

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
- 2) Configure Group Policy and enforce password change to 30 days
- 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
- 4) On your domain DNS Server, create forwarder and forward all requests to 8.8.8.8
- 5) Create a storage pool and a virtual disk
- 6) Create in ISCSI disk on server 2 and attach it to Server 3
- 7) Install Hyper-V Role on server 2 and create a virtual machine
- 8) Install Hyper-V role on server 3 and configure Hyper-v Replica
- 9) Install and Configure WSUS
 - a) Enforce WSUS settings to clients using group policy and remove pause option.

~~~~~

Paste your screenshots here

# Windows Server Security

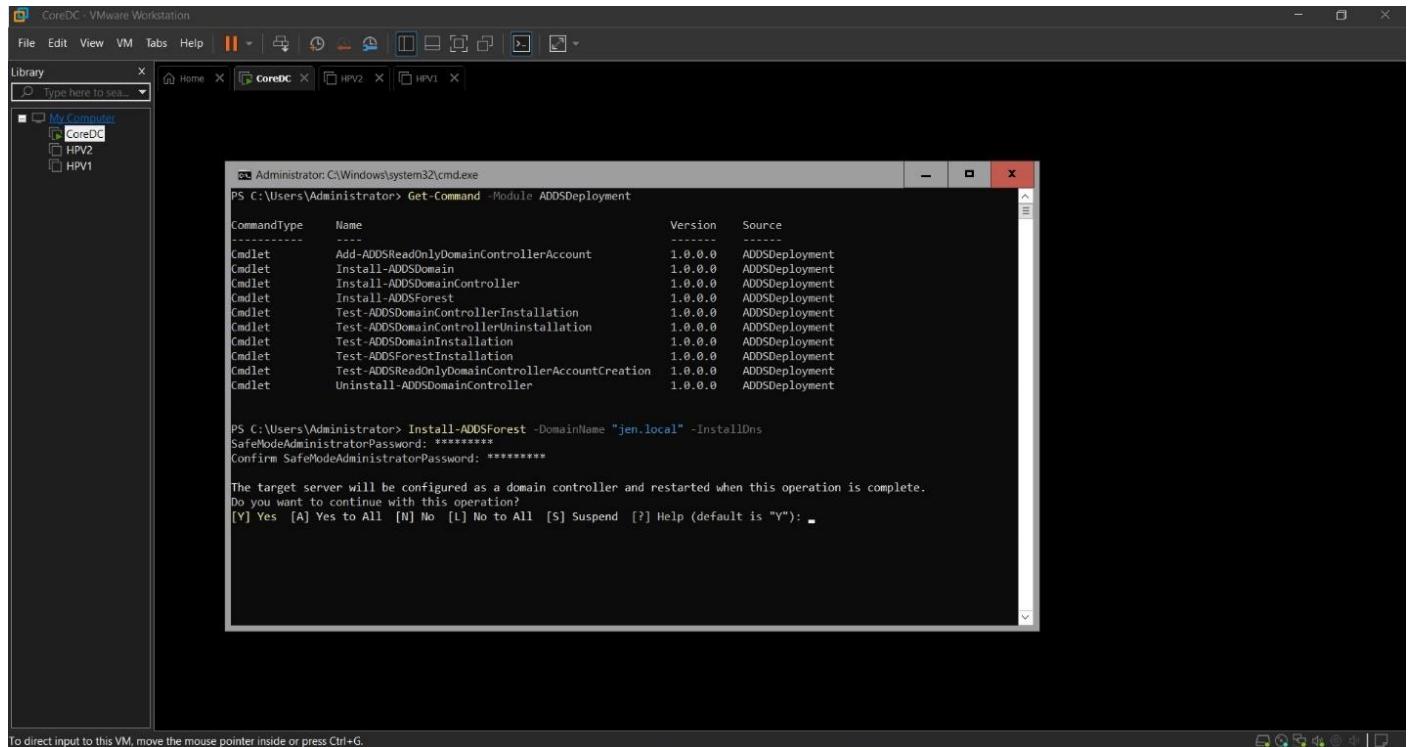


Figure 1 Installed Active Directory and Promoted to Domain Controller jen.local

# Windows Server Security

---

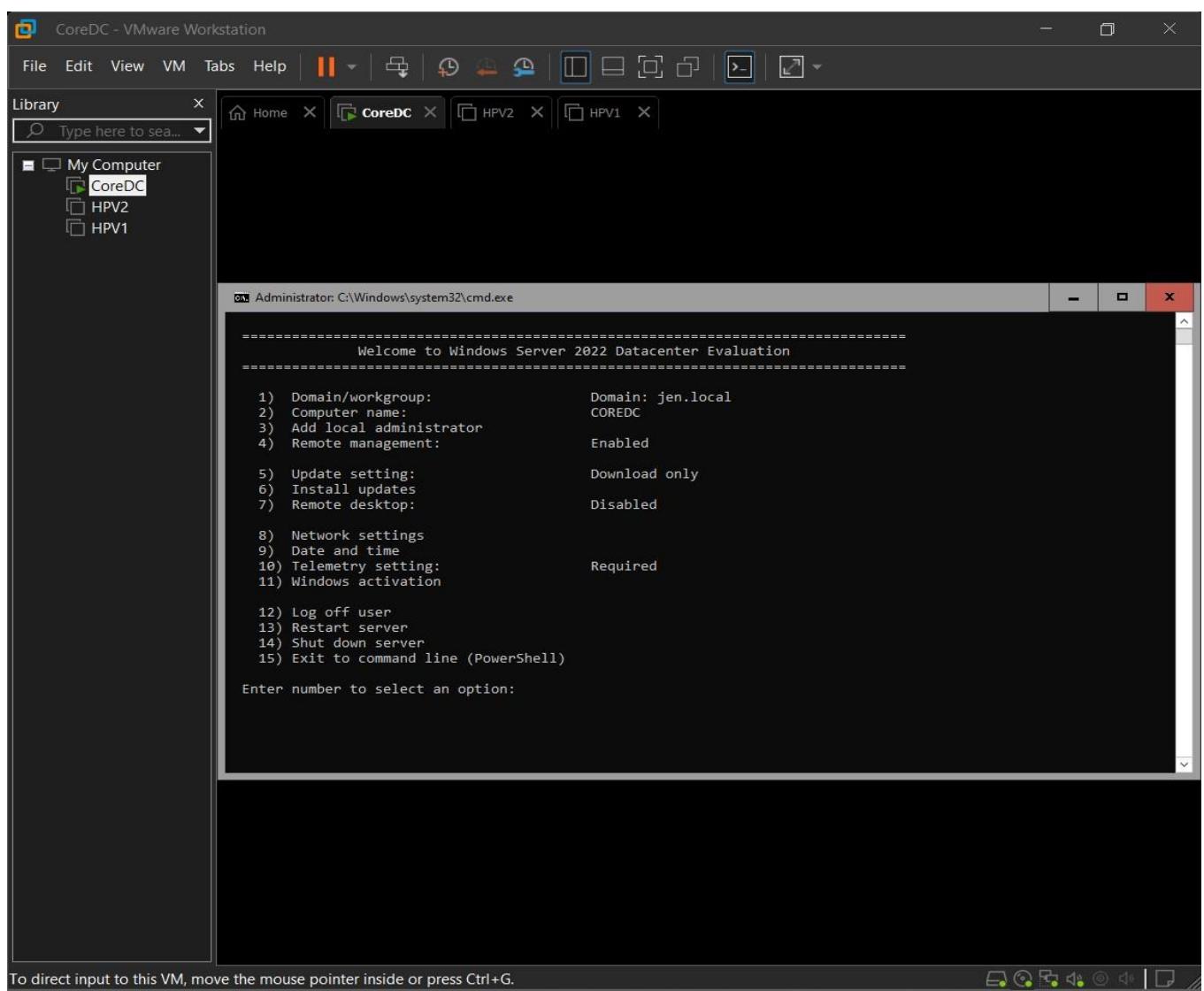


Figure 2Server Core Interface as Domain Controller

# Windows Server Security

---

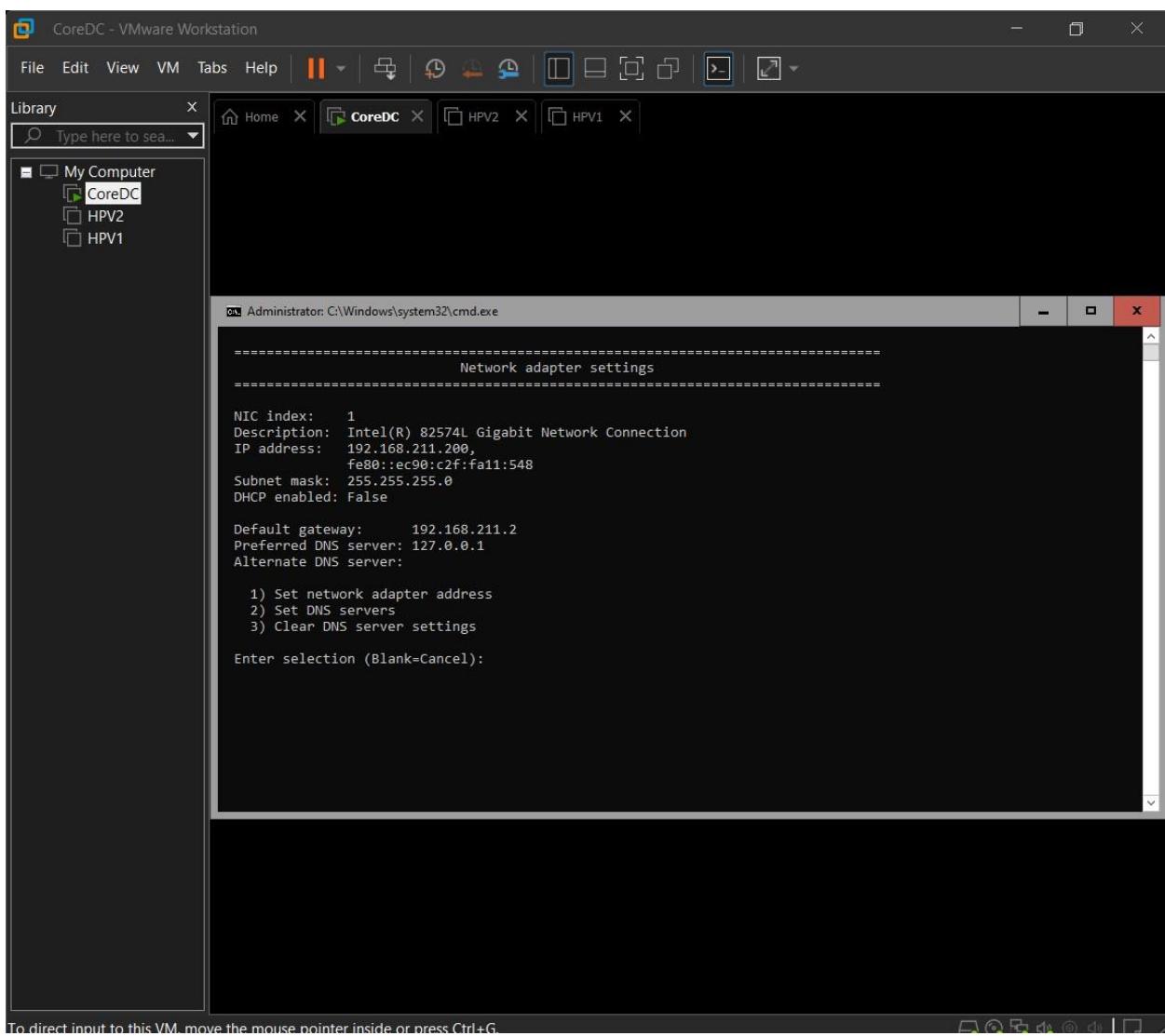
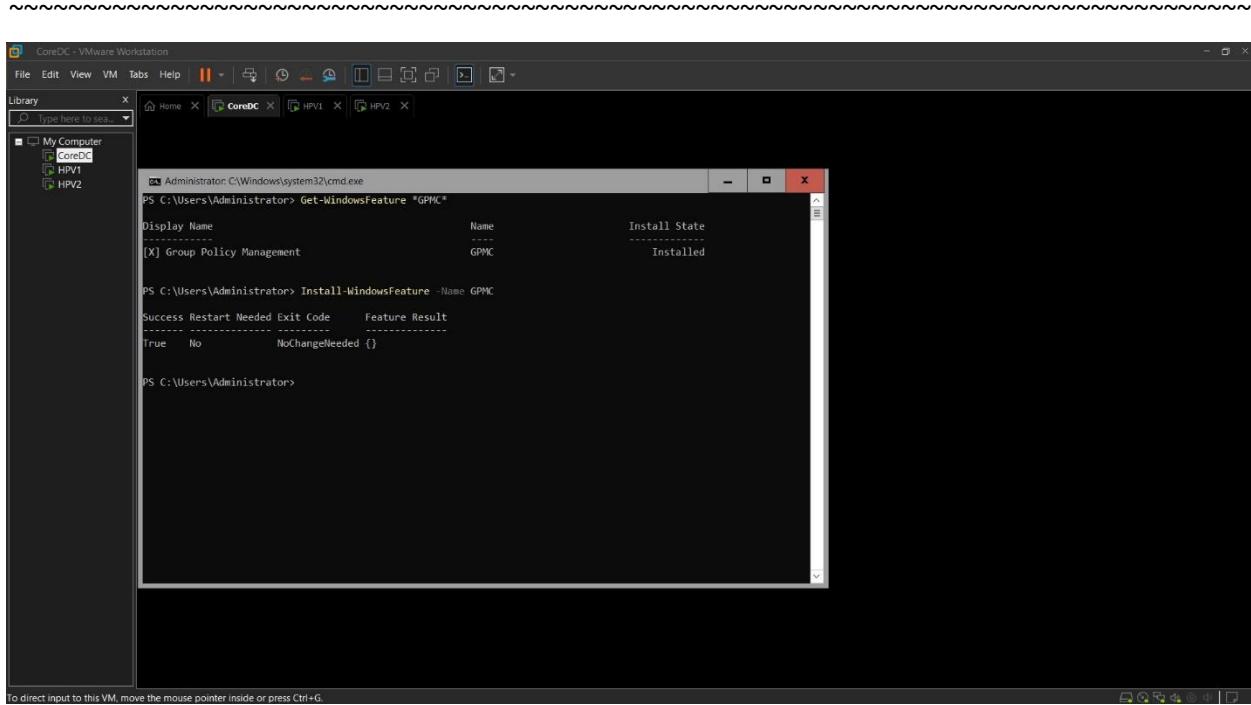


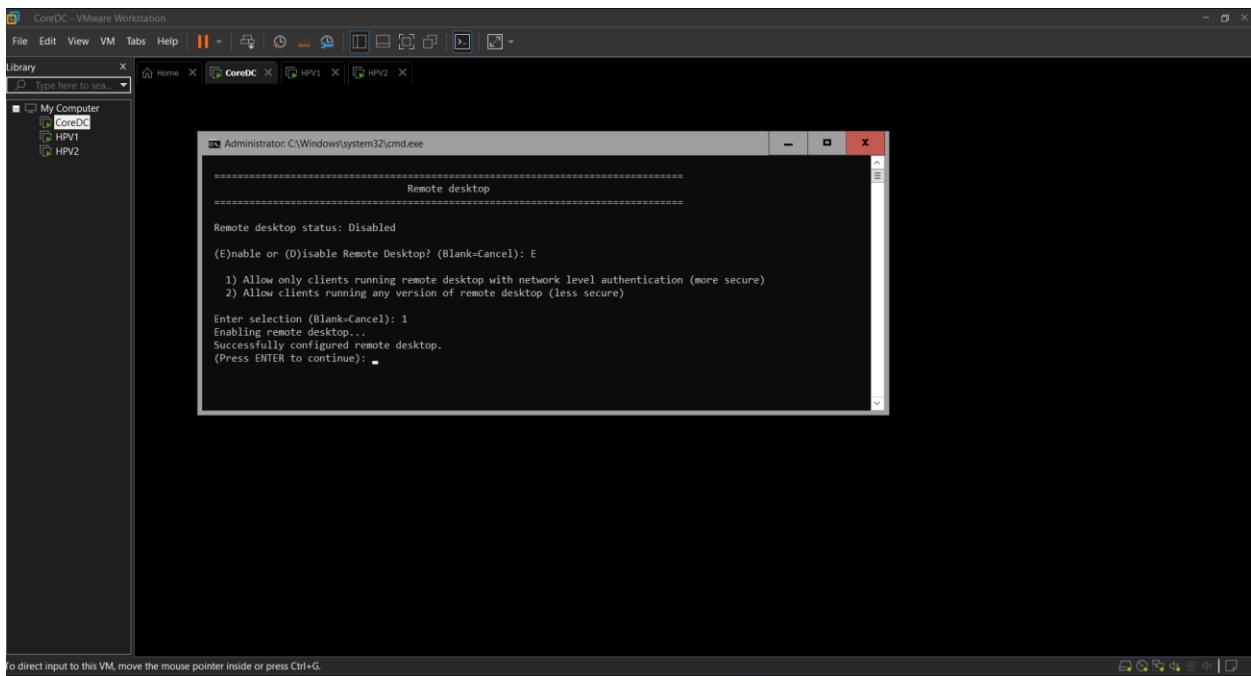
Figure 3 Network Configuration

# Windows Server Security



The screenshot shows a VMware Workstation window titled "CoreDC - VMware Workstation". Inside, a command prompt window is open under the "Administrator" account. The command "Get-WindowsFeature \*GPMC\*" is run, displaying a table with one row: "Group Policy Management" is listed with an "Install State" of "Installed". Another command, "Install-WindowsFeature -Name GPMC", is run, showing a success message with "Exit Code" 0 and "Feature Result" "NoChangeNeeded". The prompt then closes with "PS C:\Users\Administrator>".

Figure 4 Group Policy Management Console Installed



The screenshot shows a VMware Workstation window titled "CoreDC - VMware Workstation". Inside, a command prompt window is open under the "Administrator" account. The command "Set-Service -Name RemoteDesktop -Status Enabled" is run, followed by a confirmation step where the user selects option 1 ("Allow only clients running remote desktop with network level authentication (more secure)"). The command "Enter selection (Blank=Cancel): 1" is typed, followed by "Enabling remote desktop...". The final message "Successfully configured remote desktop. (Press ENTER to continue):" is displayed.

