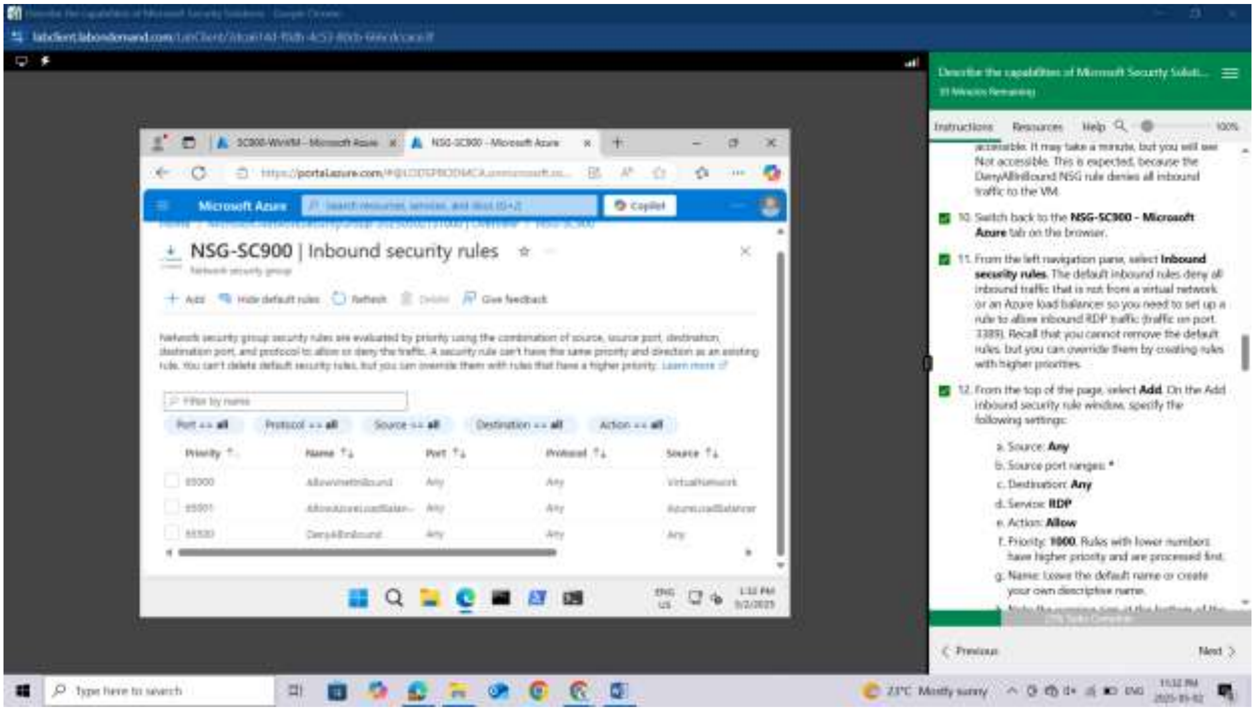
☑ 10. Switch back to the **NSG-SC900 - Microsoft Azure** tab on the browser.

☑ 11. From the left navigation pane, select **Inbound security rules**. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.

☐ 12. From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:

a. Source: **Any**
b. Source port ranges: *
c. Destination: **Any**
d. Service: **RDP**
e. Action: **Allow**
f. Priority: **1000**. Rules with lower numbers have higher priority and are processed first.
g. Name: Leave the default name or create your own descriptive name.

The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.



NSG-SC900 | 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

Port == all · Protocol == all · Source == all · Destination == all · Action == all

Priority	Name	Port	Protocol	Source
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any

Describe the capabilities of Microsoft Security Soluti...

accessible. It may take a minute, but you will see Not accessible. This is expected, because the DenyAllInBound NSG rule denies all inbound traffic to the VM.

10. Switch back to the **NSG-SC900 - Microsoft Azure** tab on the browser.

11. From the left navigation pane, select **Inbound security rules**. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.

12. From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:

a. Source: **Any**
b. Source port ranges: *
c. Destination: **Any**
d. Service: **RDP**
e. Action: **Allow**
f. Priority: **1000**. Rules with lower numbers have higher priority and are processed first.
g. Name: Leave the default name or create your own descriptive name.

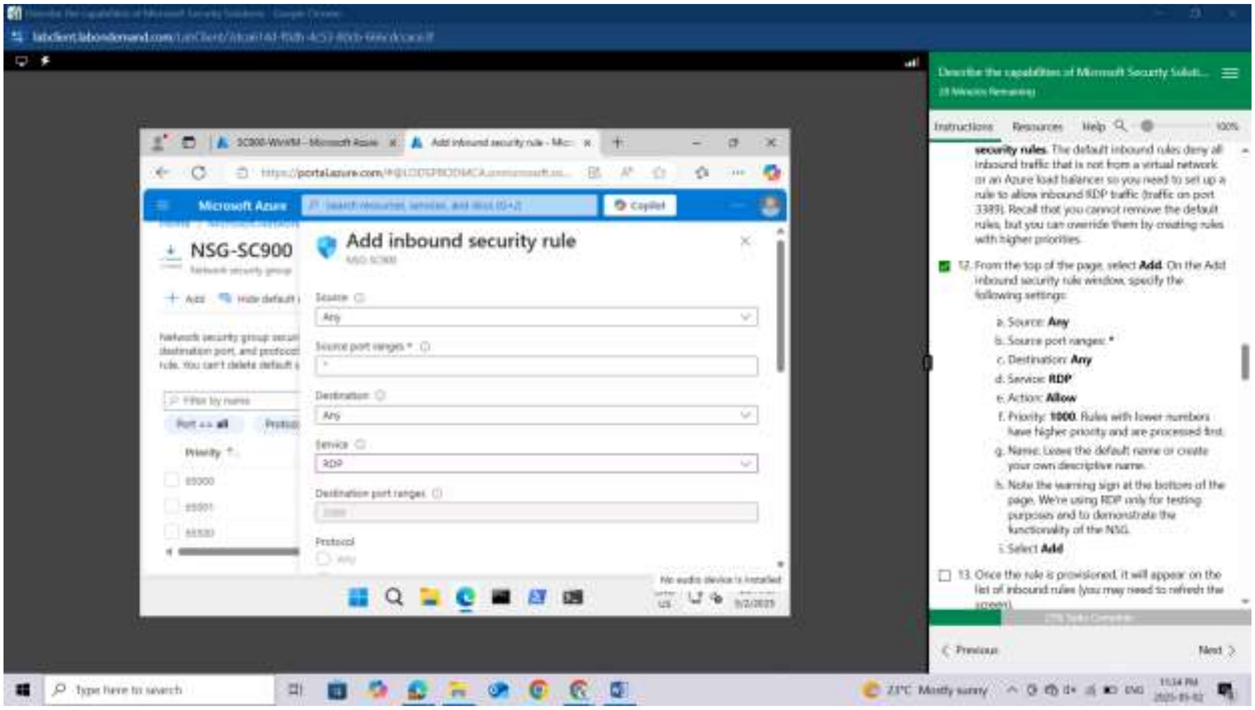
From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:

Source: **Any**

Source port ranges: *****

Destination: **Any**

Service: **RDP**



Add inbound security rule

NSG-SC900

Source: Any

Source port ranges *: *

Destination: Any

Service: RDP

Destination port ranges: 3389

Protocol

security rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.

☑ 12. From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:

a. Source: **Any**
b. Source port ranges: *****
c. Destination: **Any**
d. Service: **RDP**
e. Action: **Allow**
f. Priority: **1000**. Rules with lower numbers have higher priority and are processed first.
g. Name: Leave the default name or create your own descriptive name.
h. Note the warning sign at the bottom of the page. We're using RDP only for testing purposes and to demonstrate the functionality of the NSG.
i. Select **Add**

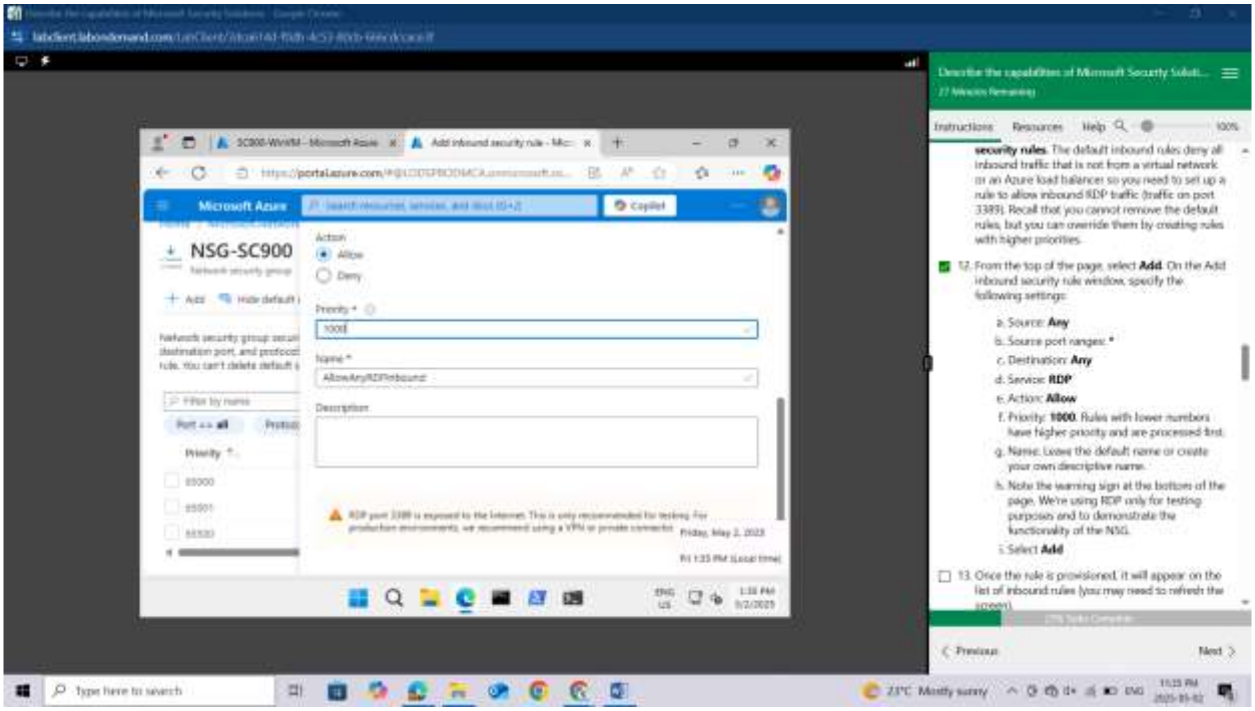
□ 13. Once the rule is provisioned, it will appear on the list of inbound rules (you may need to refresh the screen).

Action: **Allow**

Priority: **1000**. Rules with lower numbers have higher priority and are processed first.

Name: Leave the default name or create your own descriptive name.

Note the warning sign at the bottom of the page. We're using RDP only for testing purposes and to demonstrate the functionality of the NSG.



Action

● Allow
○ Deny

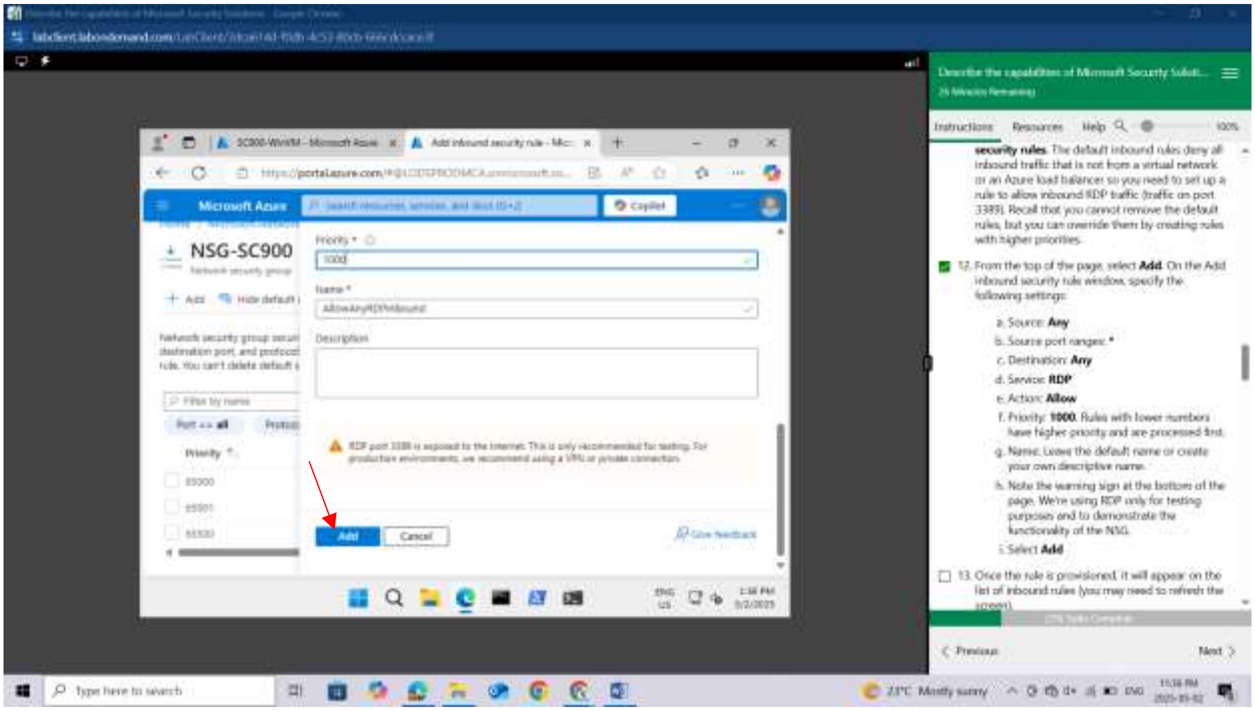
Priority *: 1000

Name *: AllowAnyRDPInbound

Description

RDP port 3389 is exposed to the Internet. This is only recommended for testing. For production environments, we recommend using a VPN or private connection.

