

# Windows Server Security

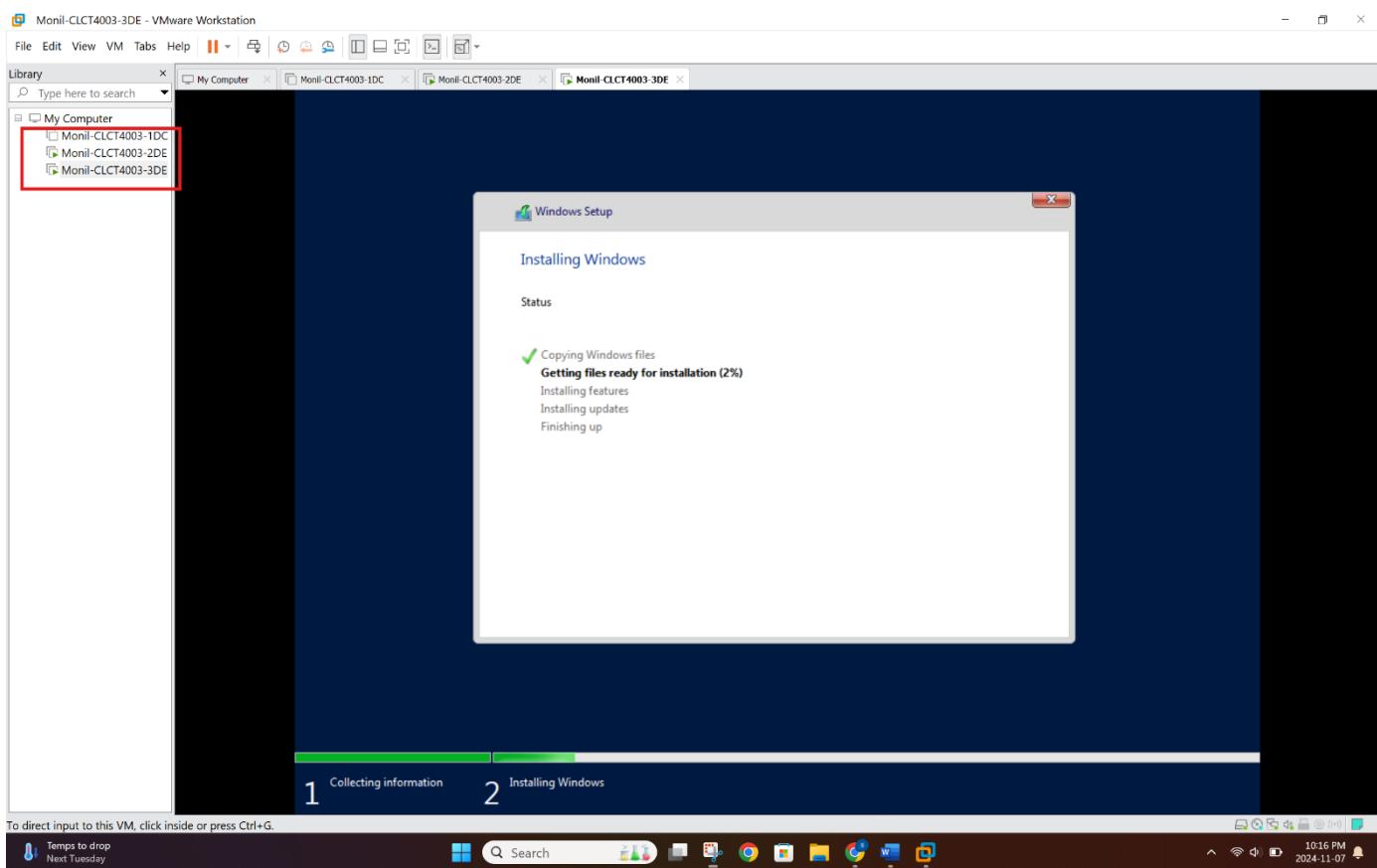
## Case Project

### Scenario

Contoso Pharmaceuticals is a medical research company with about 5,000 employees worldwide. They have specific needs for ensuring that medical records and data remain private. The company has a headquarters location and multiple worldwide sites. Contoso has recently deployed a Windows Server and Windows client infrastructure. You have been asked to Complete tasks below

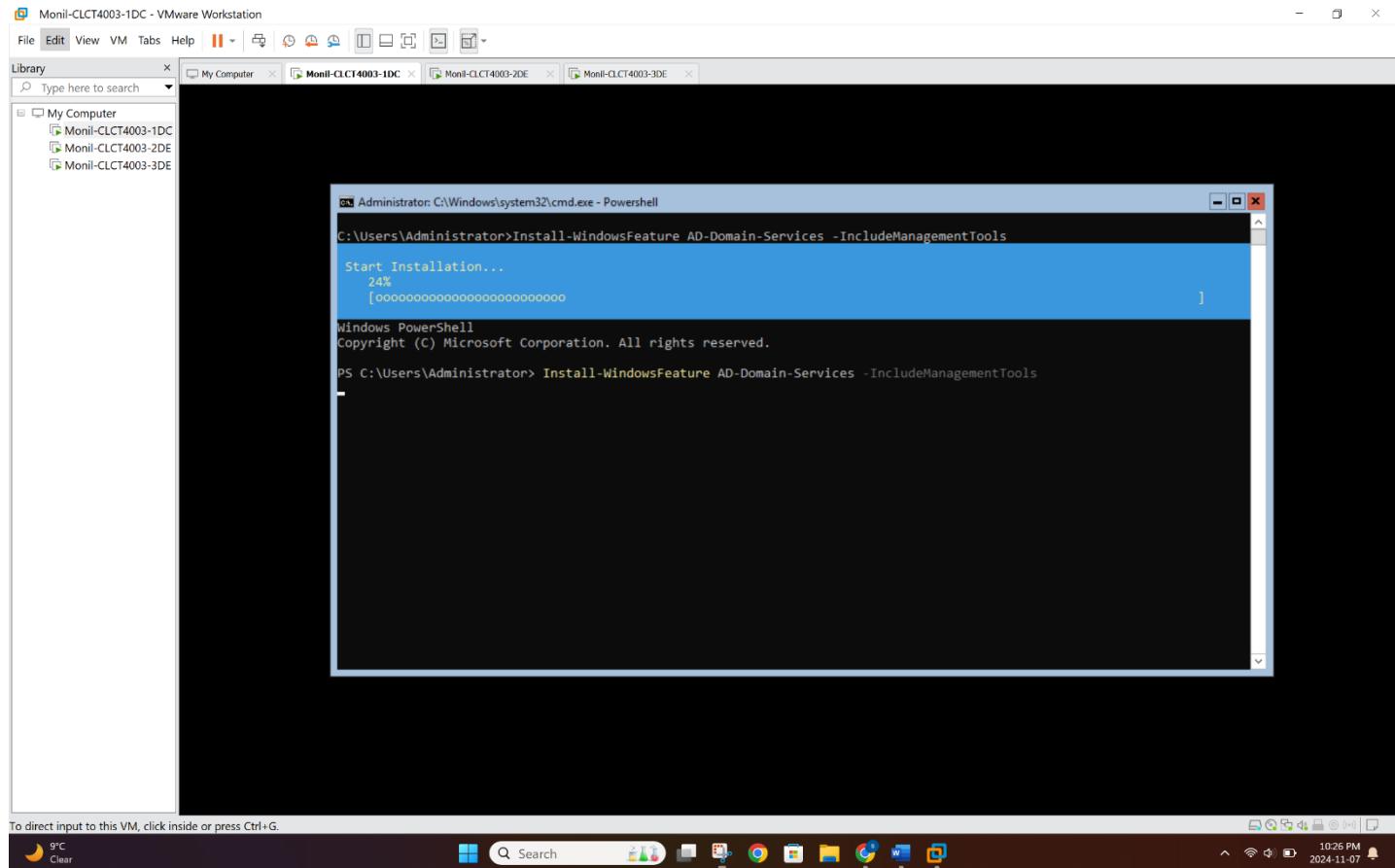
### Objectives

- 1) Install a domain called yourname.local on Server core.



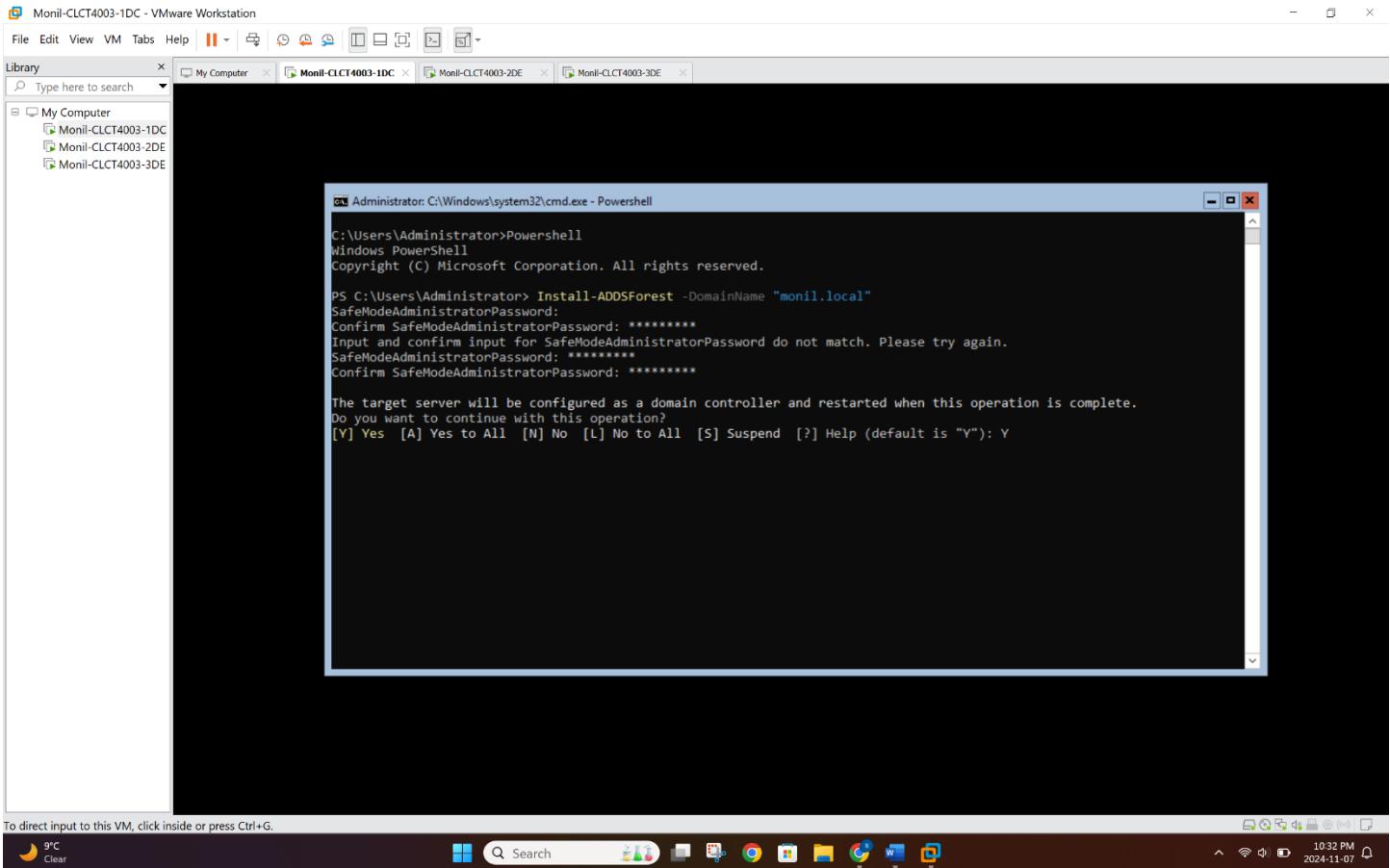
*SS-1: Installed three VMs. First one is server core and other two are datacenter evaluation with desktop experience.*

# Windows Server Security



SS-2: Installing AD DS on Server Core (First VM)

# Windows Server Security



*SS-3: Promoting VM1 as Domain controller, after restart its promoted!*

# Windows Server Security

- 2) Configure Group Policy and enforce password change to 30 days

The screenshot shows a Windows Server desktop environment. A VMware Workstation window titled "Monil-CLCT4003-1DC - VMware Workstation" is open. Inside, there are three tabs: "My Computer", "Monil-CLCT4003-1DC", and "Monil-CLCT4003-2DE". The "Monil-CLCT4003-1DC" tab is active and contains a PowerShell window. The PowerShell session is run as Administrator and shows the following commands:

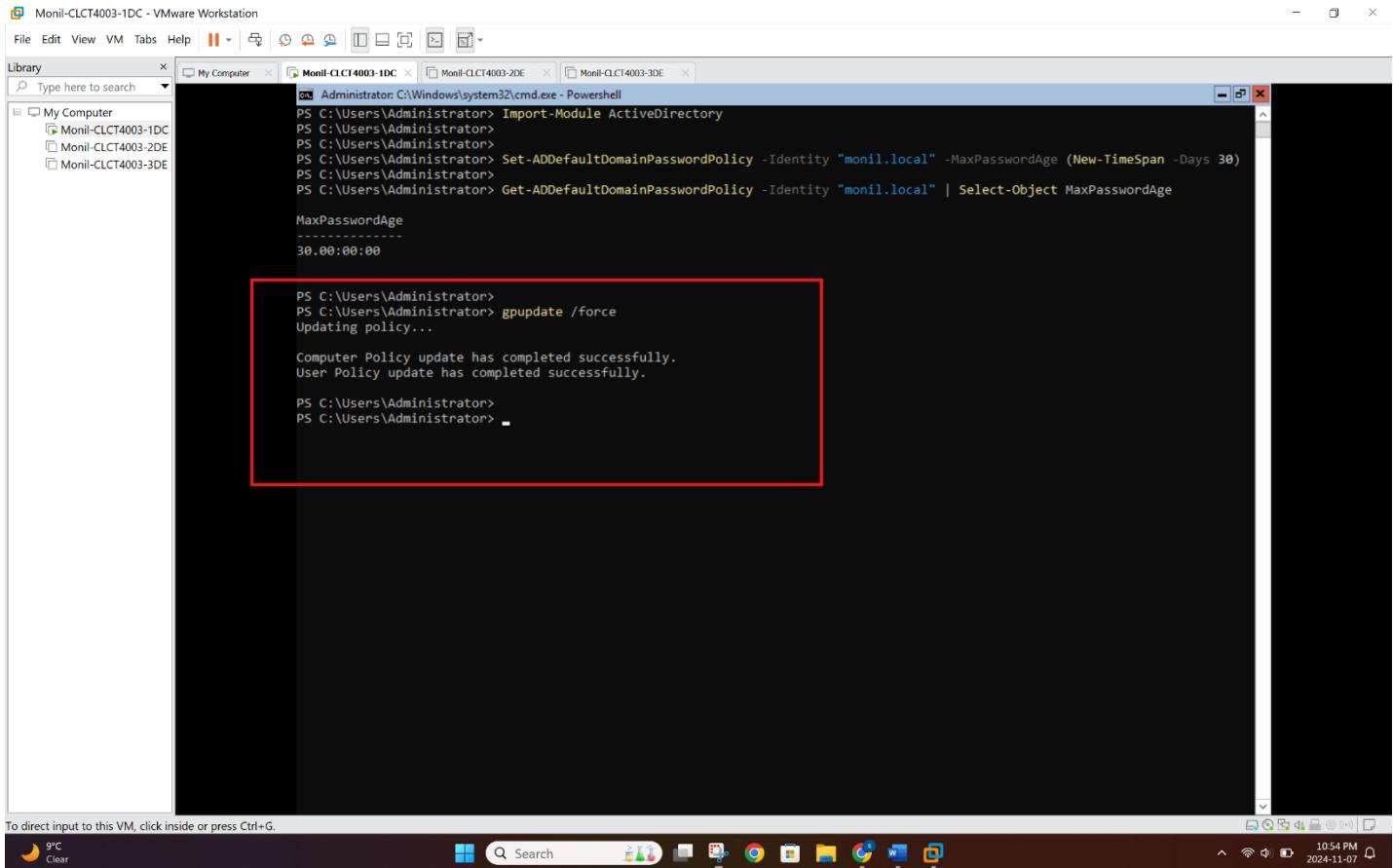
```
PS C:\Users\Administrator> Import-Module ActiveDirectory
PS C:\Users\Administrator>
PS C:\Users\Administrator> Set-ADDefaultDomainPasswordPolicy -Identity "monil.local" -MaxPasswordAge (New-TimeSpan -Days 30)
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy -Identity "monil.local" | Select-Object MaxPasswordAge
MaxPasswordAge
-----
30.00:00:00

PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

The taskbar at the bottom of the screen shows various icons for system monitoring and connectivity.

*SS-4: Enforcing to change the password to 30 days via PowerShell and confirming it!*

# Windows Server Security



The screenshot shows a Windows Server 2022 desktop environment with a VMware Workstation window titled "Monil-CLCT4003-1DC - VMware Workstation". Inside the window, there is a "My Computer" library view and a PowerShell window titled "Administrator: C:\Windows\system32\cmd.exe - Powershell". The PowerShell session contains the following commands:

```
PS C:\Users\Administrator> Import-Module ActiveDirectory
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Set-ADDefaultDomainPasswordPolicy -Identity "monil.local" -MaxPasswordAge (New-TimeSpan -Days 30)
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy -Identity "monil.local" | Select-Object MaxPasswordAge
MaxPasswordAge
-----
30.00:00:00

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

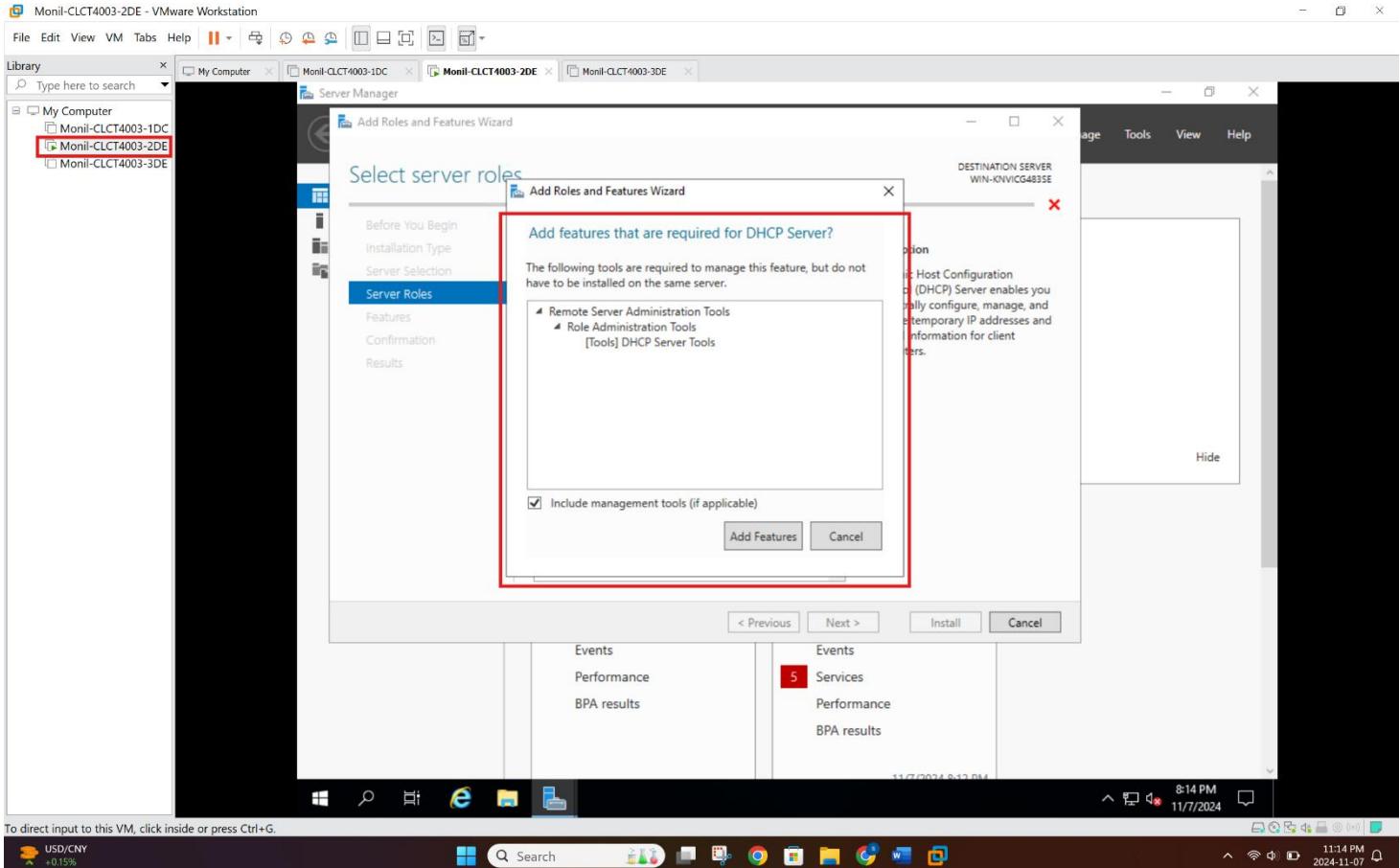
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

A red box highlights the output of the `gpupdate /force` command, which shows the successful update of both computer and user policies.