Figure 5 Enabled Remote Desktop

# Windows Server Security

Install and Configure a Group Policy Object and enforce Password change to 30 days

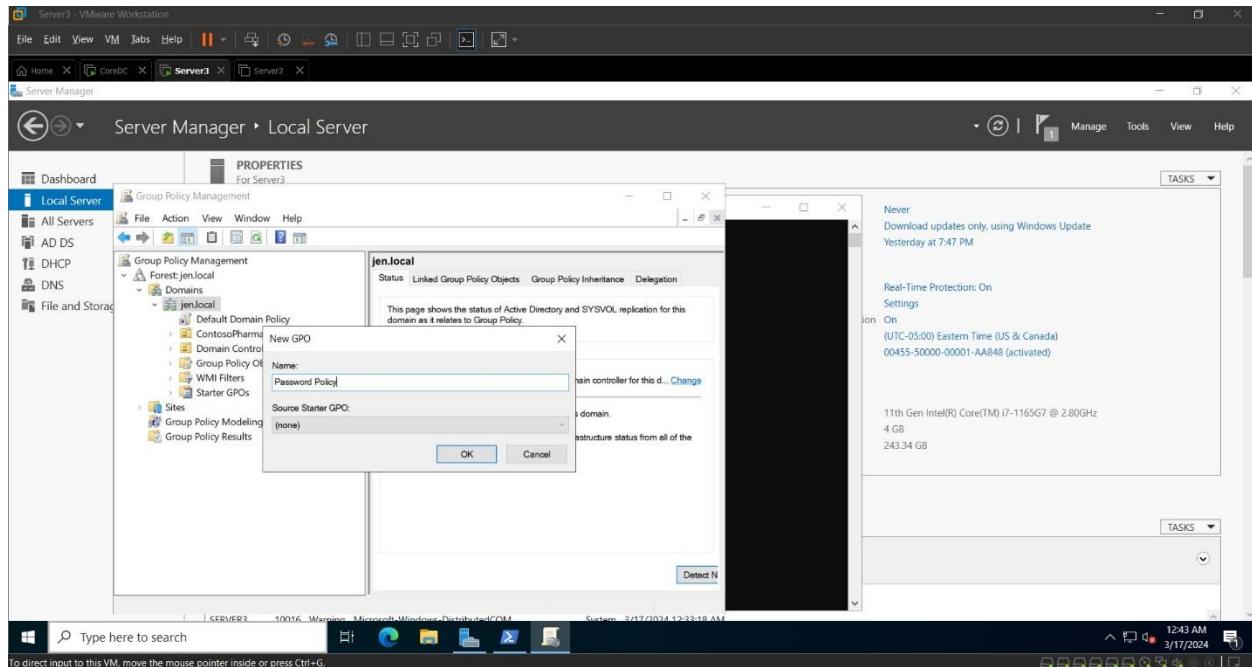


Figure 6: Created new Group Policy Object – Password Policy

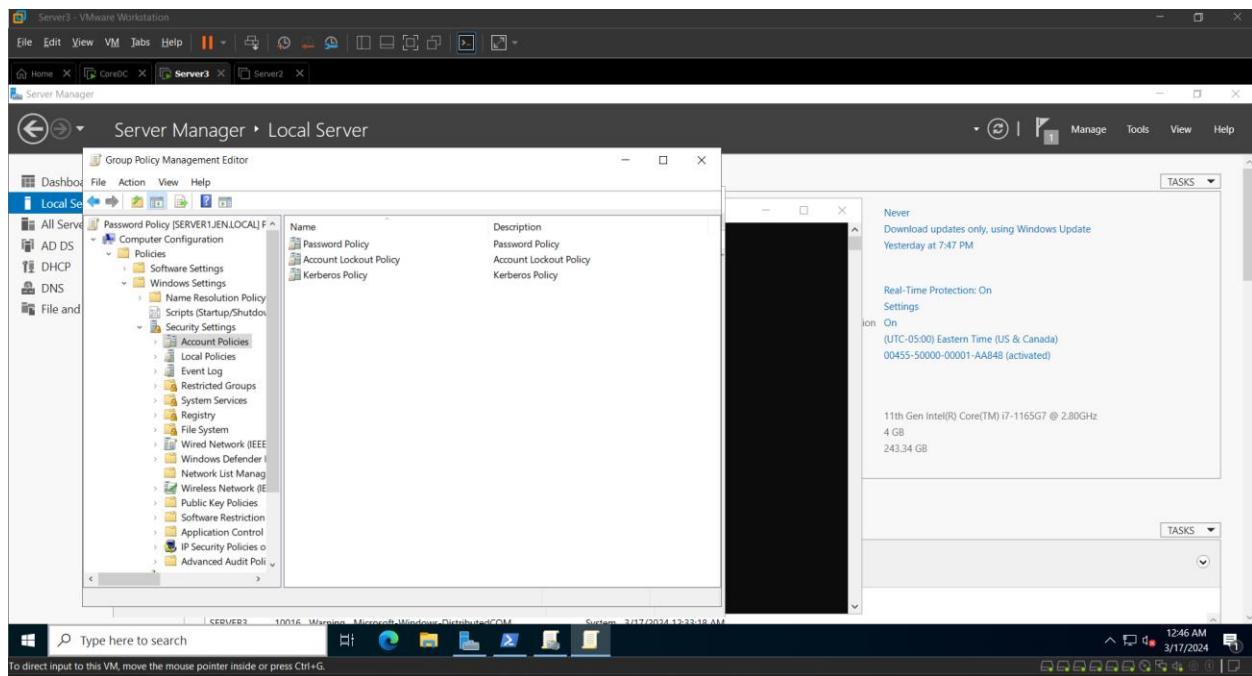


Figure 7 Edit Password Policy

# Windows Server Security

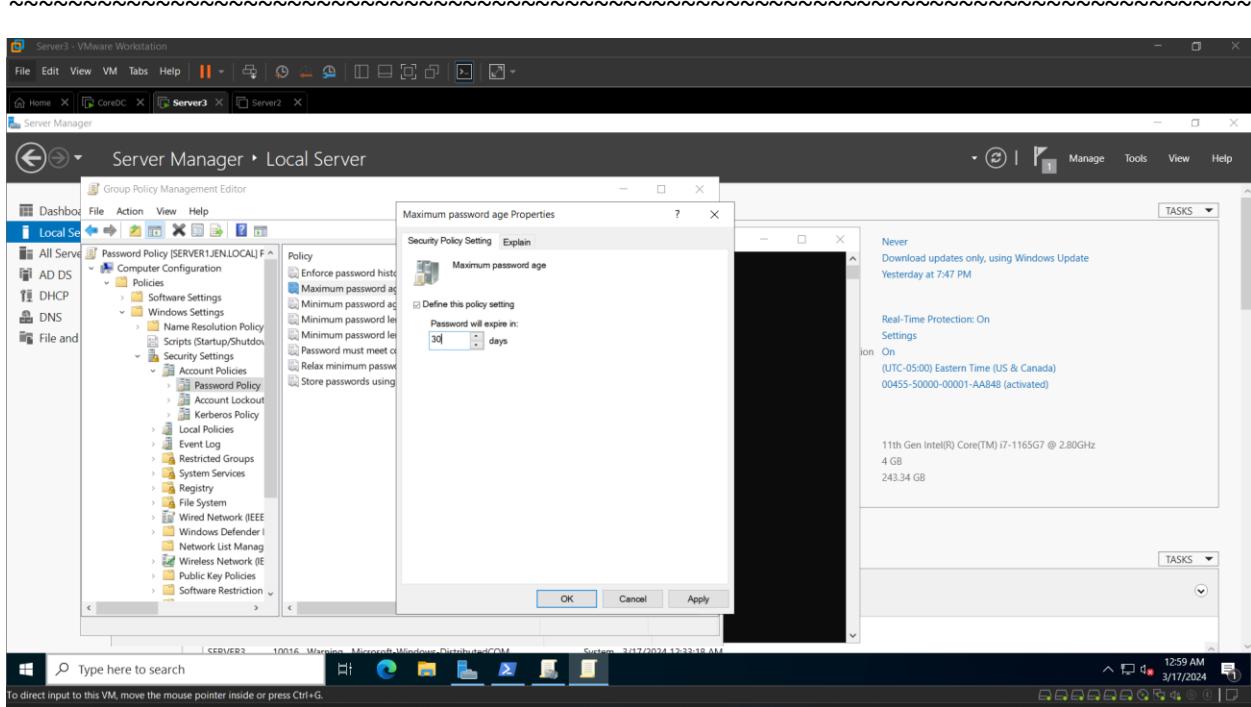


Figure 8 Edit Maximum password properties

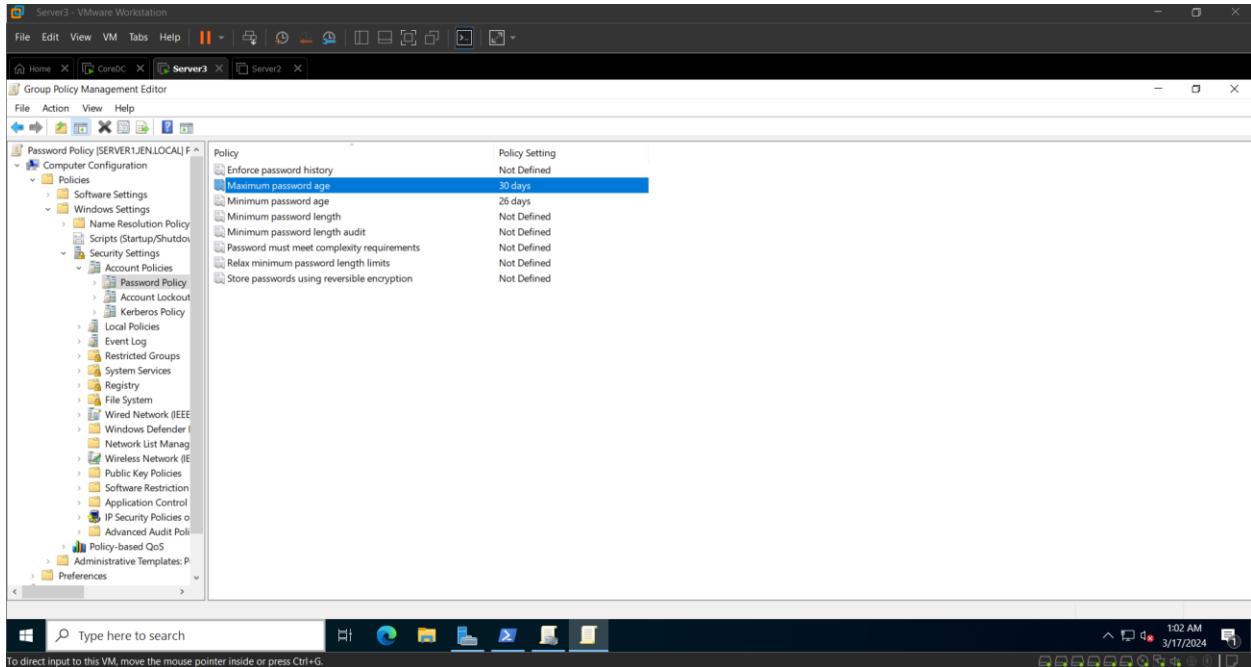
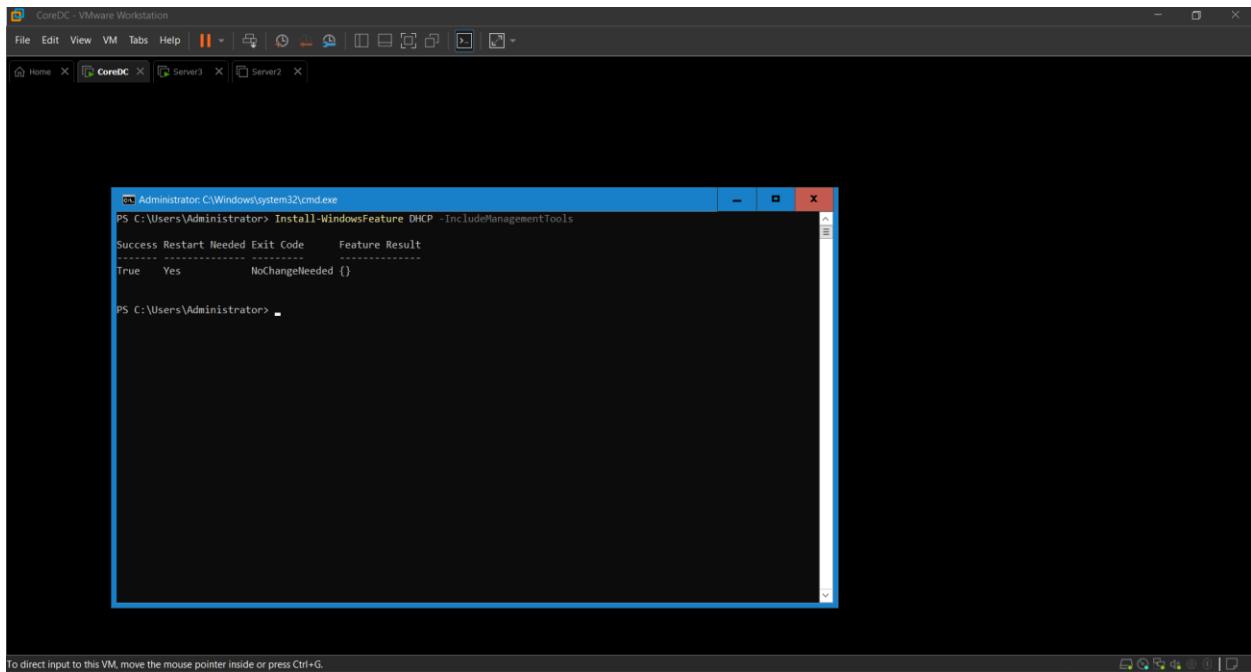


Figure 9 Maximum password age changed to 30 days

# Windows Server Security

---

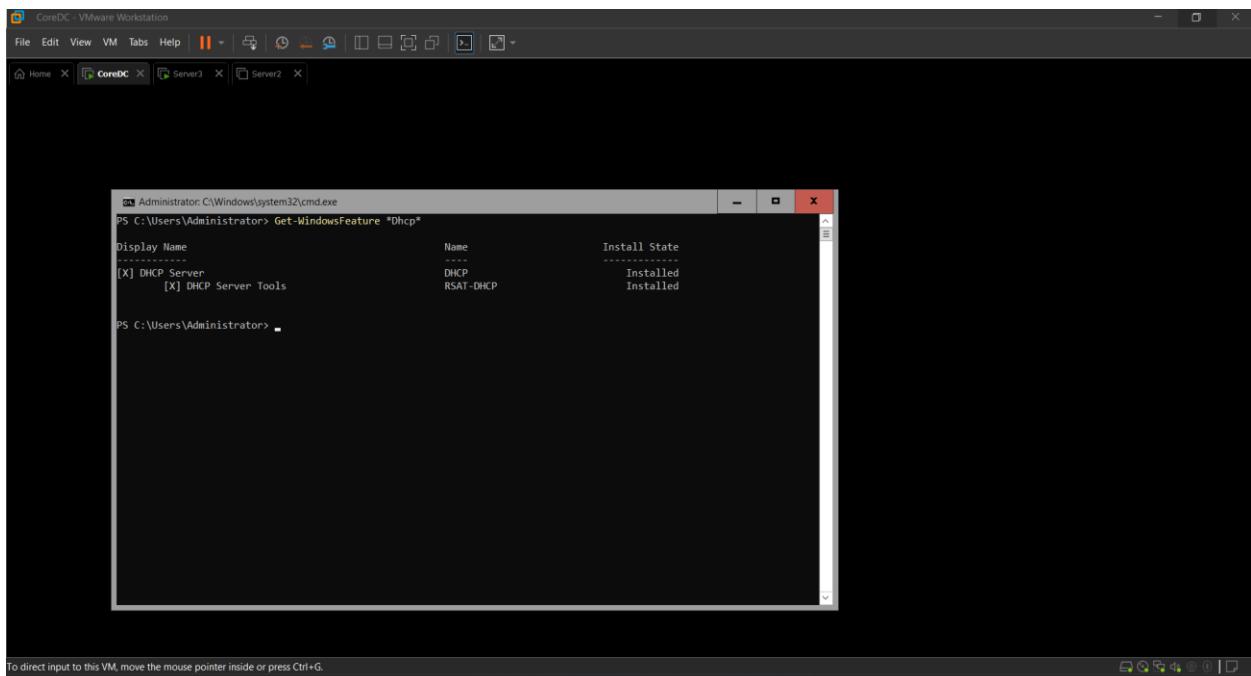
## Install DHCP Server



```
Administrator: C:\Windows\system32\cmd.exe
PS C:\Users\Administrator> Install-WindowsFeature DHCP -IncludeManagementTools