Select **Add**



Describe the capabilities of Microsoft Security Soluti...

NSG-SC900

Network security group

Priority * 1000

Name * AllowAnyRDPInbound

Description

RDP port 3389 is exposed to the Internet. This is only recommended for testing. For production environments, we recommend using a VPN or private connection.

security rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.

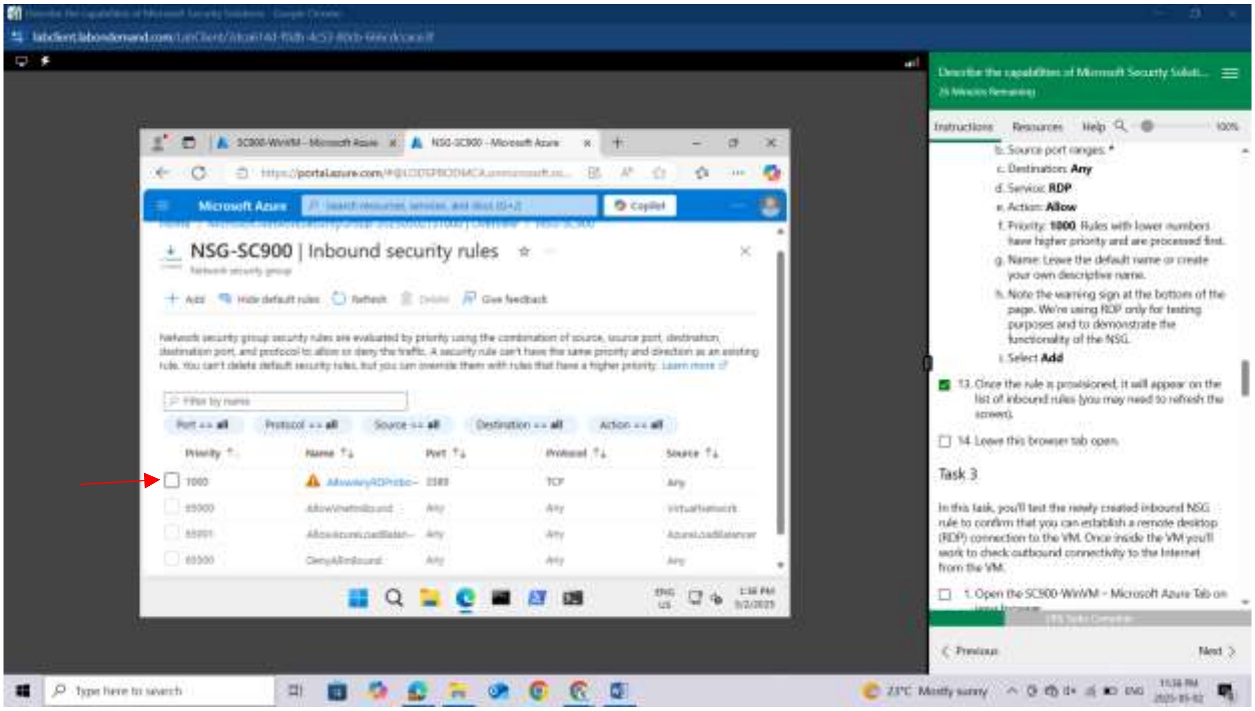
☑ 12. From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:

a. Source: **Any**
b. Source port ranges: *
c. Destination: **Any**
d. Service: **RDP**
e. Action: **Allow**
f. Priority: **1000**. Rules with lower numbers have higher priority and are processed first.
g. Name: Leave the default name or create your own descriptive name.
h. Note the warning sign at the bottom of the page. We're using RDP only for testing purposes and to demonstrate the functionality of the NSG.
i. Select **Add**

☐ 13. Once the rule is provisioned, it will appear on the list of inbound rules (you may need to refresh the screen).

Once the rule is provisioned, it will appear on the list of inbound rules (you may need to refresh the screen).

Leave this browser tab open.



Describe the capabilities of Microsoft Security Soluti...

NSG-SC900 | 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
1000	AllowAnyRDPInbo...	3389	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any

b. Source port ranges: *
c. Destination: **Any**
d. Service: **RDP**
e. Action: **Allow**
f. Priority: **1000**. Rules with lower numbers have higher priority and are processed first.
g. Name: Leave the default name or create your own descriptive name.
h. Note the warning sign at the bottom of the page. We're using RDP only for testing purposes and to demonstrate the functionality of the NSG.
i. Select **Add**

☑ 13. Once the rule is provisioned, it will appear on the list of inbound rules (you may need to refresh the screen).

☐ 14. Leave this browser tab open.

Task 3

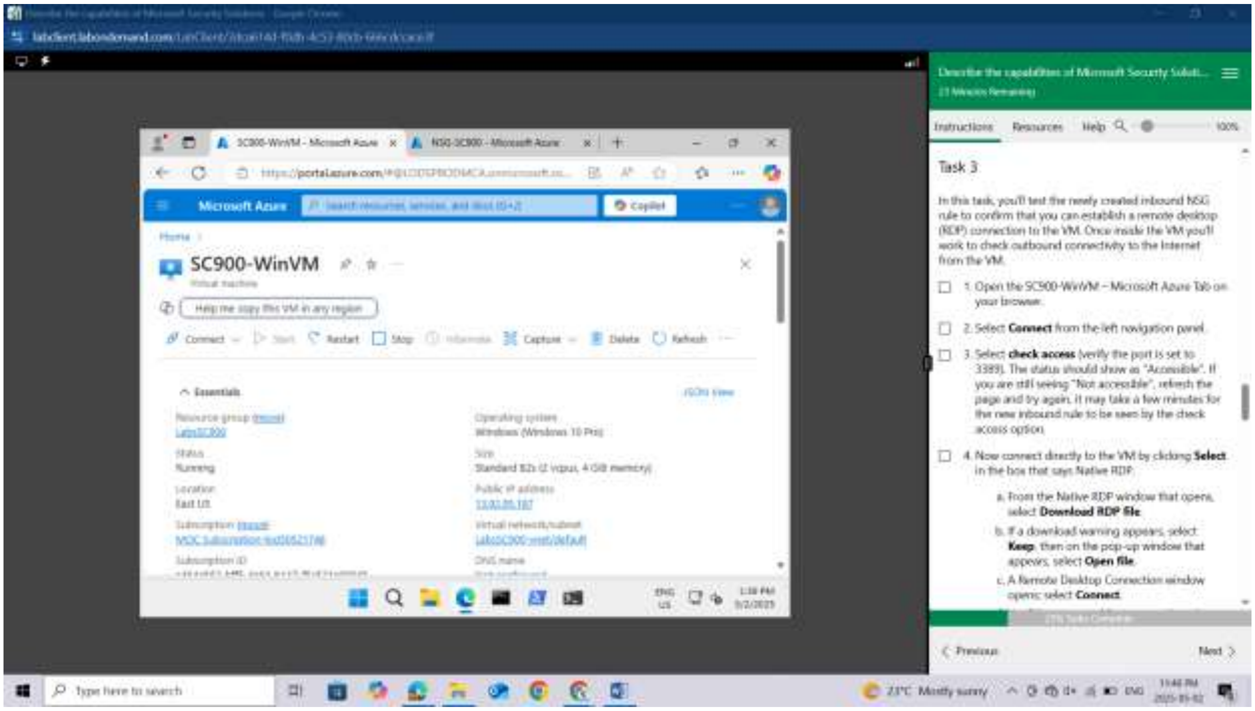
In this task, you'll test the newly created inbound NSG rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

☐ 1. Open the SC900-WinVM – Microsoft Azure Tab on

Task 3

In this task, you'll test the newly created inbound NSG rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

Open the **SC900-WinVM – Microsoft Azure** Tab on your browser.



SC900-WinVM
Virtual machine

Resource group (move)
LabsSC900

Status
Running

Location
East US

Subscription (move)
MOC Subscription-lod50521748

Subscription ID

Operating system
Windows (Windows 10 Pro)

Size
Standard B2s (2 vcpus, 4 GiB memory)

Public IP address
13.92.95.107

Virtual network/subnet
LabsSC900-vnet/default

DNS name
Not configured

Describe the capabilities of Microsoft Security Soluti...

Task 3

In this task, you'll test the newly created inbound NSG rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

□ 1. Open the SC900-WinVM – Microsoft Azure Tab on your browser.

□ 2. Select **Connect** from the left navigation panel.

□ 3. Select **check access** (verify the port is set to 3389). The status should show as "Accessible". If you are still seeing "Not accessible", refresh the page and try again. It may take a few minutes for the new inbound rule to be seen by the check access option.

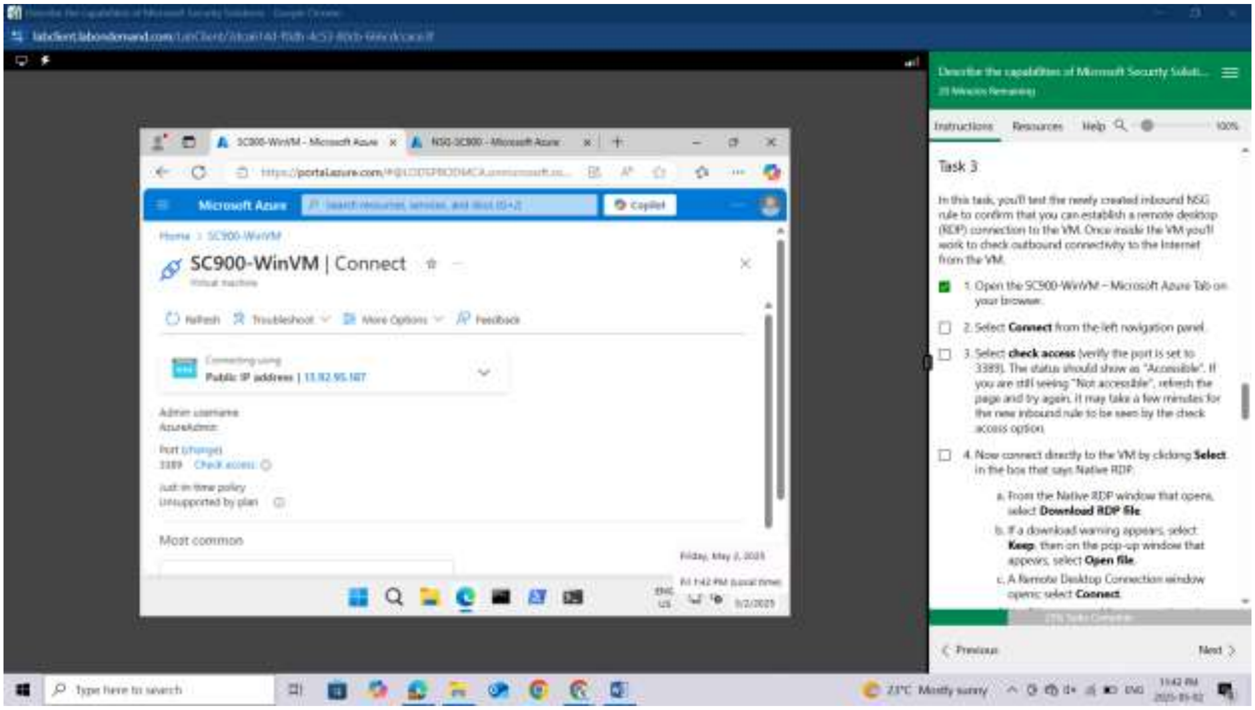
□ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

Select **Connect** from the left navigation panel.



SC900-WinVM | Connect
Virtual machine

Connecting using
Public IP address | 13.92.95.107

Admin username
AzureAdmin

Port (change)
3389

Just-in-time policy
Unsupported by plan

Describe the capabilities of Microsoft Security Soluti...

Task 3

In this task, you'll test the newly created inbound NSG rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

☑ 1. Open the SC900-WinVM – Microsoft Azure Tab on your browser.

□ 2. Select **Connect** from the left navigation panel.

□ 3. Select **check access** (verify the port is set to 3389). The status should show as "Accessible". If you are still seeing "Not accessible", refresh the page and try again. It may take a few minutes for the new inbound rule to be seen by the check access option.