*SS-5: Forcing the password change setting in group policy via cmdlet!*

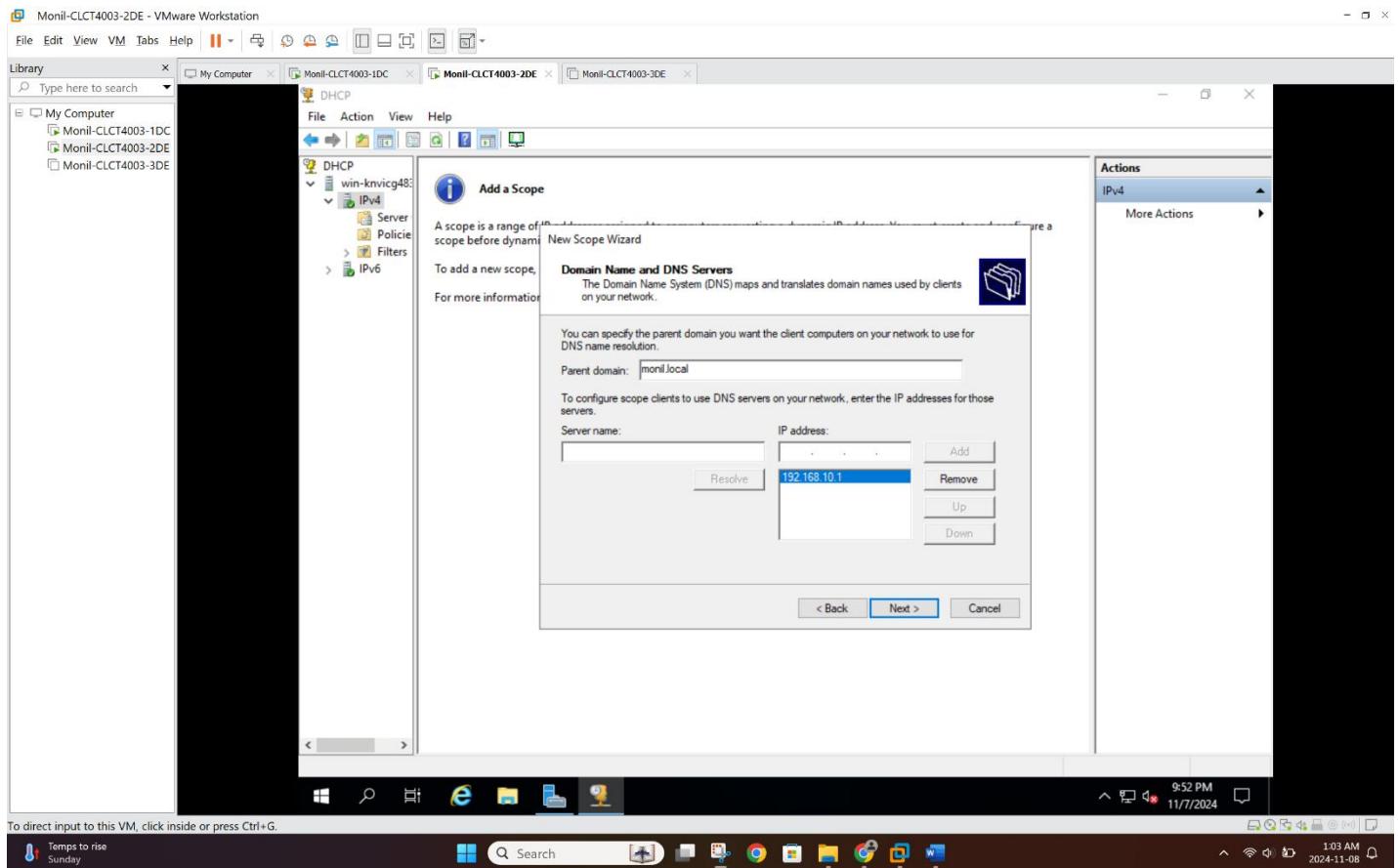
- 3) Install DHCP server,
  - a) Create 4 scopes named yourname-TorontoLab, Yourname-TorontoOffice, Yourname-MontrealLab, yourname-montrealOffice (use any ip range you like)
  - b) Create 1 Superscope for Montreal (yourname-Superscope)
  - c) Create 1 Multicast scope (yourname Multicast scope)
  - d) Create a reservation
  - e) Configure options

# Windows Server Security



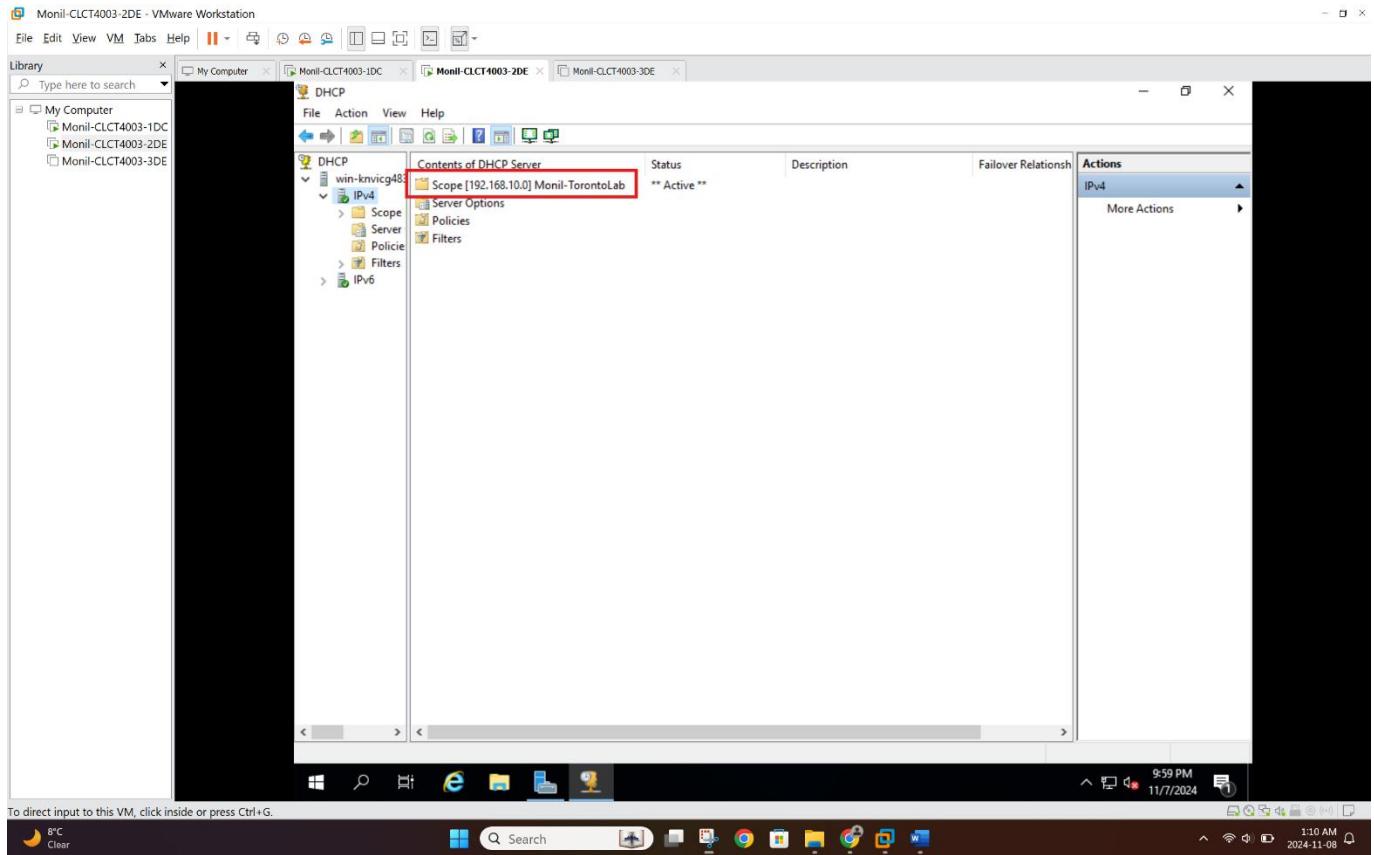
SS-6: Installing DHCP role on VM2 (Monil-CLCT4003-2DE)

# Windows Server Security



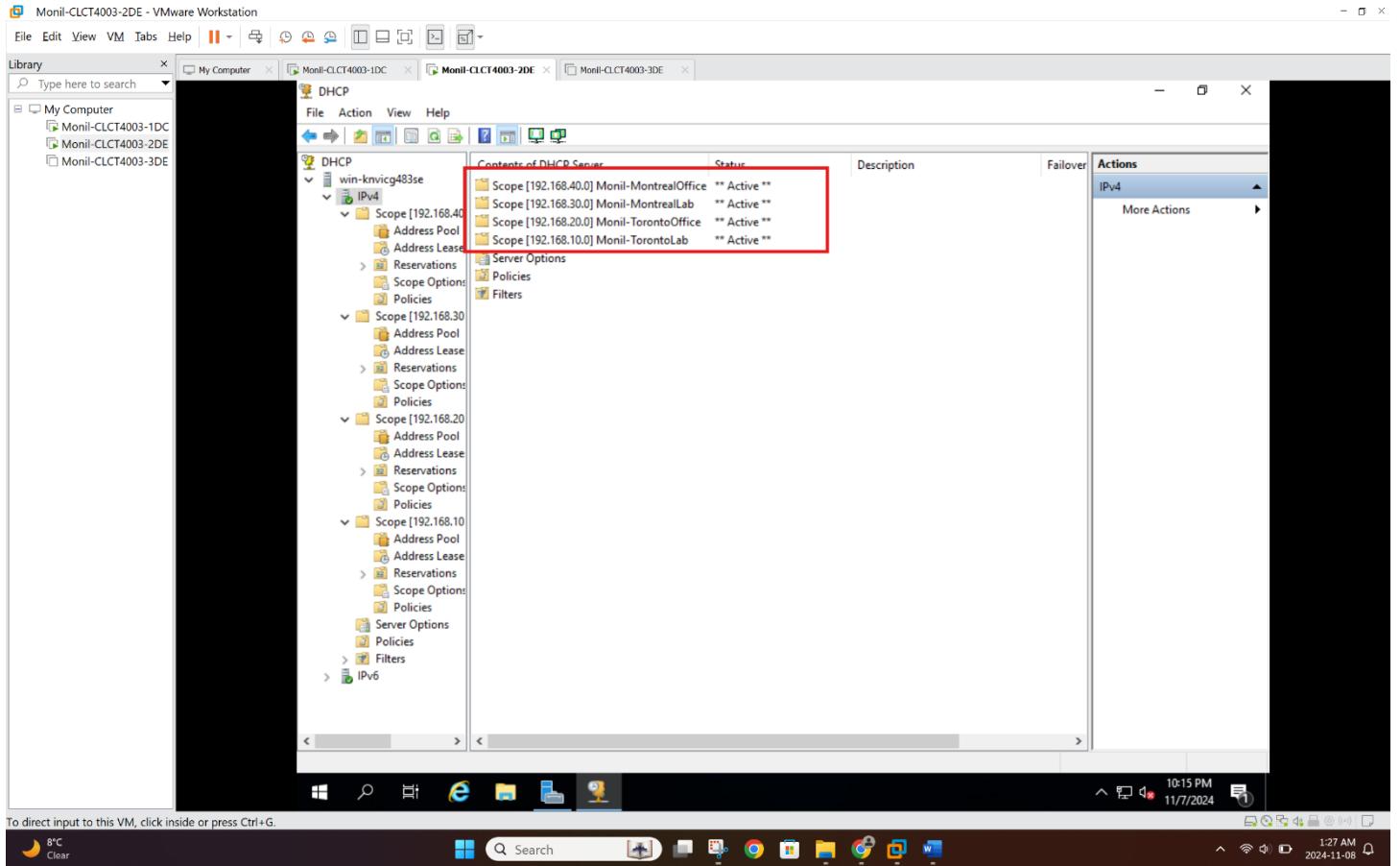
SS-7: Adding New scope in DHCP IPV4

# Windows Server Security



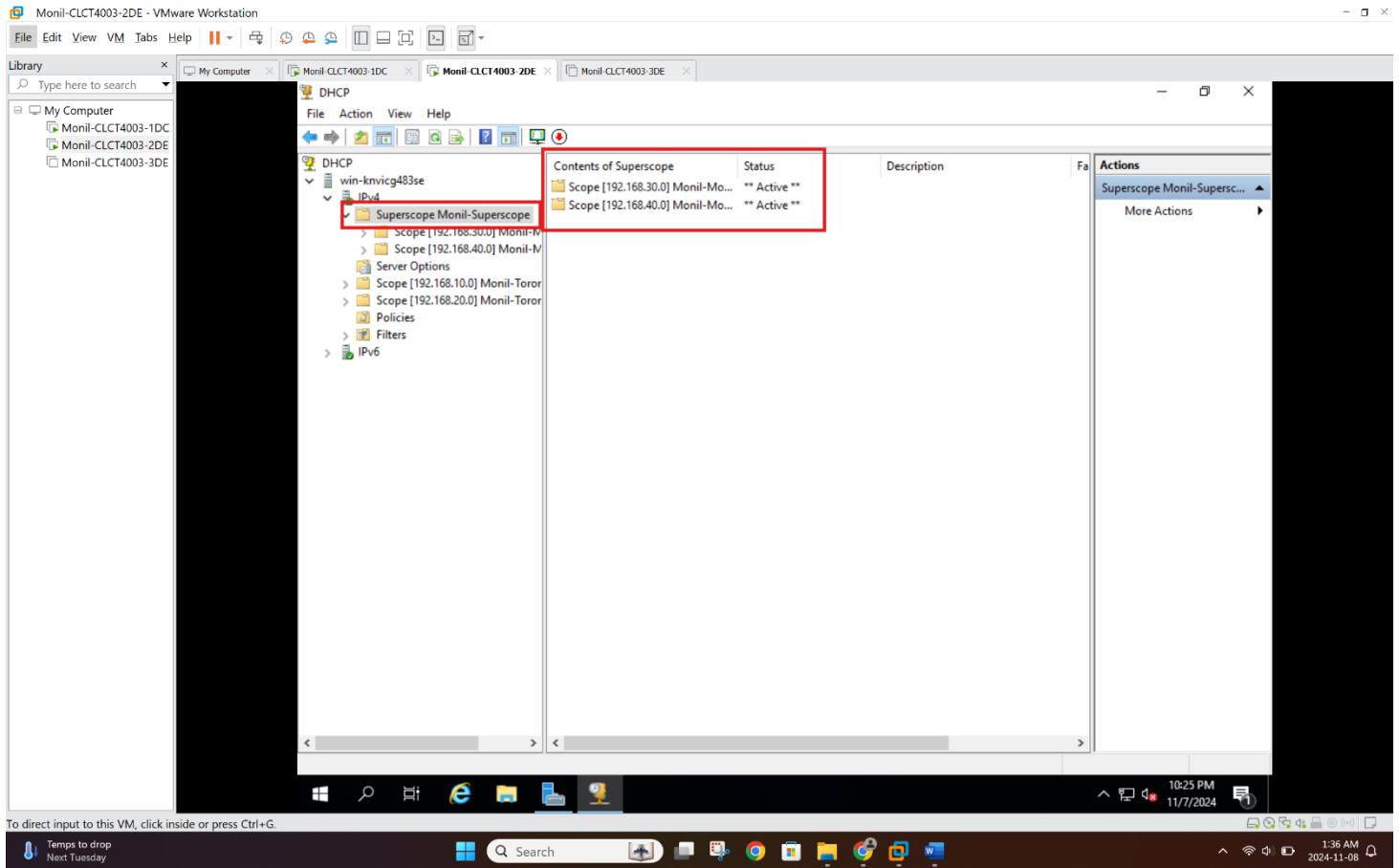
SS-8: We can see that 1 new scope named as “Monil-TorontoLab” is created. Let’s create another 3 Scopes using the same method!

# Windows Server Security



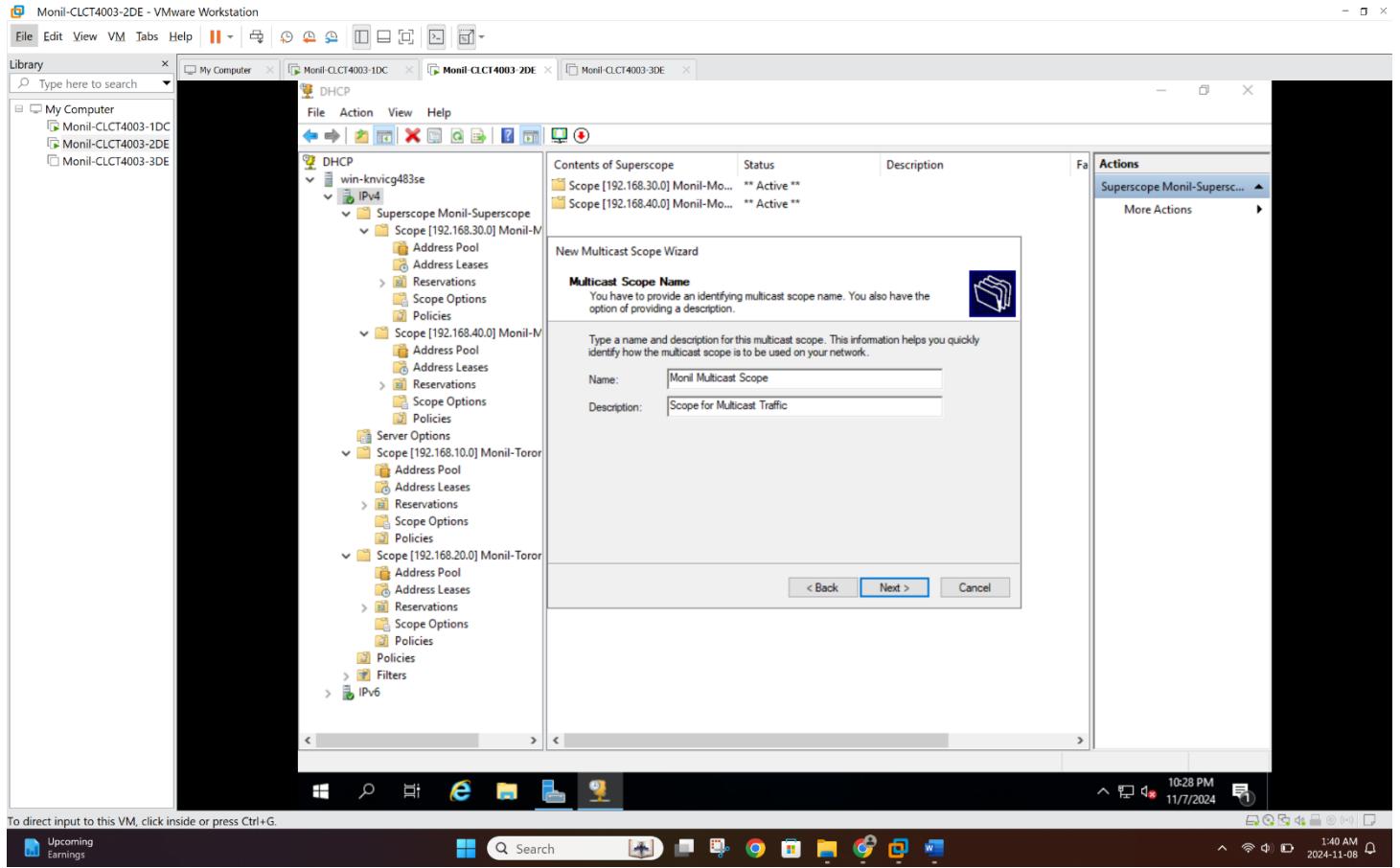
SS-9: As per the requirements, 4 scopes are now created!