Success Restart Needed Exit Code Feature Result
----- ----- ----- -----
True Yes NoChangeNeeded {}

PS C:\Users\Administrator>
```

Figure 10: Installed DHCP Server



```
Administrator: C:\Windows\system32\cmd.exe
PS C:\Users\Administrator> Get-WindowsFeature *Dhcp*
Display Name           Name          Install State
----- -----
[X] DHCP Server        DHCP         Installed
[X] DHCP Server Tools  RSAT-DHCP   Installed

PS C:\Users\Administrator>
```

Figure 11DHCP Installed

# Windows Server Security

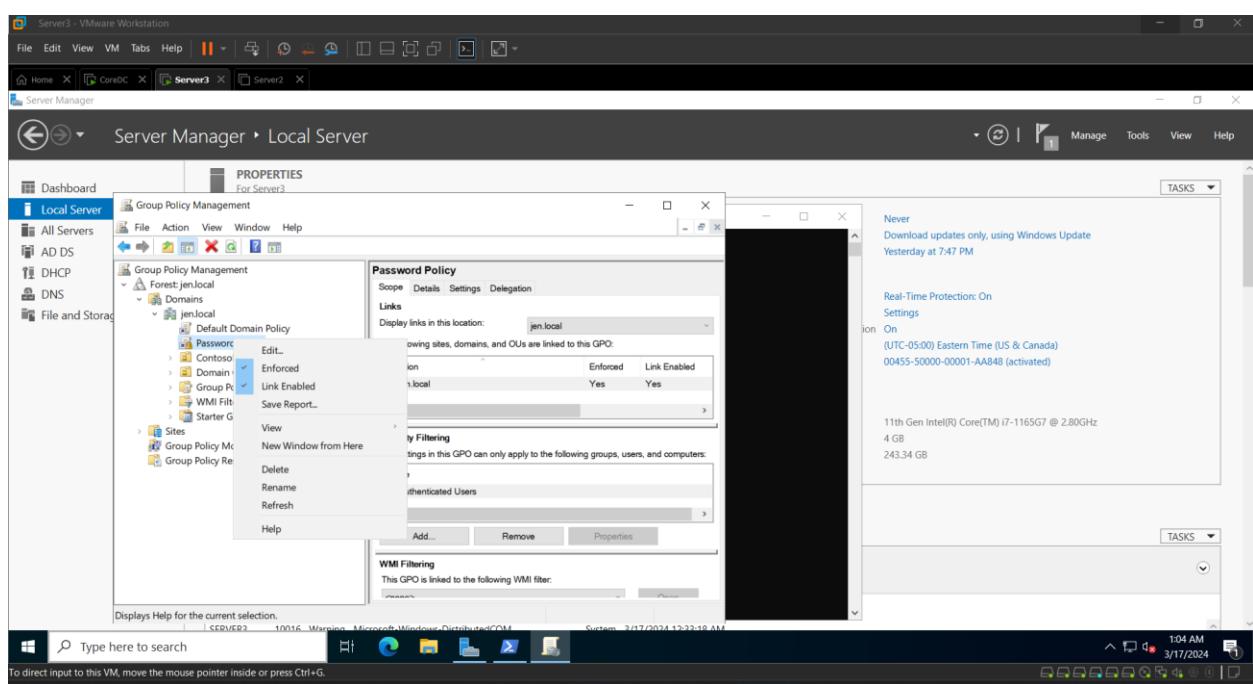


Figure 12 Password Policy Link Enabled and Enforced

## Install and Configure DHCP and DHCP Scope

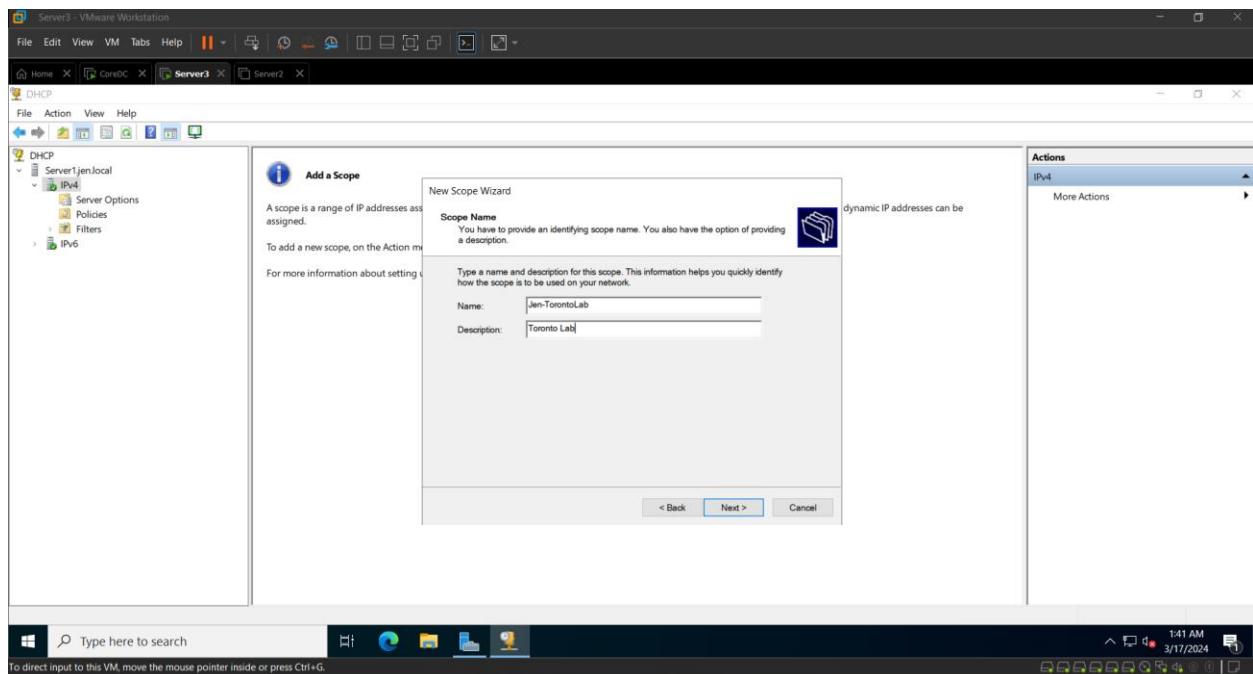


Figure 13 Configure Scope for Jen-TorontoLab