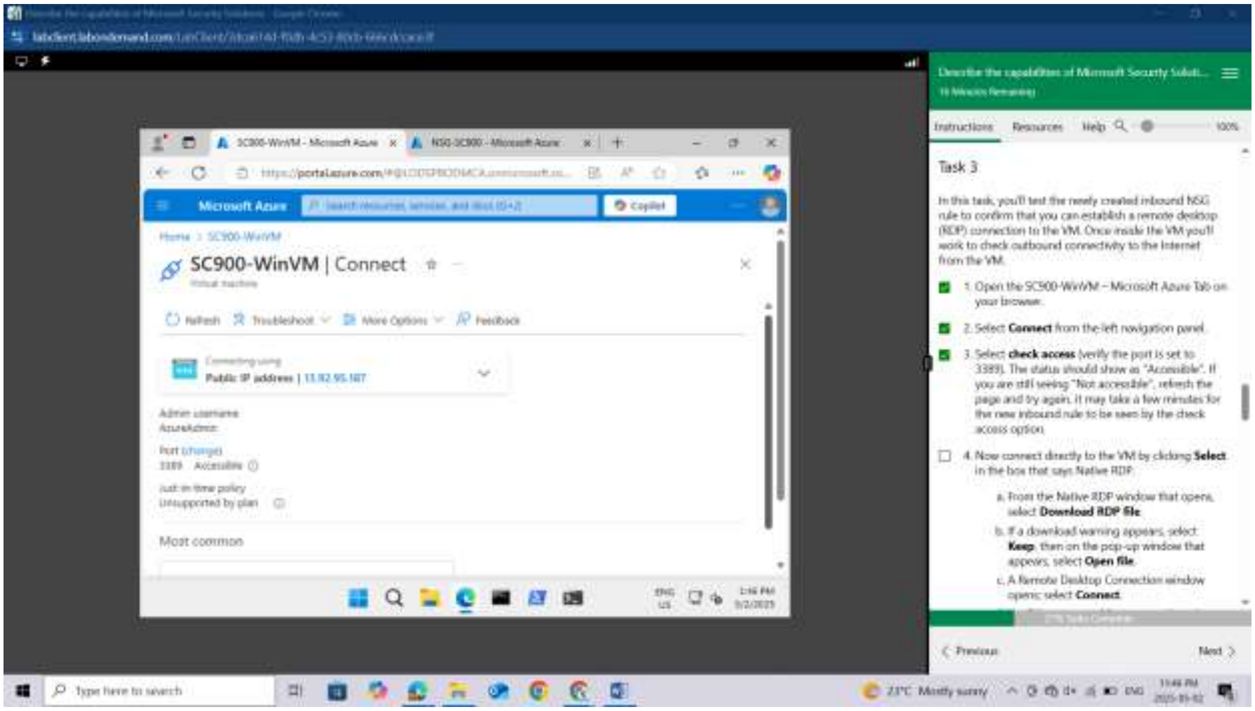
□ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

Select **check access** (verify the port is set to 3389). The status should show as "**Accessible**". If you are still seeing "Not accessible", refresh the page and try again, it may take a few minutes for the new inbound rule to be seen by the check access option.



SC900-WinVM | Connect

Virtual machine

Connecting using
Public IP address | 13.92.95.107

Admin username
AzureAdmin

Port (change)
3389 Accessible

Just-in-time policy
Unsupported by plan

Most common

Describe the capabilities of Microsoft Security Soluti...

Task 3

In this task, you'll test the newly created inbound NSG rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

☑ 1. Open the SC900-WinVM – Microsoft Azure Tab on your browser.

☑ 2. Select **Connect** from the left navigation panel.

☑ 3. Select **check access** (verify the port is set to 3389). The status should show as "Accessible". If you are still seeing "Not accessible", refresh the page and try again, it may take a few minutes for the new inbound rule to be seen by the check access option.

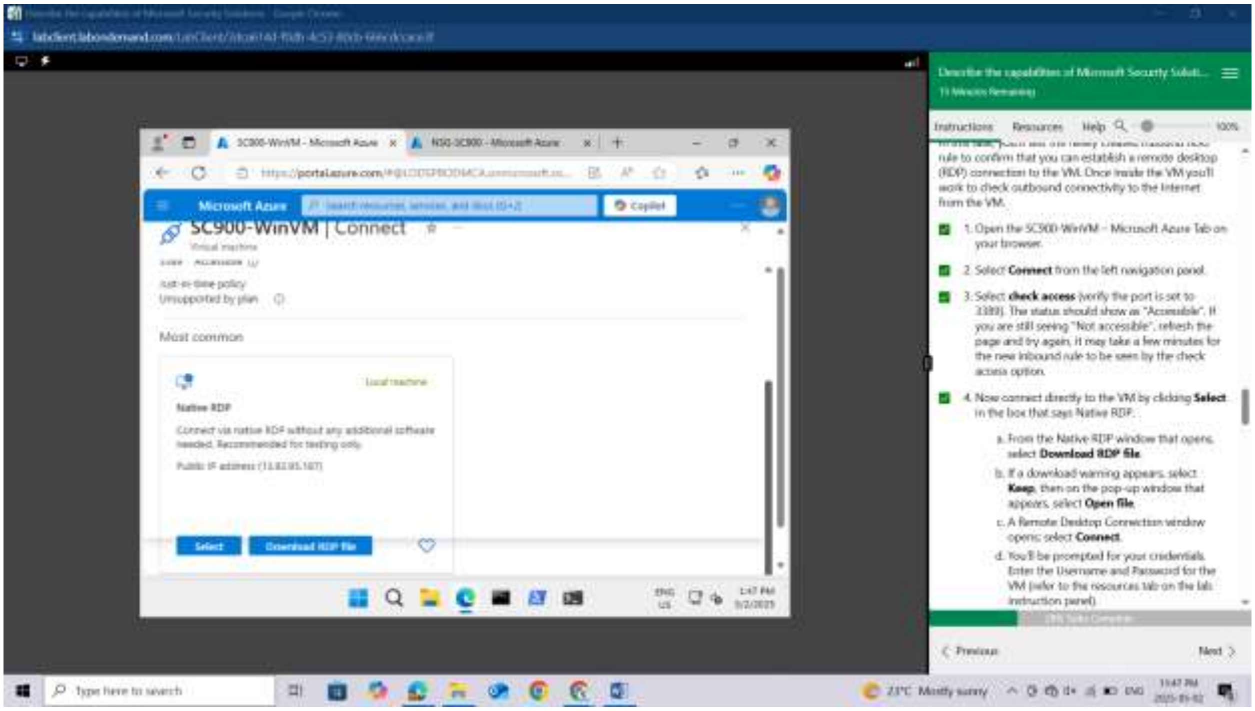
☐ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

Now connect directly to the VM by clicking **Select** in the box that says Native RDP.



SC900-WinVM | Connect

Virtual machine

Just-in-time policy
Unsupported by plan

Most common

Native RDP

Local machine

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

Public IP address (13.92.95.107)

Select | Download RDP file

rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

☑ 1. Open the SC900-WinVM – Microsoft Azure Tab on your browser.

☑ 2. Select **Connect** from the left navigation panel.

☑ 3. Select **check access** (verify the port is set to 3389). The status should show as "Accessible". If you are still seeing "Not accessible", refresh the page and try again, it may take a few minutes for the new inbound rule to be seen by the check access option.

☑ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

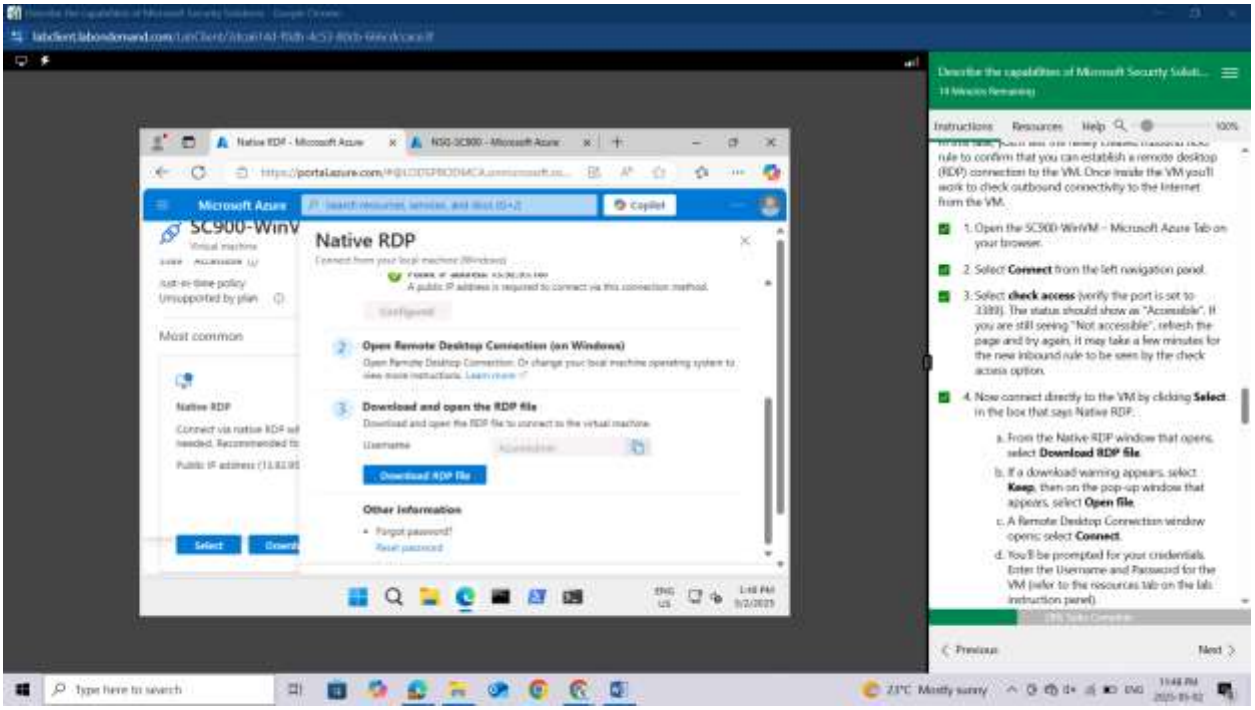
a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

d. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).

From the Native RDP window that opens, select **Download RDP file**.



Native RDP

Connect from your local machine (Windows)

A public IP address is required to connect via this connection method.

2 Open Remote Desktop Connection (on Windows)

Open Remote Desktop Connection. Or change your local machine operating system to view more instructions. Learn more

3 Download and open the RDP file

Download and open the RDP file to connect to the virtual machine.

Username

Download RDP file

Other information

- Forgot password?
  Reset password

Describe the capabilities of Microsoft Security Soluti...

Instructions Resources Help 100%

rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

☑ 1. Open the SC900-WinVM – Microsoft Azure Tab on your browser.

☑ 2. Select **Connect** from the left navigation panel.

☑ 3. Select **check access** (verify the port is set to 3389). The status should show as "Accessible". If you are still seeing "Not accessible", refresh the page and try again, it may take a few minutes for the new inbound rule to be seen by the check access option.

☑ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

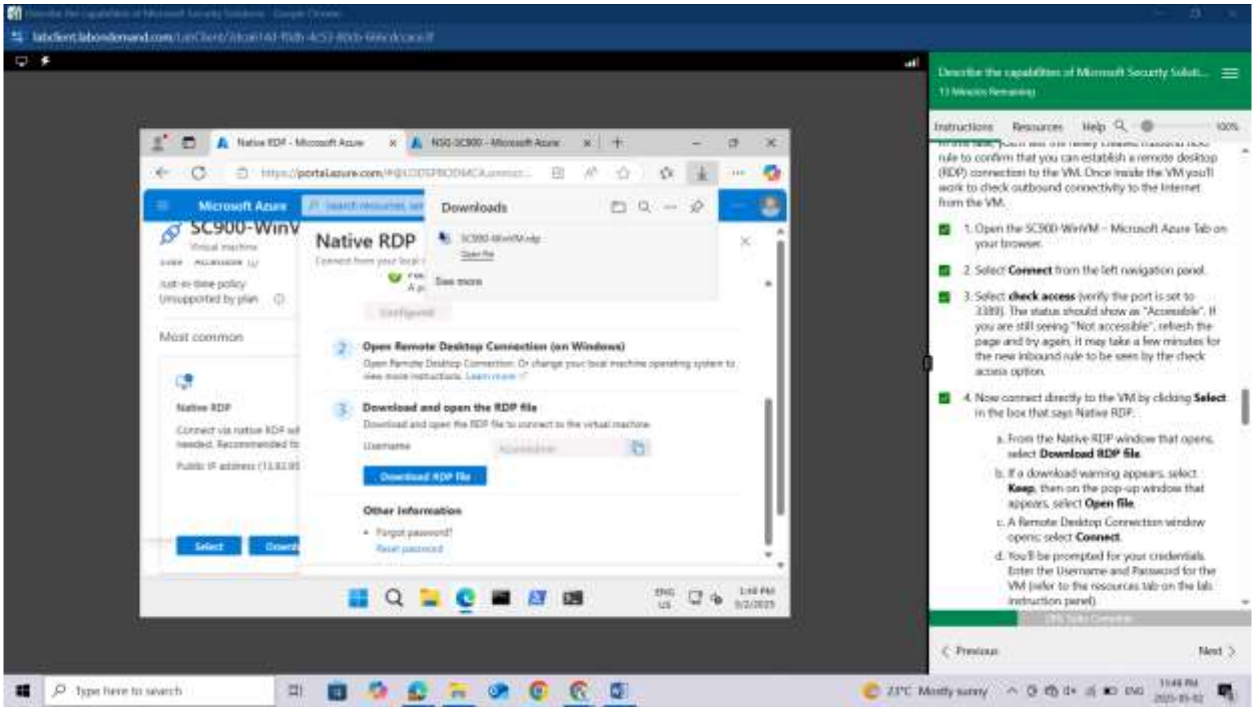
a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

d. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).