# Windows Server Security



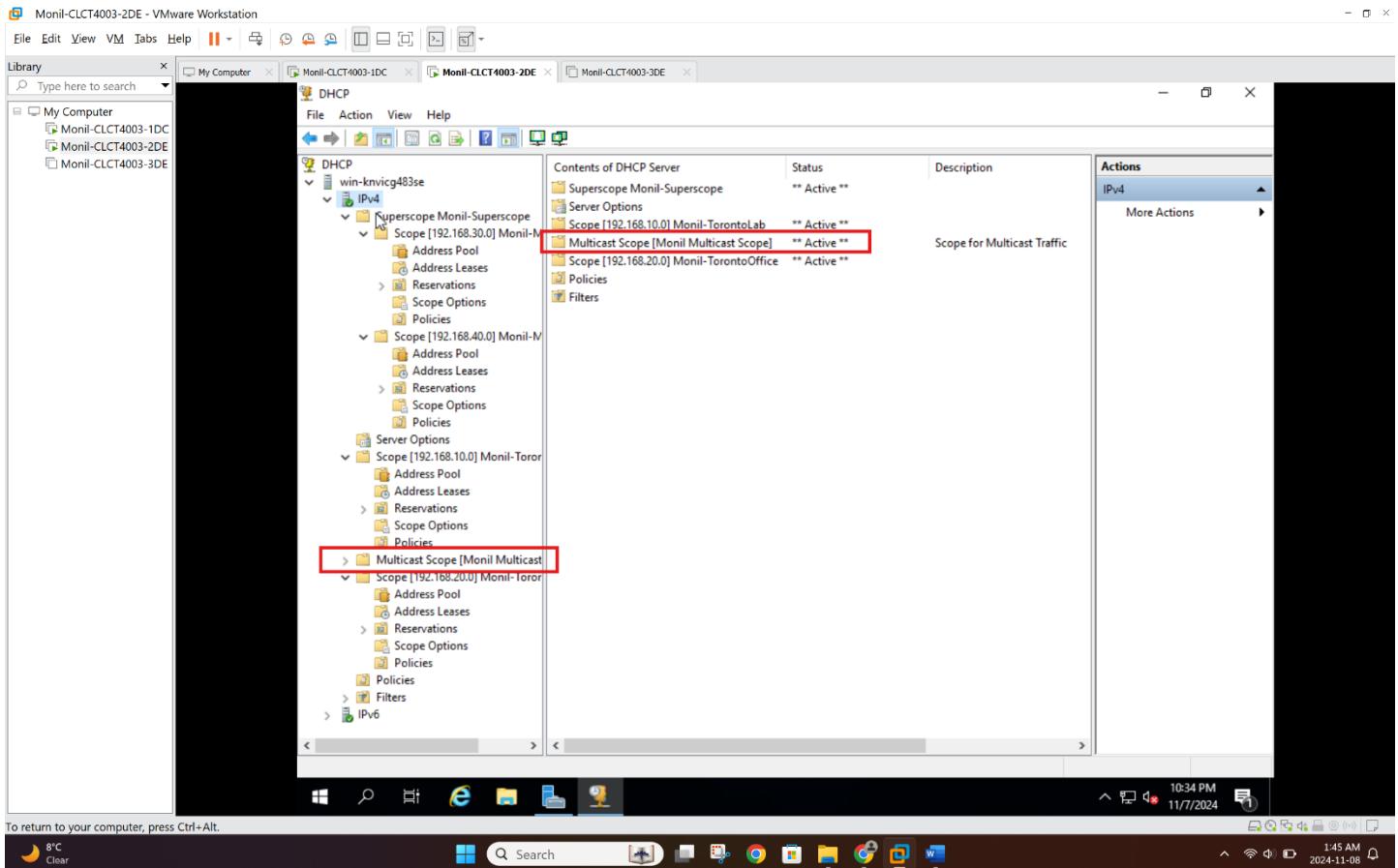
SS-10: New Superscope is created named as “Monil-Superscope” which includes “Monil-MontrealLab” and “Monil-MontrealOffice” scopes!

# Windows Server Security



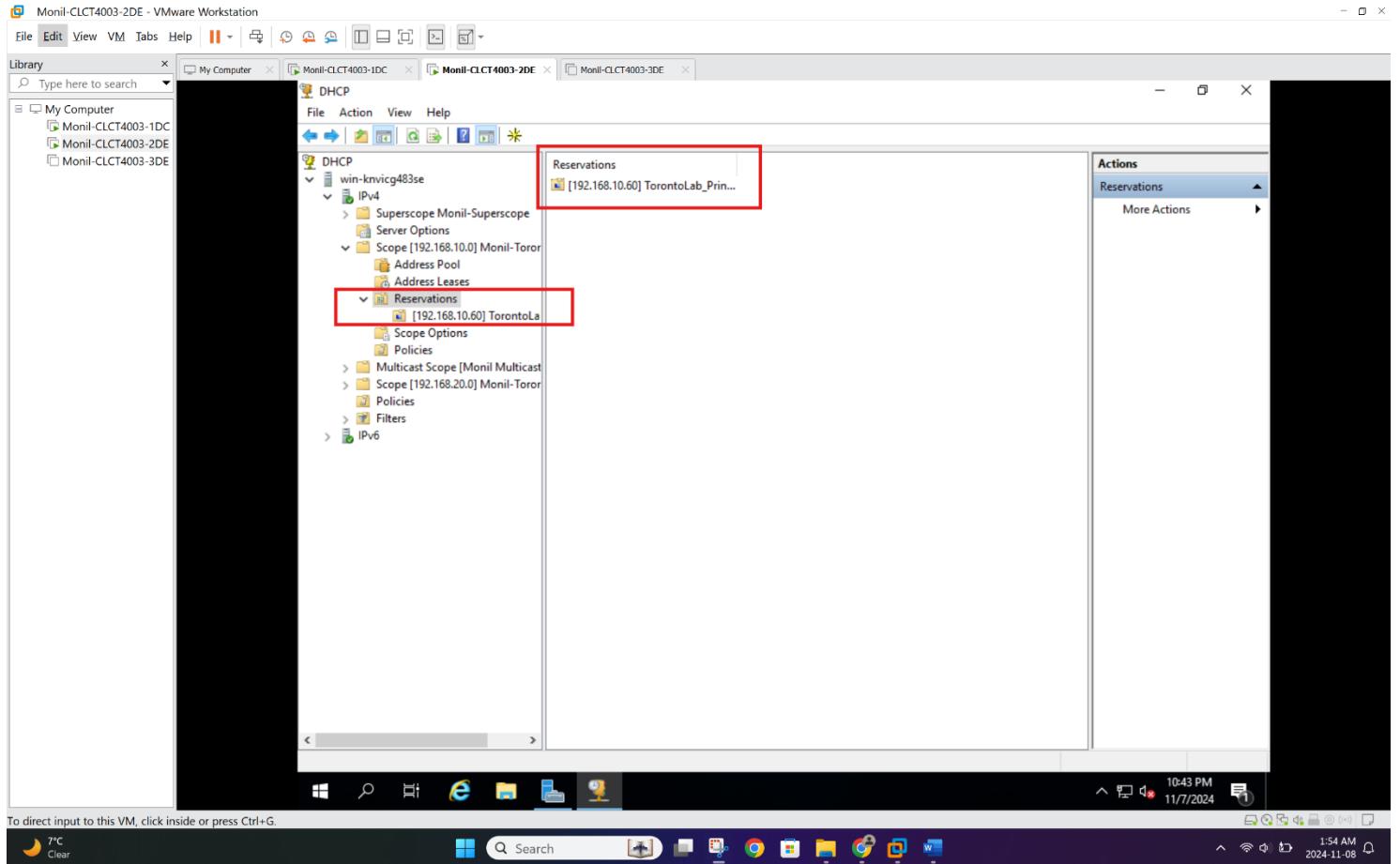
SS-11: Creating The Multitask scope

# Windows Server Security



SS-12: Monil Multicast Scope is now created!

# Windows Server Security

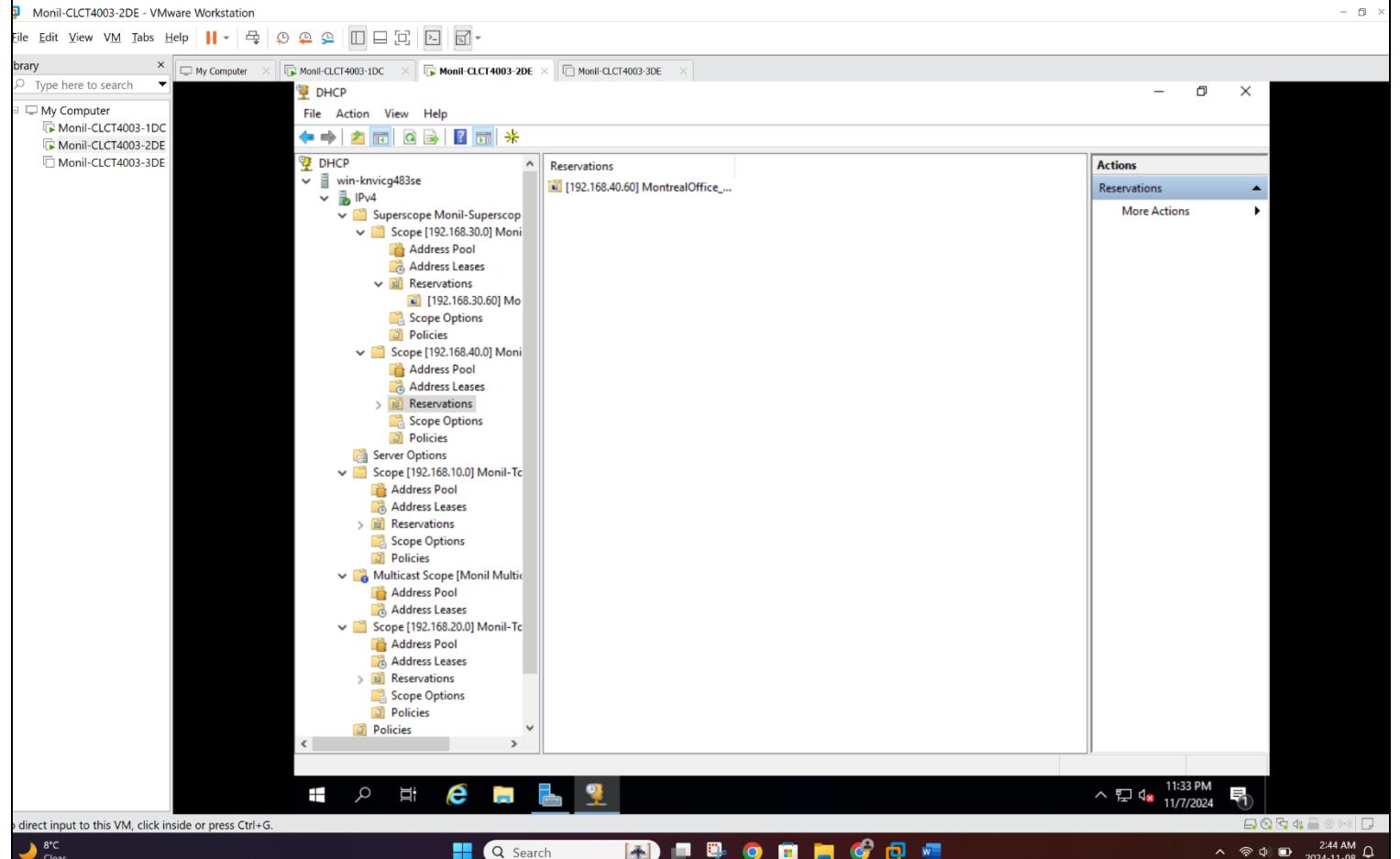


To direct input to this VM, click inside or press Ctrl+G.

7°C Clear 10:43 PM 11/7/2024 1:54 AM 2024-11-08

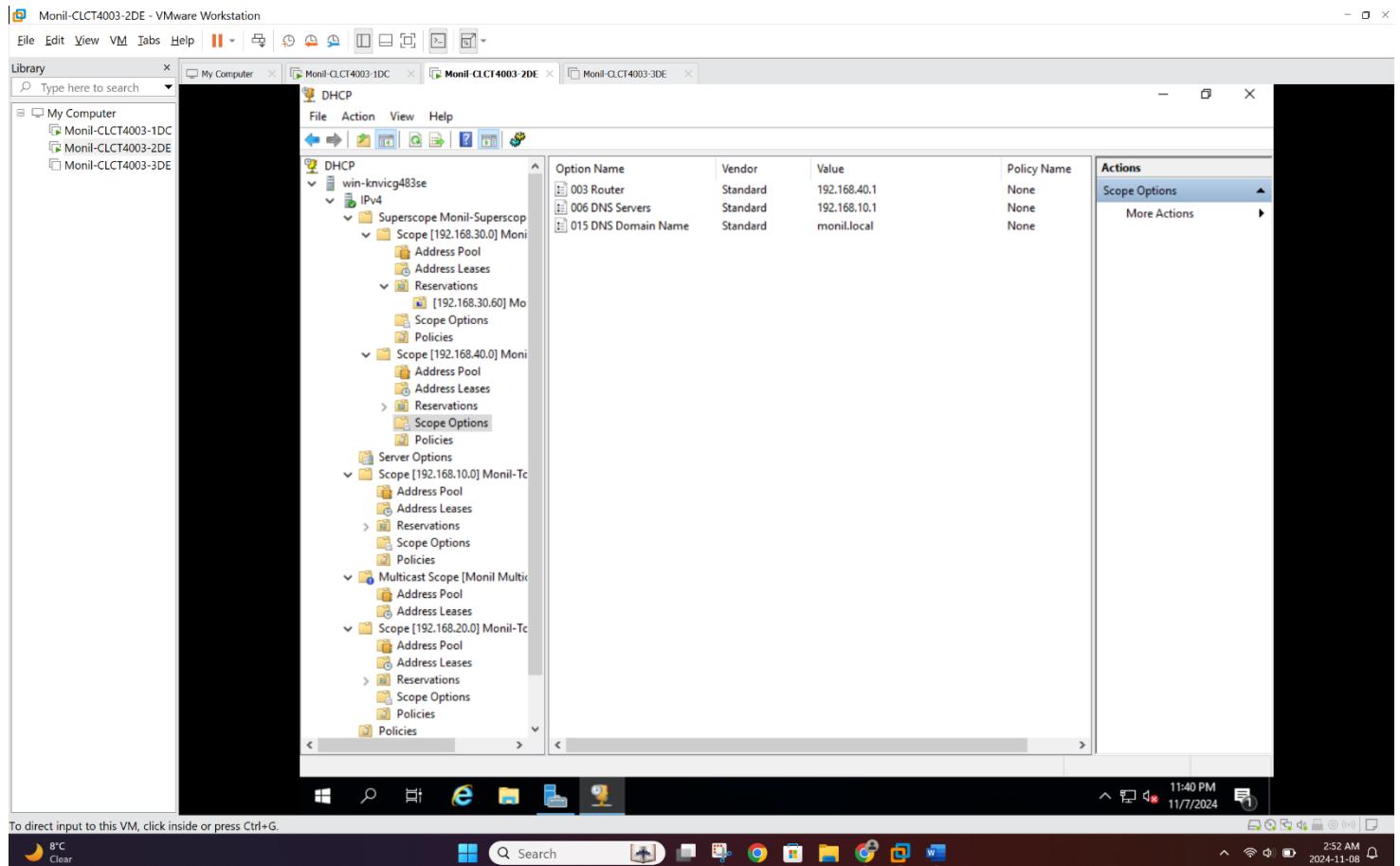
SS-13: Created the reservation for Monil-TorontoLab

# Windows Server Security



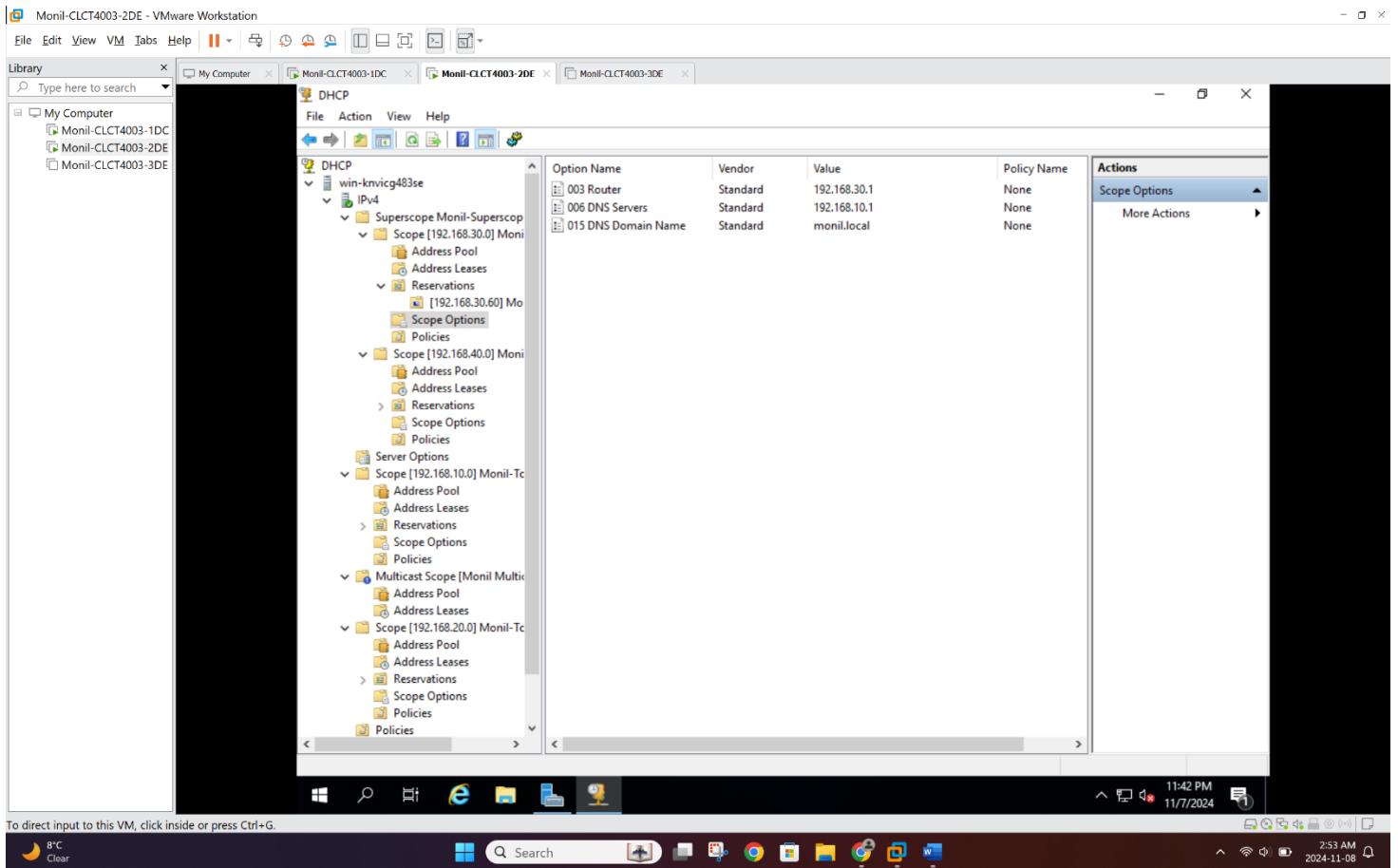
SS-14: Created reservations for other three scopes!

# Windows Server Security



SS-15: Configuring Scope options for Monil-MontrealOffice!

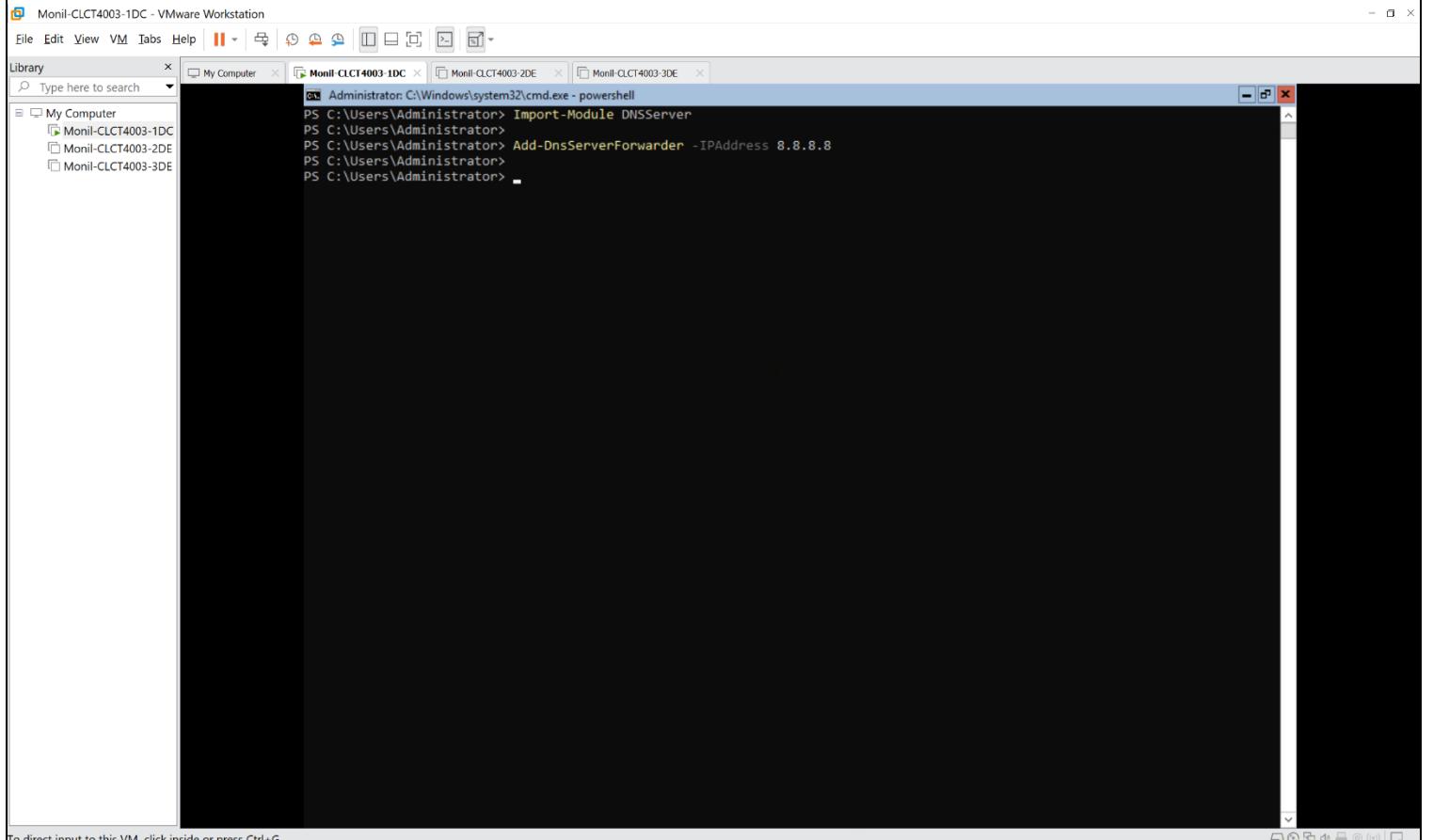
# Windows Server Security



SS-16: Configuring Scope options for Monil-MontrealLab and other two scopes accordingly!