# Windows Server Security

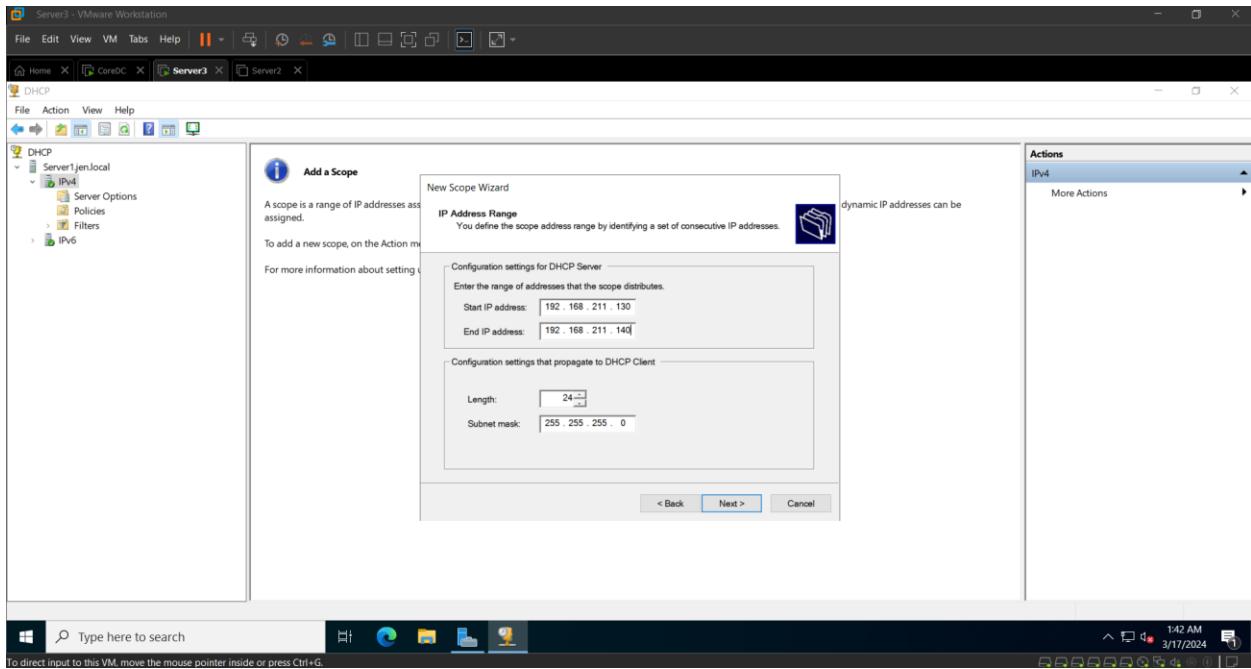


Figure 14 IP StartRange and EndRange for Jen-TorontoLab

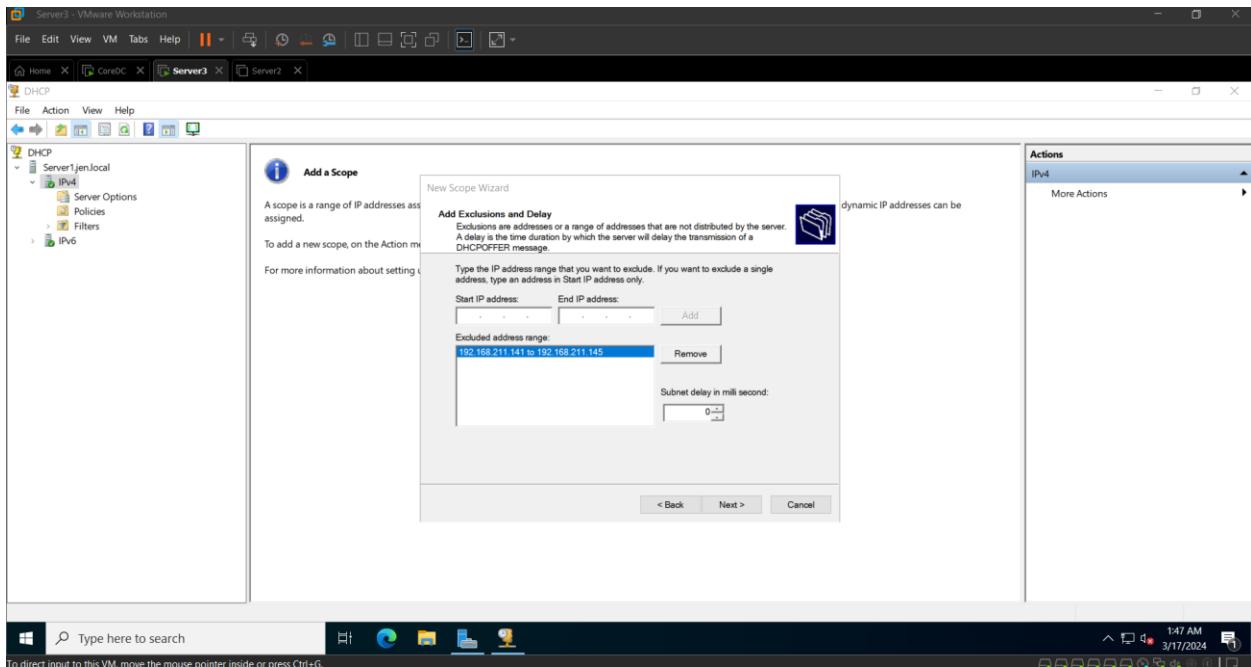


Figure 15: Excluded IP Address ranges Jen-TorontoLab

# Windows Server Security

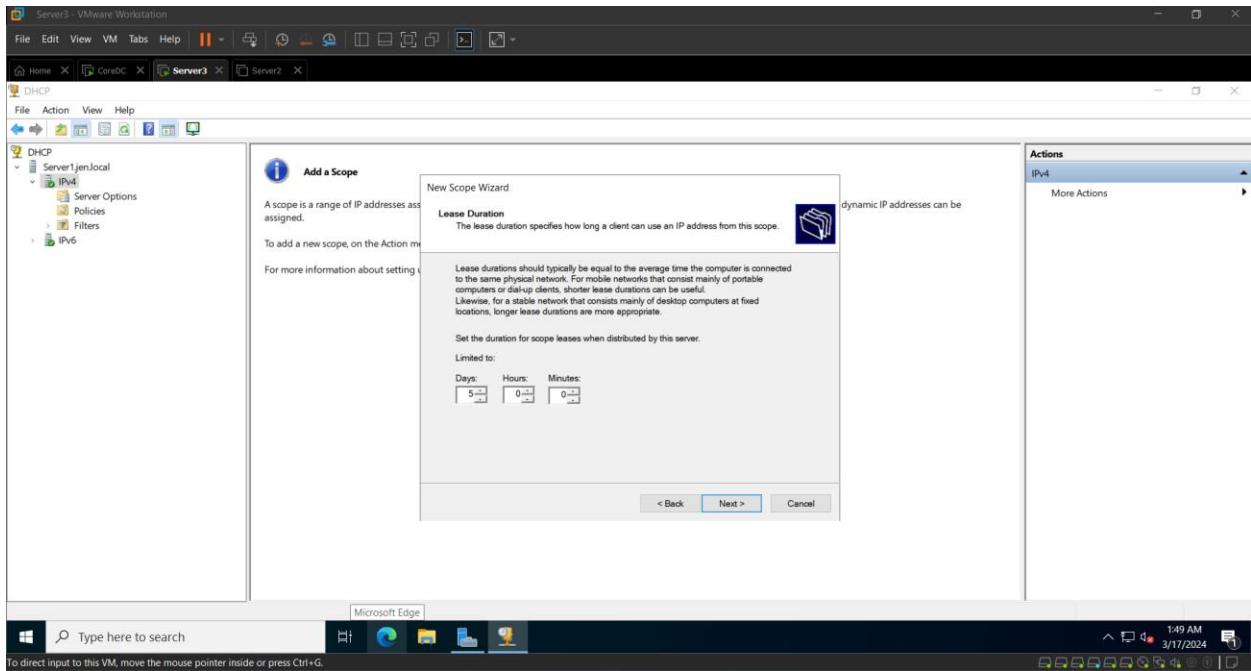


Figure 16: Lease period configured for 5 days

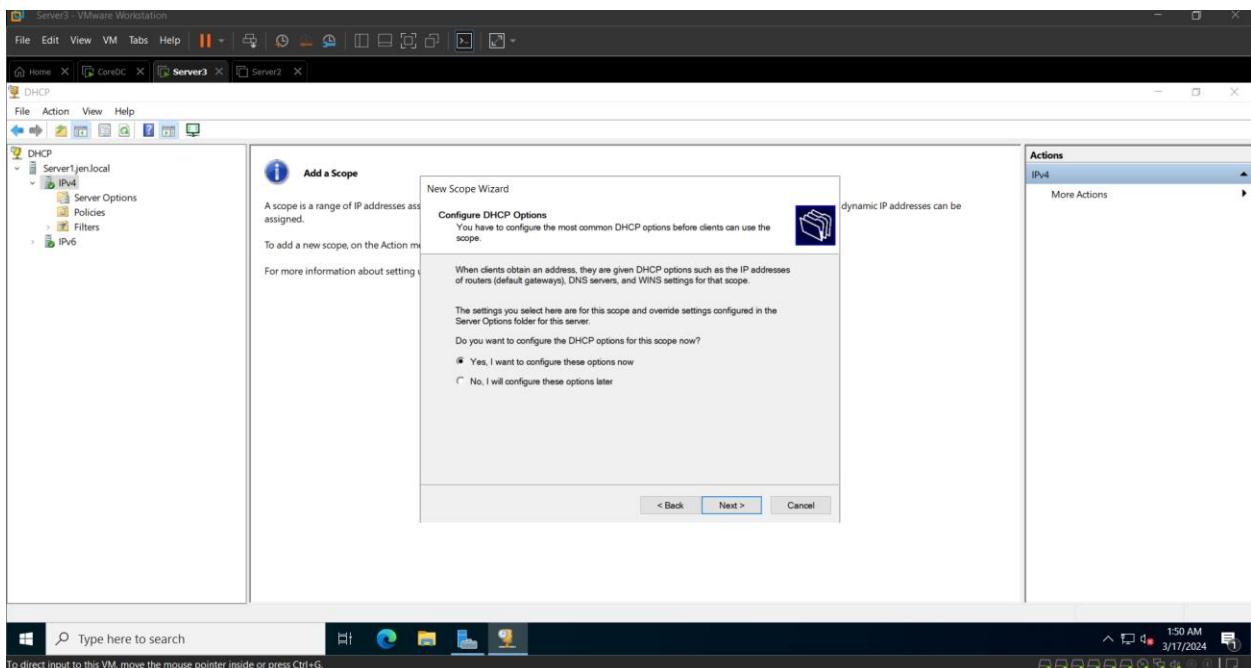


Figure 17: Configuration Time line

# Windows Server Security

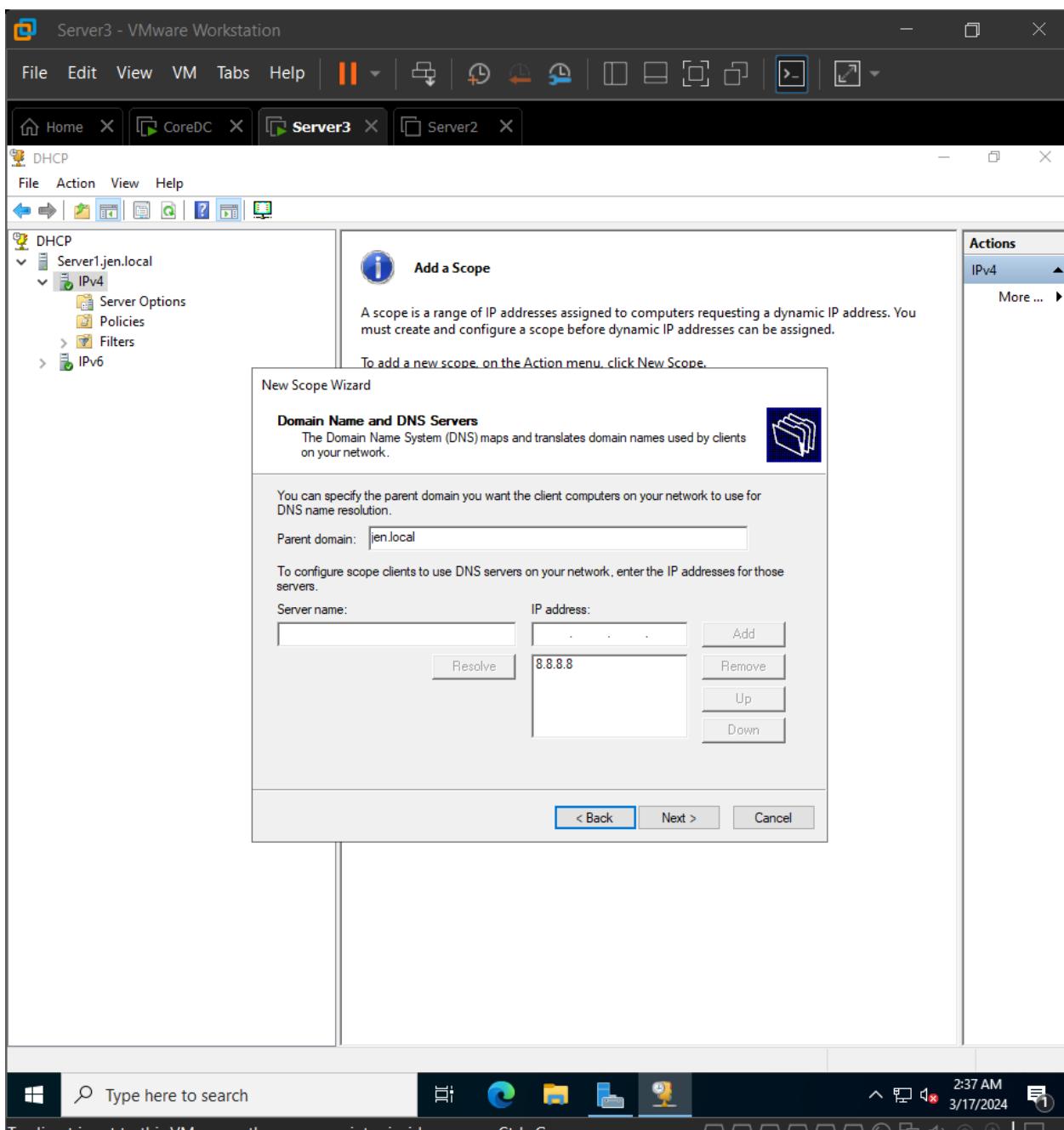


Figure 18: Domain Name and DNS Servers

# Windows Server Security

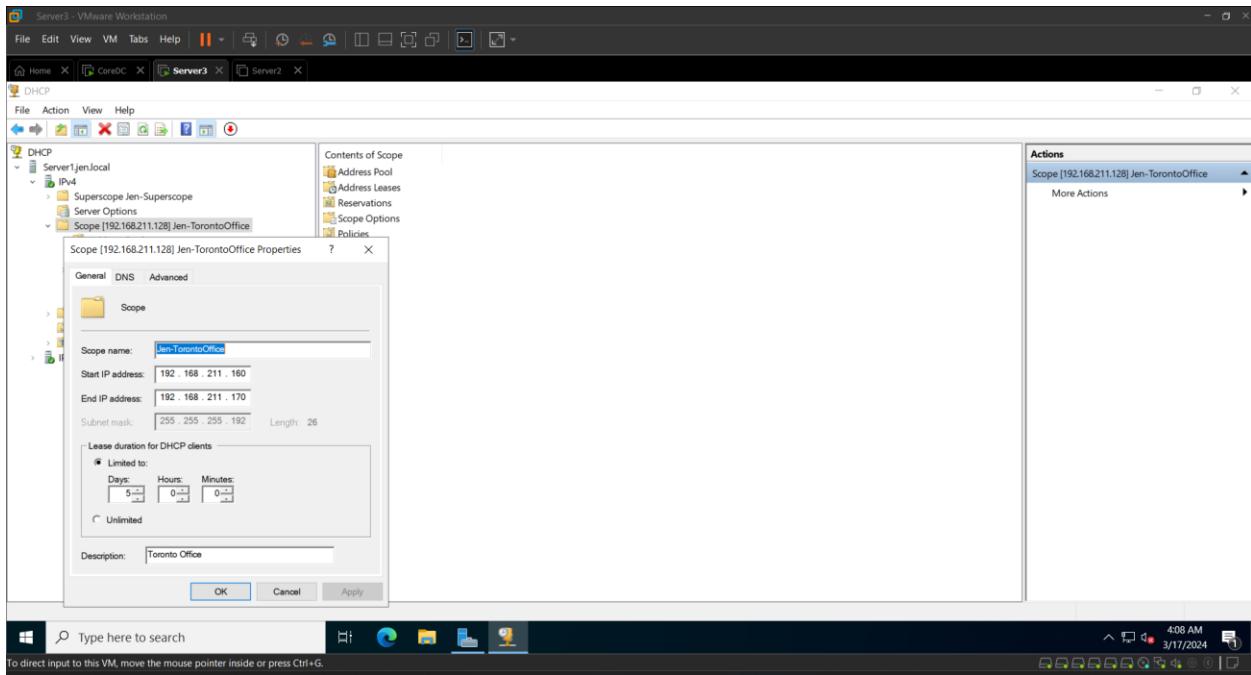


Figure 19: Jen-Toronto Office

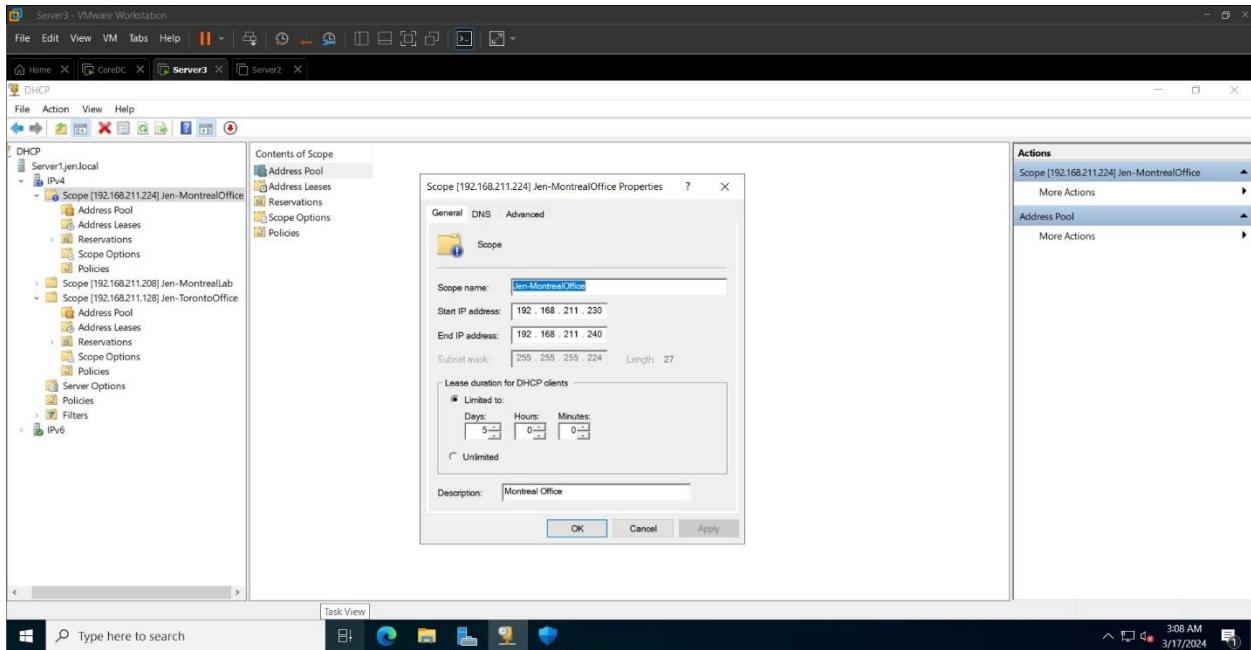


Figure 20: Jen-Montreal Office

# Windows Server Security

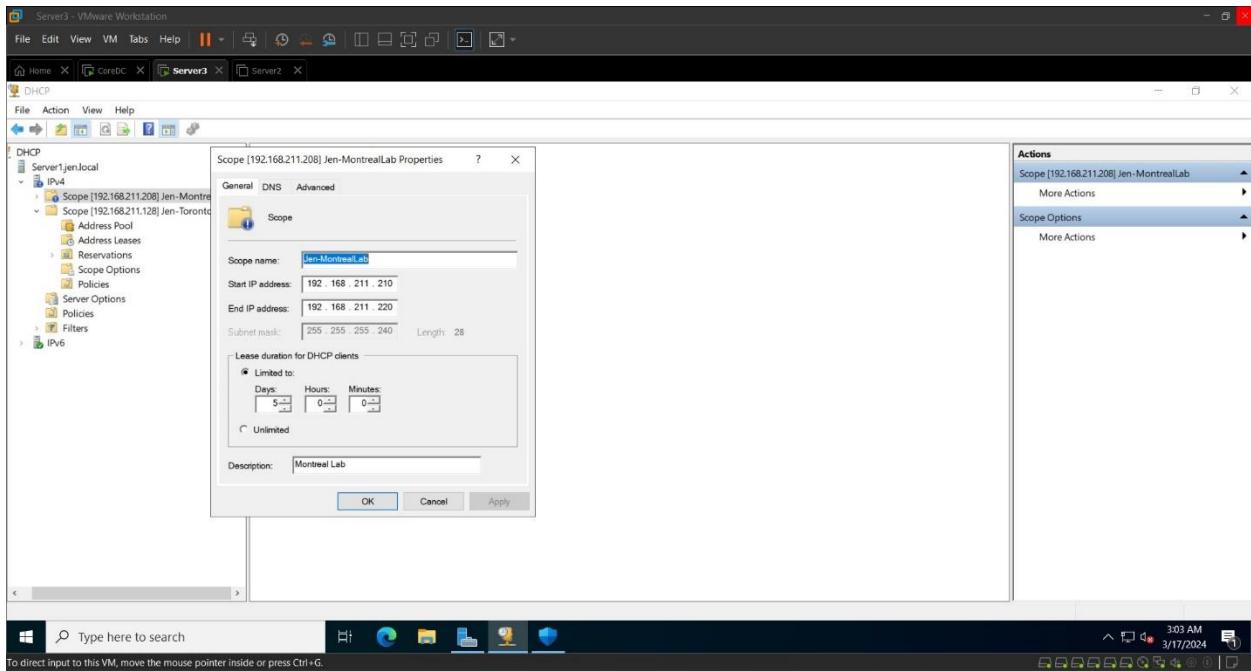


Figure 21: Jen-MontrealLab