If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.



Downloads

SC900-WinVM.rdp

Open file

See more

Native RDP

3 Download and open the RDP file

Download RDP file

☑ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

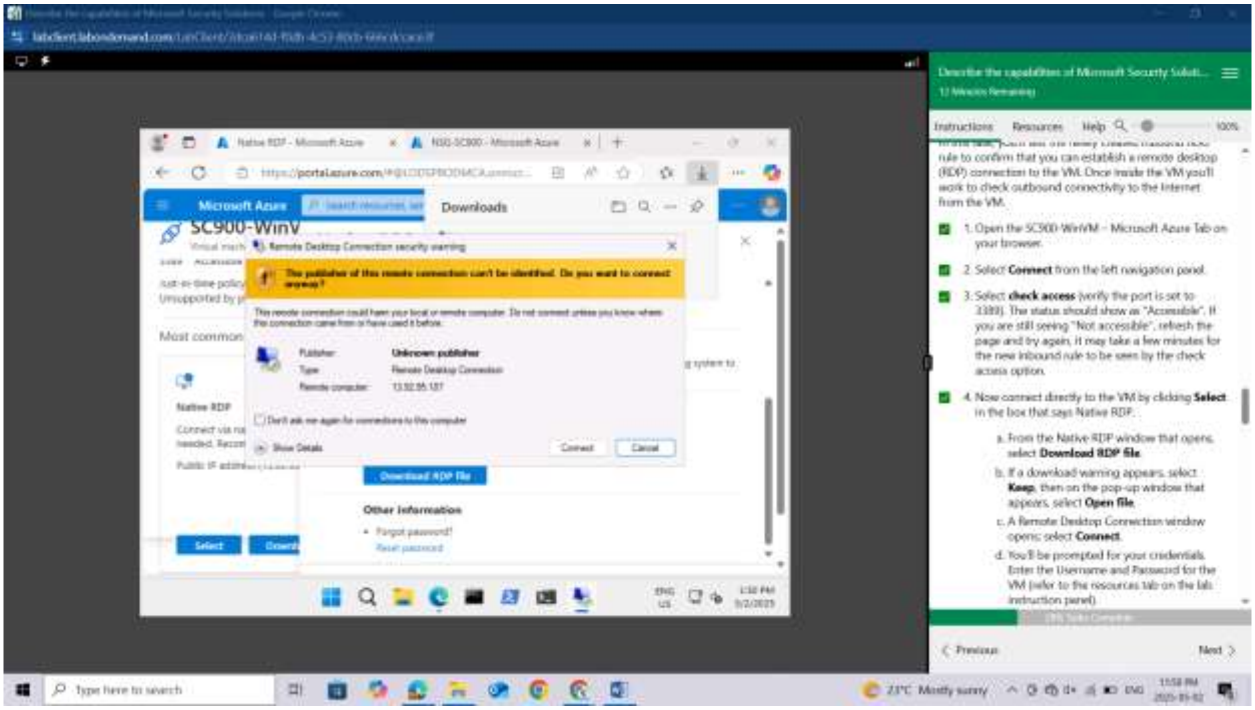
a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

d. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).

A Remote Desktop Connection window opens; select **Connect**.



Remote Desktop Connection security warning

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: **Unknown publisher**
Type: Remote Desktop Connection
Remote computer: 13.92.95.187

□ Don't ask me again for connections to this computer

rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

☑ 1. Open the SC900-WinVM – Microsoft Azure Tab on your browser.

☑ 2. Select **Connect** from the left navigation panel.

☑ 3. Select **check access** (verify the port is set to 3389). The status should show as "Accessible". If you are still seeing "Not accessible", refresh the page and try again, it may take a few minutes for the new inbound rule to be seen by the check access option.

☑ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

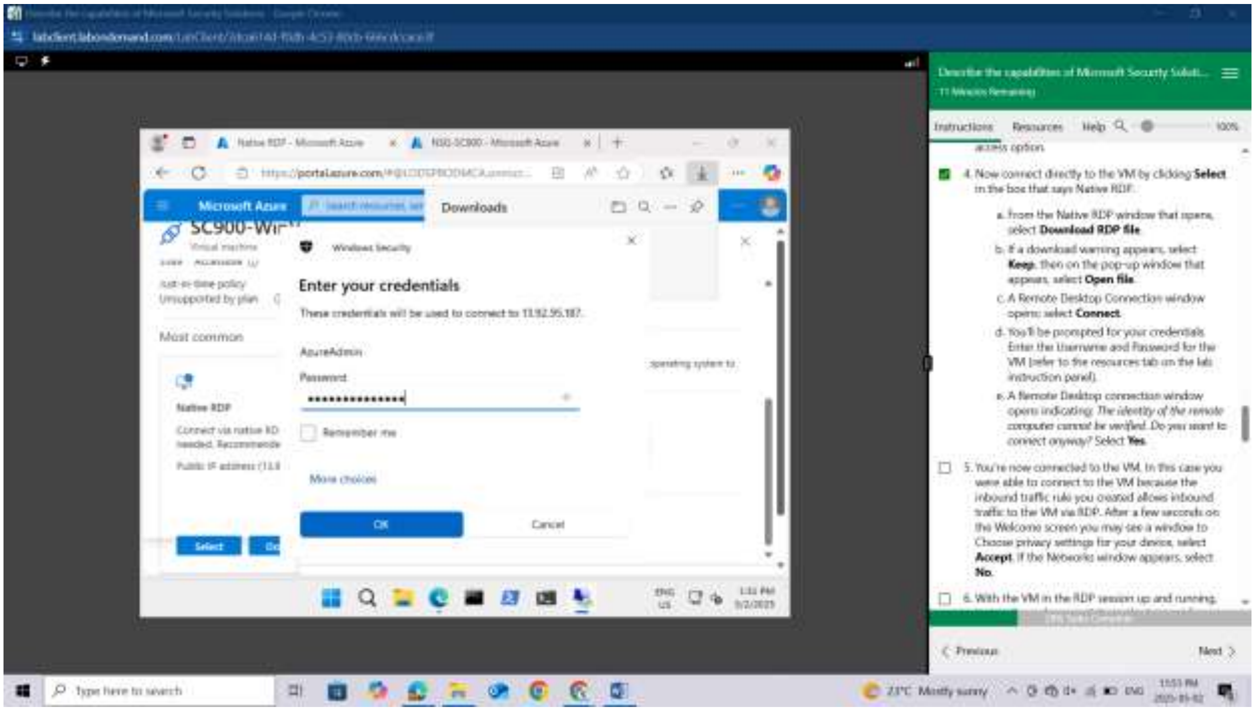
a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

d. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).

You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).



Windows Security

Enter your credentials

These credentials will be used to connect to 13.92.95.187.

AzureAdmin

Password: •••••••••••••••

□ Remember me

access option.

☑ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens; select **Connect**.

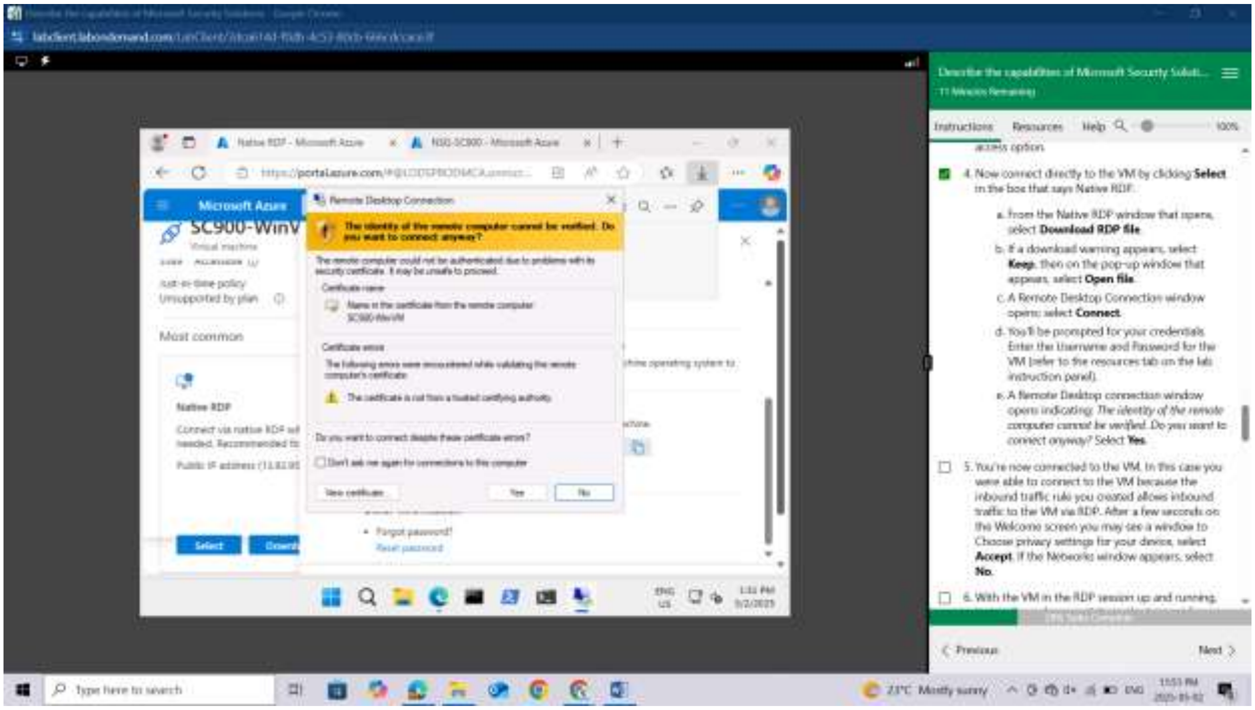
d. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).

e. A Remote Desktop connection window opens indicating: *The identity of the remote computer cannot be verified. Do you want to connect anyway?* Select **Yes**.

□ 5. You're now connected to the VM. In this case you were able to connect to the VM because the inbound traffic rule you created allows inbound traffic to the VM via RDP. After a few seconds on the Welcome screen you may see a window to Choose privacy settings for your device, select **Accept**. If the Networks window appears, select **No**.

□ 6. With the VM in the RDP session up and running,

A Remote Desktop connection window opens indicating: The identity of the remote computer cannot be verified. Do you want to connect anyway? Select **Yes**.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
SC900-WinVM

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

Describe the capabilities of Microsoft Security Soluti...
11 Minutes Remaining

access option.

☑ 4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.

a. From the Native RDP window that opens, select **Download RDP file**.

b. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens: select **Connect**.

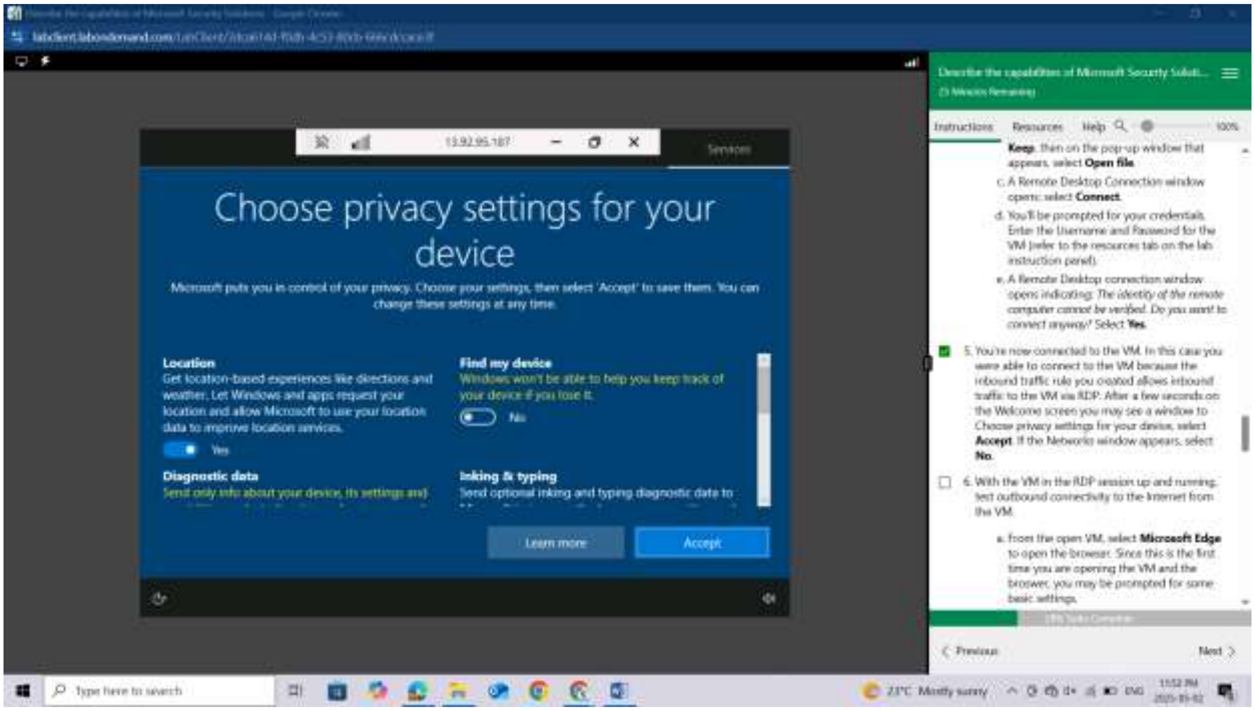
d. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).

e. A Remote Desktop connection window opens indicating: *The identity of the remote computer cannot be verified. Do you want to connect anyway?* Select **Yes**.