# Windows Server Security

- 4) On your domain DNS Server, create forwarder and forward all requests to 8.8.8.8

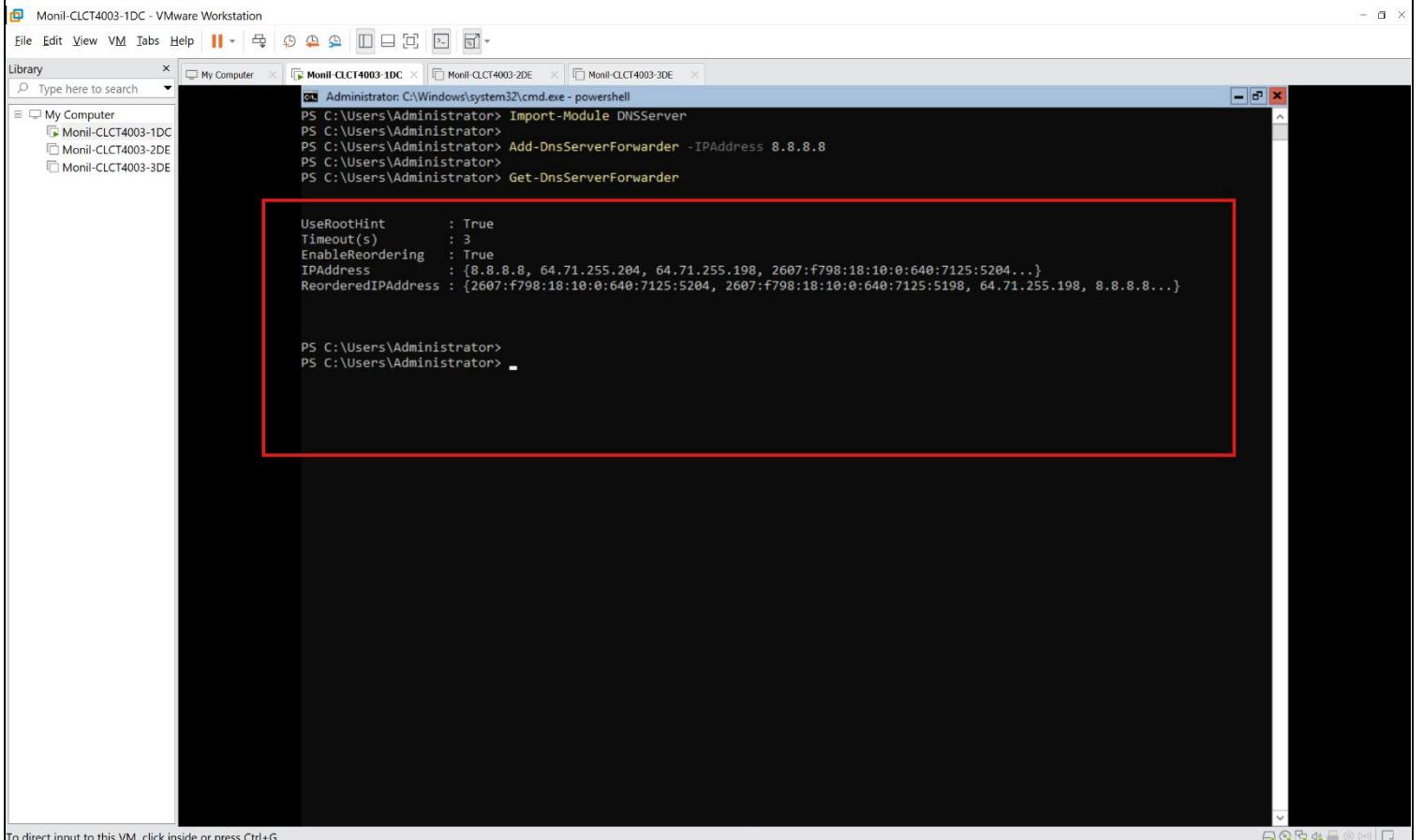


```
Administrator: C:\Windows\System32\cmd.exe - powershell
PS C:\Users\Administrator> Import-Module DNSServer
PS C:\Users\Administrator> PS C:\Users\Administrator> Add-DnsServerForwarder -IPAddress 8.8.8.8
PS C:\Users\Administrator> PS C:\Users\Administrator>
```

To direct input to this VM, click inside or press Ctrl+G.

*SS-17: Importing DNS module and add DNS forwarder to forward all requests to 8.8.8.8 via powershell!*

# Windows Server Security



The screenshot shows a VMware Workstation interface with three tabs open: "Monil-CLCT4003-1DC", "Monil-CLCT4003-2DE", and "Monil-CLCT4003-3DE". The "Monil-CLCT4003-1DC" tab is active and displays a PowerShell window. The command history is as follows:

```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrator> Import-Module DnsServer
PS C:\Users\Administrator> PS C:\Users\Administrator> Add-DnsServerForwarder -IPAddress 8.8.8.8
PS C:\Users\Administrator> PS C:\Users\Administrator> Get-DnsServerForwarder

UseRootHint      : True
Timeout(s)       : 3
EnableReordering  : True
IPAddress        : {8.8.8.8, 64.71.255.204, 64.71.255.198, 2607:f798:18:10:0:640:7125:5204...}
ReorderedIPAddress : {2607:f798:18:10:0:640:7125:5204, 2607:f798:18:10:0:640:7125:5198, 64.71.255.198, 8.8.8.8...}

PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

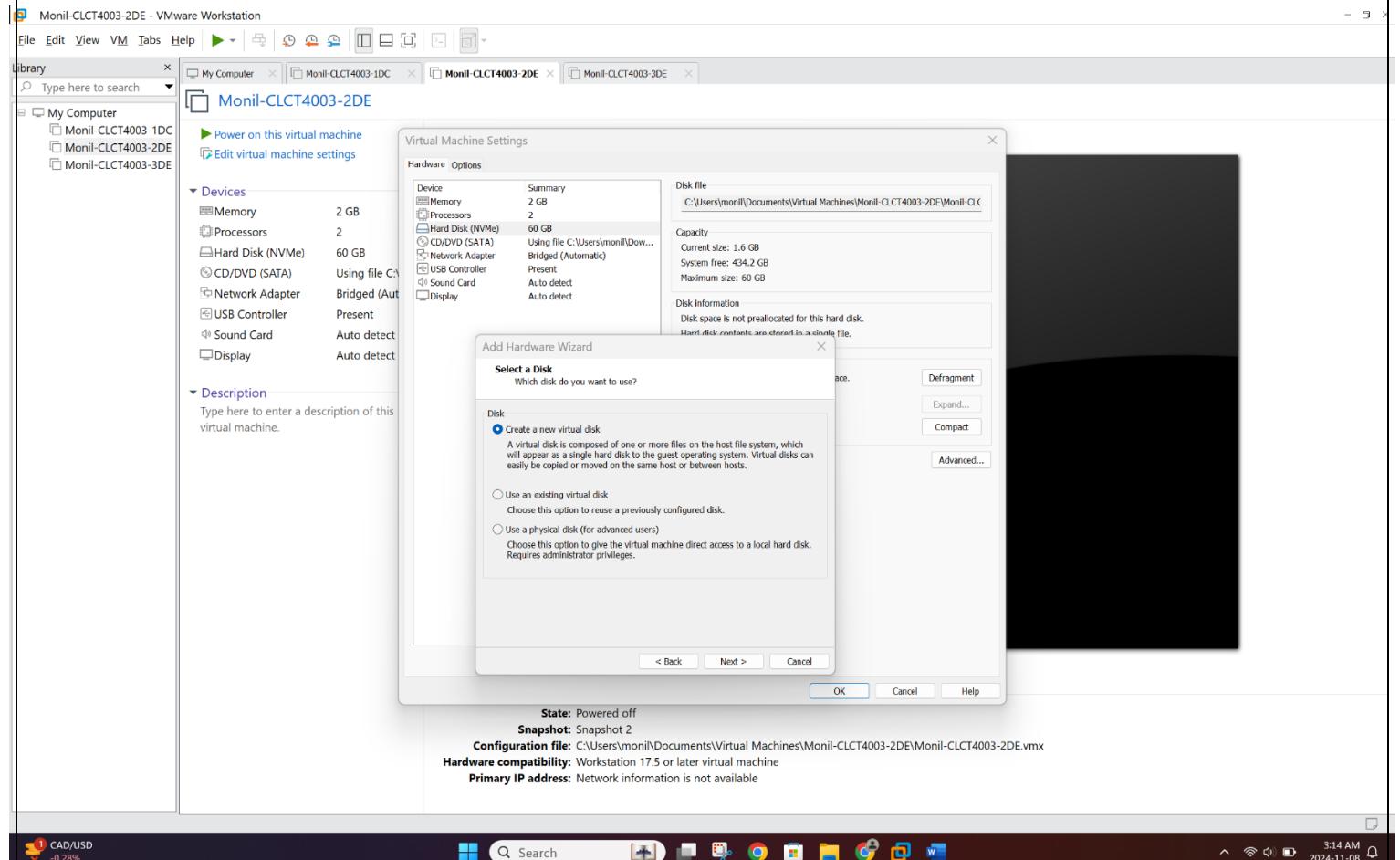
To direct input to this VM, click inside or press Ctrl+G.



*SS-18: Verifying the forwarder verifies that all requests are now being forwarded to 8.8.8.8!*

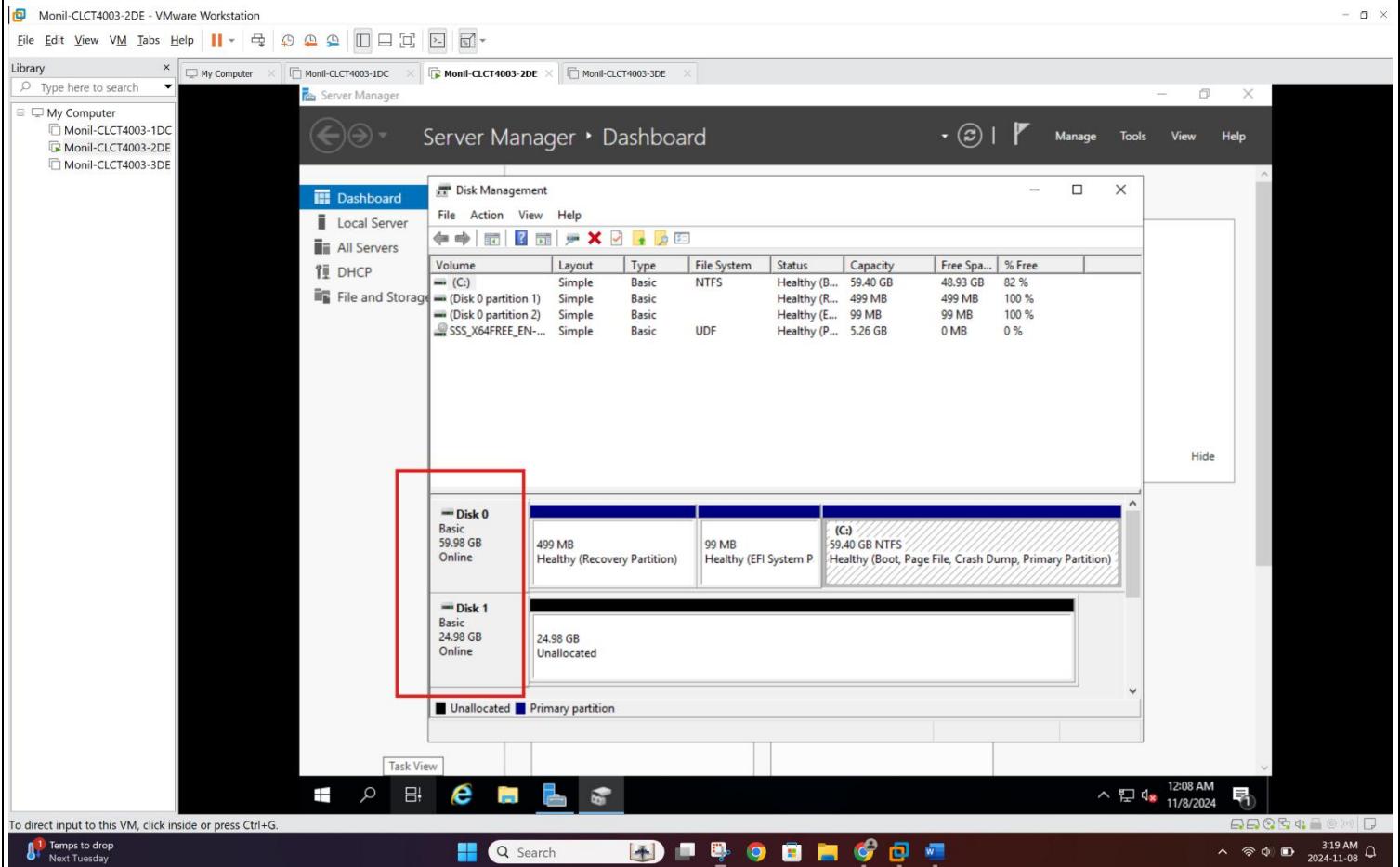
# Windows Server Security

## 5) Create a storage pool and a virtual disk



SS-19: Creating New Virtual Disk in VM2 to create the storage pool!

# Windows Server Security



To direct input to this VM, click inside or press Ctrl+G.

Tems to drop  
Next Tuesday

Search

12:08 AM 11/8/2024

3:19 AM 2024-11-08

*SS-20: Disk Management verifies that additional disk is added!*

# Windows Server Security

```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> # Create the storage pool
PS C:\Users\Administrator> PS C:\Users\Administrator> New-StoragePool -FriendlyName "Monil_StoragePool" -StorageSubSystemFriendlyName "Windows Storage" -PhysicalDisks (Get-PhysicalDisk | Where-Object CanPool -eq $True)

FriendlyName OperationalStatus HealthStatus IsPrimordial IsReadOnly Size AllocatedSize
----- ----- ----- ----- ----- ----- -----
Monil_StoragePool OK Healthy False False 59.48 GB 256 MB

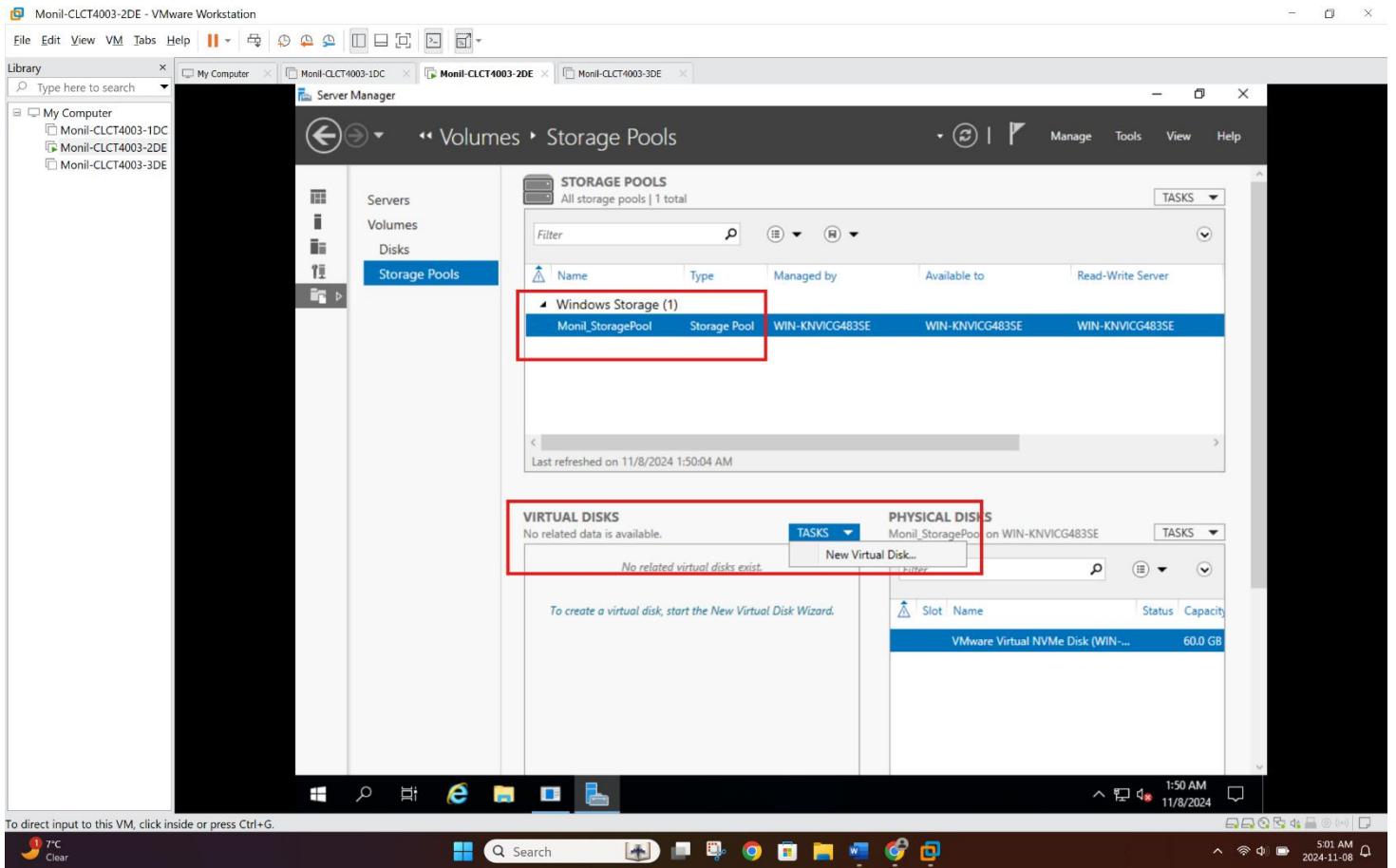
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Verify the storage pool creation
PS C:\Users\Administrator> PS C:\Users\Administrator> Get-StoragePool -FriendlyName "Monil_StoragePool"

FriendlyName Operationalstatus HealthStatus IsPrimordial IsReadOnly Size AllocatedSize
----- ----- ----- ----- ----- ----- -----
Monil_StoragePool OK Healthy False False 59.48 GB 256 MB

PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

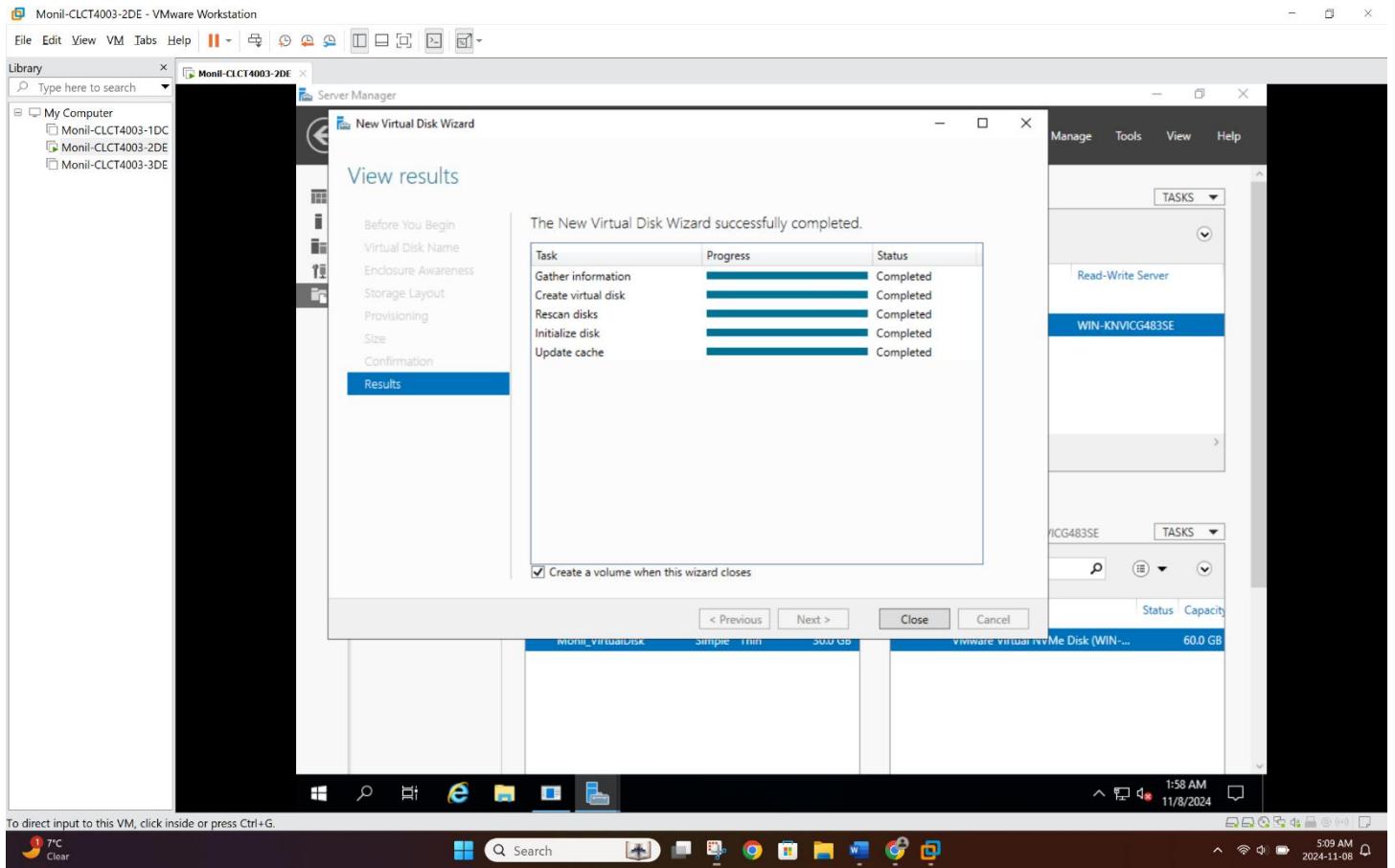
SS-21: Created the storage pool using powershell on VM2!