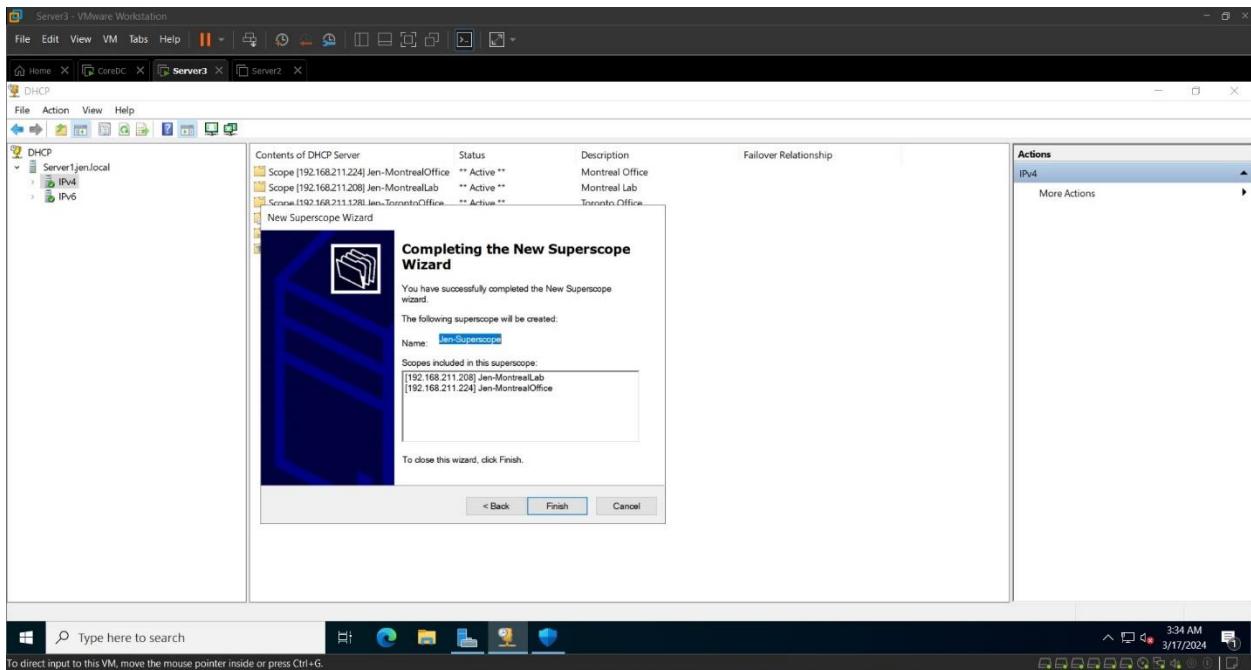


Figure 22: Jen-Superscope-Montreal

# Windows Server Security

---

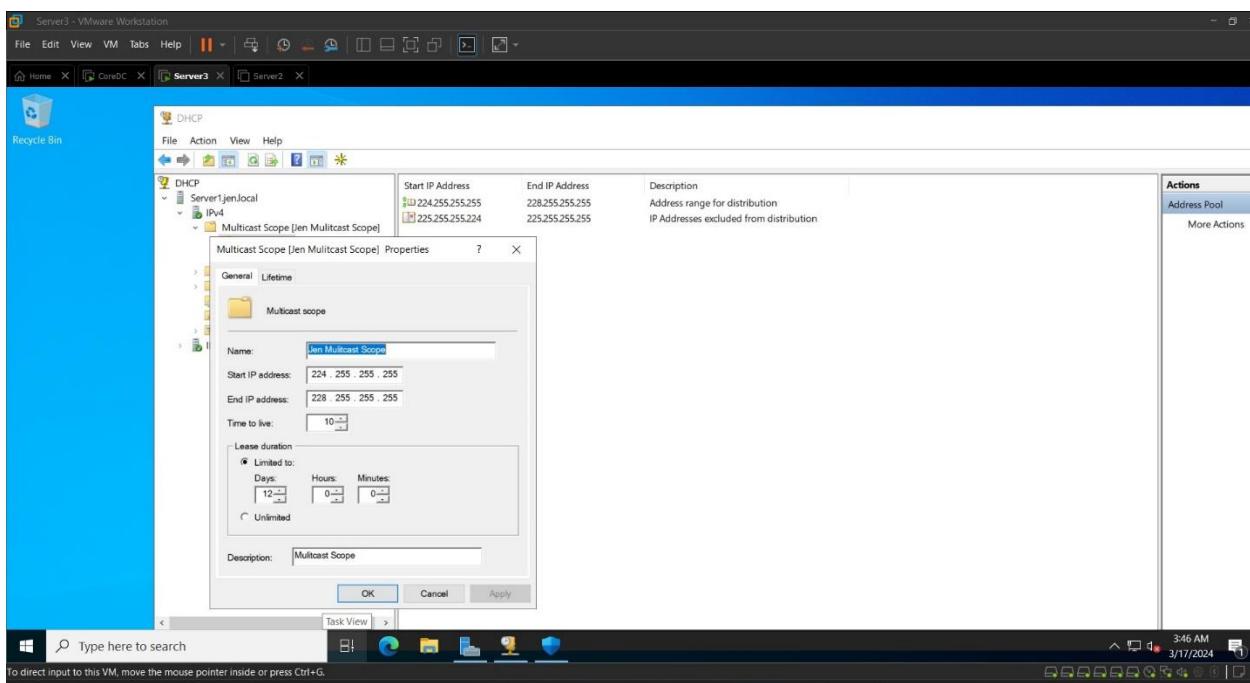


Figure 23: Multiscope

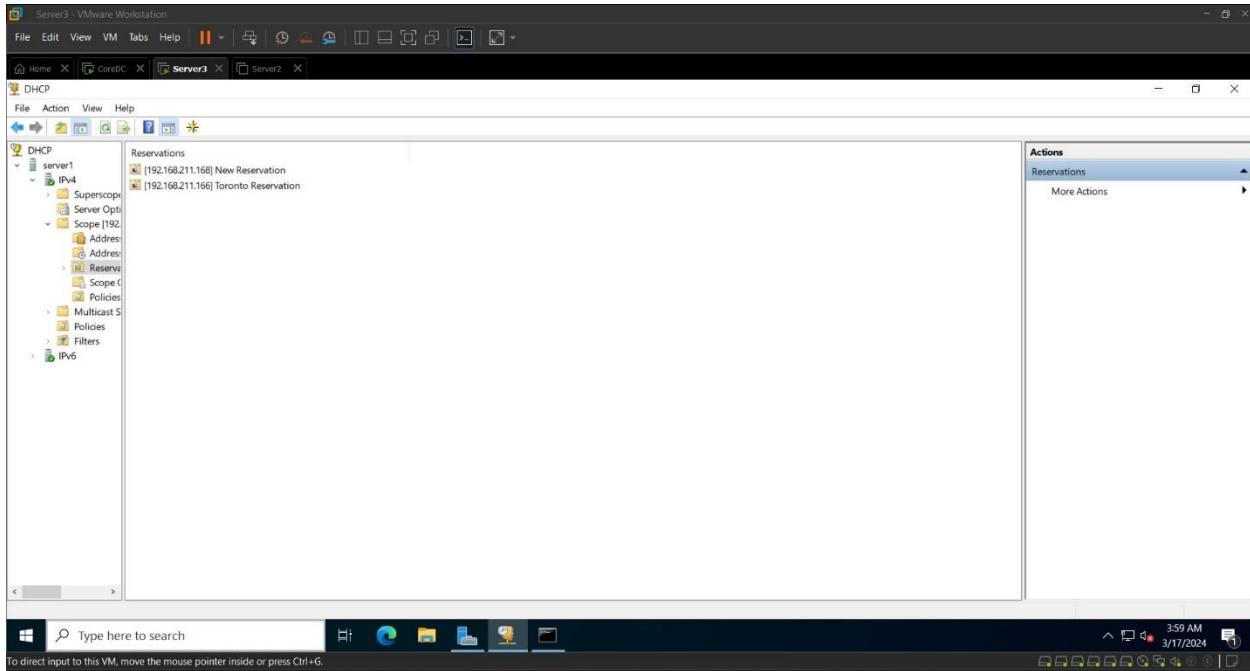


Figure 24 Reservation

# Windows Server Security

---

## Domain DNS Server and forwarder

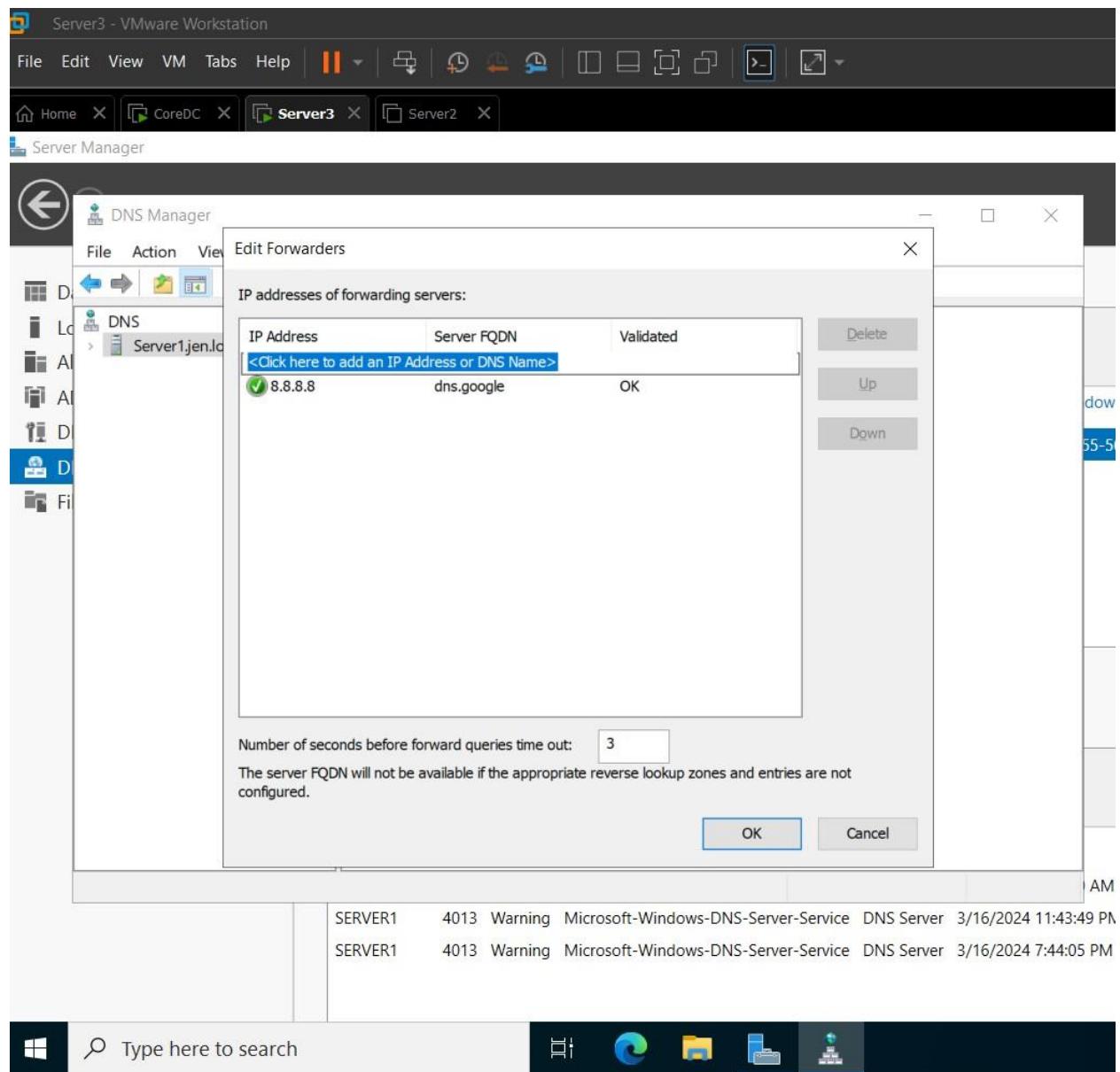


Figure 25: DNS Forwarder to 8.8.8.8

# Windows Server Security

## Storage Pool and vDisk

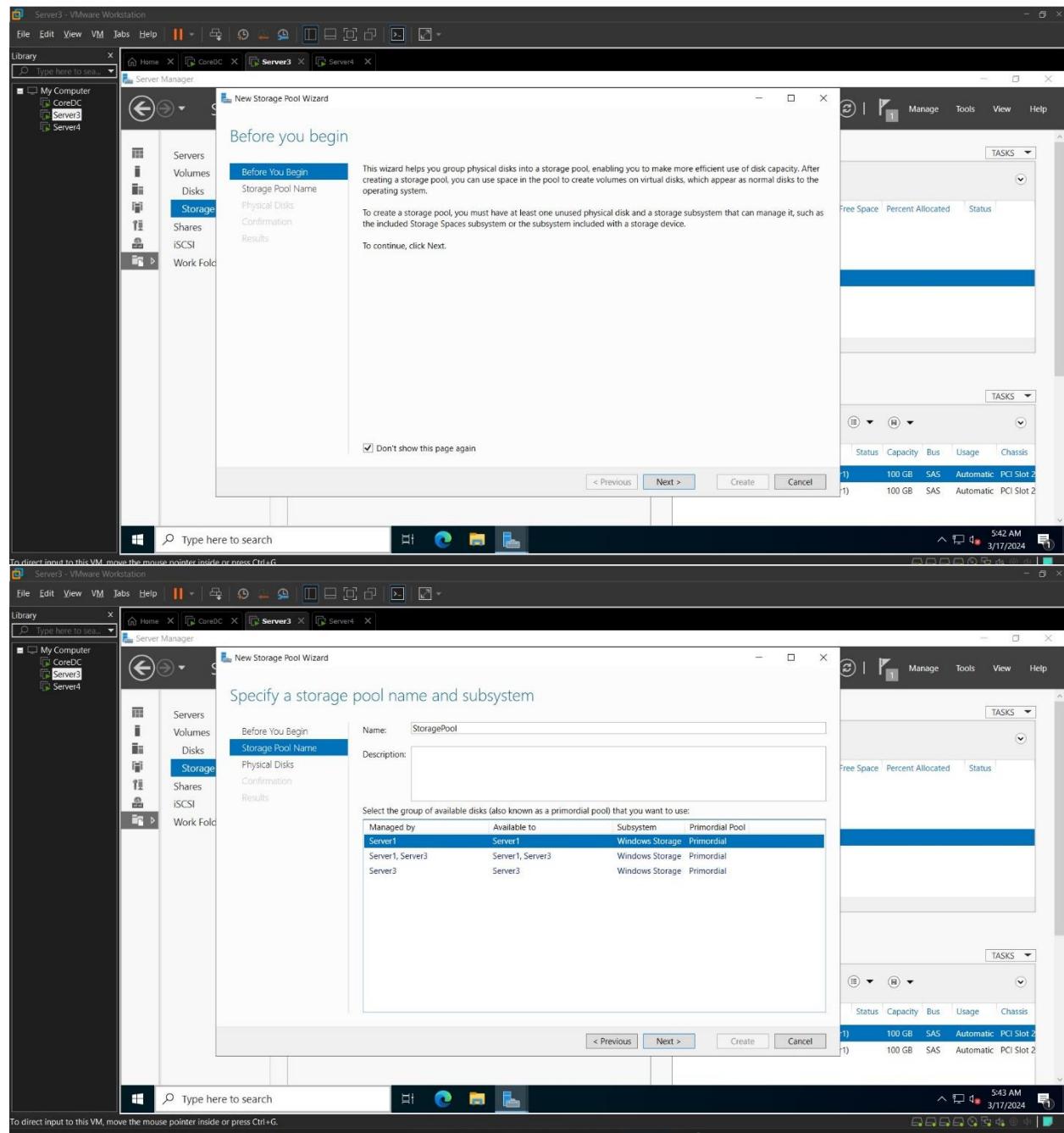
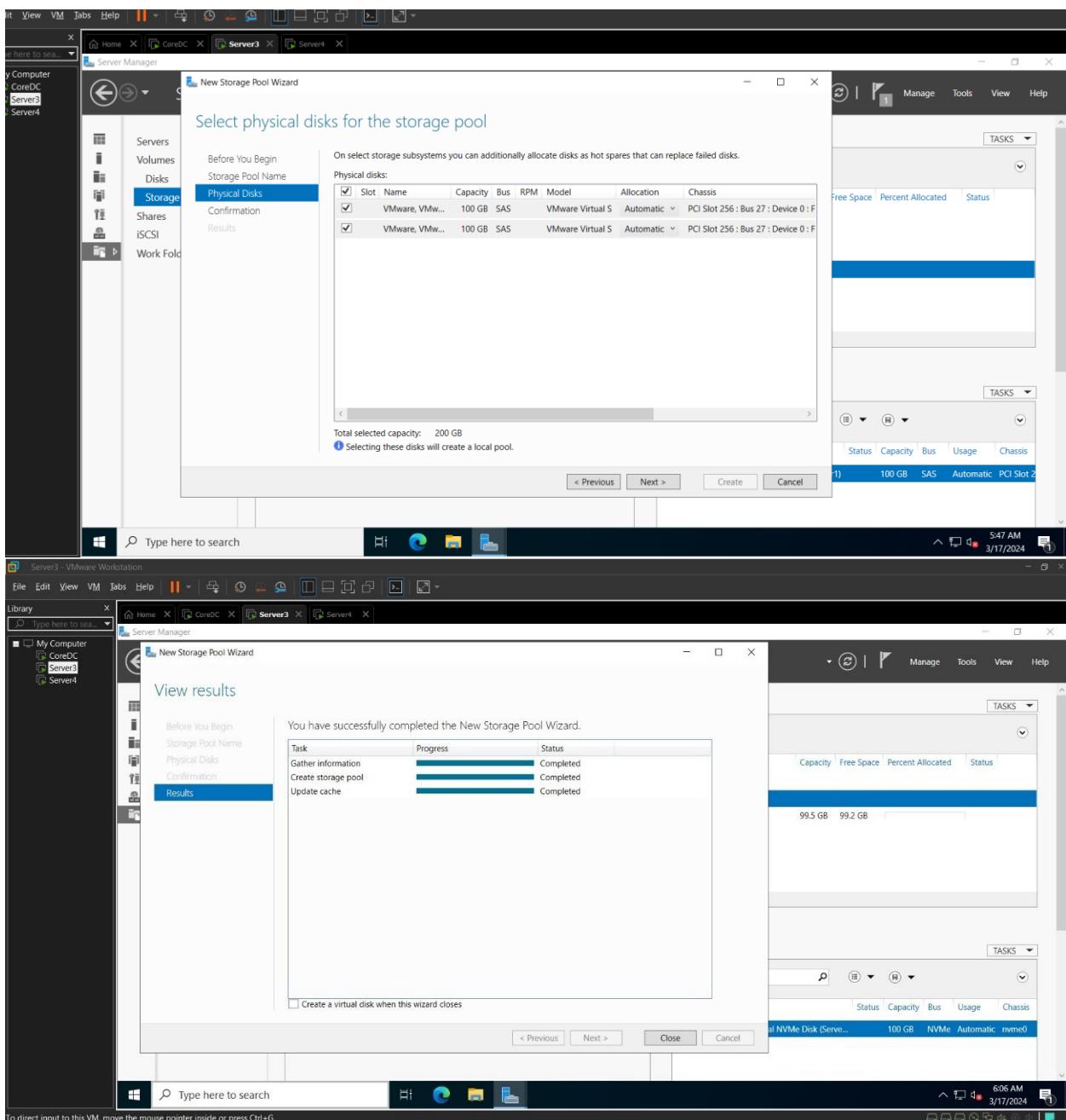


Figure 26: Configuring storage on Local Server

# Windows Server Security



# Windows Server Security

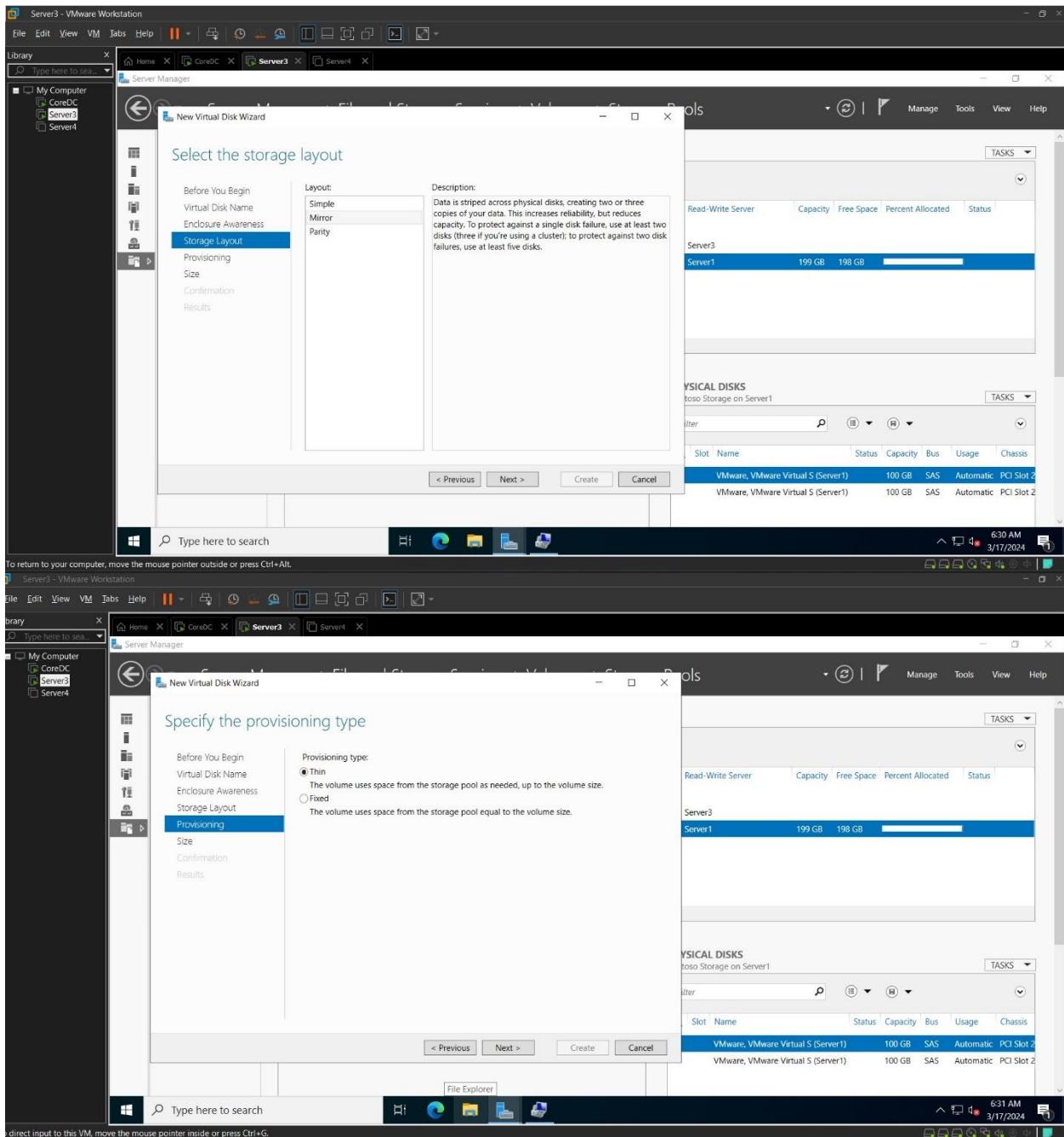
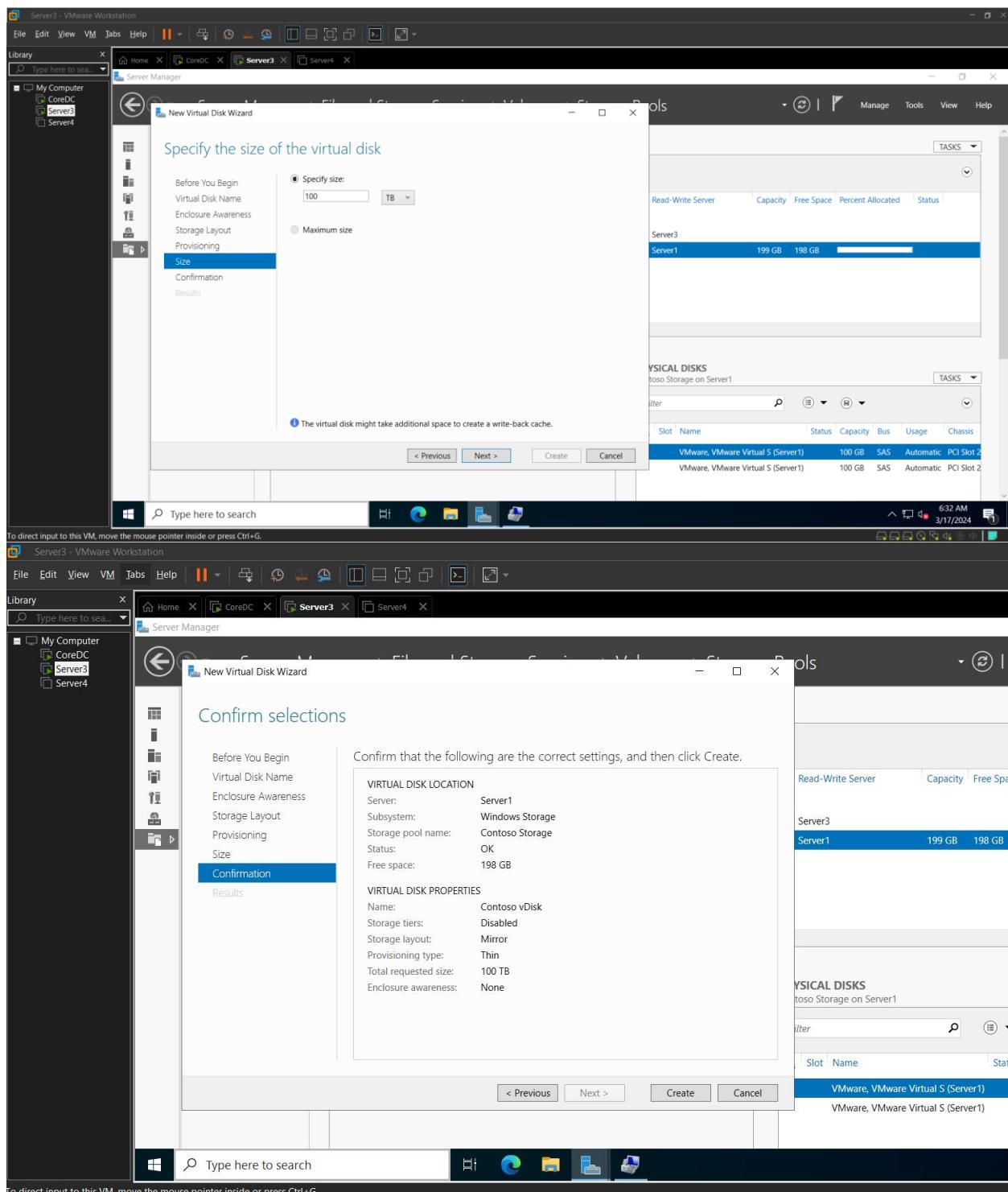


Figure 27: Configuring a Dynamic Storage for high availability