□ 5. You're now connected to the VM. In this case you were able to connect to the VM because the inbound traffic rule you created allows inbound traffic to the VM via RDP. After a few seconds on the Welcome screen you may see a window to Choose privacy settings for your device, select **Accept**. If the Networks window appears, select **No**.

□ 6. With the VM in the RDP session up and running,

You're now connected to the VM. In this case you were able to connect to the VM because the inbound traffic rule you created allows inbound traffic to the VM via RDP. After a few seconds on the Welcome screen you may see a window to Choose privacy settings for your device, select **Accept**.



13.92.95.187

Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

Location
Get location-based experiences like directions and weather. Let Windows and apps request your location and allow Microsoft to use your location data to improve location services.
Yes

Find my device
Windows won't be able to help you keep track of your device if you lose it.
No

Diagnostic data
Send only info about your device, its settings and

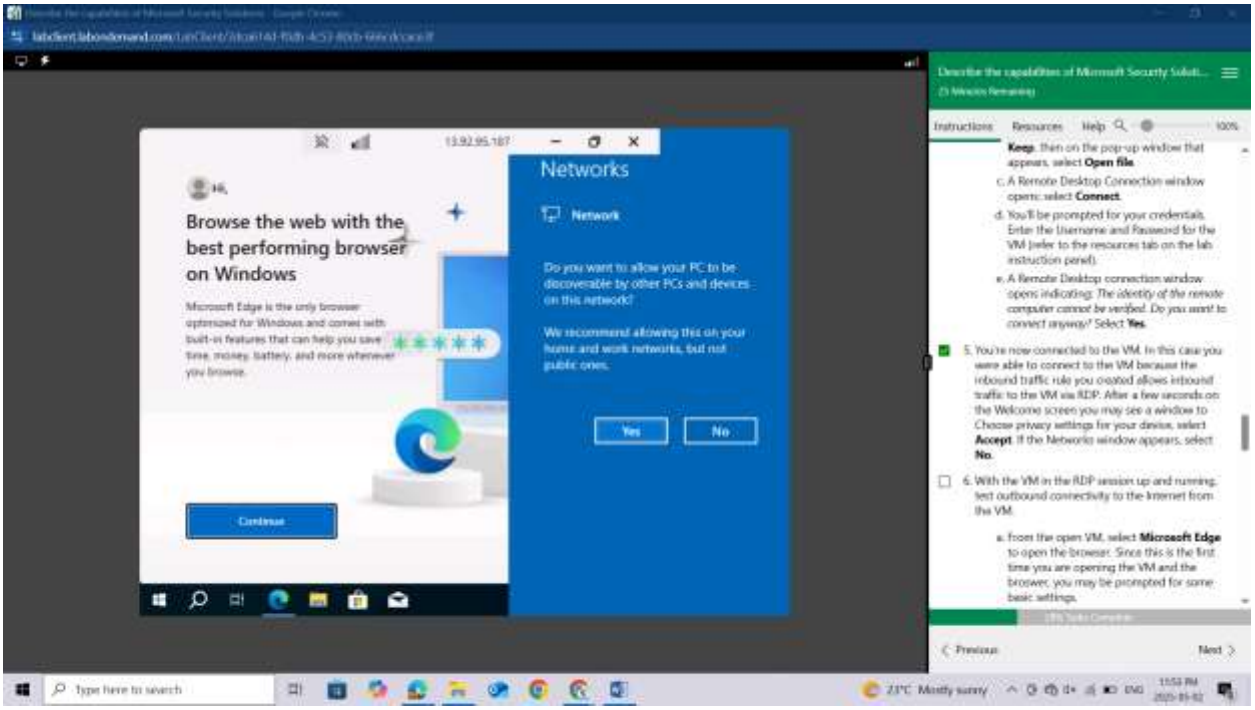
Inking & typing
Send optional inking and typing diagnostic data to

☑ 5. You're now connected to the VM. In this case you were able to connect to the VM because the inbound traffic rule you created allows inbound traffic to the VM via RDP. After a few seconds on the Welcome screen you may see a window to Choose privacy settings for your device, select **Accept**. If the Networks window appears, select **No**.

□ 6. With the VM in the RDP session up and running, test outbound connectivity to the Internet from the VM.

a. From the open VM, select **Microsoft Edge** to open the browser. Since this is the first time you are opening the VM and the browser, you may be prompted for some basic settings.

If the Networks window appears, select **No**.



Browse the web with the best performing browser on Windows

Microsoft Edge is the only browser optimized for Windows and comes with built-in features that can help you save time, money, battery, and more whenever you browse.

Networks

Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

Keep, then on the pop-up window that appears, select **Open file**.

c. A Remote Desktop Connection window opens: select **Connect**.

d. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).

e. A Remote Desktop connection window opens indicating: *The identity of the remote computer cannot be verified. Do you want to connect anyway?* Select **Yes**.

☑ 5. You're now connected to the VM. In this case you were able to connect to the VM because the inbound traffic rule you created allows inbound traffic to the VM via RDP. After a few seconds on the Welcome screen you may see a window to Choose privacy settings for your device, select **Accept**. If the Networks window appears, select **No**.

☐ 6. With the VM in the RDP session up and running, test outbound connectivity to the Internet from the VM.

a. From the open VM, select **Microsoft Edge** to open the browser. Since this is the first time you are opening the VM and the broswer, you may be prompted for some basic settings.

With the VM in the RDP session up and running, test outbound connectivity to the Internet from the VM.

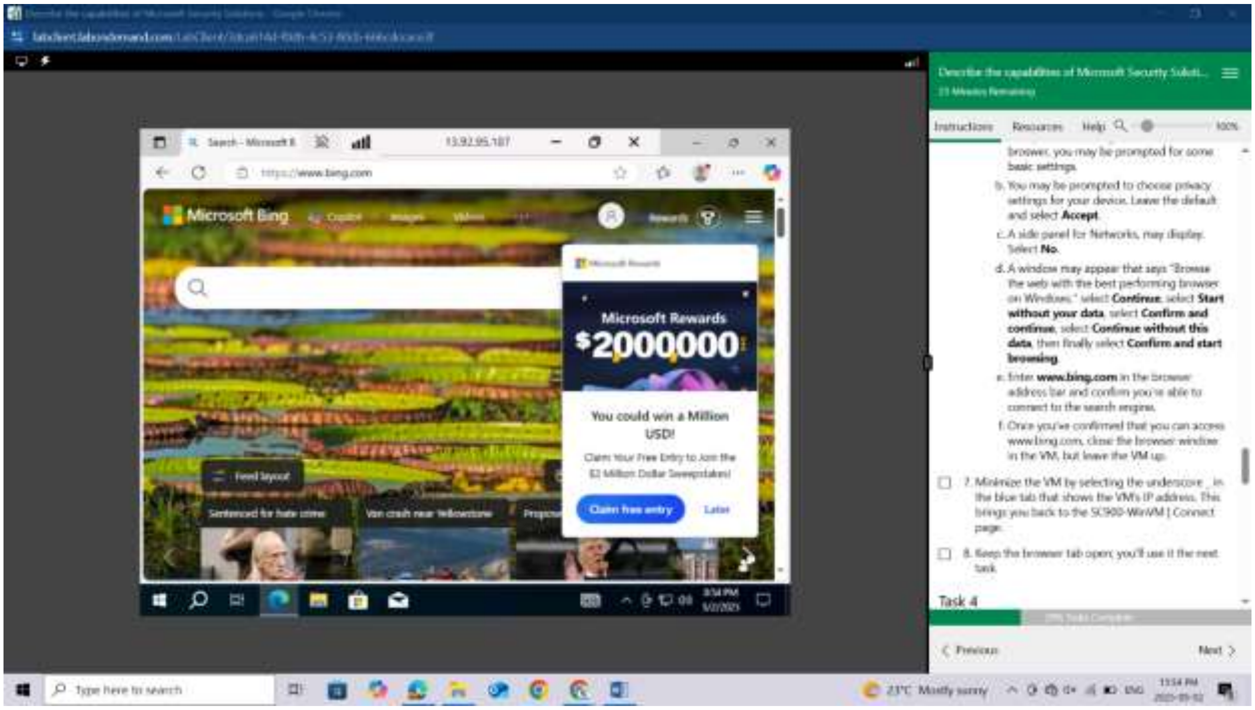
From the open VM, select Microsoft Edge to open the browser. Since this is the first time you are opening the VM and the broswer, you may be prompted for some basic settings.

You may be prompted to choose privacy settings for your device. Leave the default and select Accept.

A side panel for Networks, may display. Select **No**.

A window may appear that says "Browse the web with the best performing browser on Windows," select **Continue**, select **Start without your data**, select **Confirm and continue**, select **Continue without this data**, then finally select **Confirm and start browsing**.

Enter **www.bing.com** in the browser address bar and confirm you're able to connect to the search engine.



Describe the capabilities of Microsoft Security Soluti...

Instructions Resources Help 100%

browser, you may be prompted for some basic settings.

b. You may be prompted to choose privacy settings for your device. Leave the default and select **Accept**.

c. A side panel for Networks, may display. Select **No**.

d. A window may appear that says "Browse the web with the best performing browser on Windows," select **Continue**, select **Start without your data**, select **Confirm and continue**, select **Continue without this data**, then finally select **Confirm and start browsing**.

e. Enter **www.bing.com** in the browser address bar and confirm you're able to connect to the search engine.

f. Once you've confirmed that you can access www.bing.com, close the browser window in the VM, but leave the VM up.

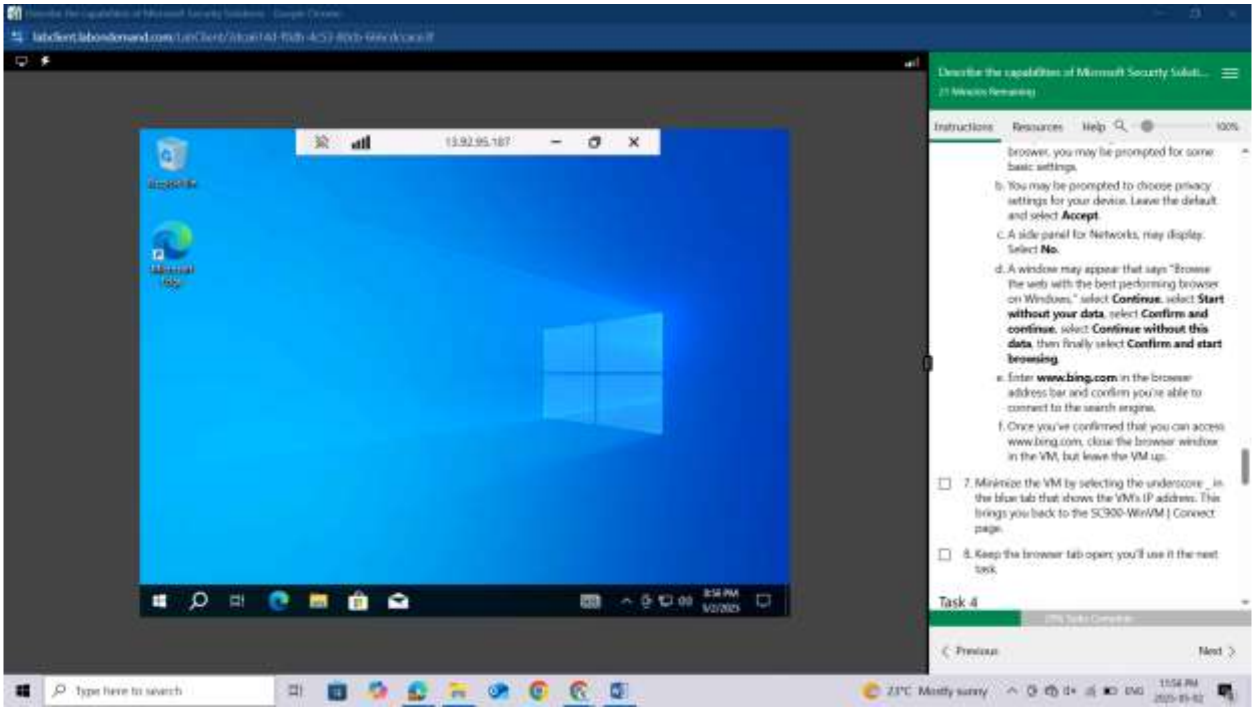
□ 7. Minimize the VM by selecting the underscore _ in the blue tab that shows the VM's IP address. This brings you back to the SC900-WinVM | Connect page.

□ 8. Keep the browser tab open; you'll use it the next task.

Task 4

Microsoft Bing
Microsoft Rewards
$2000000
You could win a Million USD!
Claim Your Free Entry to Join the $2 Million Dollar Sweepstakes!
Claim free entry
Later
Previous
Next

Once you've confirmed that you can access www.bing.com , close the browser window in the VM, but leave the VM up.



Describe the capabilities of Microsoft Security Soluti...

browser, you may be prompted for some basic settings.

b. You may be prompted to choose privacy settings for your device. Leave the default and select **Accept**.

c. A side panel for Networks, may display. Select **No**.

d. A window may appear that says "Browse the web with the best performing browser on Windows," select **Continue**, select **Start without your data**, select **Confirm and continue**, select **Continue without this data**, then finally select **Confirm and start browsing**.

e. Enter **www.bing.com** in the browser address bar and confirm you're able to connect to the search engine.

f. Once you've confirmed that you can access www.bing.com, close the browser window in the VM, but leave the VM up.