# Windows Server Security



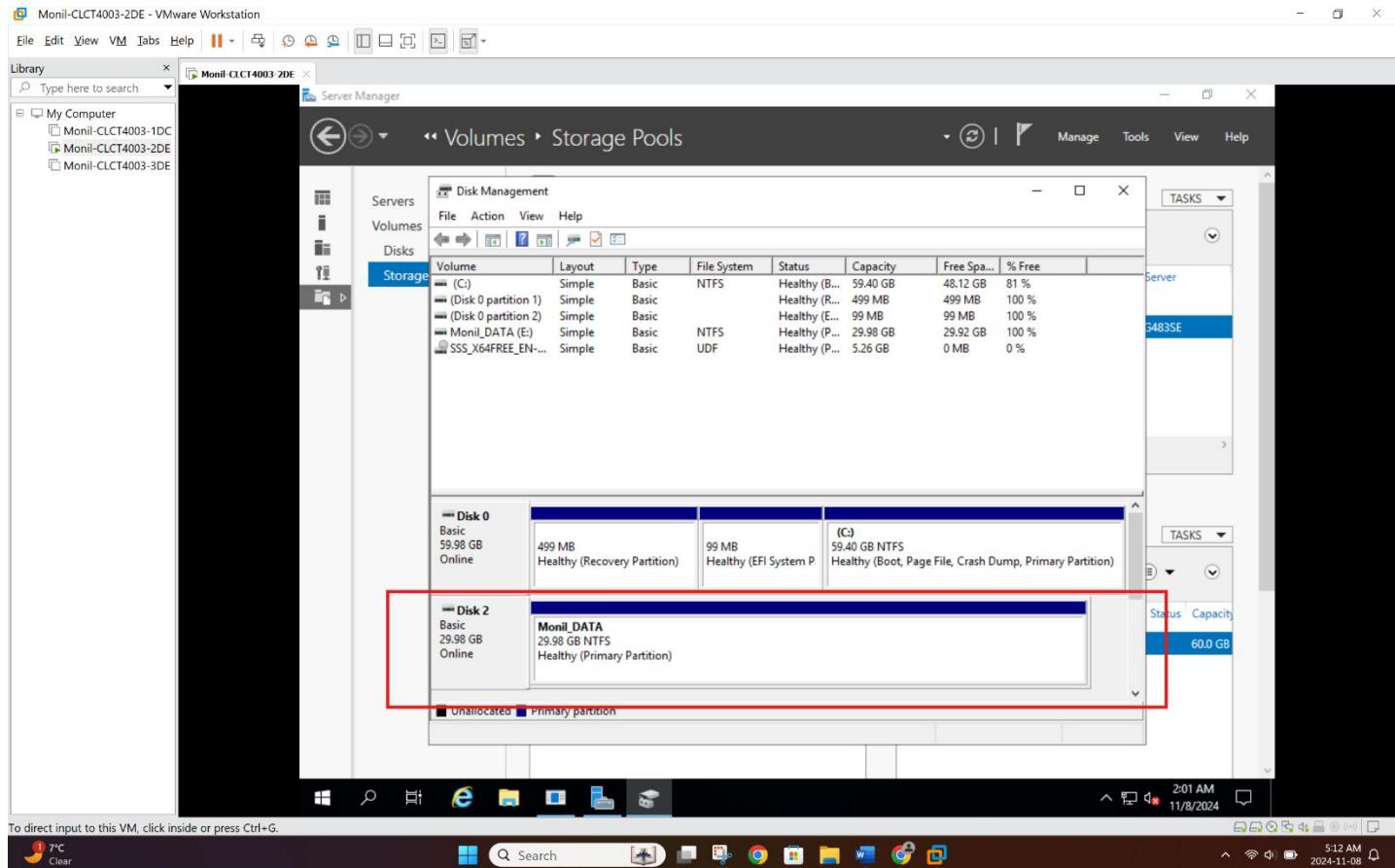
SS-22: As we can see, the storage pool is now created and we are now creating virtual disk!

# Windows Server Security



Ss-23: Virtual Hard Disk is now created!

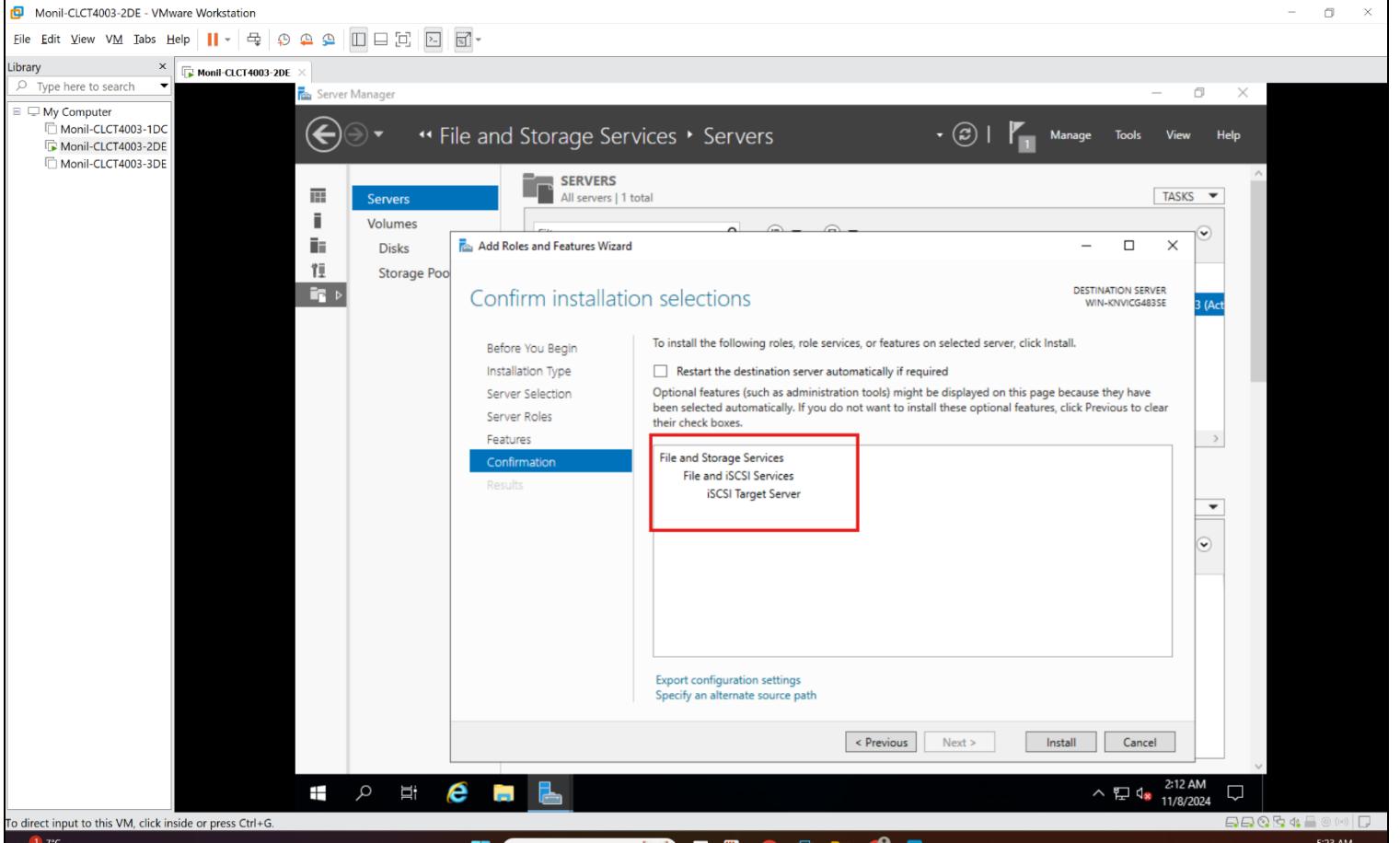
# Windows Server Security



SS-24: Our newly created virtual disk is now ready to use!

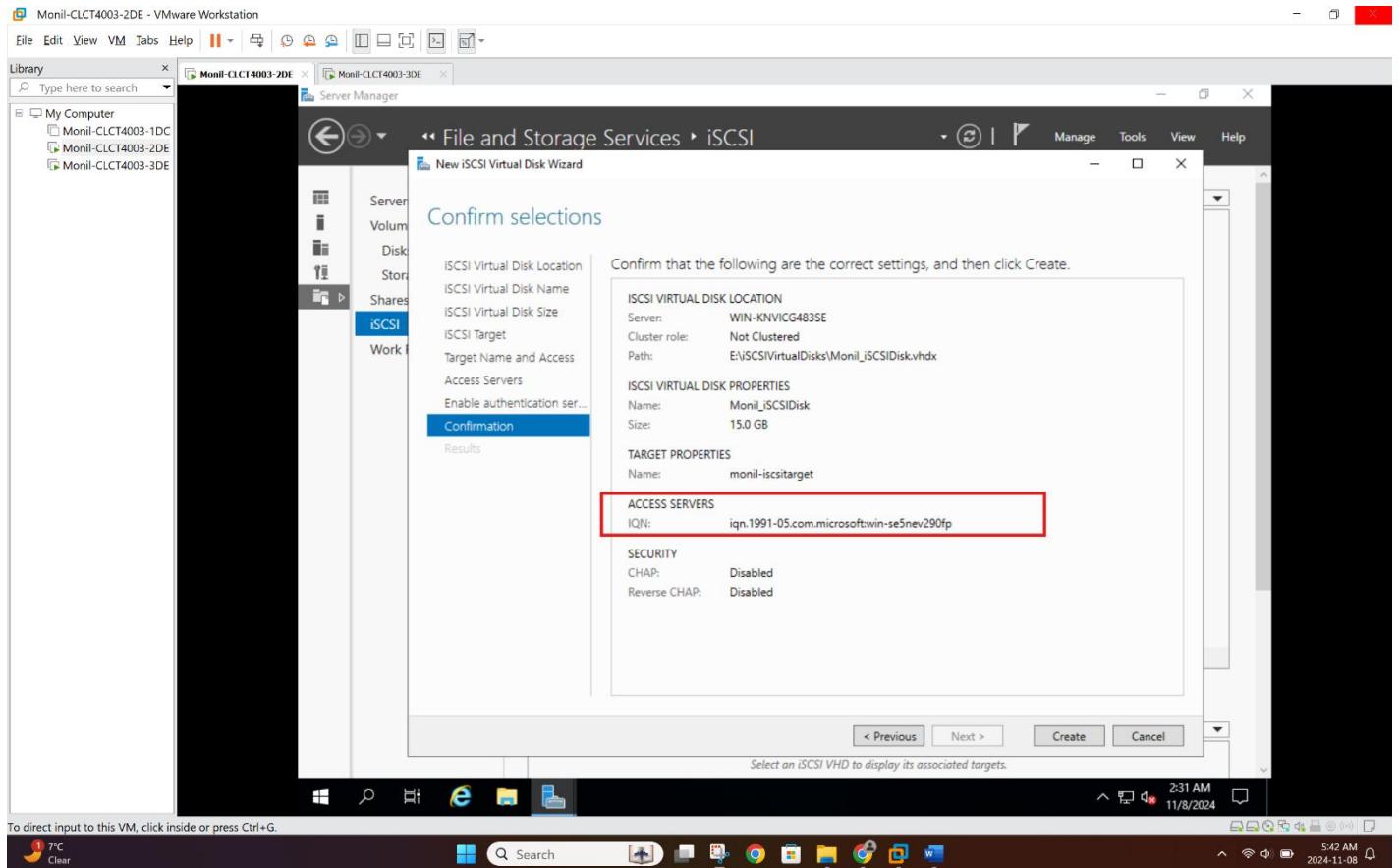
# Windows Server Security

- 6) Create an iSCSI disk on server 2 and attach it to Server 3



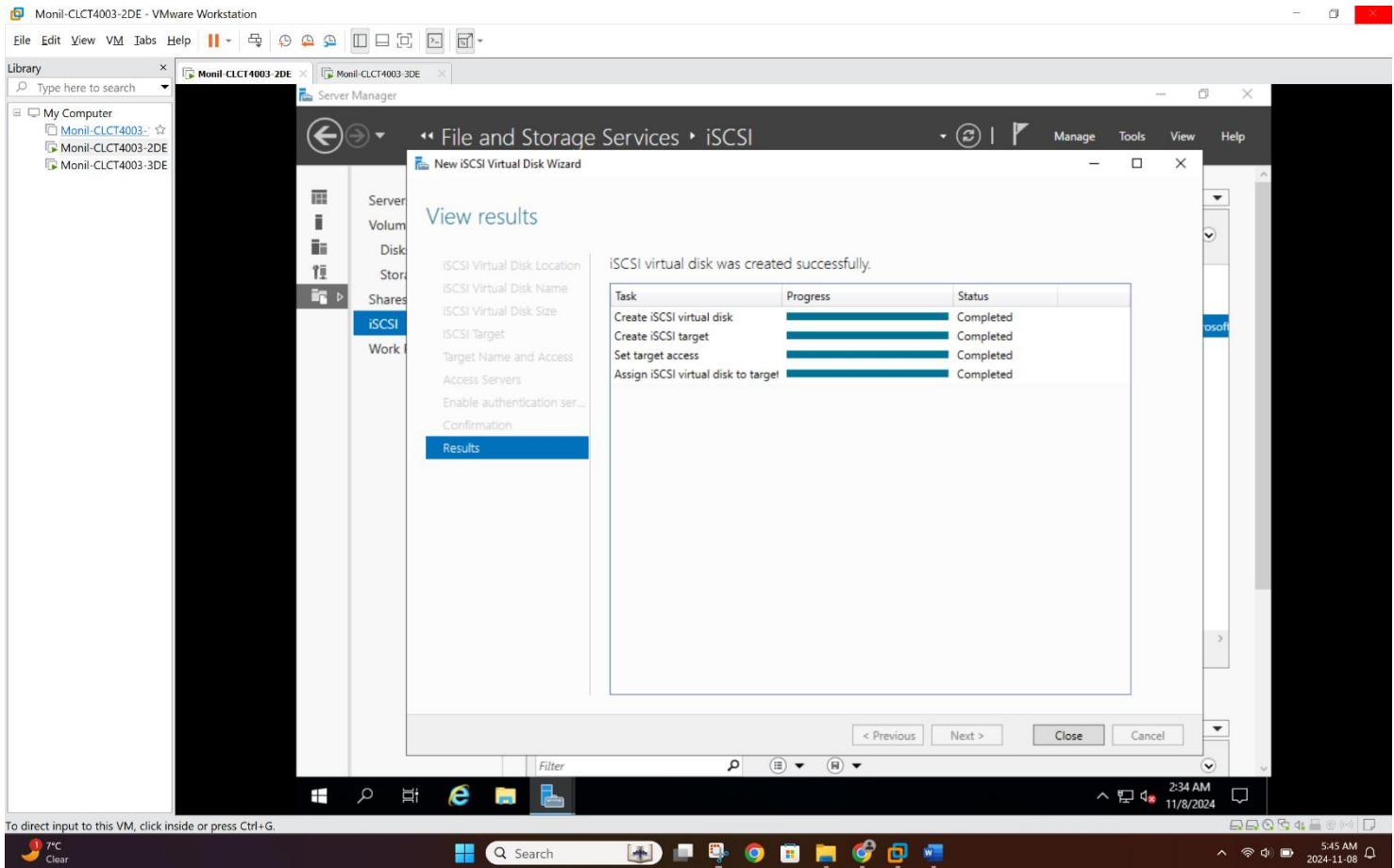
SS-25: Installing iSCSI services role on VM2

# Windows Server Security



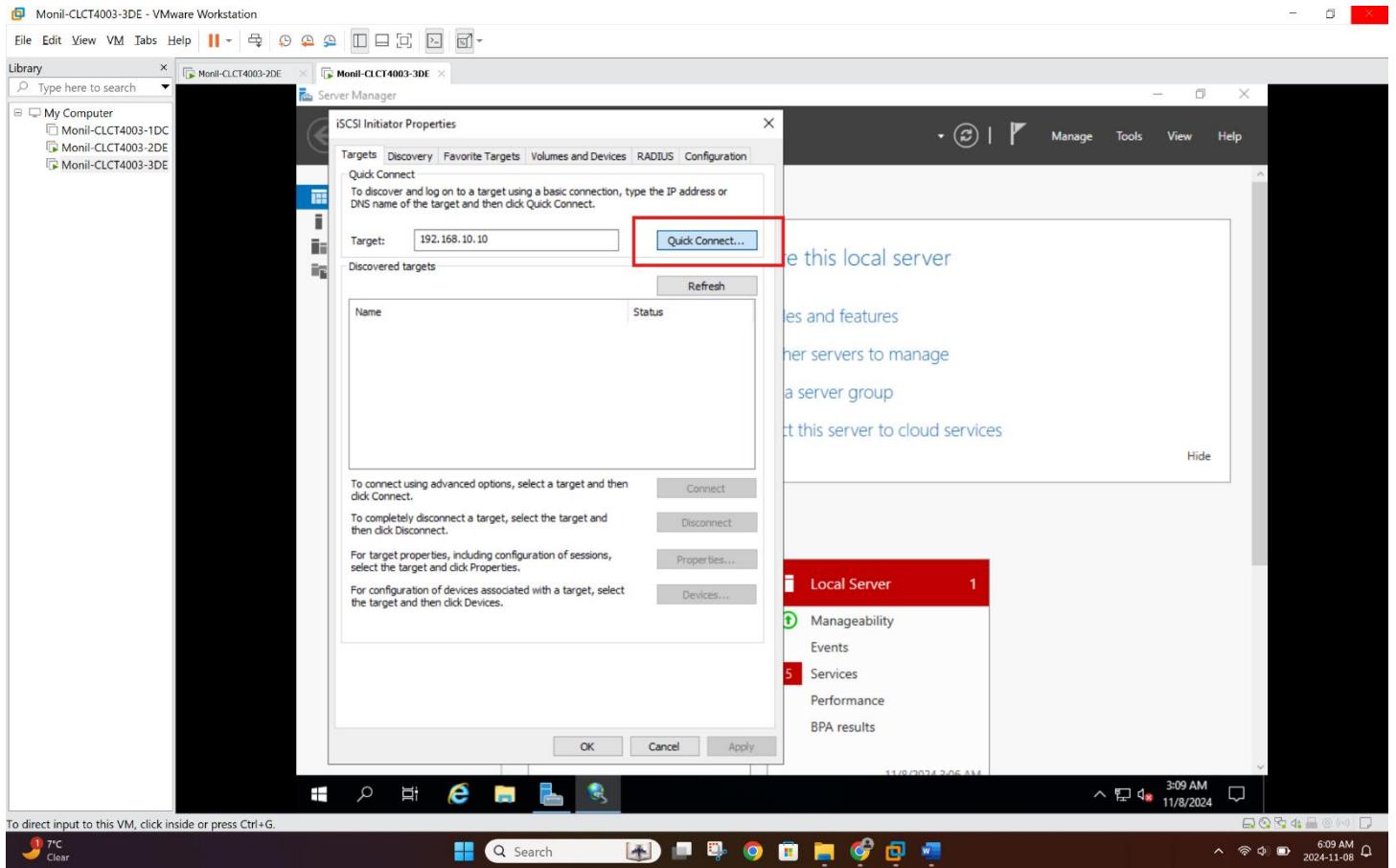
SS-26: Creating iscsi virtual disk by retrieving the IQN on VM3!