# Windows Server Security



# Windows Server Security

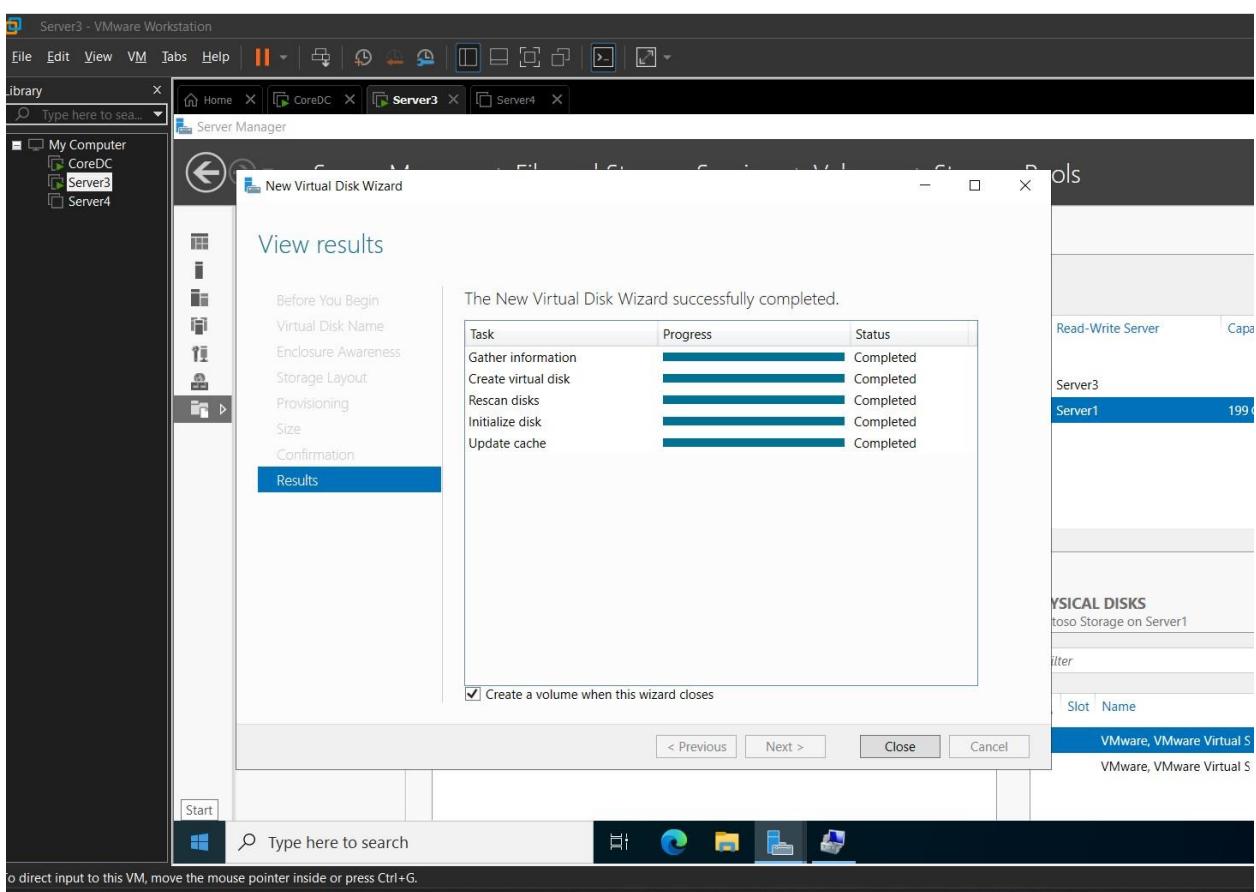
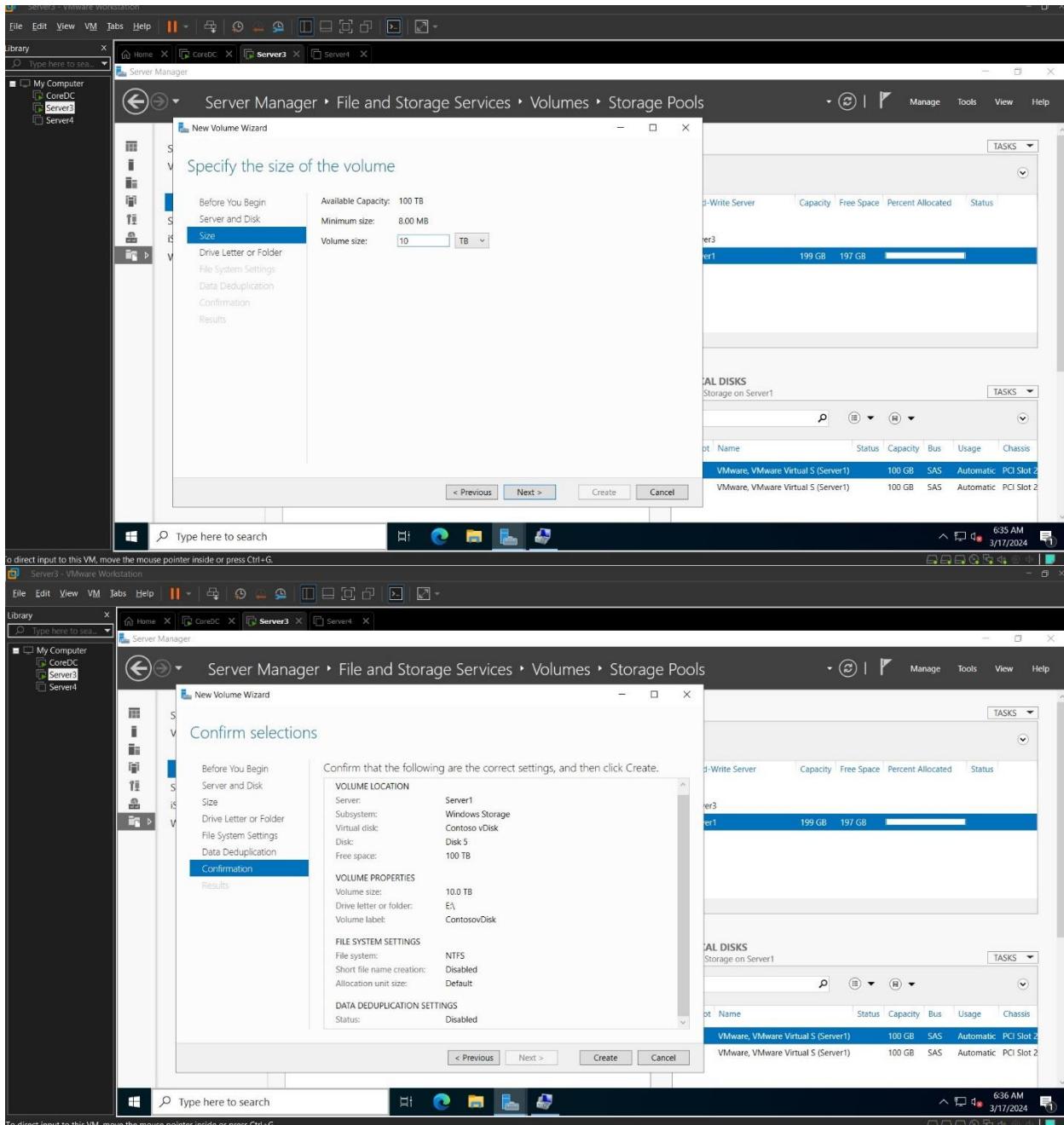


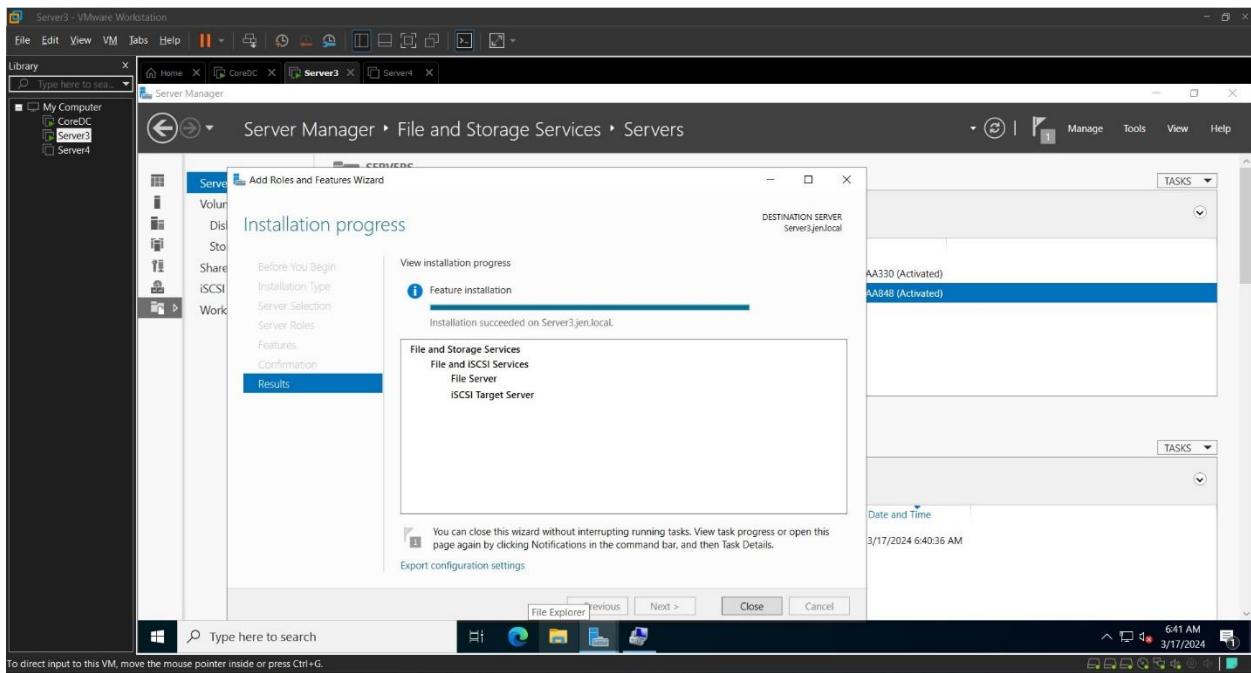
Figure 28: Creating a Virtual Disk

# Windows Server Security



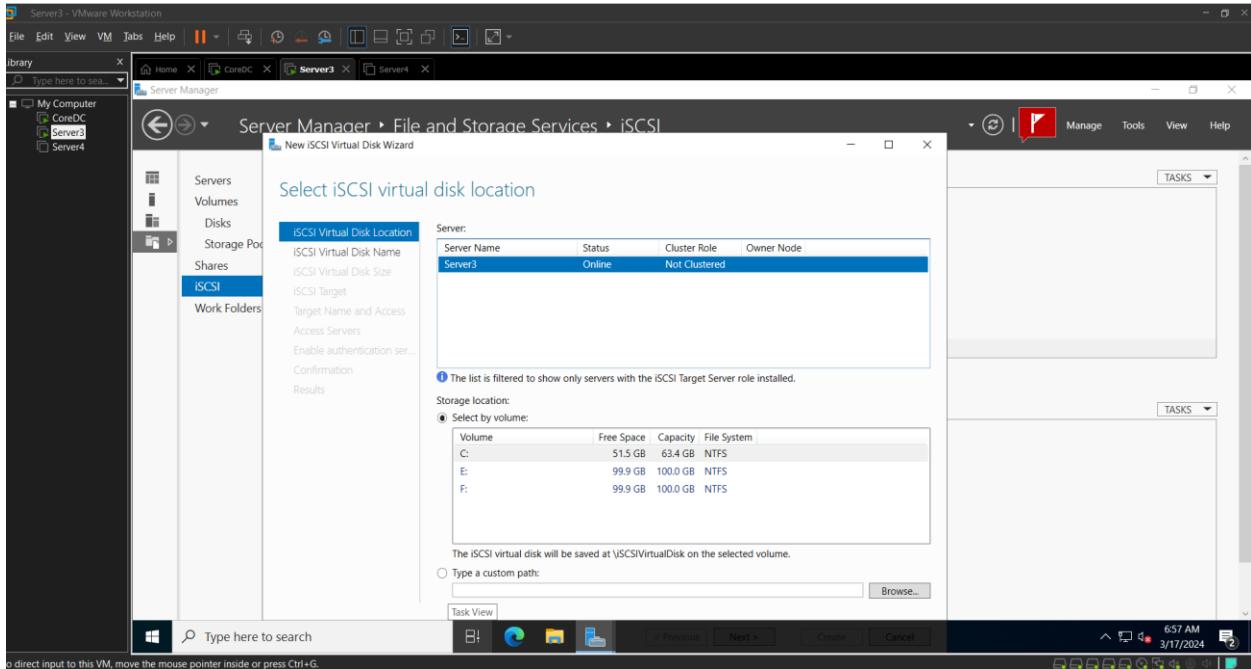
# Windows Server Security

Create and Configure iSCSI on Server 2 and Attach to Server 3 (In my case it was Server 3 and Server 4)

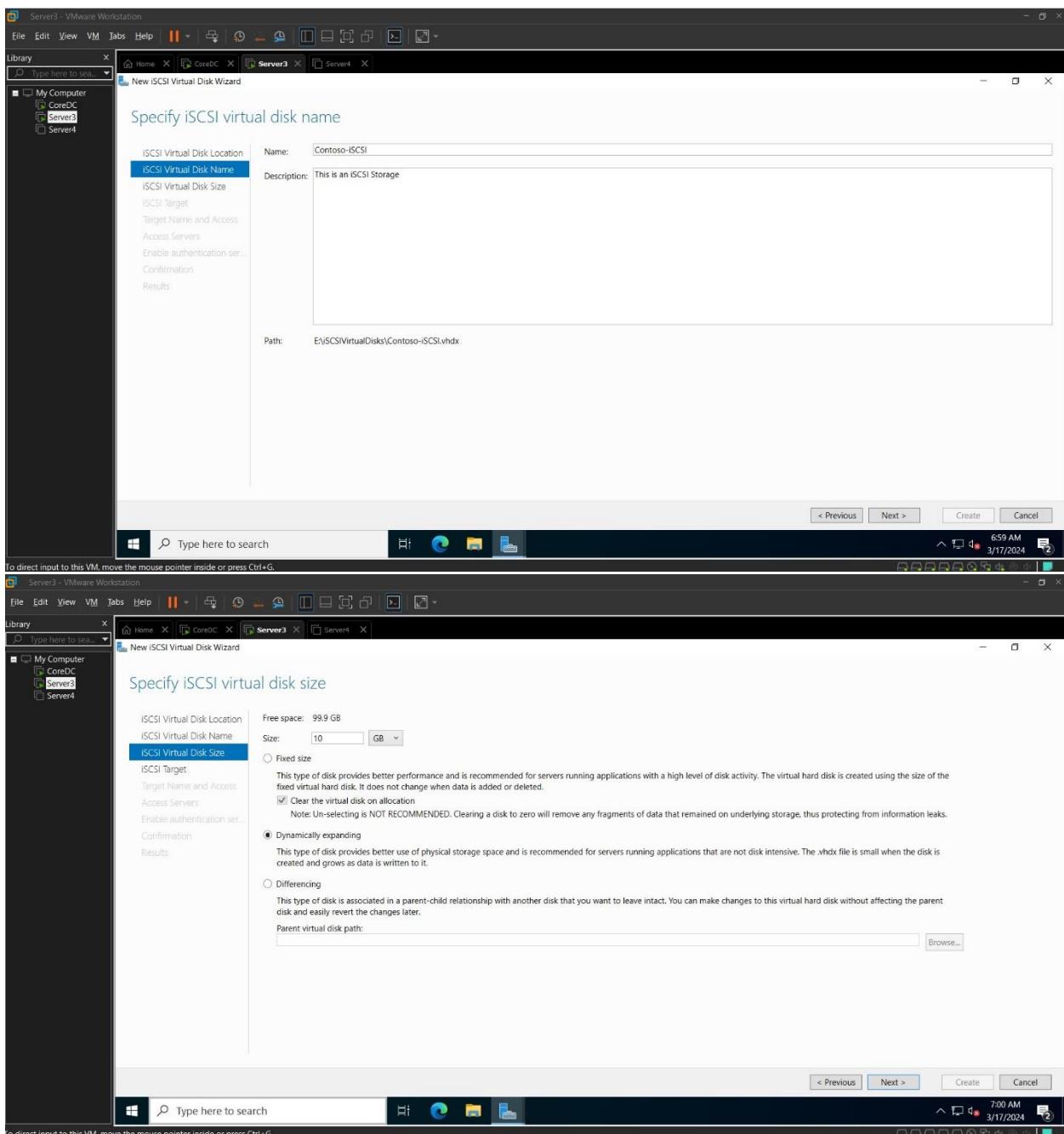


*Figure 29: Install File and iSCSI Server*

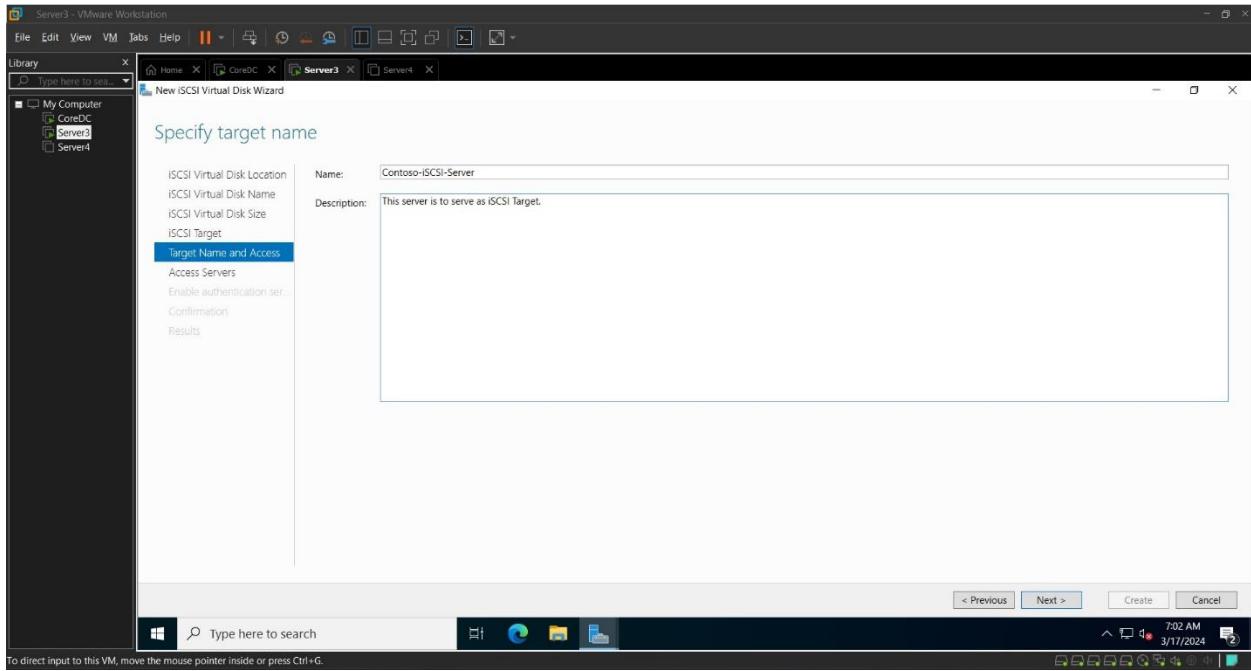
## Follow through with wizard prompt



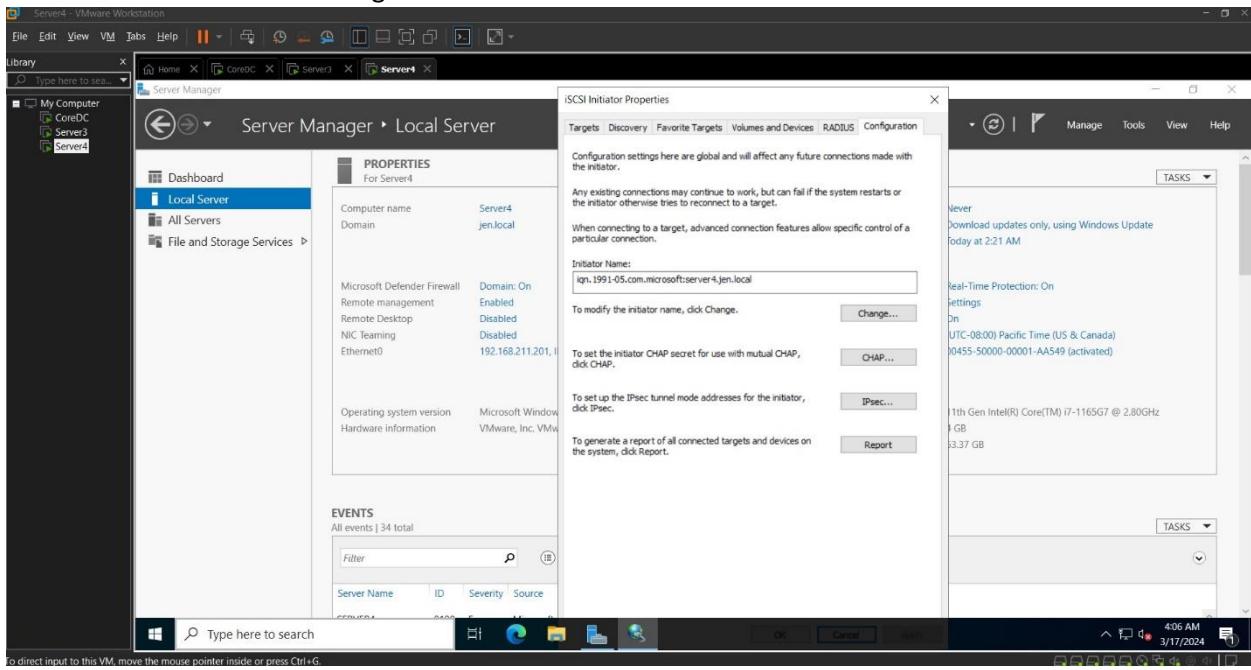
# Windows Server Security



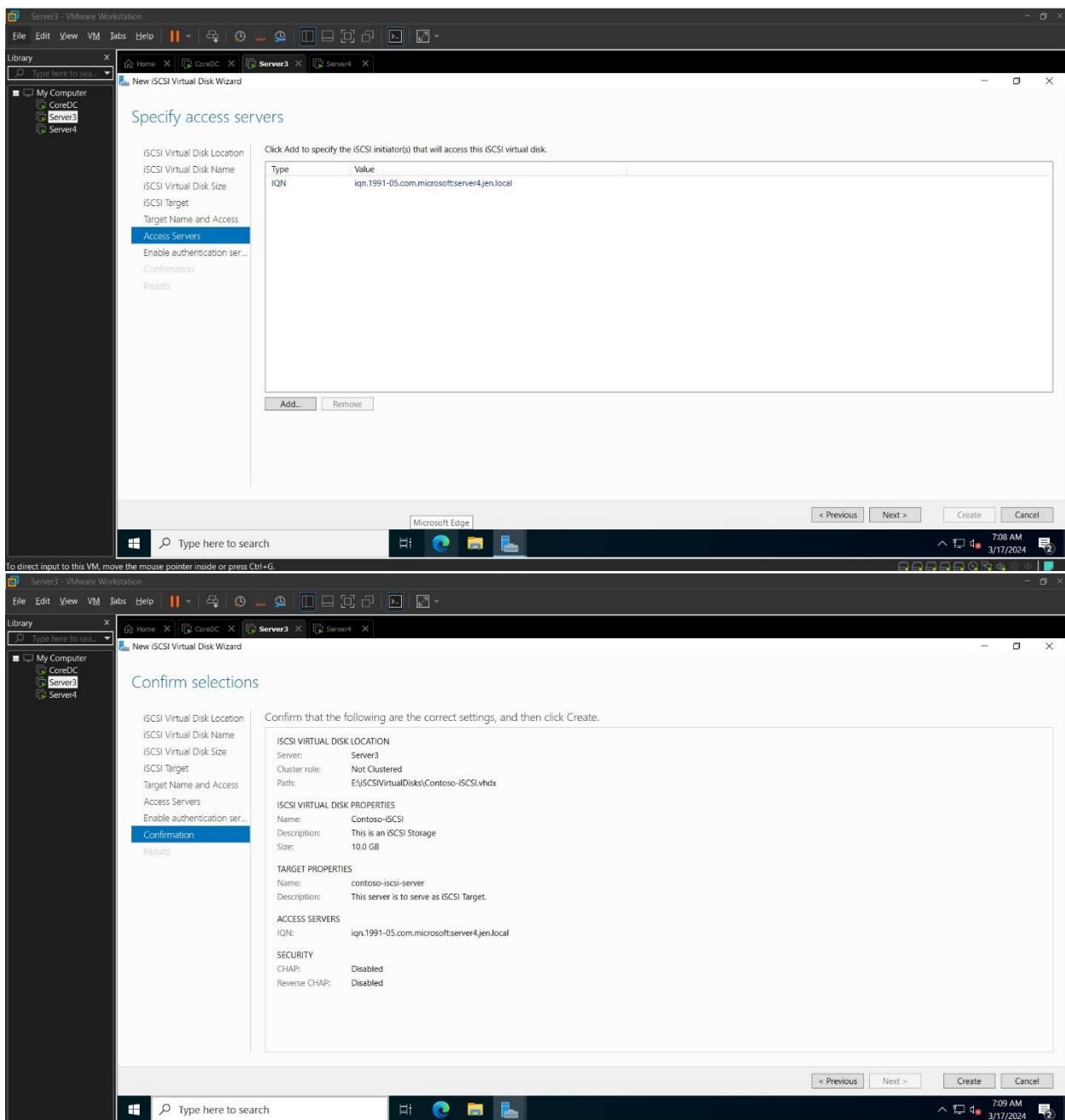
# Windows Server Security



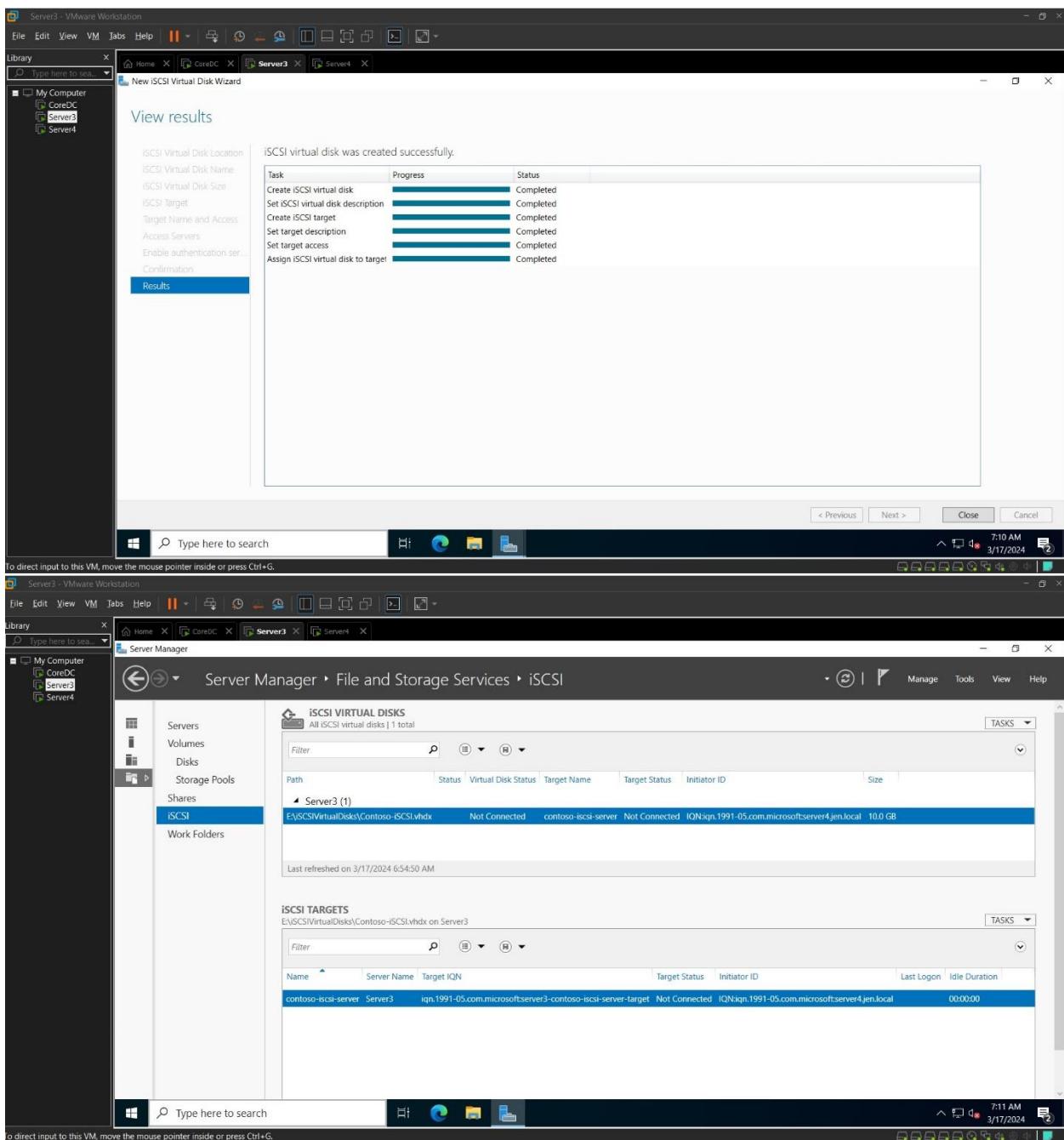