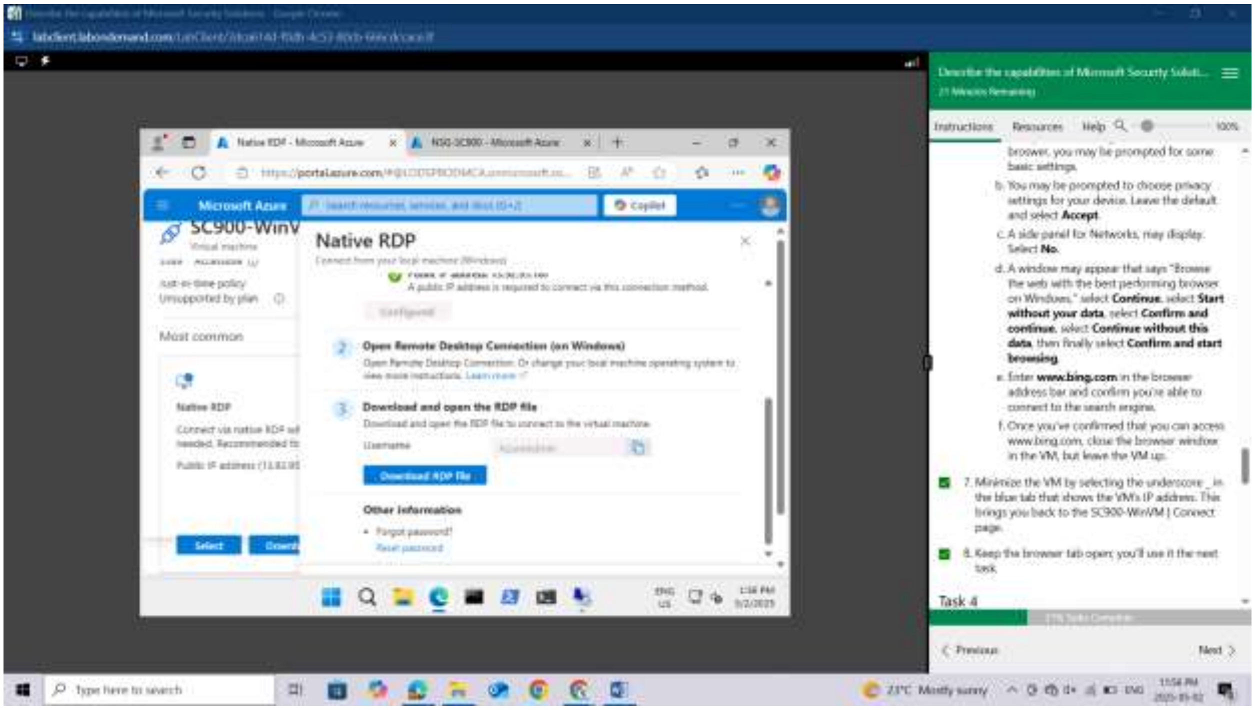
□ 7. Minimize the VM by selecting the underscore _ in the blue tab that shows the VM's IP address. This brings you back to the SC900-WinVM | Connect page.

□ 8. Keep the browser tab open; you'll use it the next task.

Task 4

Minimize the VM by selecting the underscore _ in the blue tab that shows the VM's IP address. This brings you back to the SC900-WinVM | Connect page.

Keep the browser tab open; you'll use it the next task.


Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/
Native RDP - Microsoft Azure
NSG-SC900 - Microsoft Azure
https://portal.azure.com/
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
SC900-WinV
Virtual machine
Just-in-time policy
Unsupported by plan
Most common
Native RDP
Connect via native RDP wi
needed. Recommended fo
Public IP address (13.82.95
Select
Downl
Native RDP
Connect from your local machine (Windows)
Configured
Username
Download RDP file
Other information
Forgot password?
Reset password
Describe the capabilities of Microsoft Security Soluti...
21 Minutes Remaining
Instructions
Resources
Help
100%
Task 4
Previous
Next
Type here to search
23°C Mostly sunny

A public IP address is required to connect via this connection method.

2 Open Remote Desktop Connection (on Windows)

Open Remote Desktop Connection. Or change your local machine operating system to view more instructions. Learn more

3 Download and open the RDP file

Download and open the RDP file to connect to the virtual machine.

browser, you may be prompted for some basic settings.

b. You may be prompted to choose privacy settings for your device. Leave the default and select **Accept**.

c. A side panel for Networks, may display. Select **No**.

d. A window may appear that says "Browse the web with the best performing browser on Windows," select **Continue**, select **Start without your data**, select **Confirm and continue**, select **Continue without this data**, then finally select **Confirm and start browsing**.

e. Enter **www.bing.com** in the browser address bar and confirm you're able to connect to the search engine.

f. Once you've confirmed that you can access www.bing.com, close the browser window in the VM, but leave the VM up.

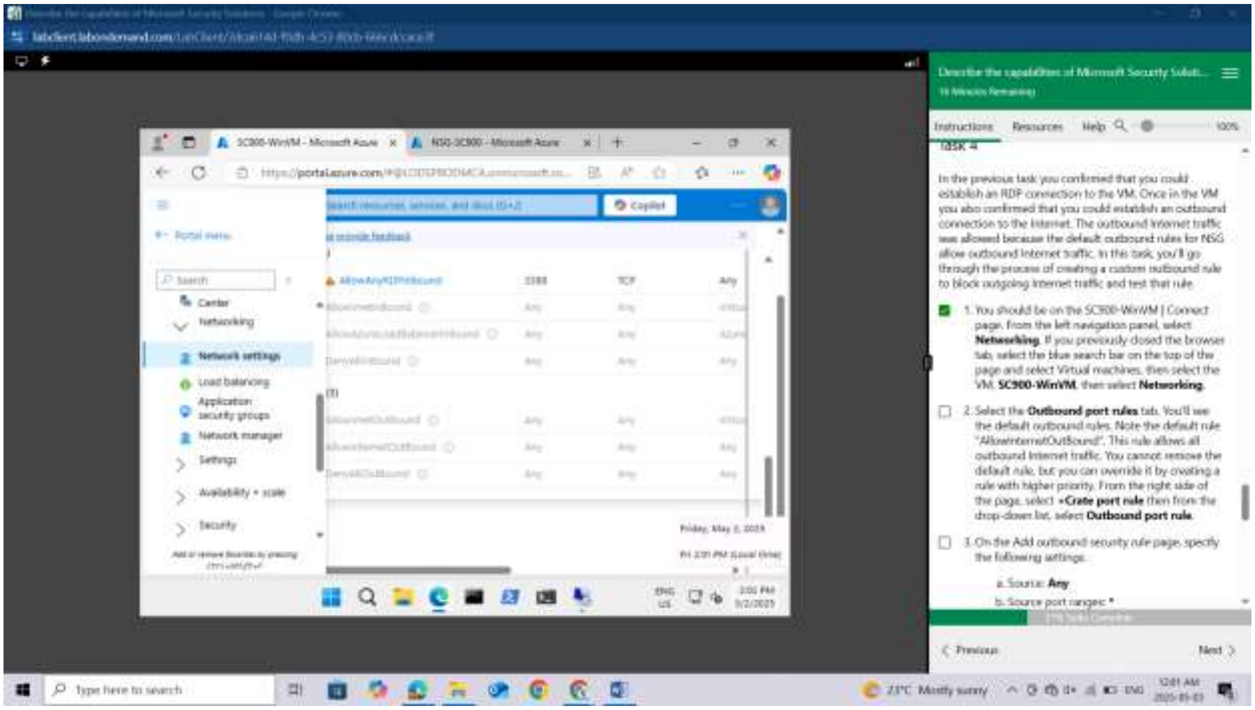
☑ 7. Minimize the VM by selecting the underscore _ in the blue tab that shows the VM's IP address. This brings you back to the SC900-WinVM | Connect page.

☑ 8. Keep the browser tab open; you'll use it the next task.

Task 4

In the previous task you confirmed that you could establish an RDP connection to the VM. Once in the VM you also confirmed that you could establish an outbound connection to the Internet. The outbound Internet traffic was allowed because the default outbound rules for NSG allow outbound Internet traffic. In this task, you'll go through the process of creating a custom outbound rule to block outgoing Internet traffic and test that rule.

You should be on the SC900-WinVM | Connect page. From the left navigation panel, select **Networking.** If you previously closed the browser tab, select the blue search bar on the top of the page and select **Virtual machines**, then select the **VM, SC900-WinVM**, then select **Networking.**



Task 4

In the previous task you confirmed that you could establish an RDP connection to the VM. Once in the VM you also confirmed that you could establish an outbound connection to the Internet. The outbound Internet traffic was allowed because the default outbound rules for NSG allow outbound Internet traffic. In this task, you'll go through the process of creating a custom outbound rule to block outgoing Internet traffic and test that rule.

☑ 1. You should be on the SC900-WinVM | Connect page. From the left navigation panel, select **Networking**. If you previously closed the browser tab, select the blue search bar on the top of the page and select Virtual machines, then select the VM, **SC900-WinVM**, then select **Networking**.

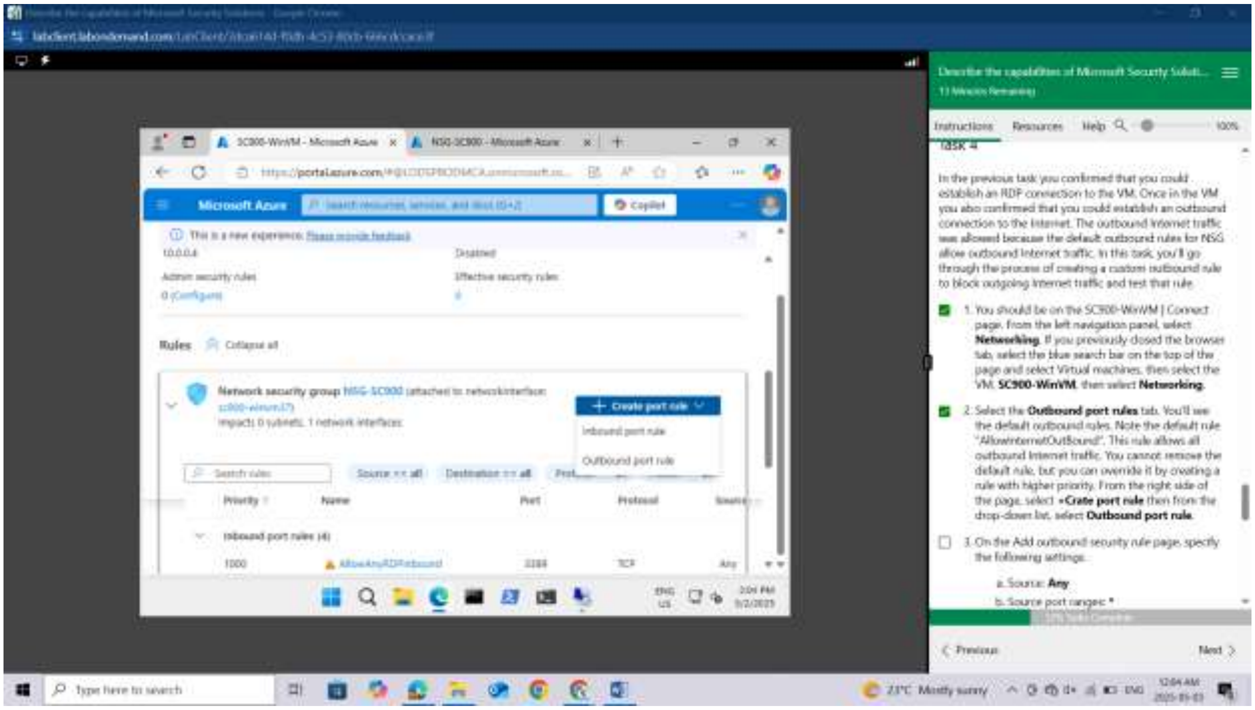
□ 2. Select the **Outbound port rules** tab. You'll see the default outbound rules. Note the default rule "AllowInternetOutBound". This rule allows all outbound Internet traffic. You cannot remove the default rule, but you can override it by creating a rule with higher priority. From the right side of the page, select **+Crate port rule** then from the drop-down list, select **Outbound port rule**.

□ 3. On the Add outbound security rule page, specify the following settings:

a. Source: **Any**

b. Source port ranges: *

Select the Outbound port rules tab. You'll see the default outbound rules. Note the default rule "**AllowInternetOutBound**". This rule allows all outbound Internet traffic. You cannot remove the default rule, but you can override it by creating a rule with higher priority. From the right side of the page, select **+Crate port rule** then from the drop-down list, select **Outbound port rule**.