# Windows Server Security



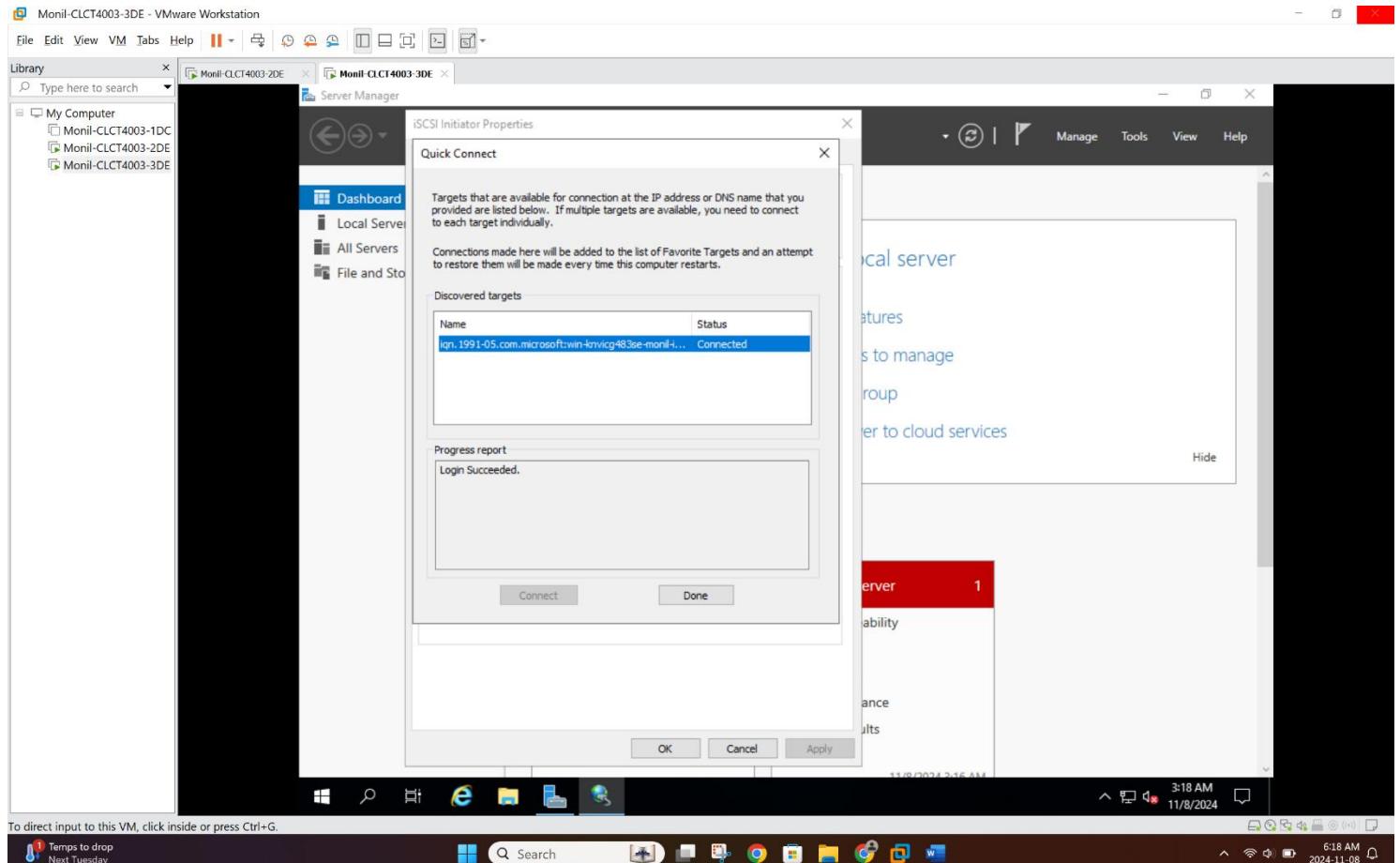
SS-27: iscsi is created successfully with valid target!

# Windows Server Security



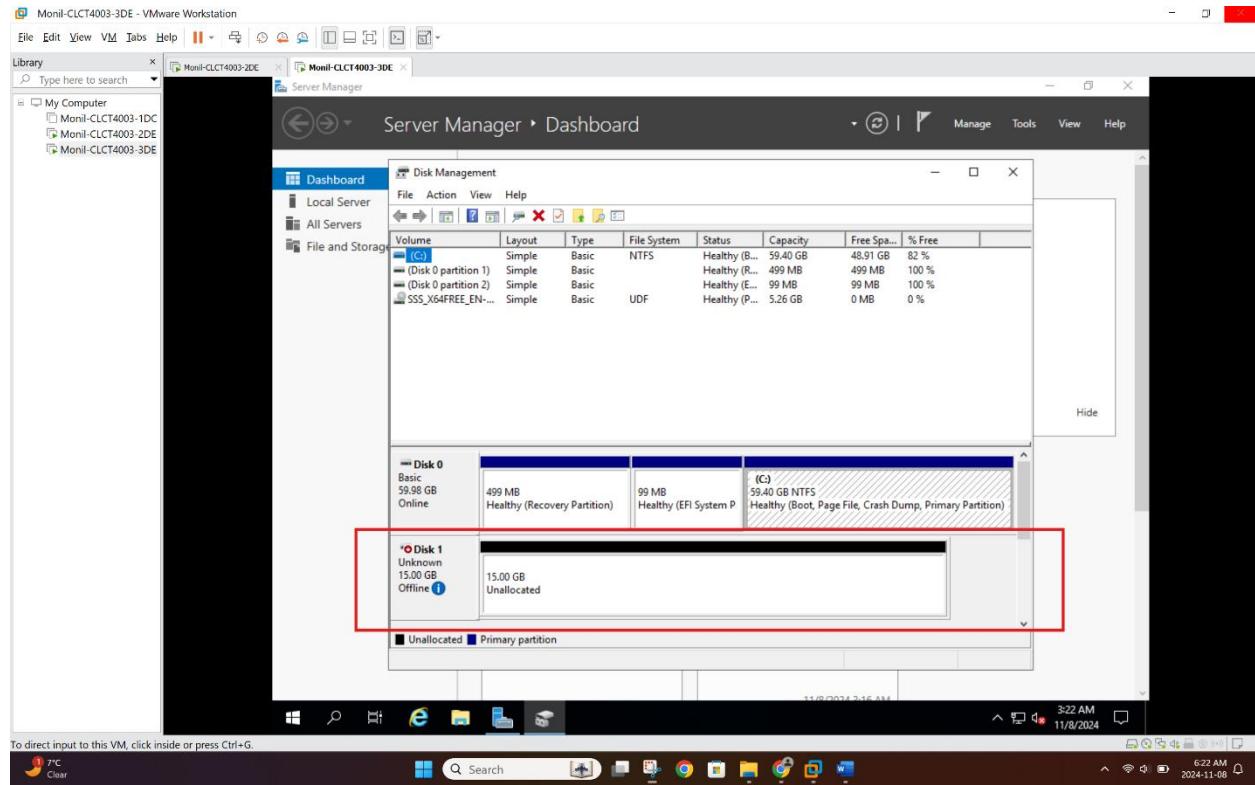
SS-28: Connecting to iSCSI target on VM2 through iSCSI initiator!

# Windows Server Security



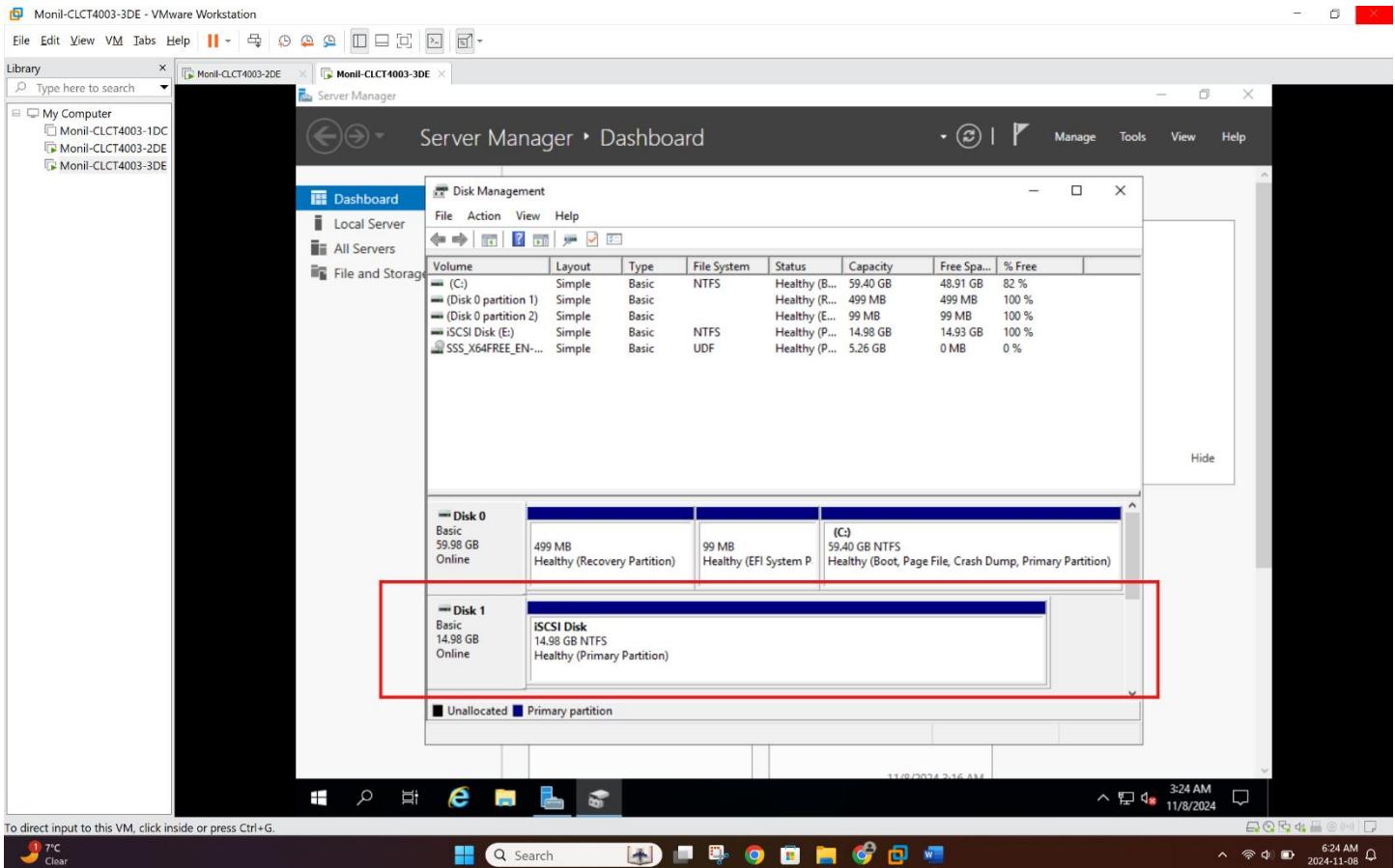
SS-29: iSCSI Target on Vm2 is successfully established on VM3!

# Windows Server Security



SS-30: We can see now iSCSI disk which was created in VM2 in VM3

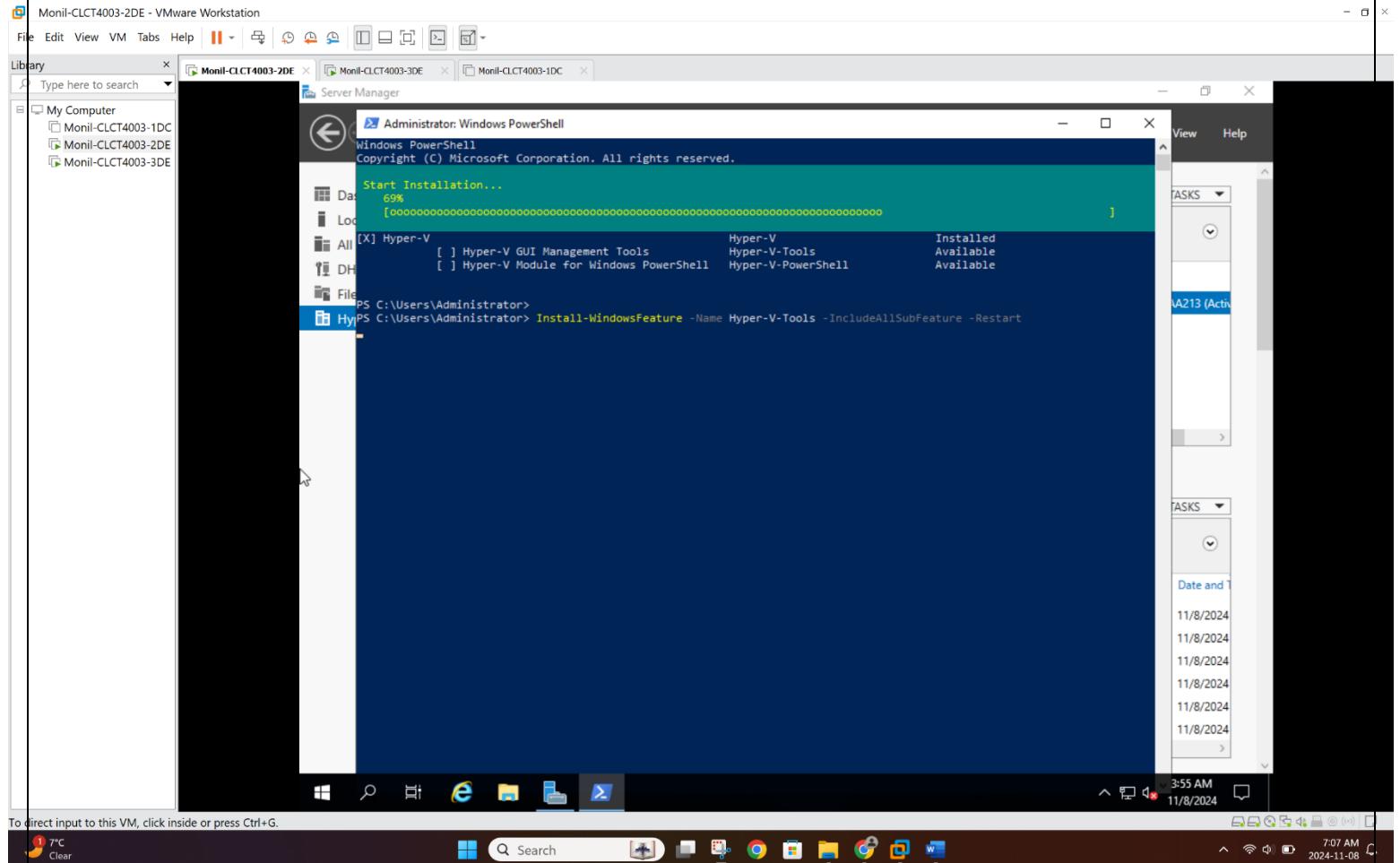
# Windows Server Security



SS-31: iSCSI Disk now ready to use on VM3!

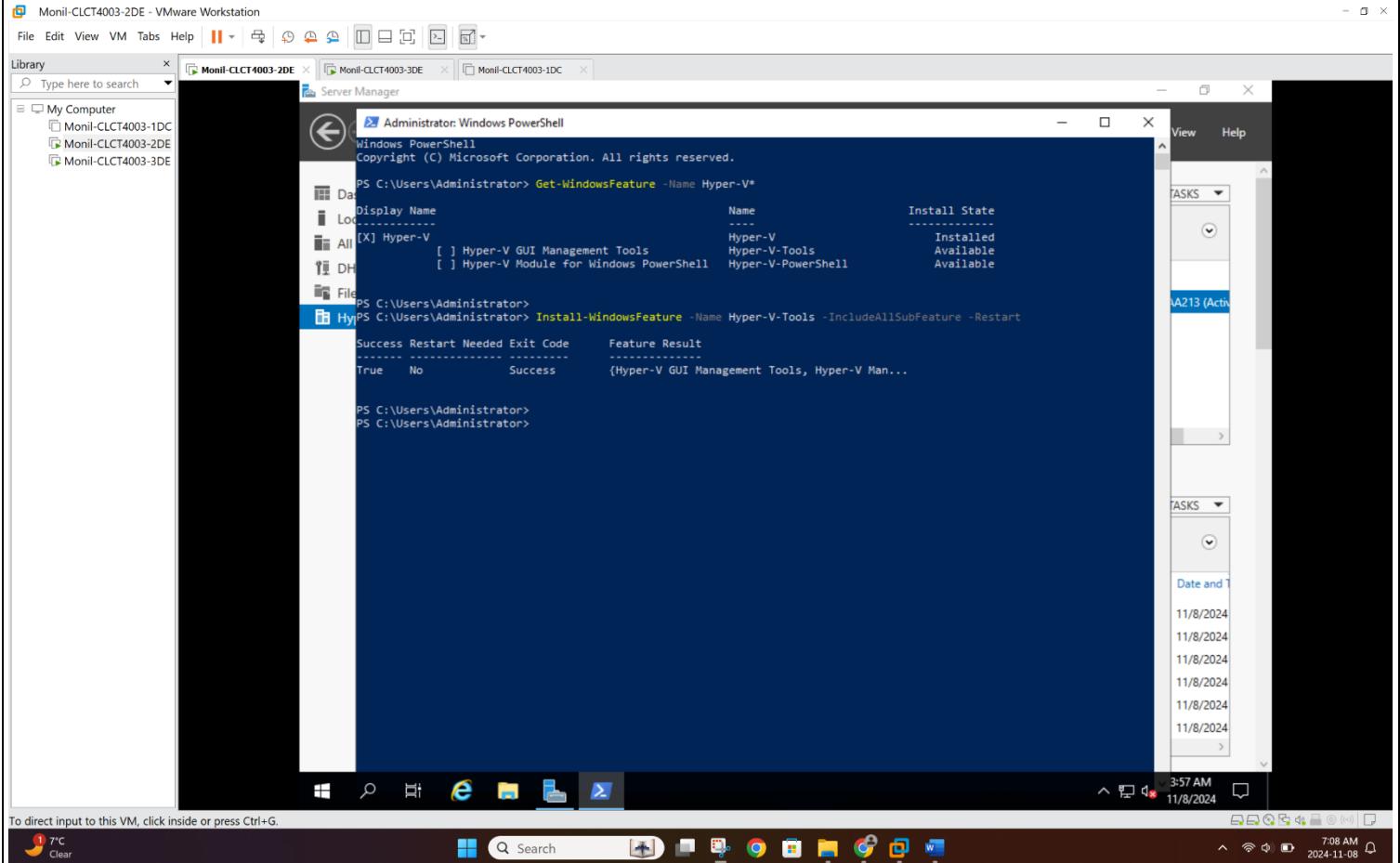
# Windows Server Security

## 7) Install Hyper-V Role on server 2 and create a virtual machine



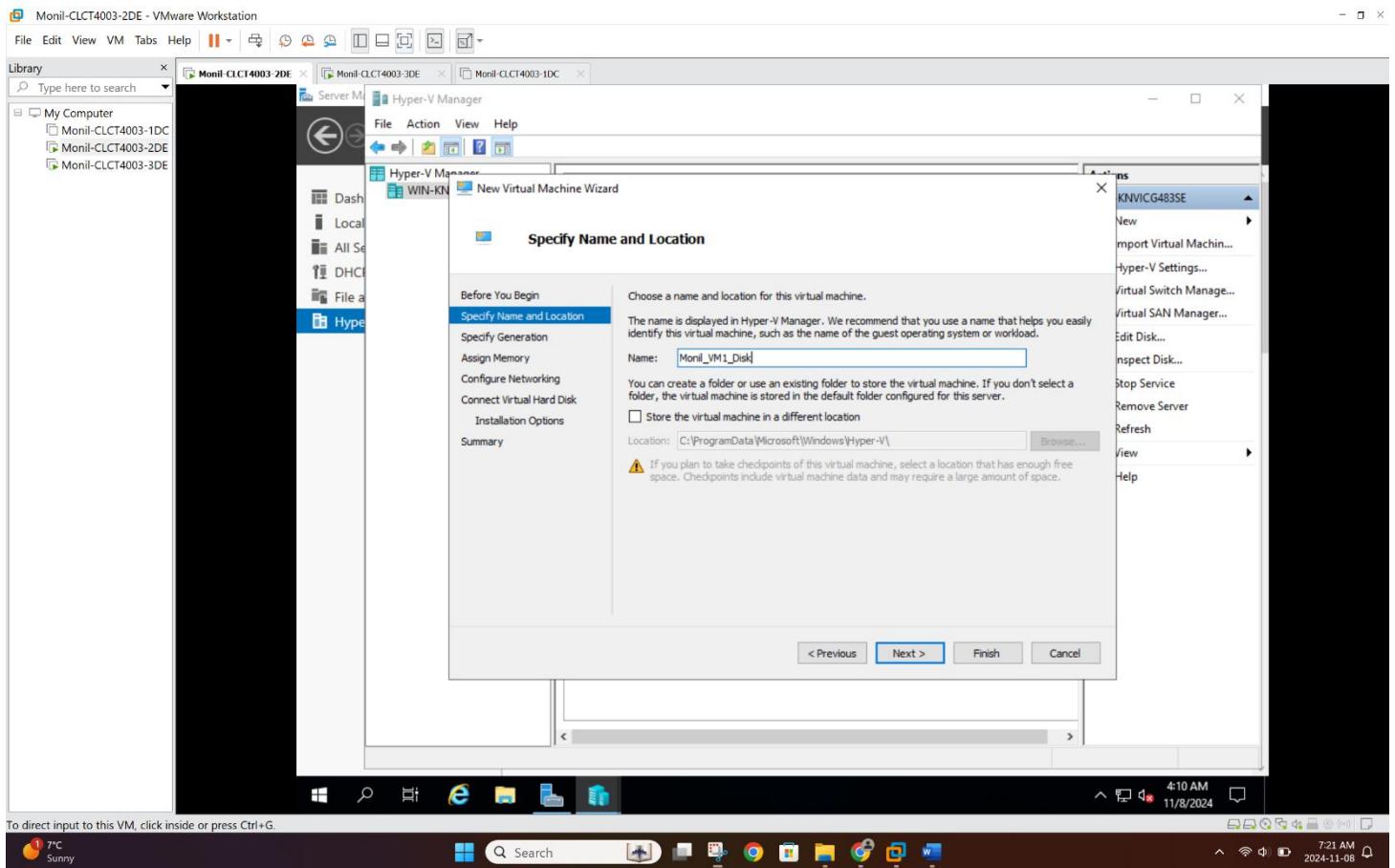
SS-32: Installing Hyper-V Roles and features on VM2 via powershell