Through iSCSI initiator tool on Server 4's Server Management, retrieve the IQN and add to Server 3 to confirm connection to iSCSI target



# Windows Server Security

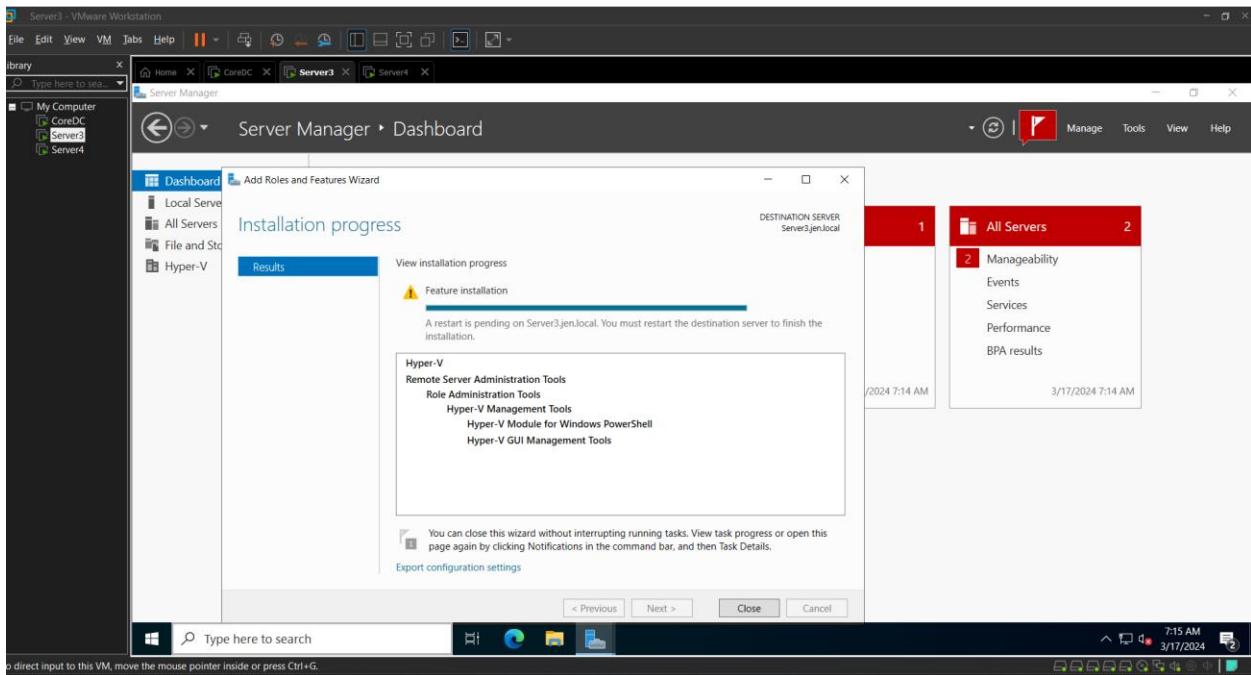


# Windows Server Security

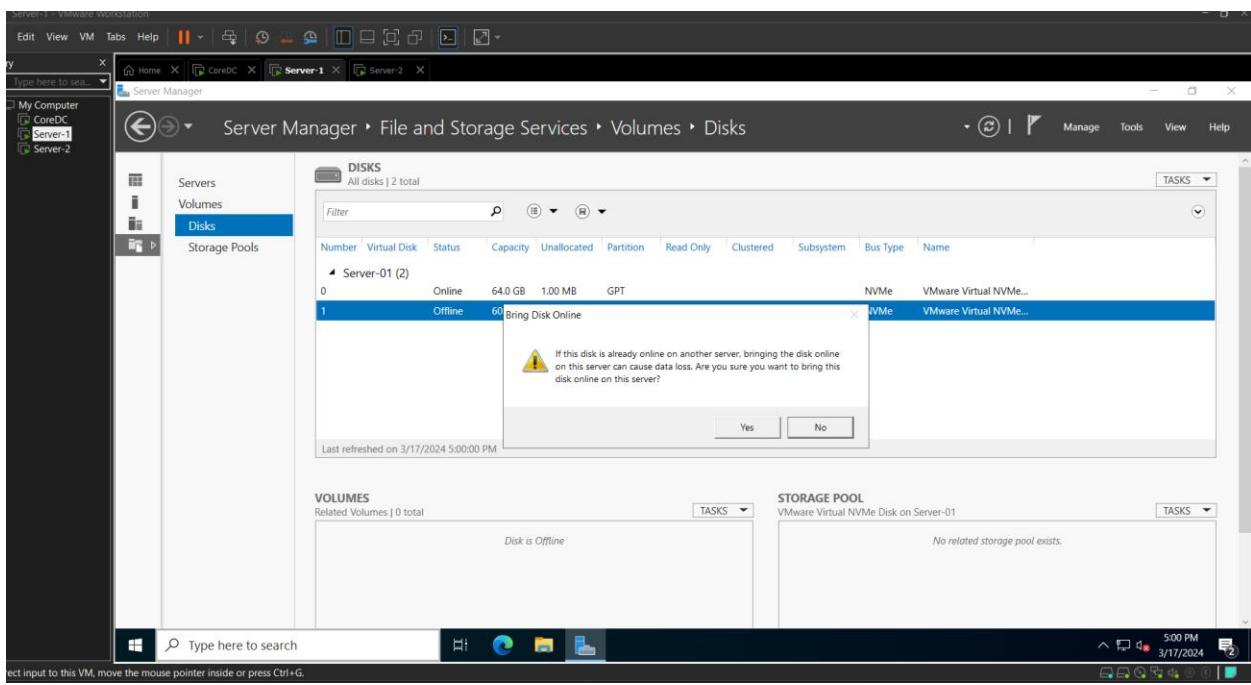


HyperV (It's a nightmare)

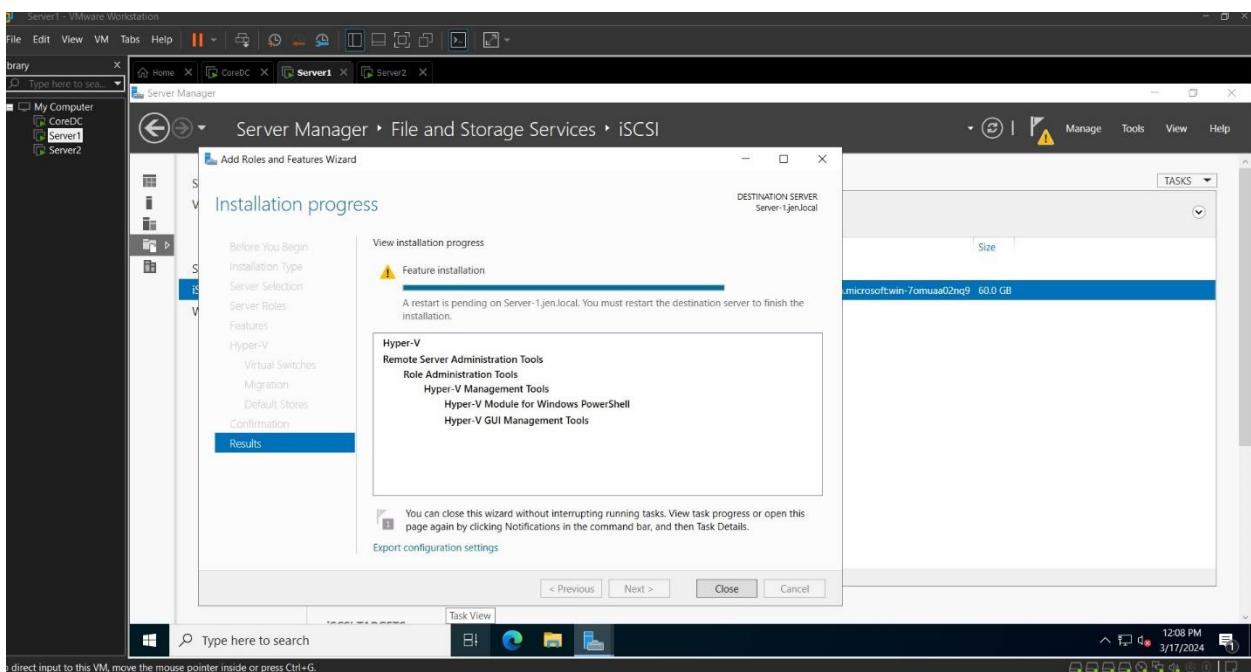
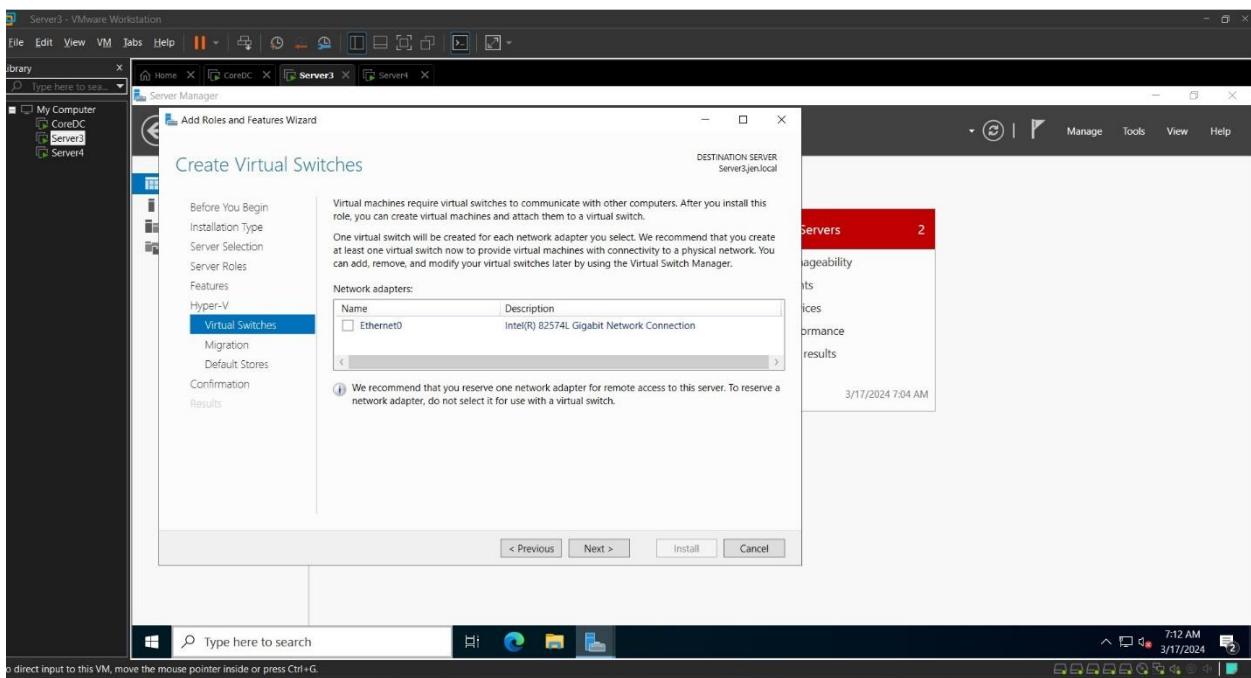
# Windows Server Security



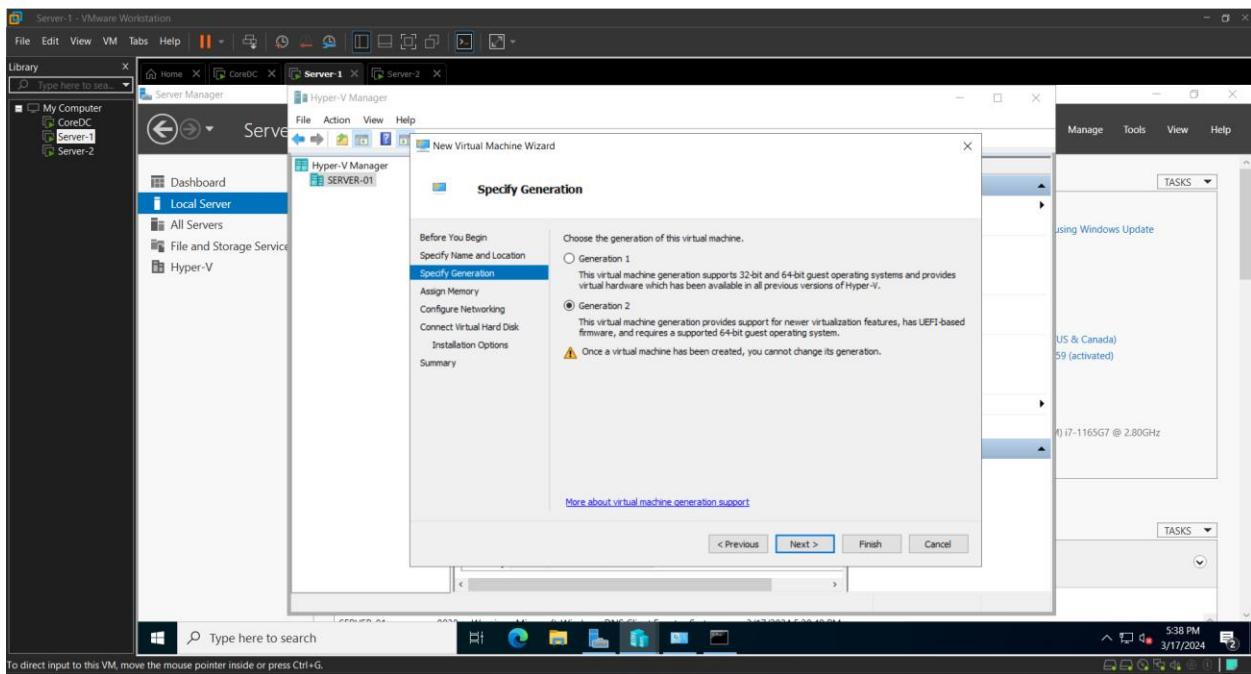
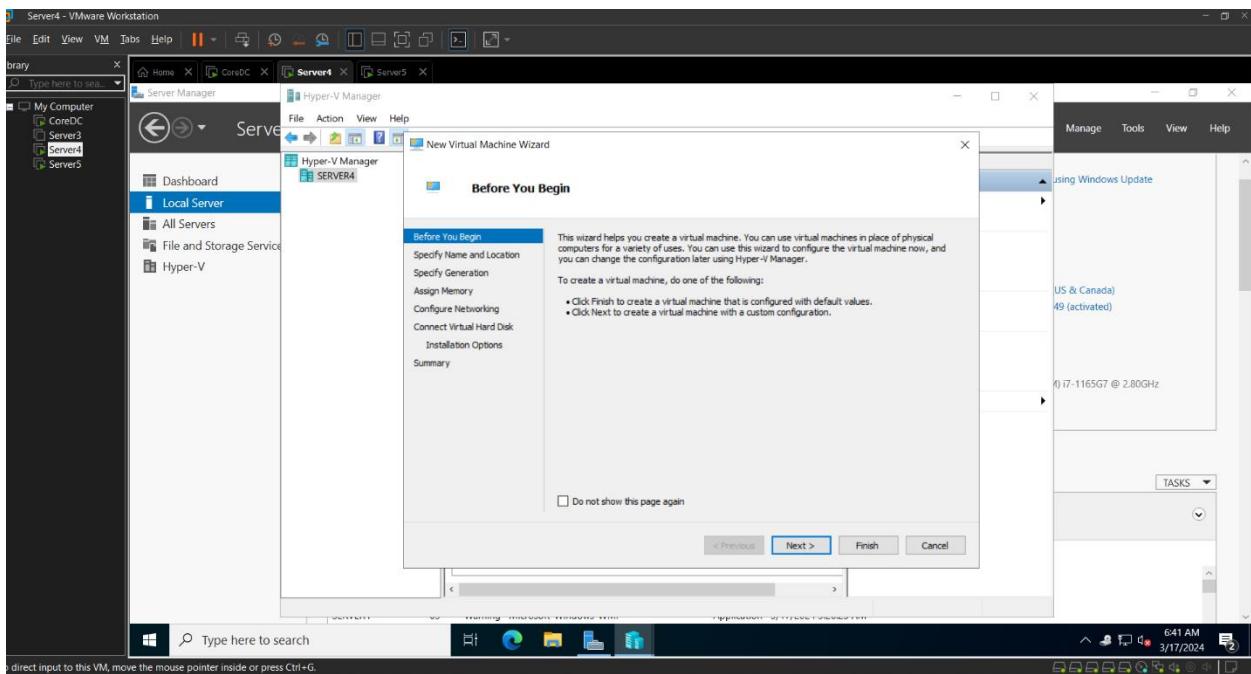
## Prepare disk for HyperV environment



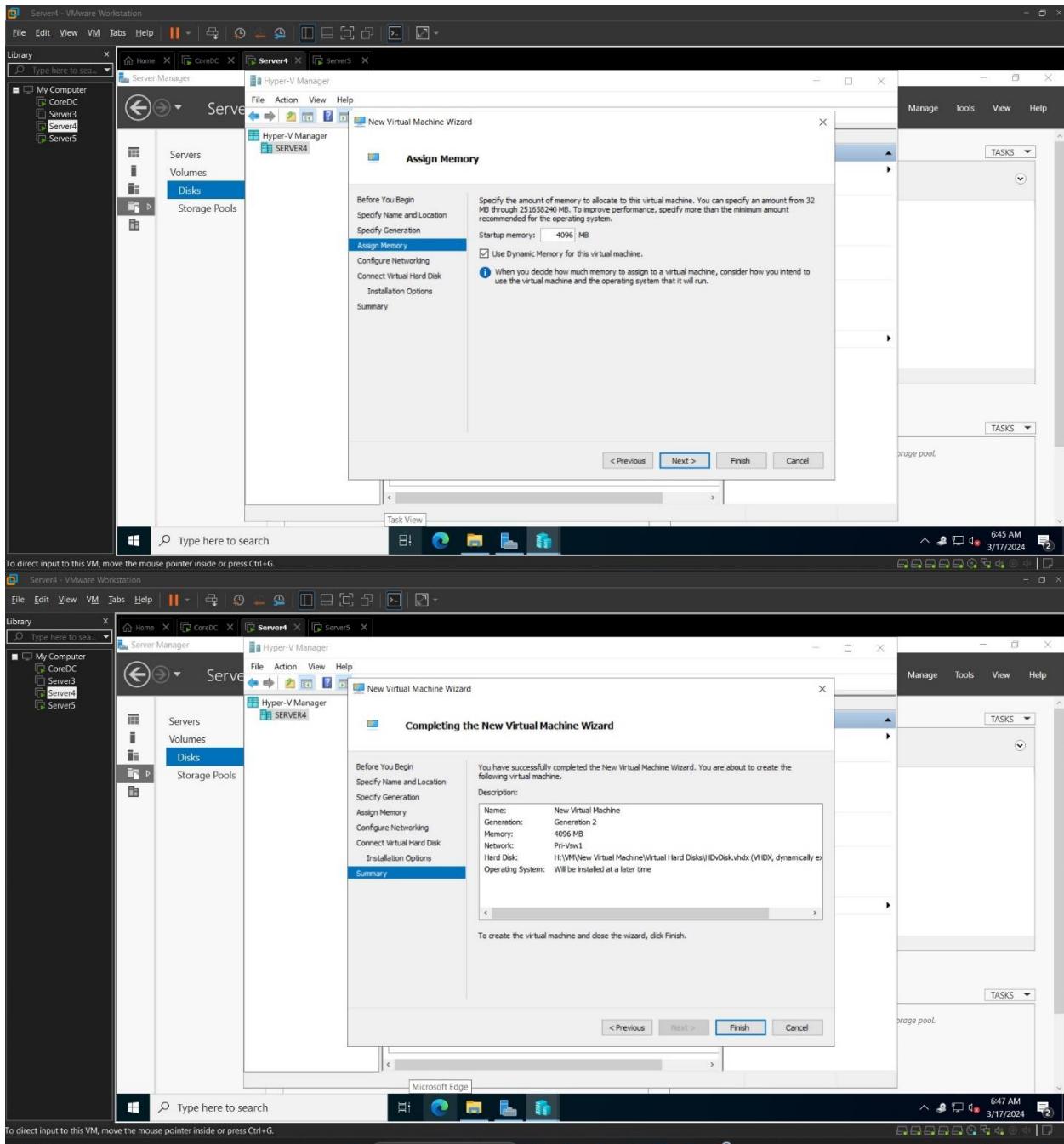
# Windows Server Security



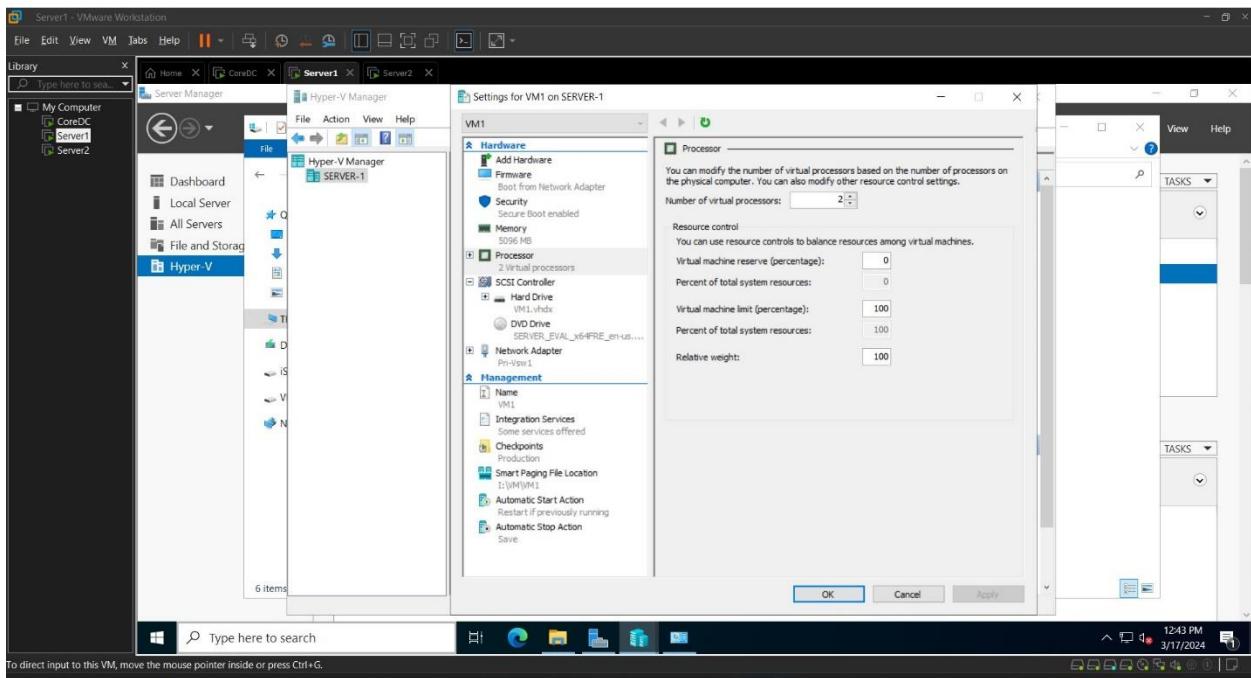
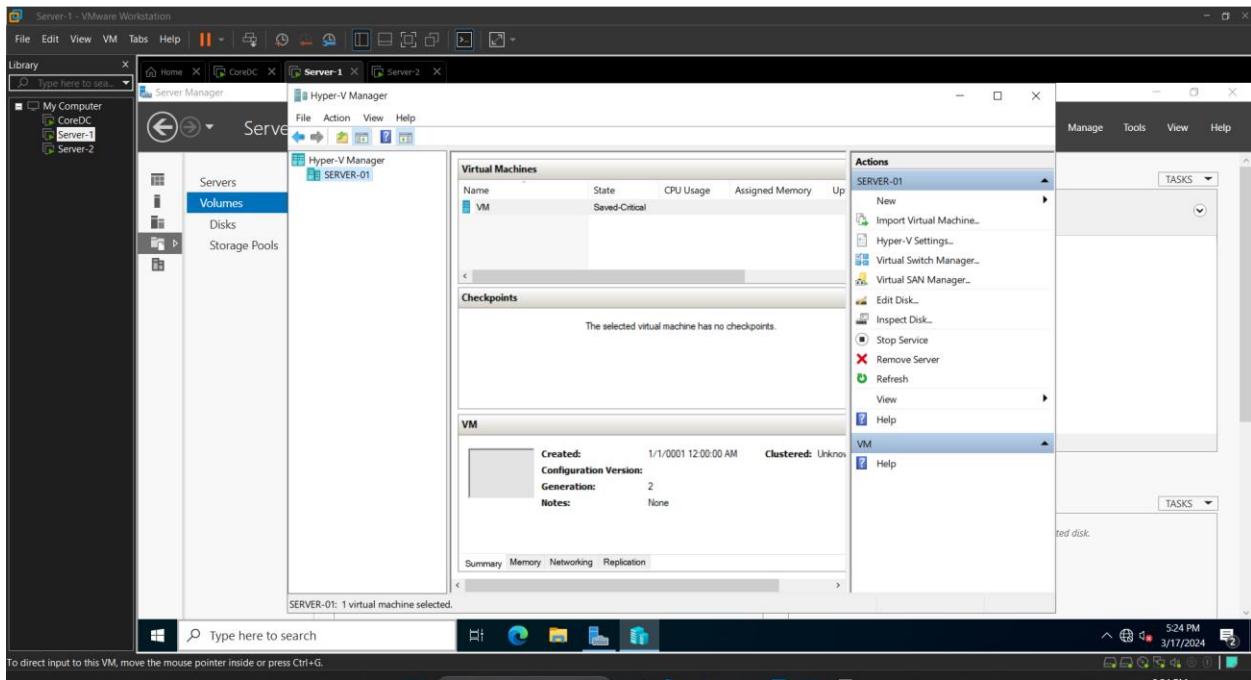
# Windows Server Security



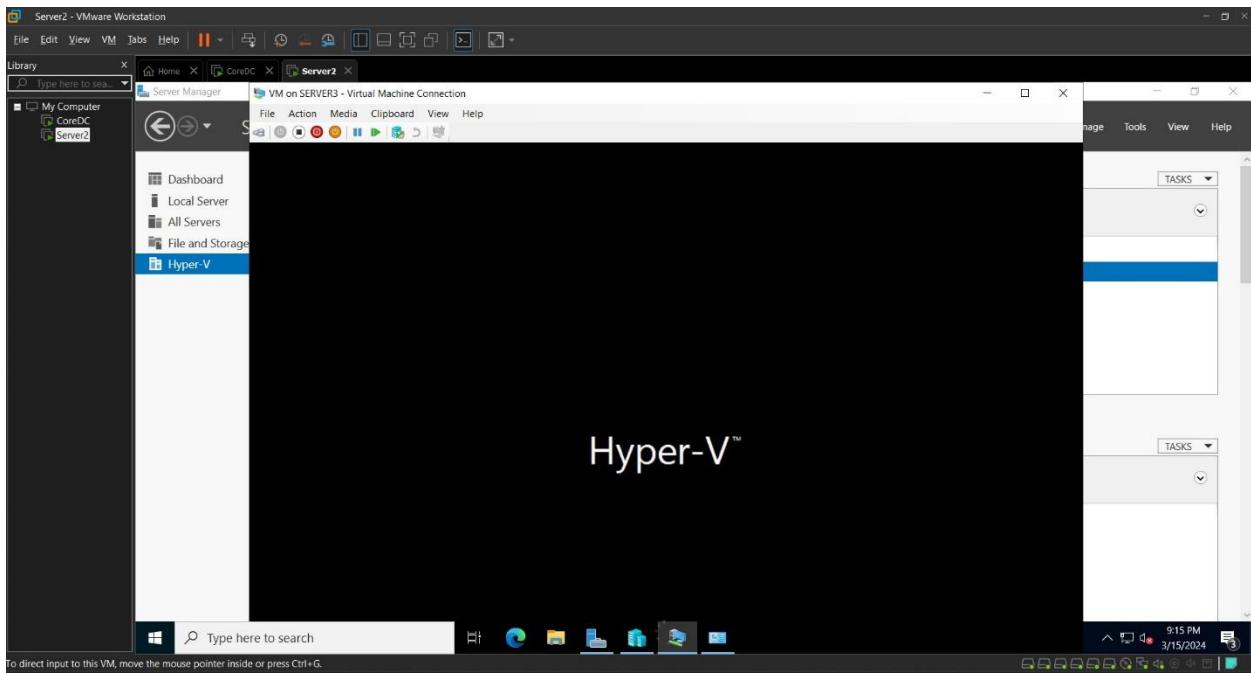
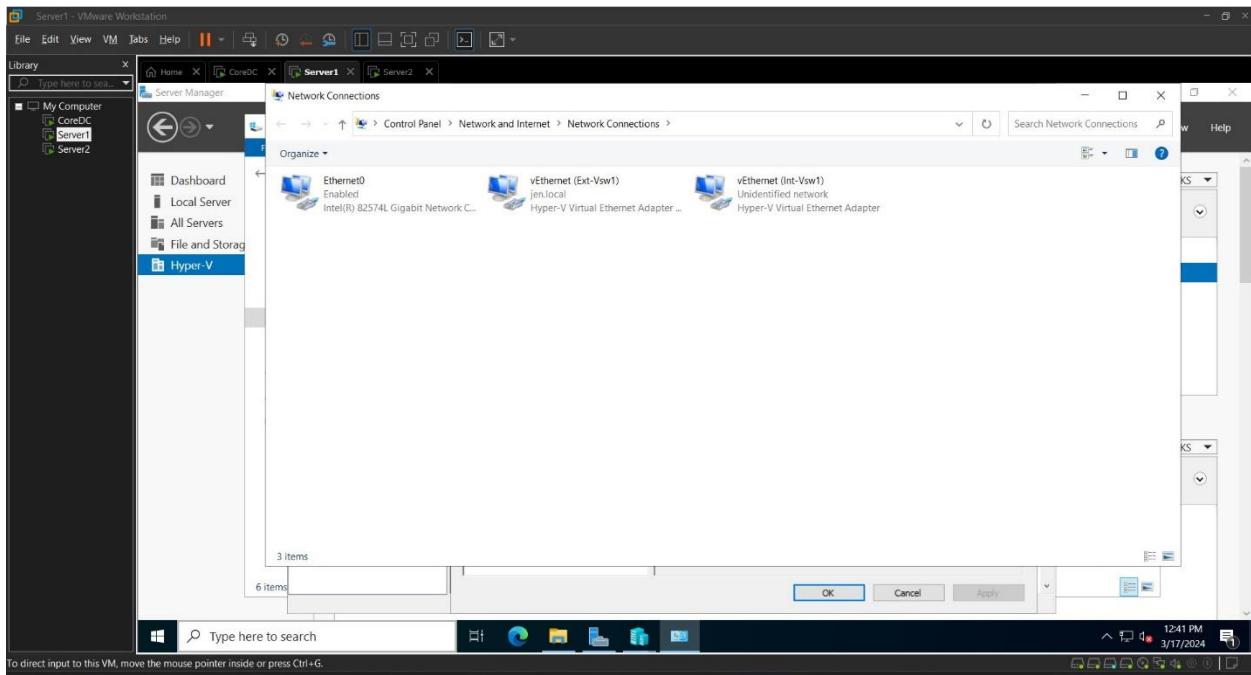