On the Add outbound security rule page, specify the following settings:

Source: **Any**

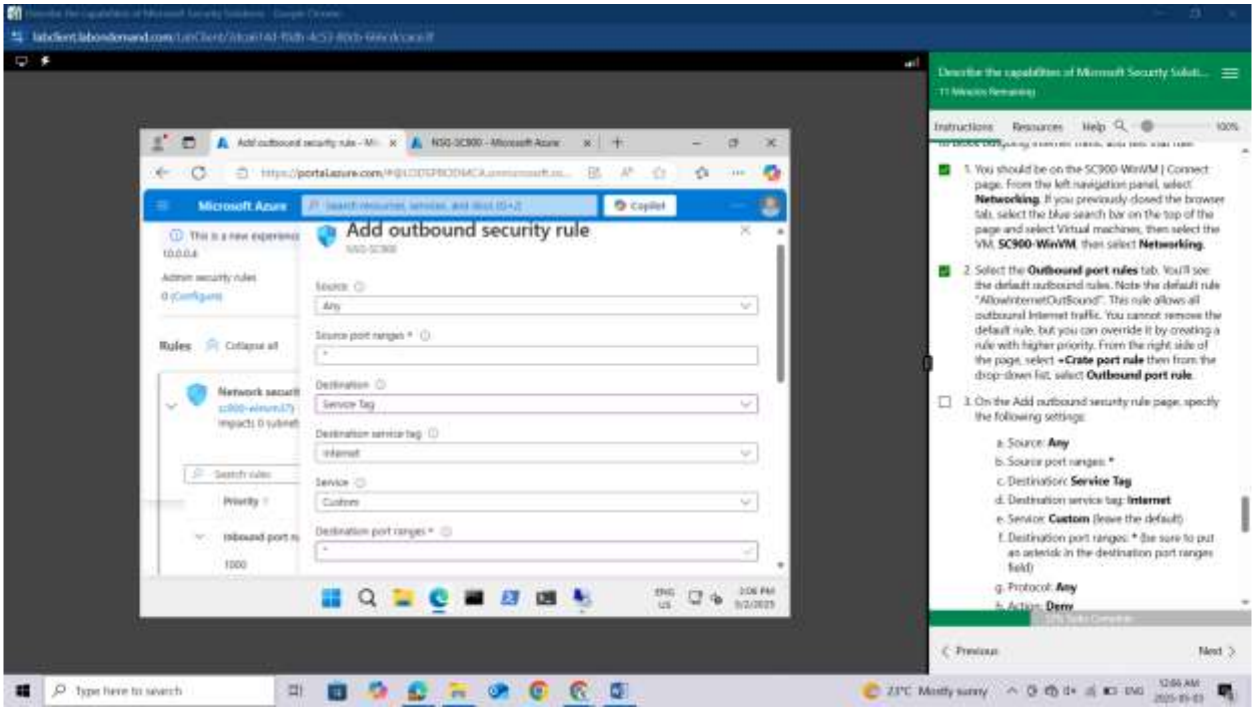
Source port ranges: *****

Destination**: Service Tag**

Destination service tag: **Internet**

Service: **Custom** (leave the default)

Destination port ranges: ***** (be sure to put an asterisk in the destination port ranges field)



Add outbound security rule

NSG-SC900

Source: Any

Source port ranges *: *

Destination: Service Tag

Destination service tag: Internet

Service: Custom

Destination port ranges *: *

Describe the capabilities of Microsoft Security Soluti...

11 Minutes Remaining

☑ 1. You should be on the SC900-WinVM | Connect page. From the left navigation panel, select **Networking**. If you previously closed the browser tab, select the blue search bar on the top of the page and select Virtual machines, then select the VM, **SC900-WinVM**, then select **Networking**.

☑ 2. Select the **Outbound port rules** tab. You'll see the default outbound rules. Note the default rule "AllowInternetOutBound". This rule allows all outbound Internet traffic. You cannot remove the default rule, but you can override it by creating a rule with higher priority. From the right side of the page, select **+Crate port rule** then from the drop-down list, select **Outbound port rule**.

□ 3. On the Add outbound security rule page, specify the following settings:

a. Source: **Any**

b. Source port ranges: *****

c. Destination: **Service Tag**

d. Destination service tag: **Internet**

e. Service: **Custom** (leave the default)

f. Destination port ranges: ***** (be sure to put an asterisk in the destination port ranges field)

g. Protocol: **Any**

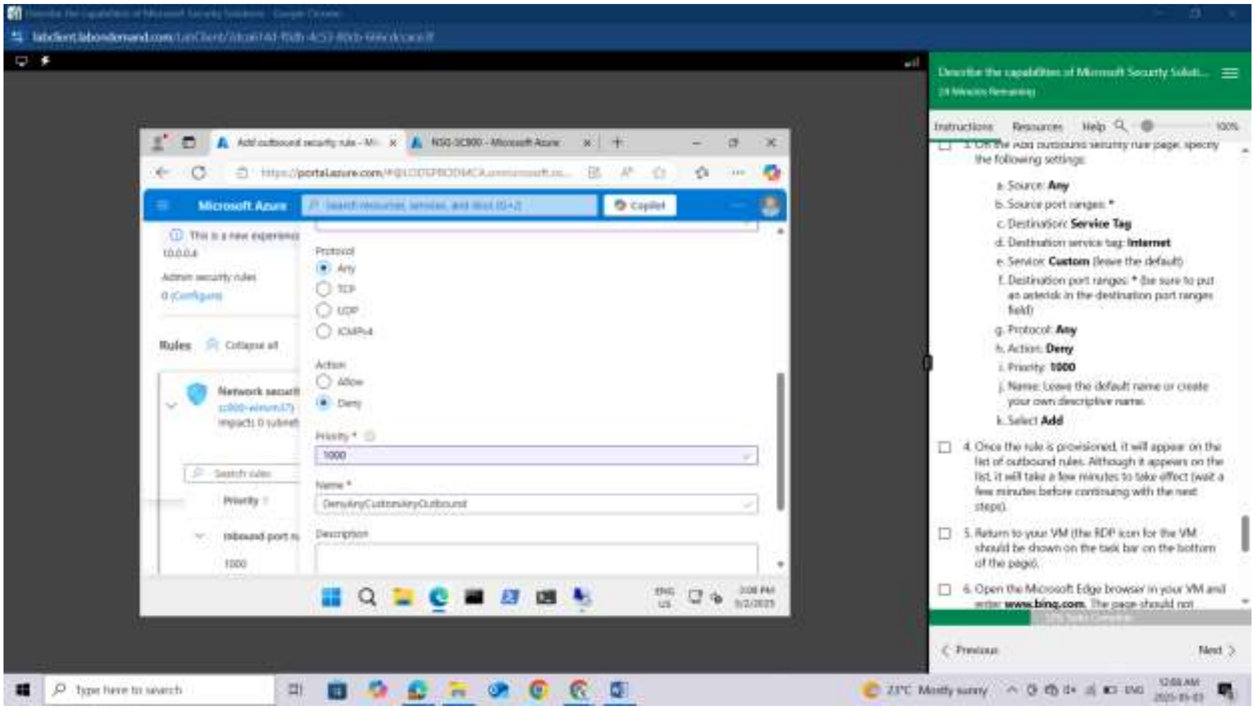
h. Action: **Deny**

Protocol: **Any**

Action: **Deny**

Priority: **1000**

Name: Leave the default name or create your own descriptive name.


Protocol

● Any
○ TCP
○ UDP
○ ICMPv4

Action

○ Allow
● Deny

Priority * : 1000

Name * : DenyAnyCustomAnyOutbound

Description

Describe the capabilities of Microsoft Security Soluti...

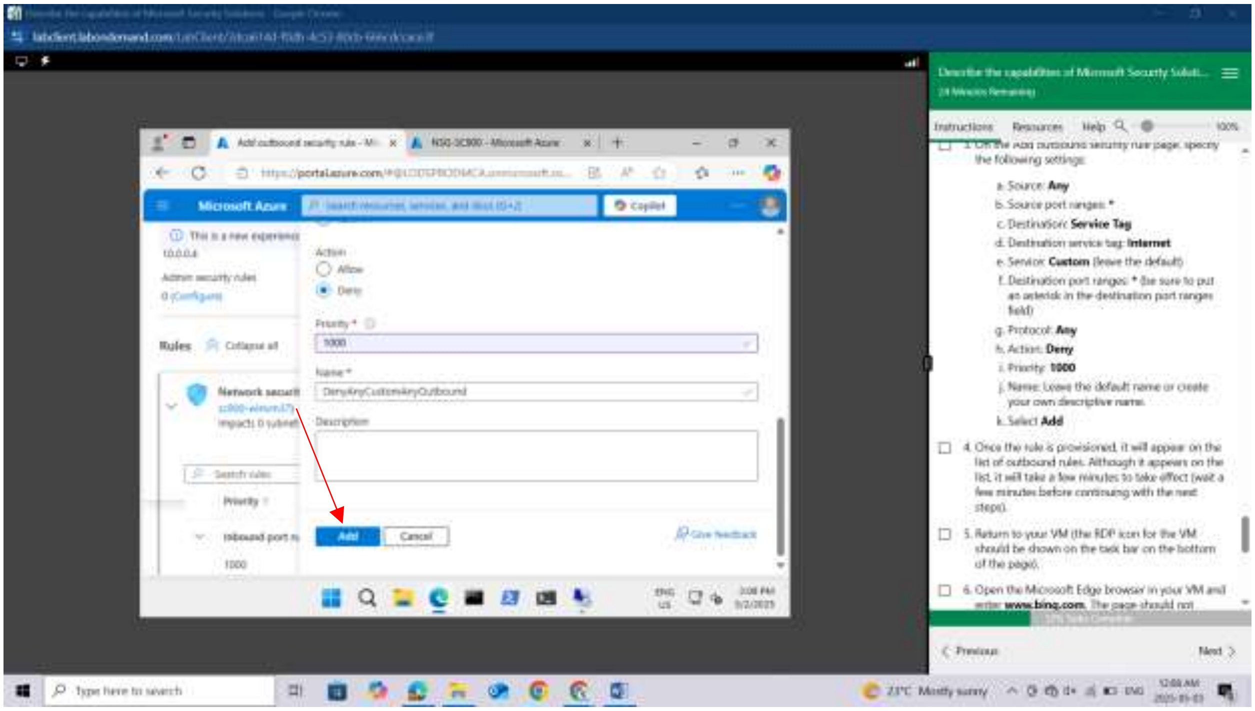
3. On the Add outbound security rule page, specify the following settings:
   a. Source: **Any**
   b. Source port ranges: *
   c. Destination: **Service Tag**
   d. Destination service tag: **Internet**
   e. Service: **Custom** (leave the default)
   f. Destination port ranges: * (be sure to put an asterisk in the destination port ranges field)
   g. Protocol: **Any**
   h. Action: **Deny**
   i. Priority: **1000**
   j. Name: Leave the default name or create your own descriptive name.
   k. Select **Add**

□ 4. Once the rule is provisioned, it will appear on the list of outbound rules. Although it appears on the list, it will take a few minutes to take effect (wait a few minutes before continuing with the next steps).

□ 5. Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).

□ 6. Open the Microsoft Edge browser in your VM and enter **www.bing.com**. The page should not

Select **Add**


Action

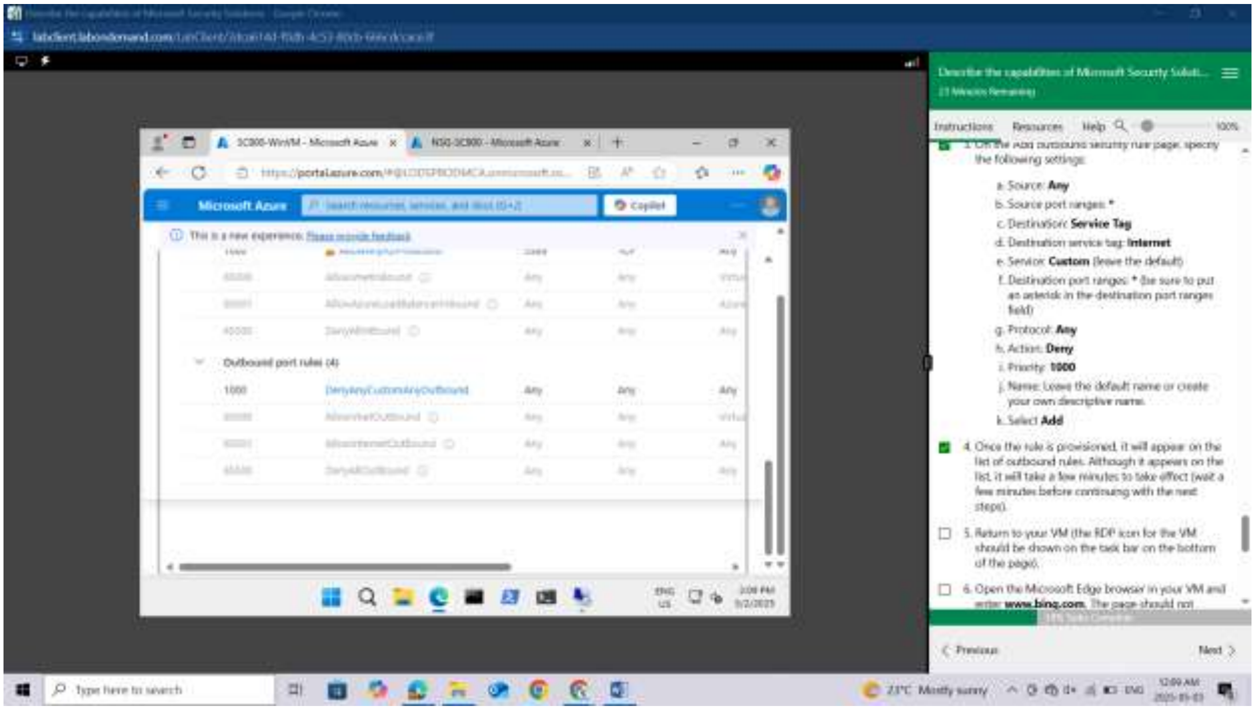
○ Allow
● Deny

Priority * : 1000

Name * : DenyAnyCustomAnyOutbound

Description

Once the rule is provisioned, it will appear on the list of outbound rules. Although it appears on the list, it will take a few minutes to take effect (wait a few minutes before continuing with the next steps).