# Windows Server Security



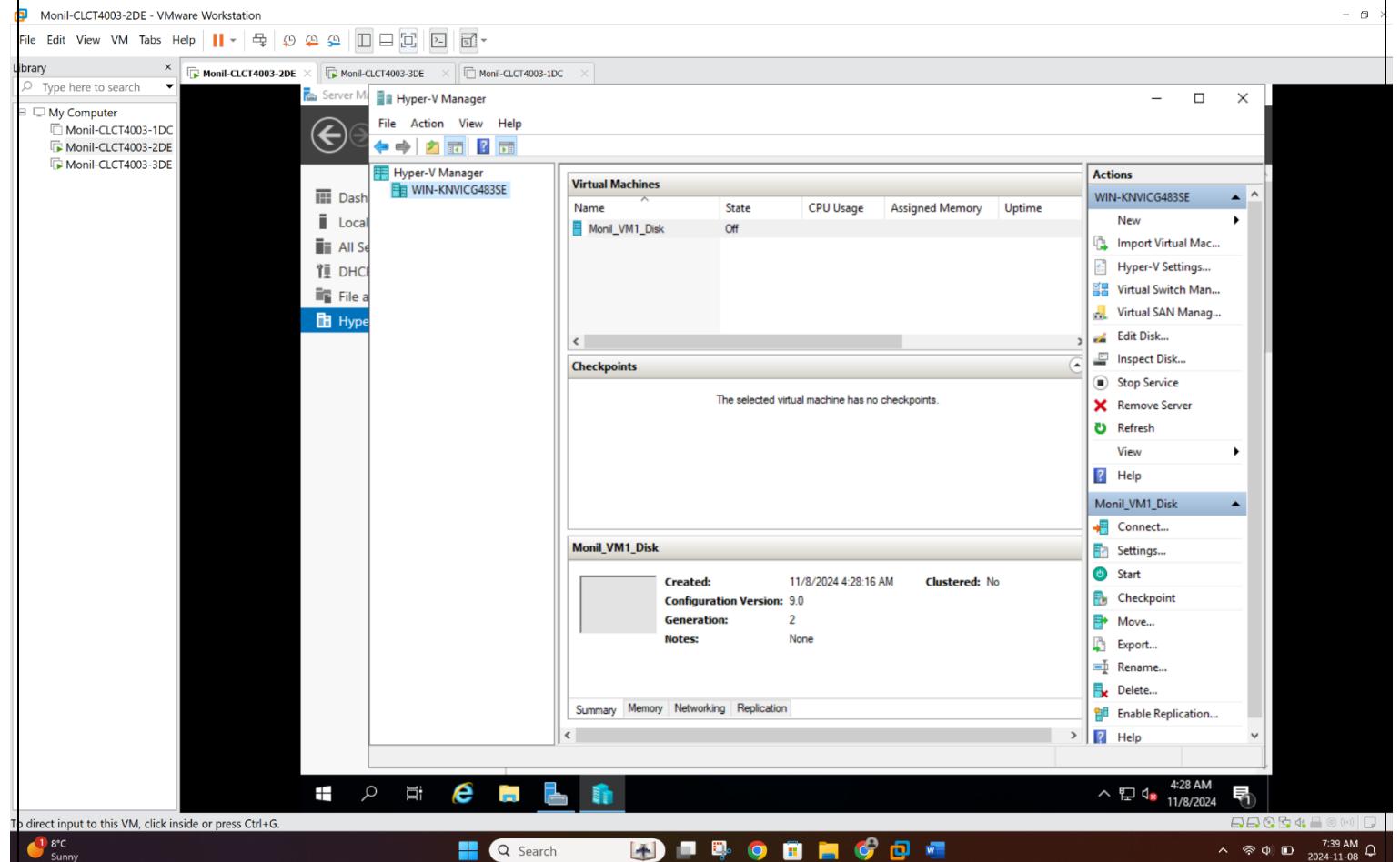
SS-33: Hyper-V Manager and it's related features are now installed on server2!

# Windows Server Security



SS-34: Creating new virtual disk via Hyper-V Manager!

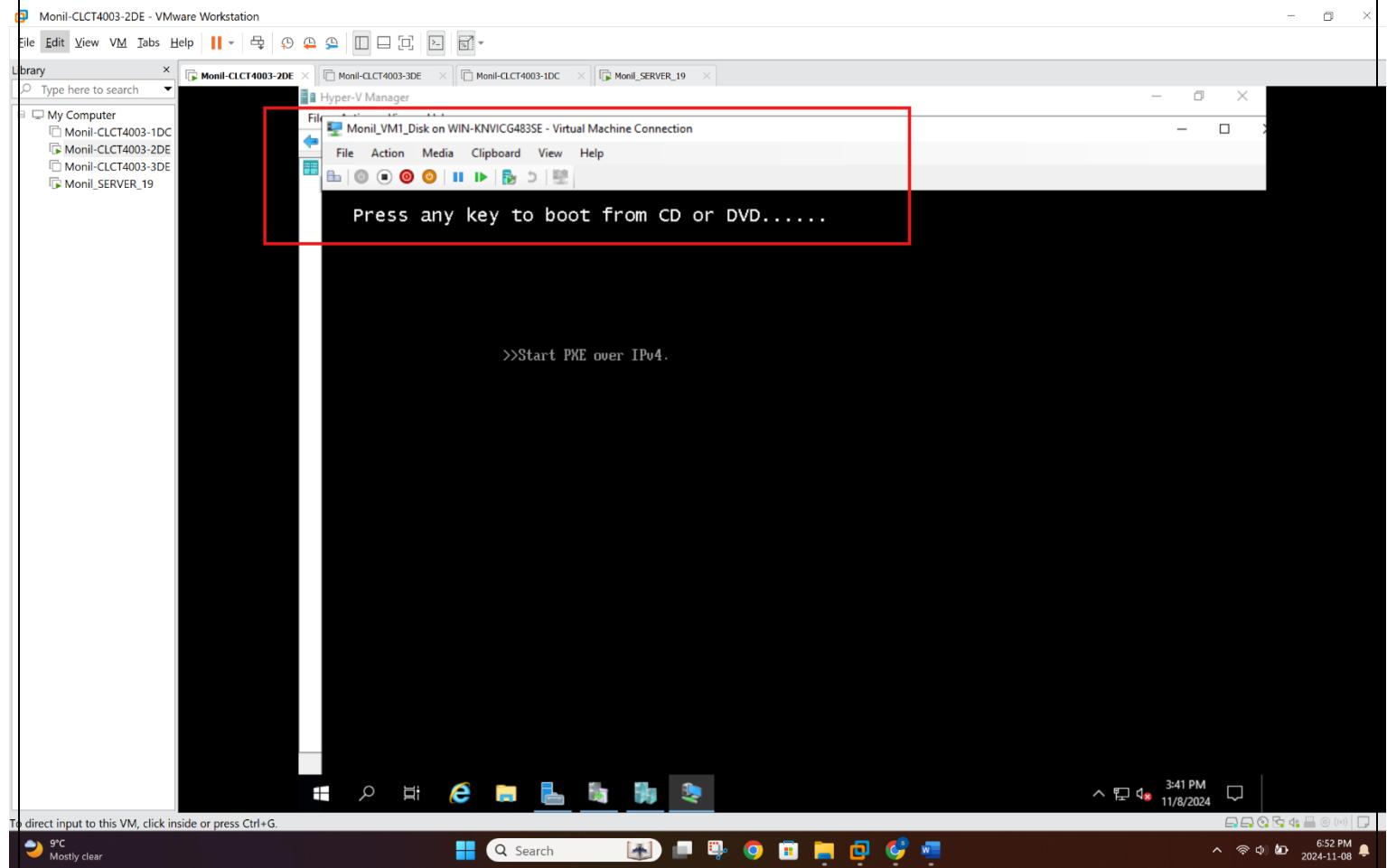
# Windows Server Security



SS-35: New VM is created on VM2 through Hyper-V Manager!

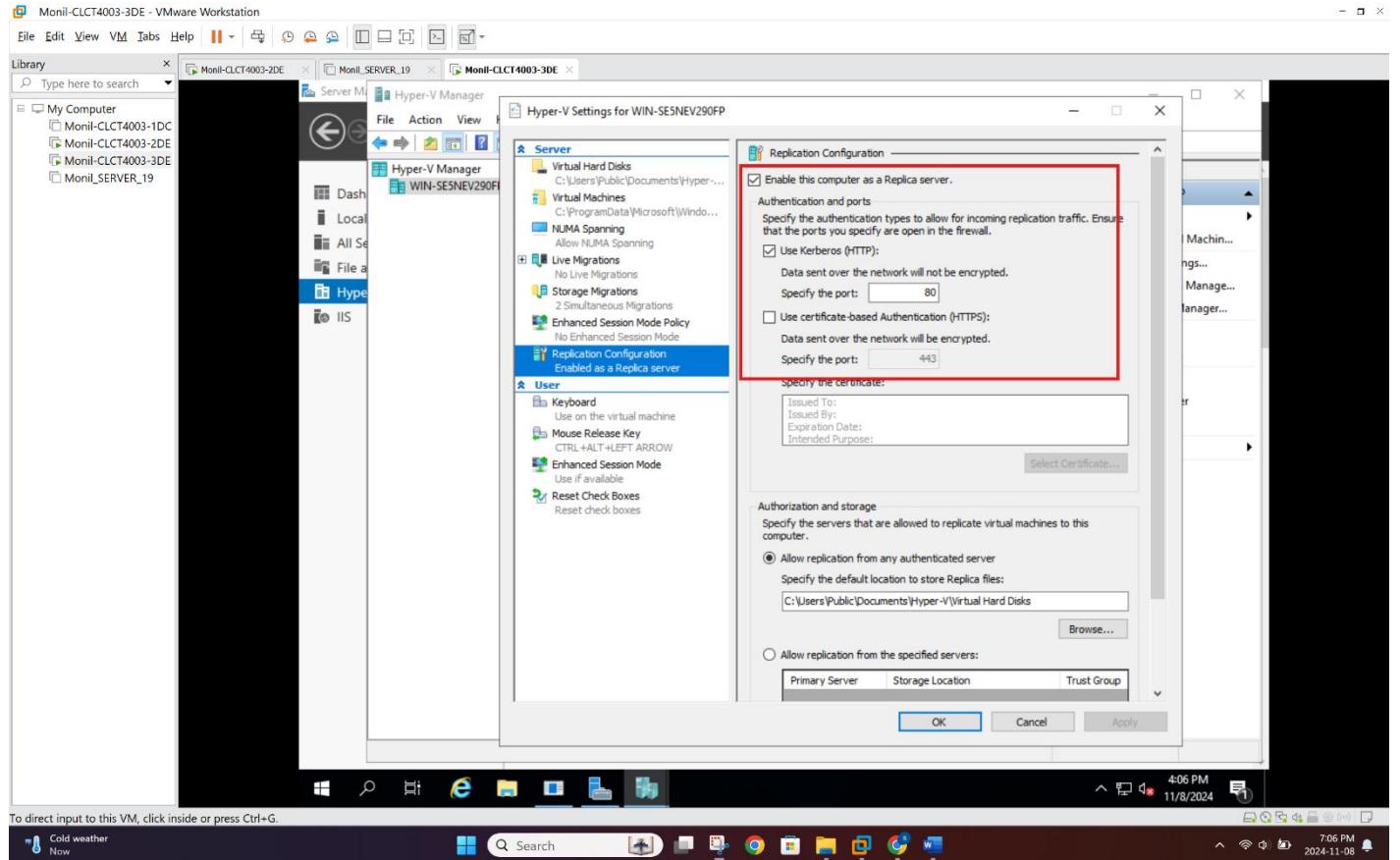
- 8) Install Hyper-V role on server 3 and configure Hyper-V Replica

# Windows Server Security



SS-36: As we can see, “Monil\_VM1\_Disk” is running completely fine!

# Windows Server Security

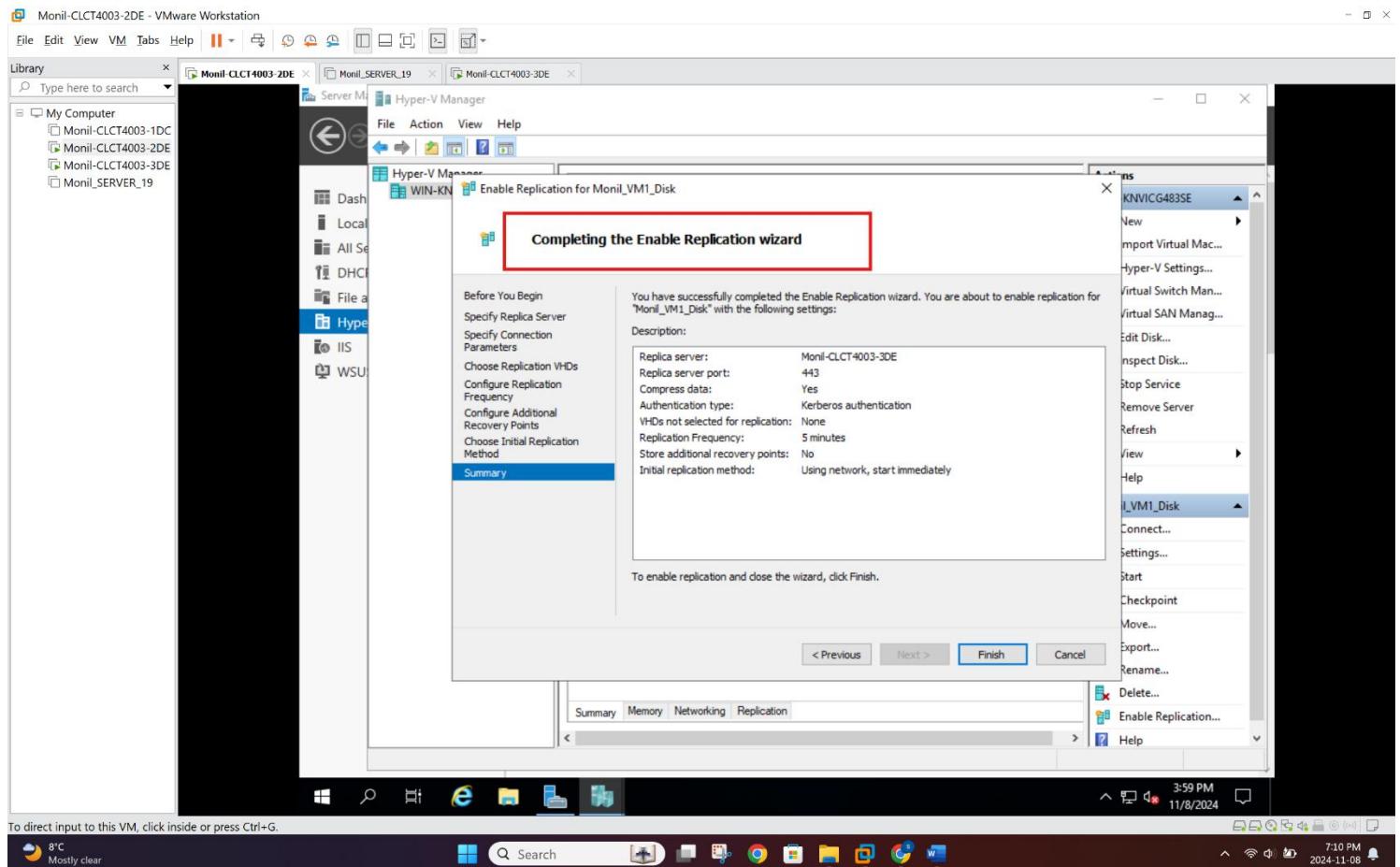


To direct input to this VM, click inside or press Ctrl+G.

Cold weather Now Search 4:06 PM 11/8/2024 7:06 PM 2024-11-08

SS-37: Choosing VM3 as replica server!

# Windows Server Security

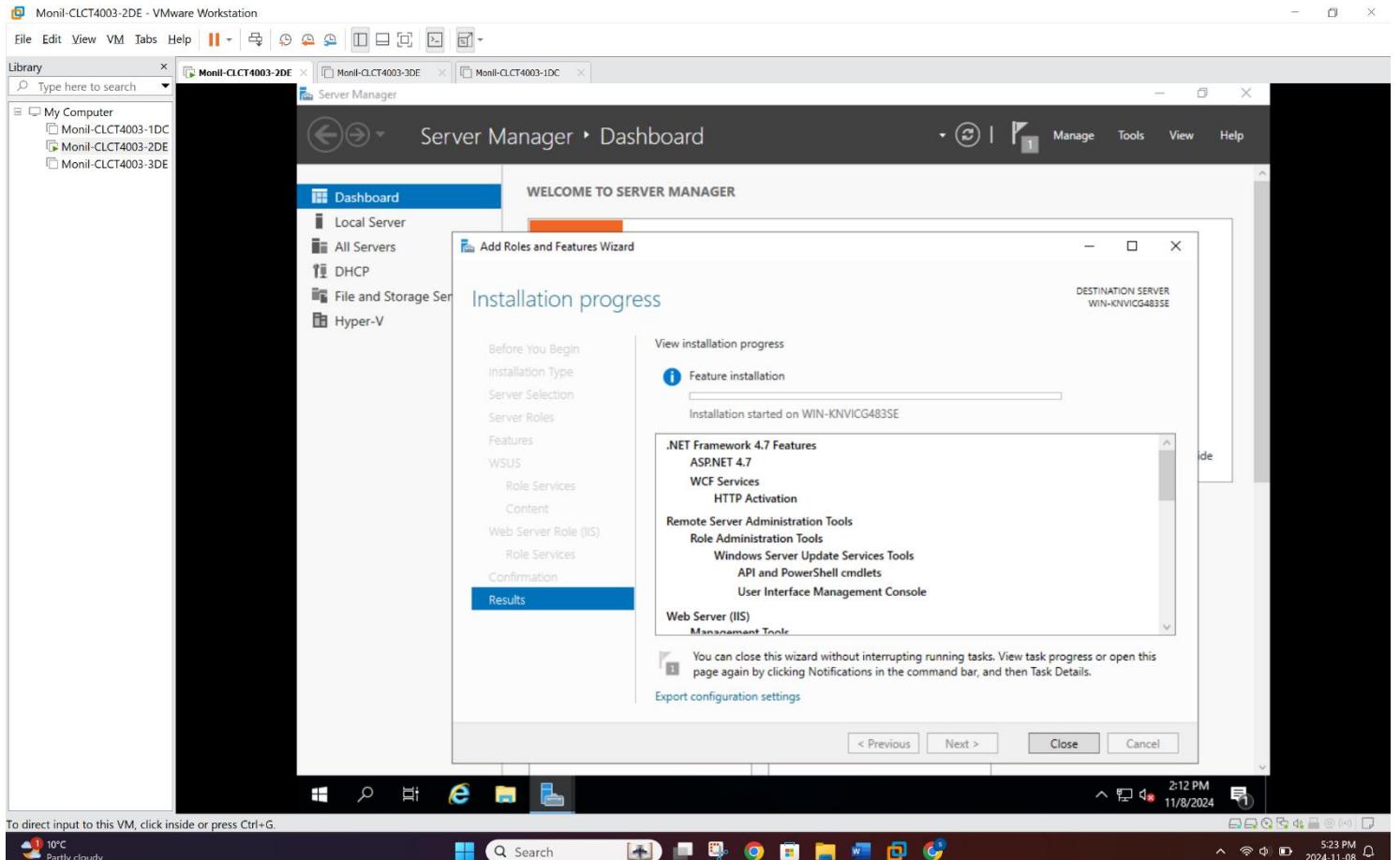


SS-38: Enabling Replica of VM on Server2

9) Install and Configure WDS

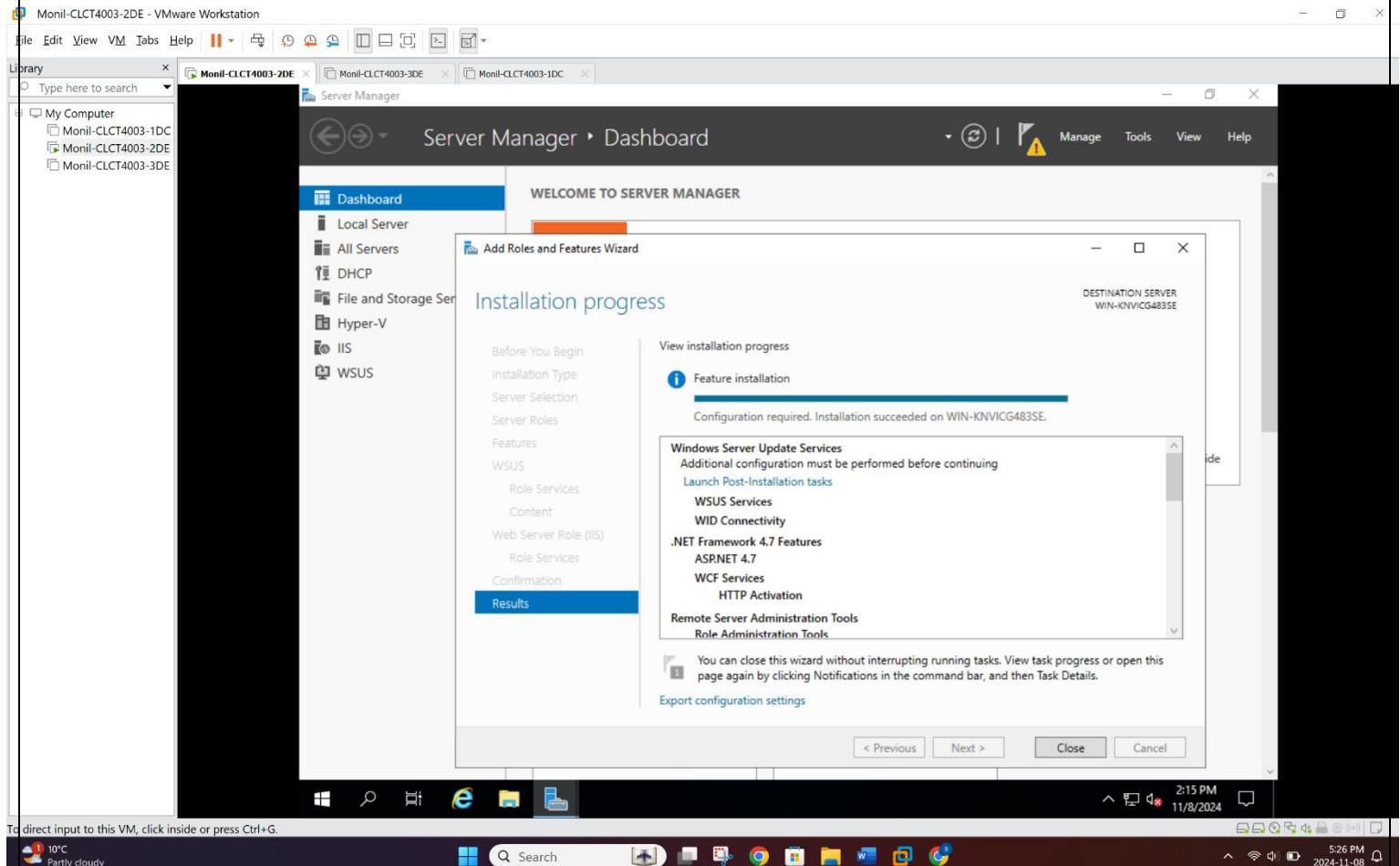
# Windows Server Security

- a) Enforce WDS settings to clients using group policy and remove pause option.