# Windows Server Security



# Windows Server Security



# Windows Server Security



WSUS Configuration

# Windows Server Security

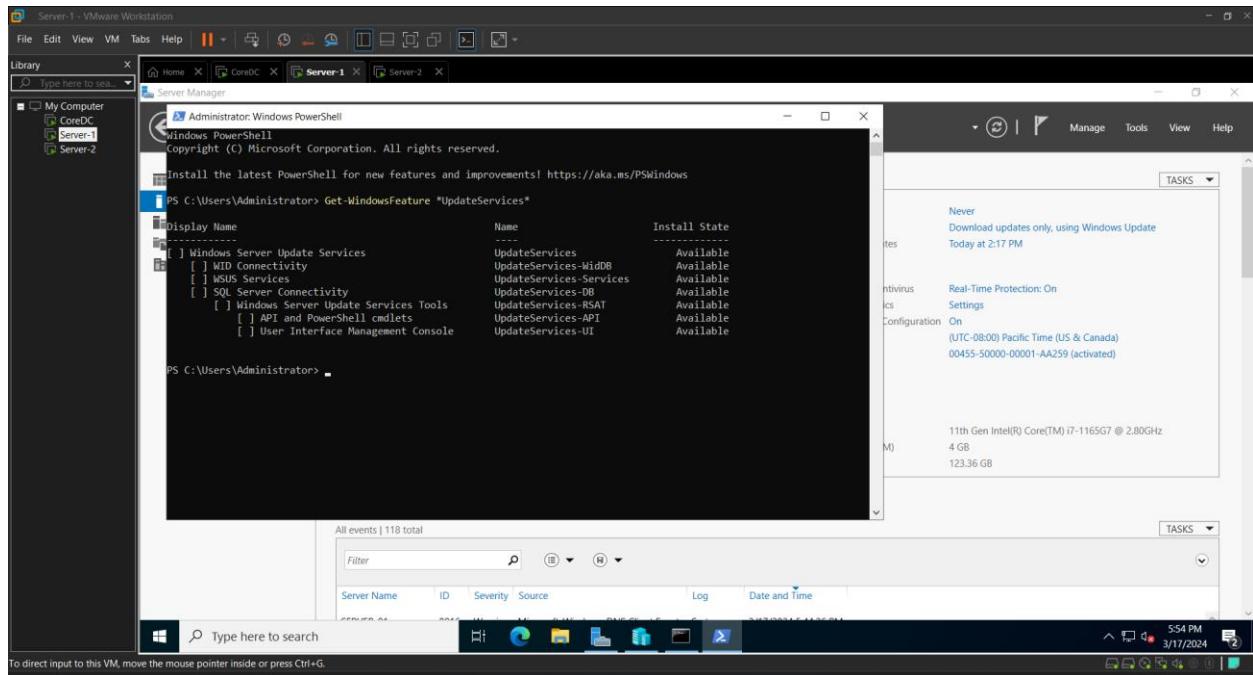
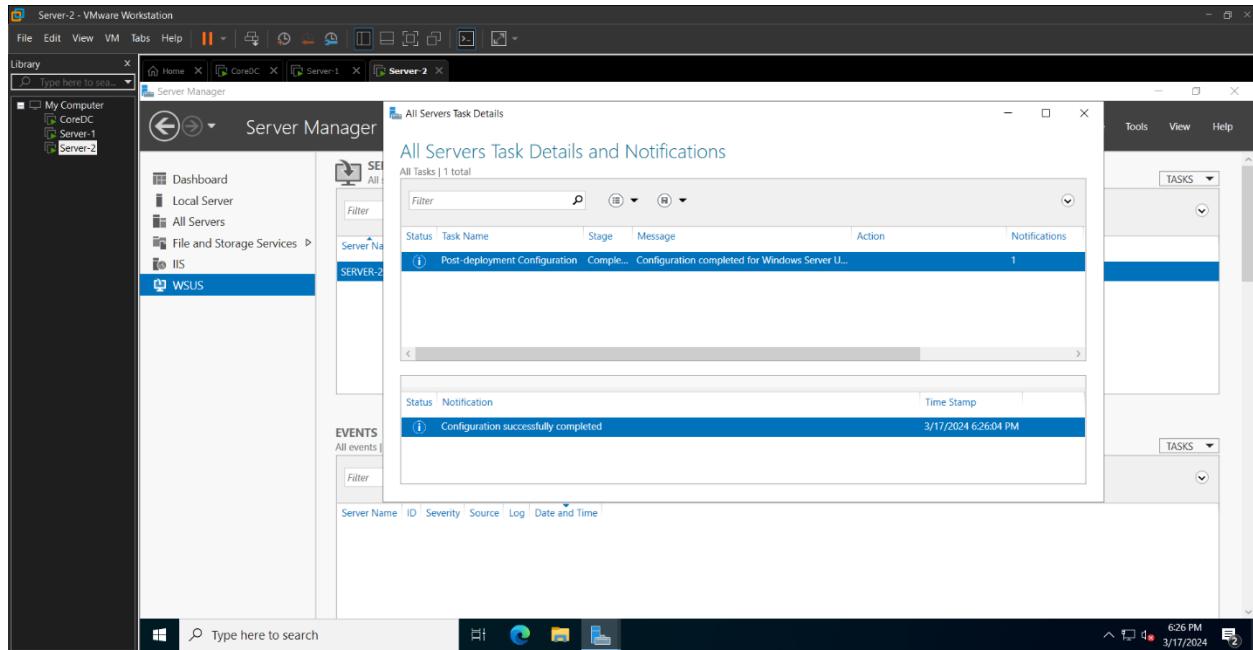


Figure 30: Installed WSUS on Server2 for GUI



# Windows Server Security

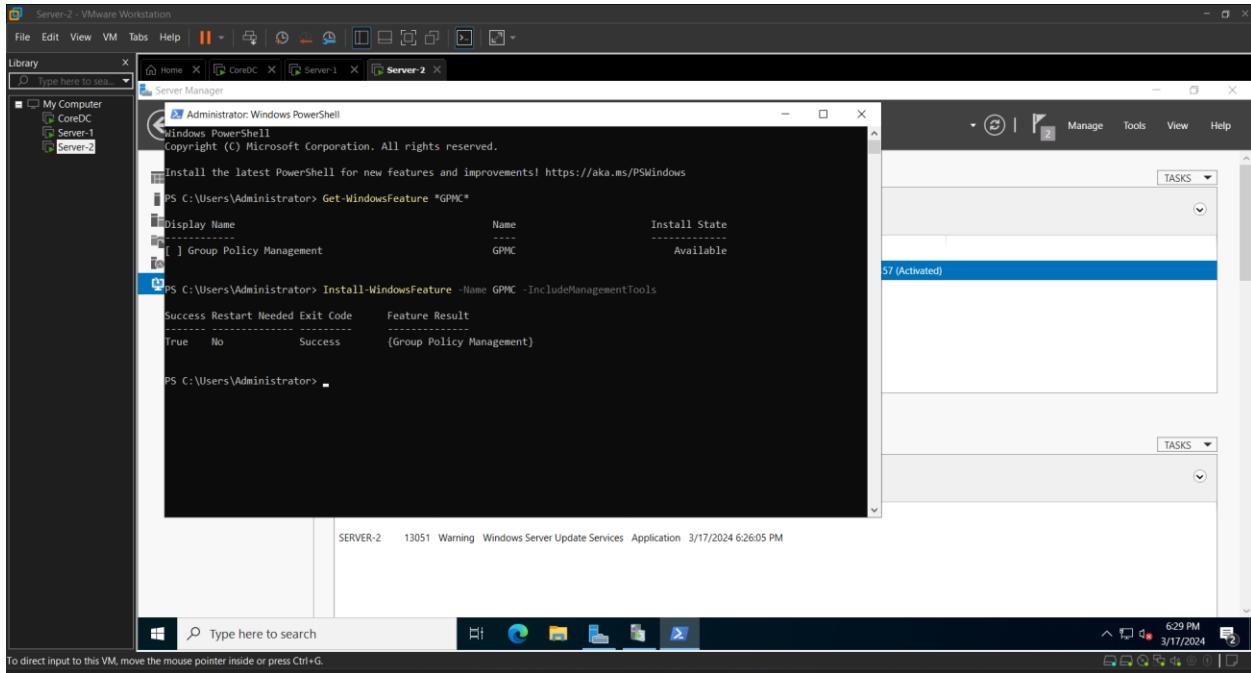


Figure 31: Group Policy Management Console Installed

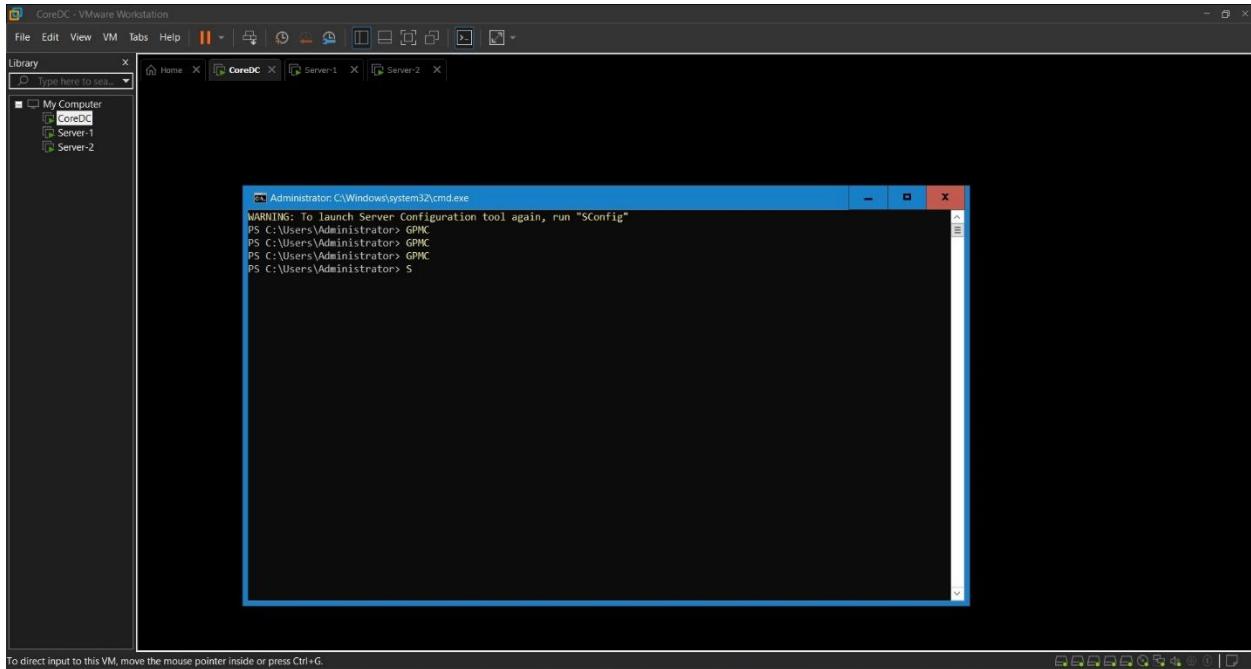


Figure 32: GPMC LAUNCHED from Domain Controller

# Windows Server Security

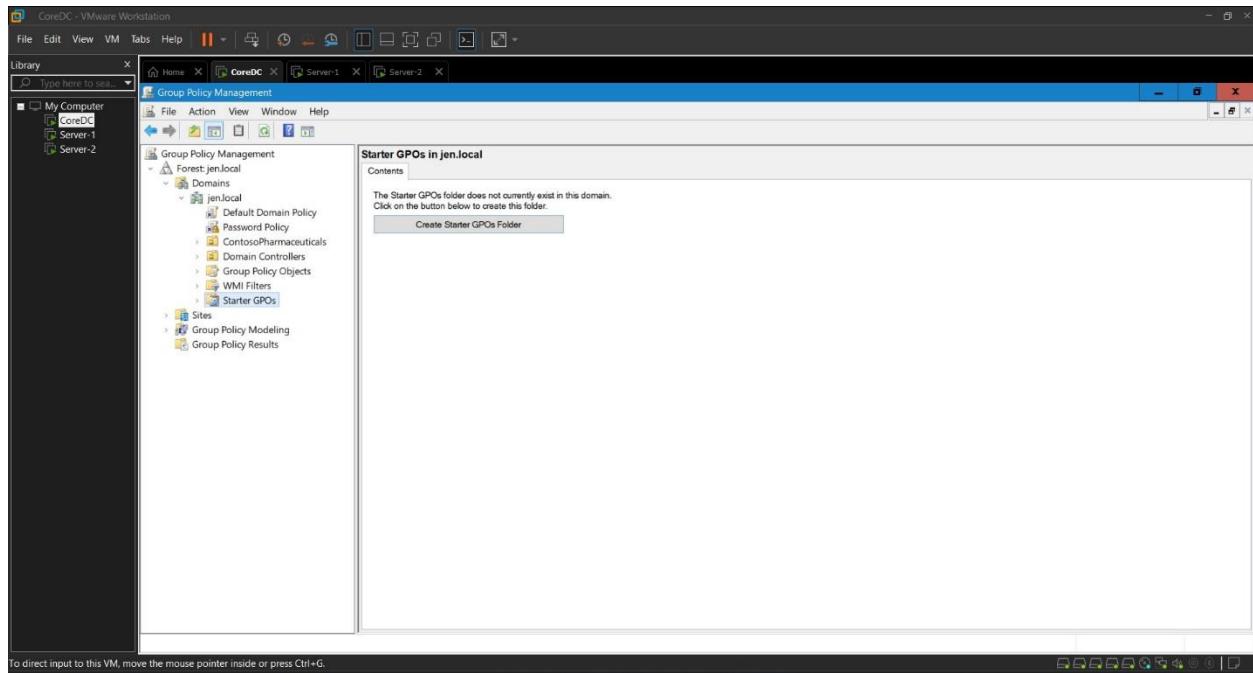
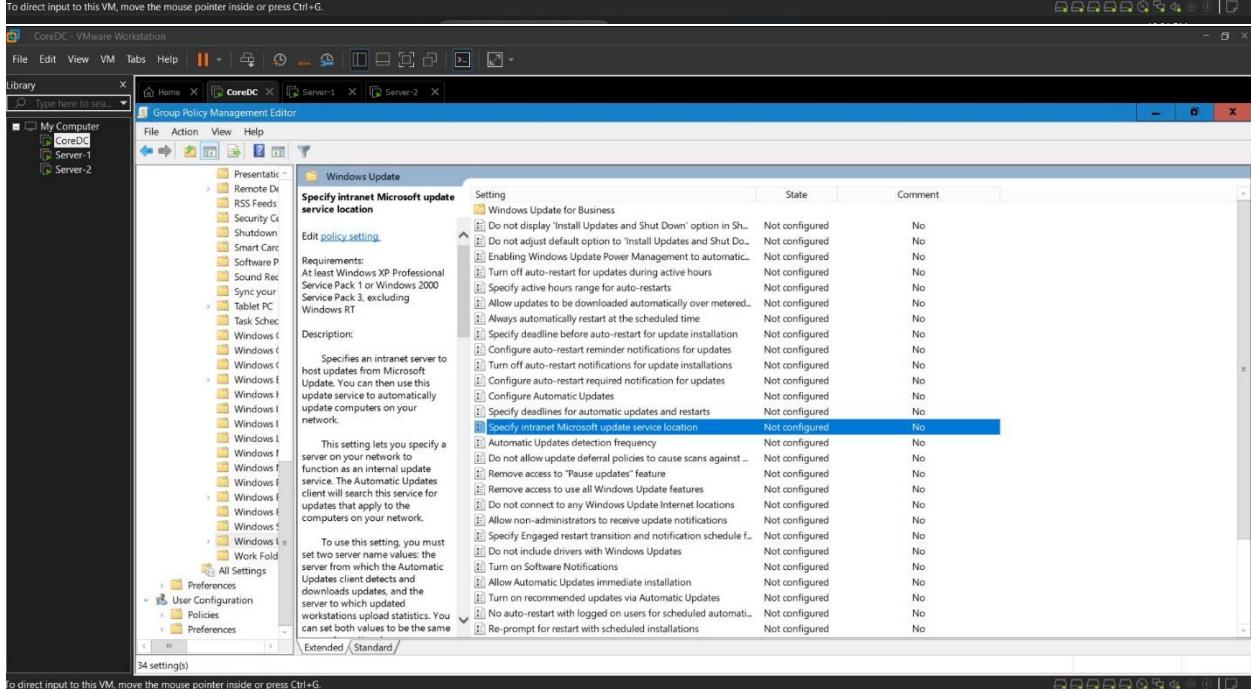
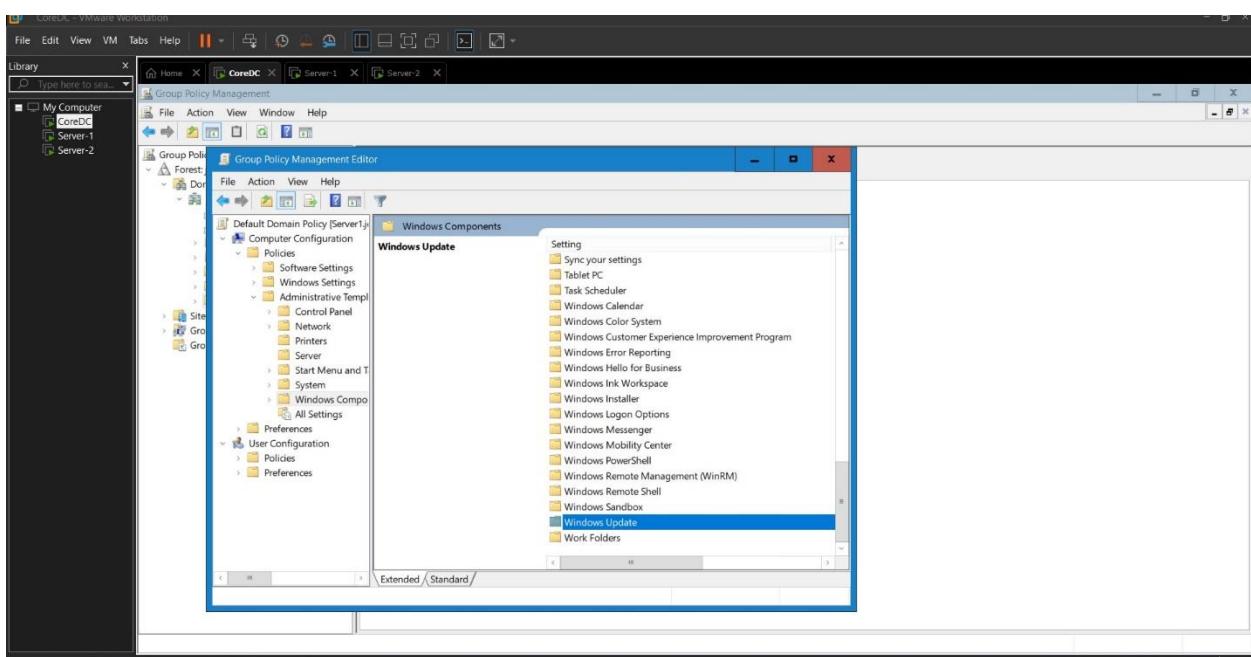


Figure 33 Navigating towards Windows Update on Group Policy Object

# Windows Server Security



# Windows Server Security