This is a new experience. Please provide feedback

65000	AllowVnetInBound	Any	Any	Virtual
65001	AllowAzureLoadBalancerInBound	Any	Any	Azure
65500	DenyAllInBound	Any	Any	Any

Outbound port rules (4)

1000	DenyAnyCustomAnyOutbound	Any	Any	Any
65000	AllowVnetOutBound	Any	Any	Virtual
65001	AllowInternetOutBound	Any	Any	Any
65500	DenyAllOutBound	Any	Any	Any

Describe the capabilities of Microsoft Security Soluti...

☑ 3. On the Add outbound security rule page, specify the following settings:

a. Source: **Any**
b. Source port ranges: *
c. Destination: **Service Tag**
d. Destination service tag: **Internet**
e. Service: **Custom** (leave the default)
f. Destination port ranges: * (be sure to put an asterisk in the destination port ranges field)
g. Protocol: **Any**
h. Action: **Deny**
i. Priority: **1000**
j. Name: Leave the default name or create your own descriptive name.
k. Select **Add**

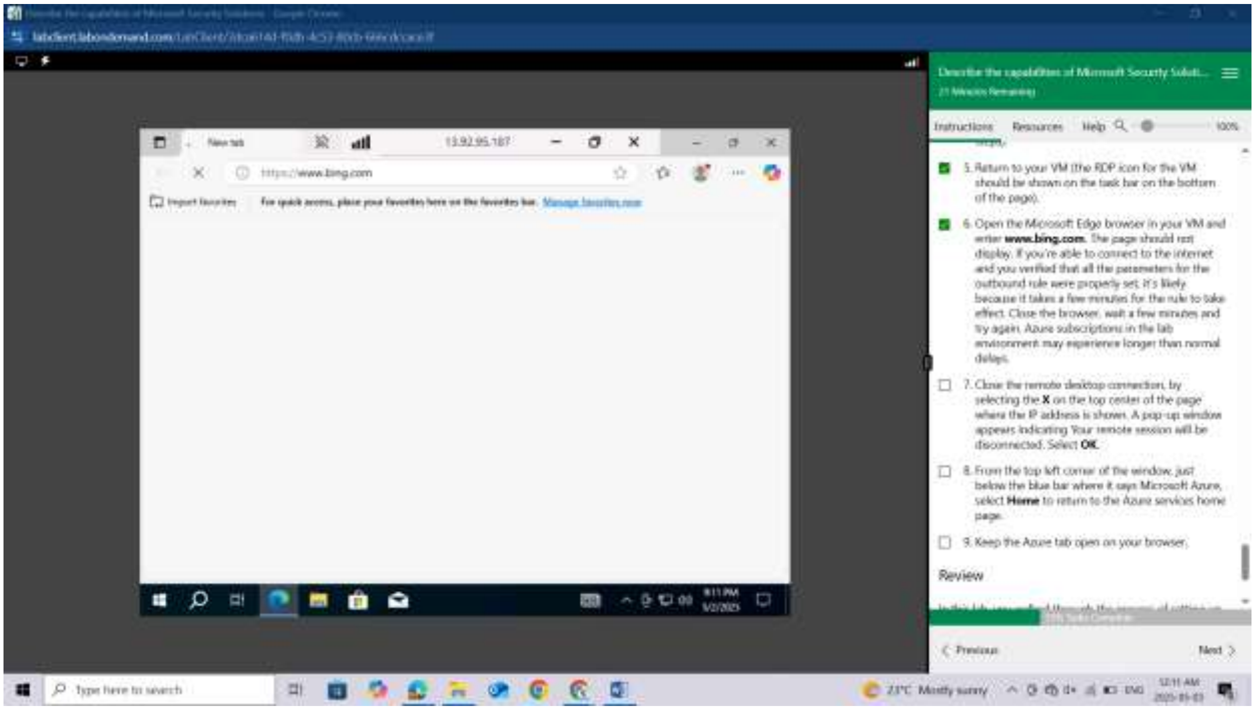
☑ 4. Once the rule is provisioned, it will appear on the list of outbound rules. Although it appears on the list, it will take a few minutes to take effect (wait a few minutes before continuing with the next steps).

☐ 5. Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).

☐ 6. Open the Microsoft Edge browser in your VM and enter **www.bing.com**. The page should not

Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).

Open the Microsoft Edge browser in your VM and enter www.bing.com. The page should not display. If you're able to connect to the internet and you verified that all the parameters for the outbound rule were properly set, it's likely because it takes a few minutes for the rule to take effect. Close the browser, wait a few minutes and try again. Azure subscriptions in the lab environment may experience longer than normal delays.



☑ 5. Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).

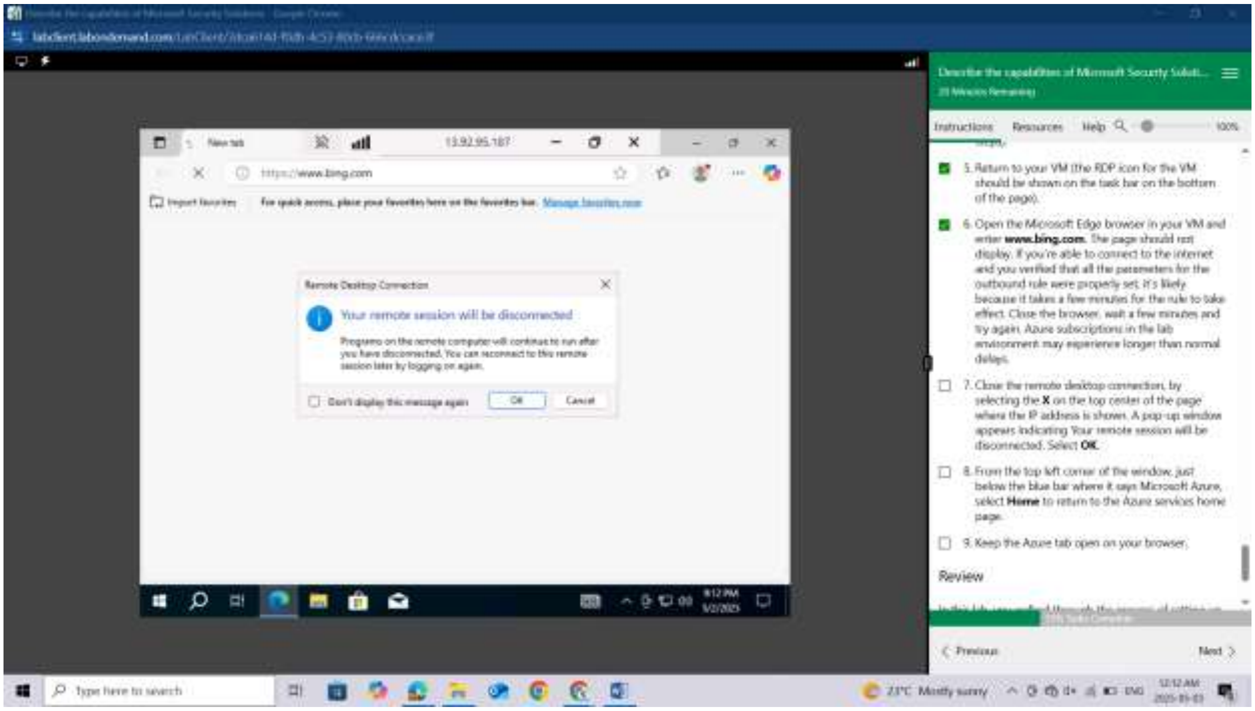
☑ 6. Open the Microsoft Edge browser in your VM and enter **www.bing.com**. The page should not display. If you're able to connect to the internet and you verified that all the parameters for the outbound rule were properly set, it's likely because it takes a few minutes for the rule to take effect. Close the browser, wait a few minutes and try again. Azure subscriptions in the lab environment may experience longer than normal delays.

☐ 7. Close the remote desktop connection, by selecting the **X** on the top center of the page where the IP address is shown. A pop-up window appears indicating Your remote session will be disconnected. Select **OK**.

☐ 8. From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.

☐ 9. Keep the Azure tab open on your browser.

Close the remote desktop connection, by selecting the **X** on the top center of the page where the IP address is shown. A pop-up window appears indicating Your remote session will be disconnected. Select **OK**.



Your remote session will be disconnected

Programs on the remote computer will continue to run after you have disconnected. You can reconnect to this remote session later by logging on again.

☐ Don't display this message again

☑ 5. Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).

☑ 6. Open the Microsoft Edge browser in your VM and enter **www.bing.com**. The page should not display. If you're able to connect to the internet and you verified that all the parameters for the outbound rule were properly set, it's likely because it takes a few minutes for the rule to take effect. Close the browser, wait a few minutes and try again. Azure subscriptions in the lab environment may experience longer than normal delays.

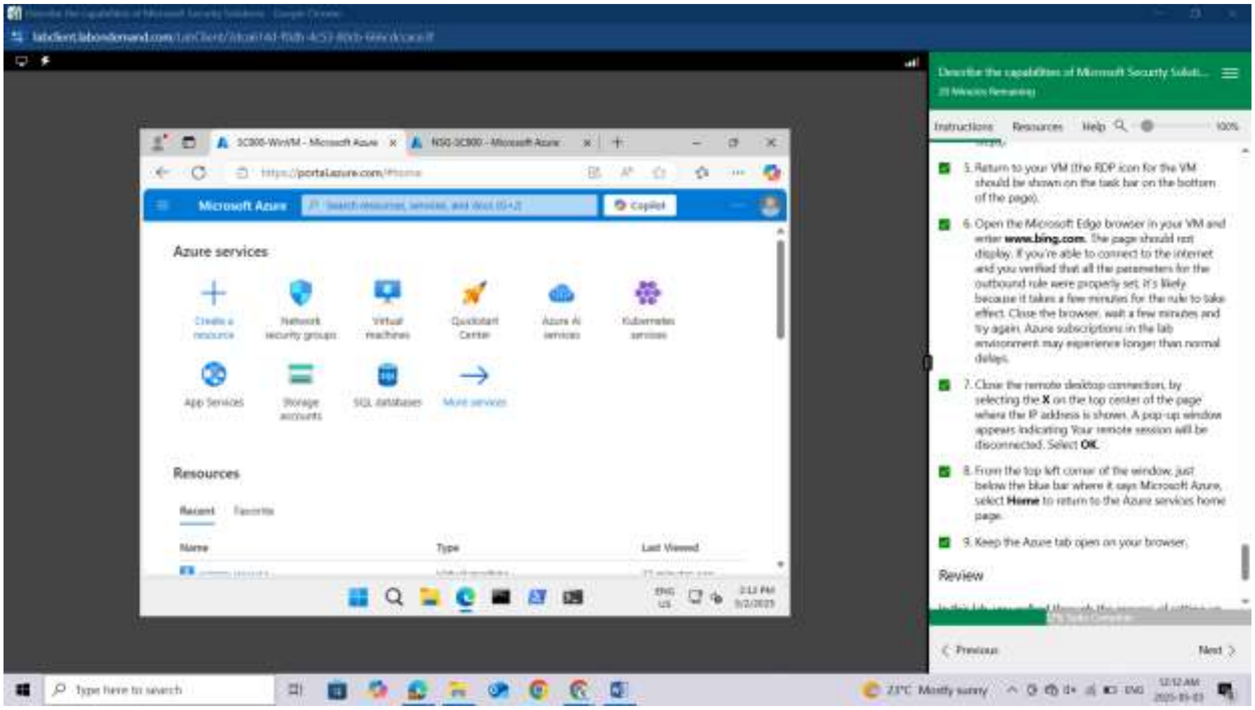
☐ 7. Close the remote desktop connection, by selecting the **X** on the top center of the page where the IP address is shown. A pop-up window appears indicating Your remote session will be disconnected. Select **OK**.

☐ 8. From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.

☐ 9. Keep the Azure tab open on your browser.

From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.

Keep the Azure tab open on your browser.



- ☑ 5. Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).
- ☑ 6. Open the Microsoft Edge browser in your VM and enter **www.bing.com**. The page should not display. If you're able to connect to the internet and you verified that all the parameters for the outbound rule were properly set, it's likely because it takes a few minutes for the rule to take effect. Close the browser, wait a few minutes and try again. Azure subscriptions in the lab environment may experience longer than normal delays.
- ☑ 7. Close the remote desktop connection, by selecting the **X** on the top center of the page where the IP address is shown. A pop-up window appears indicating Your remote session will be disconnected. Select **OK**.
- ☑ 8. From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.
- ☑ 9. Keep the Azure tab open on your browser.

Review

Review

In this lab, you walked through the process of setting up a network security group (NSG), associating that NSG to the network interface of a virtual machine, and adding new rules to the NSG to allow inbound RDP traffic and to block outbound Internet traffic.