SS-39: Installing WSUS role and features!

# Windows Server Security

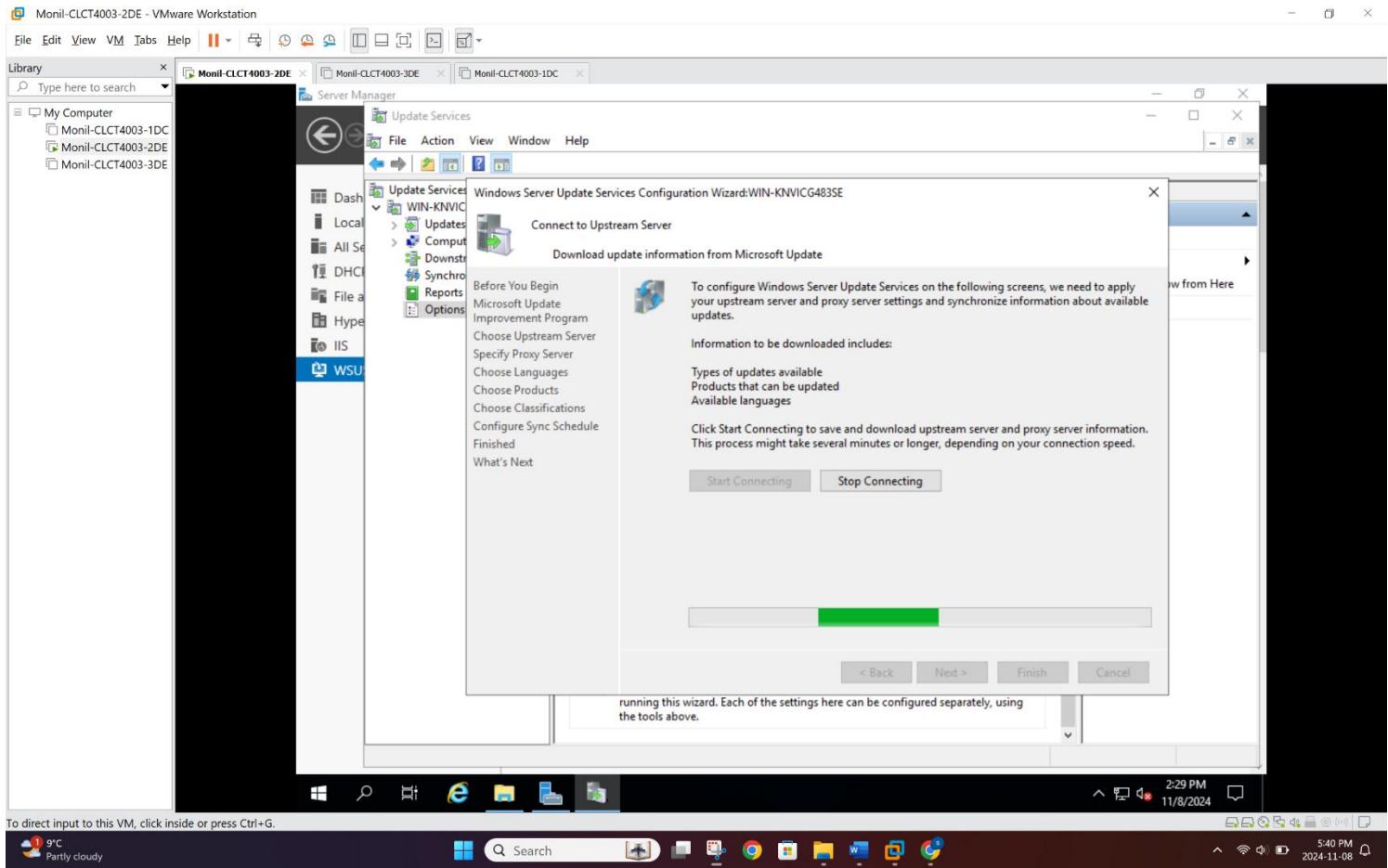


To direct input to this VM, click inside or press Ctrl+G.



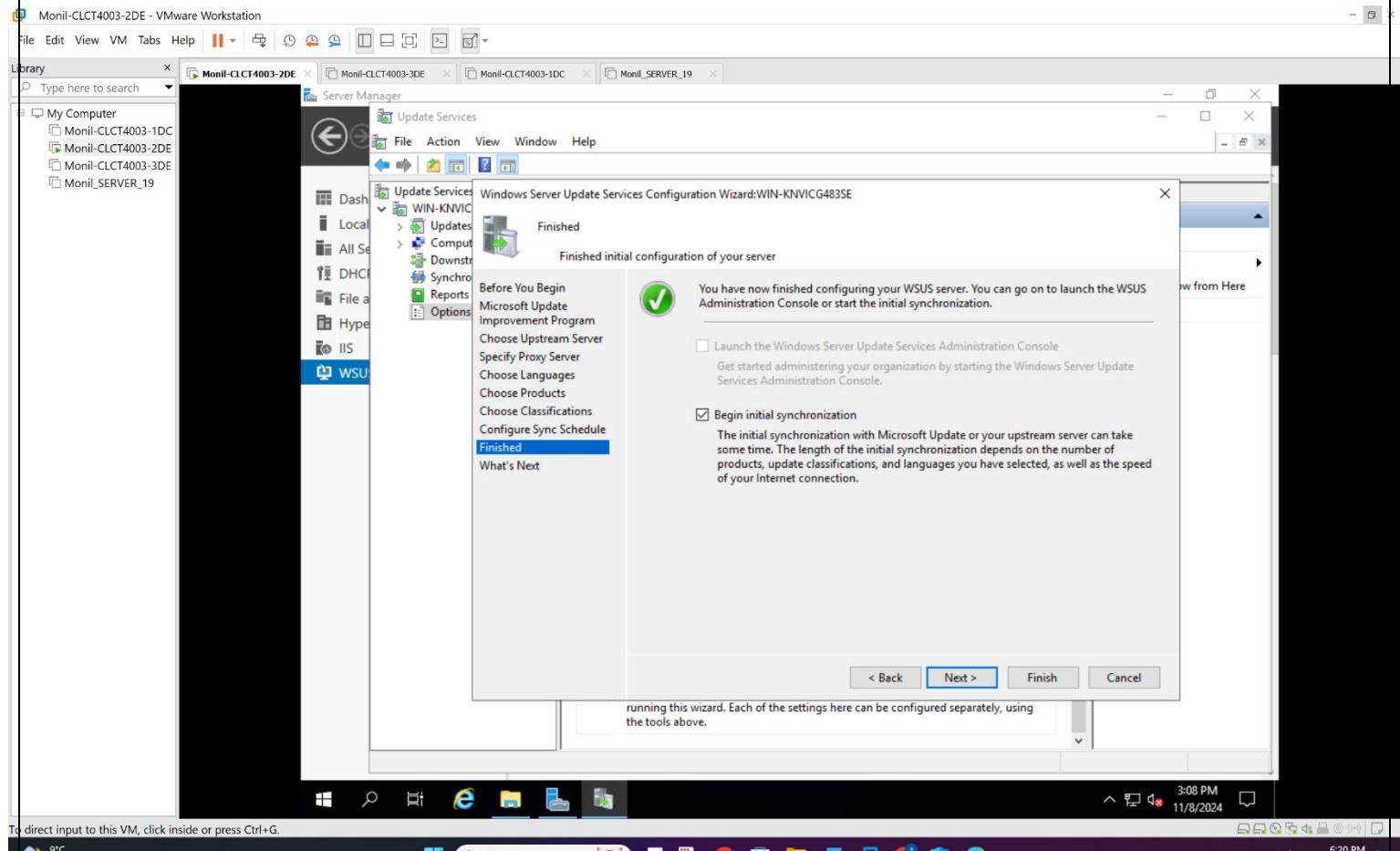
*SS-40: WSUS installation is done. Next step is to configure the post installation!*

# Windows Server Security



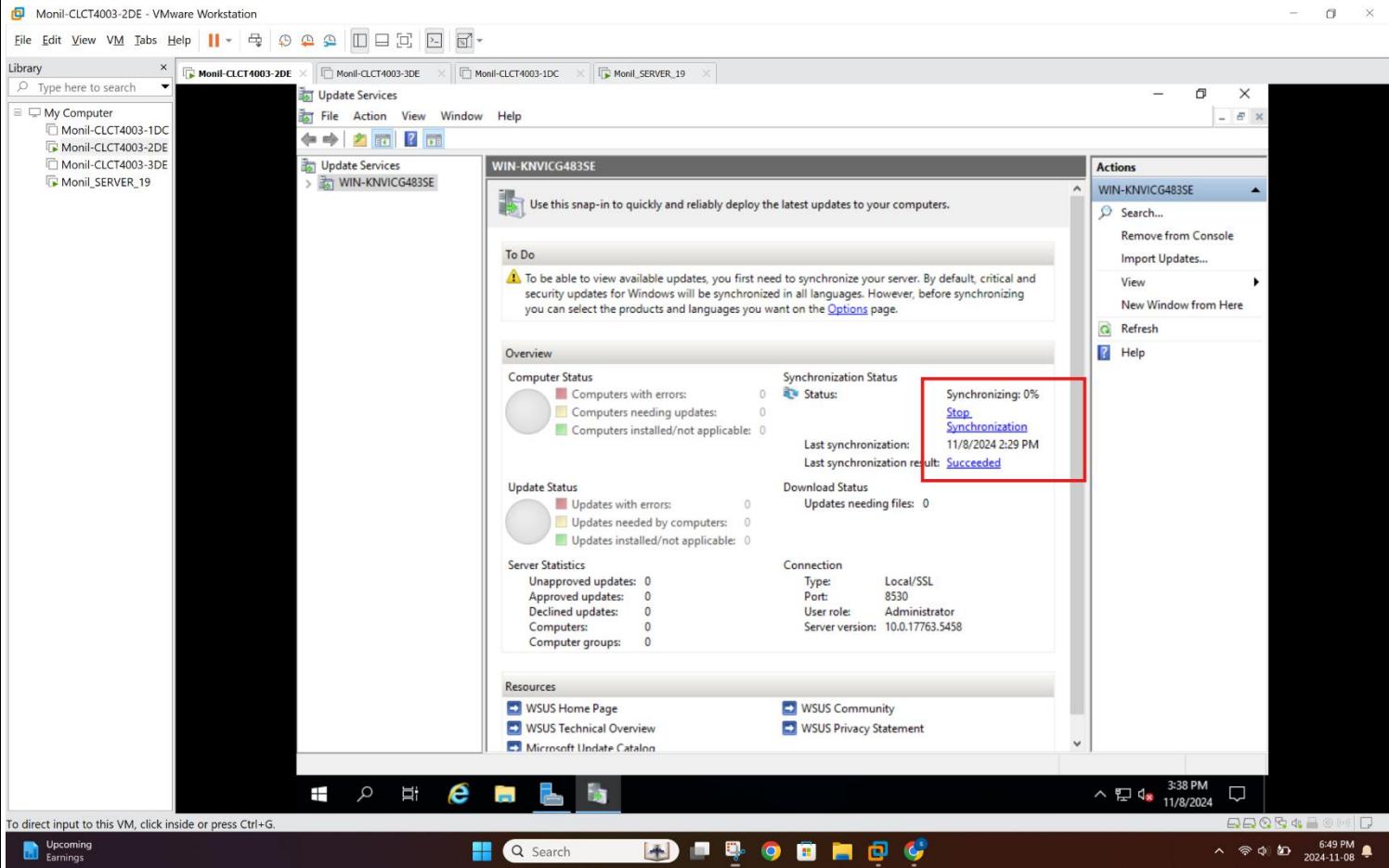
SS-41: Configuring the windows server update services configuration wizard

# Windows Server Security



SS-42: Configuring the WSUS server has been completed!

# Windows Server Security

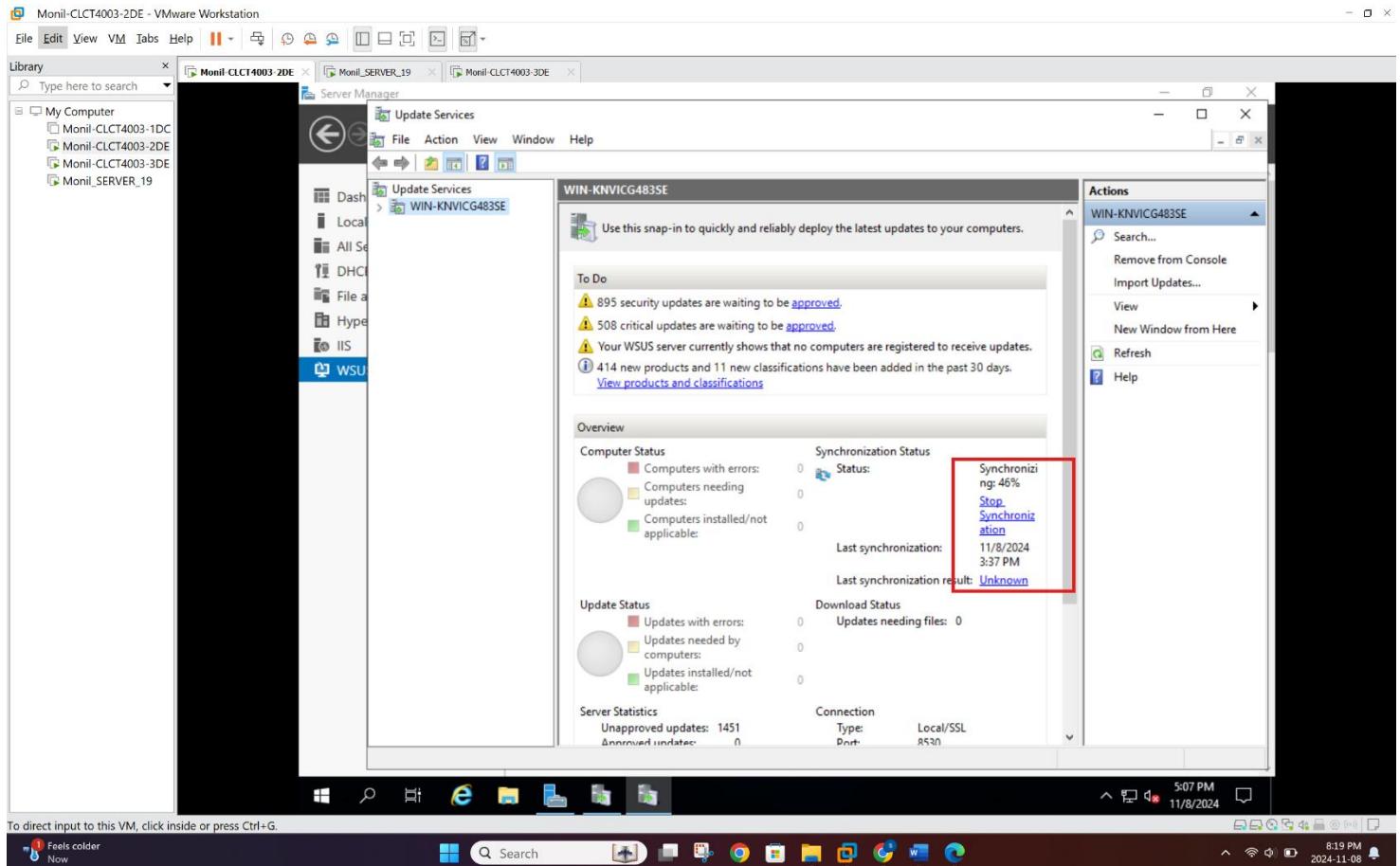


To direct input to this VM, click inside or press Ctrl+G.

Upcoming Earnings      Windows Search      Microsoft Edge      File Explorer      This PC      Control Panel      Task View      Start      6:49 PM      11/8/2024

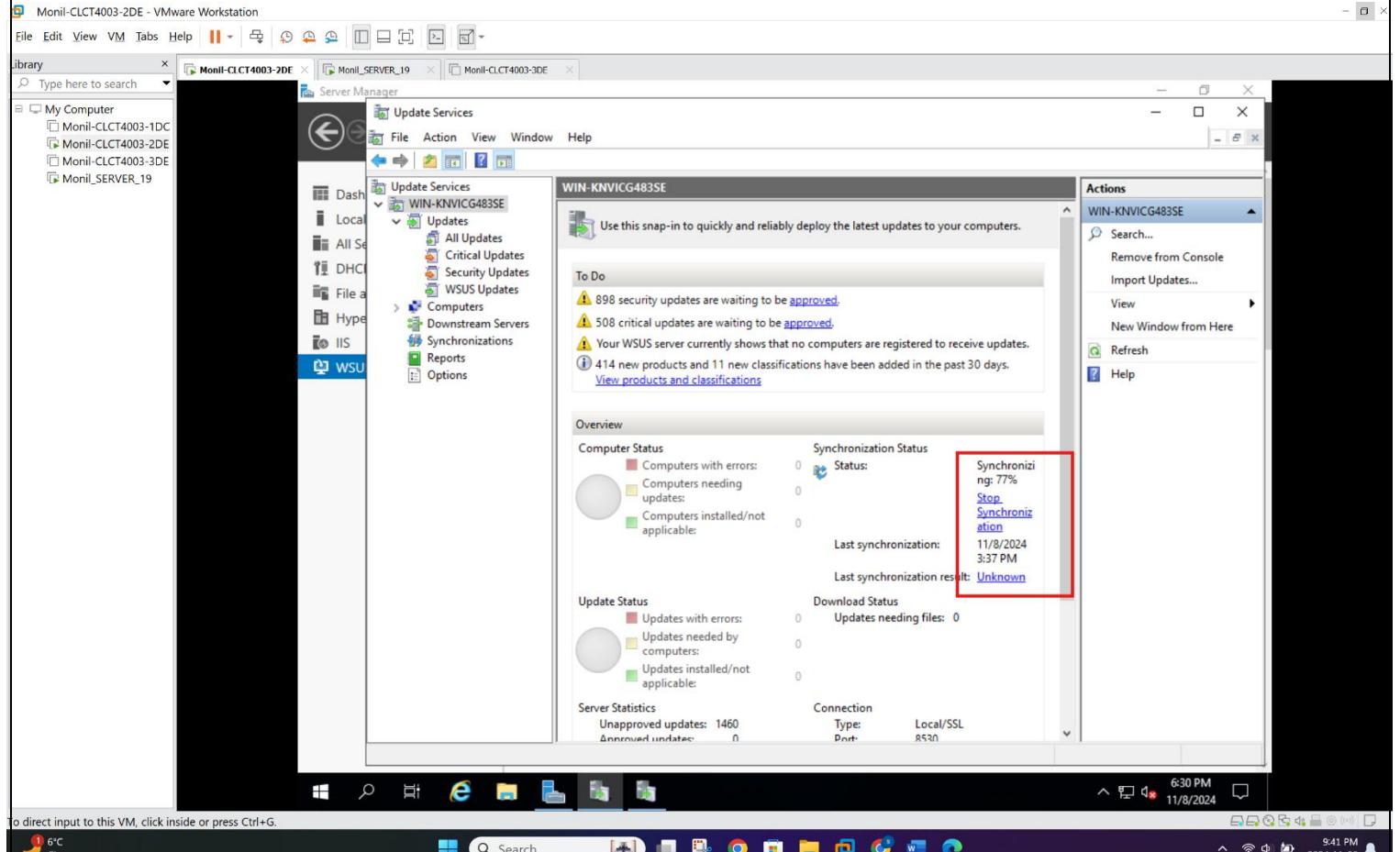
*SS-43: Synchronization is being completed!*

# Windows Server Security



SS-44: Synchronization taking time!!

# Windows Server Security



SS-45: Time is passing!!