

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

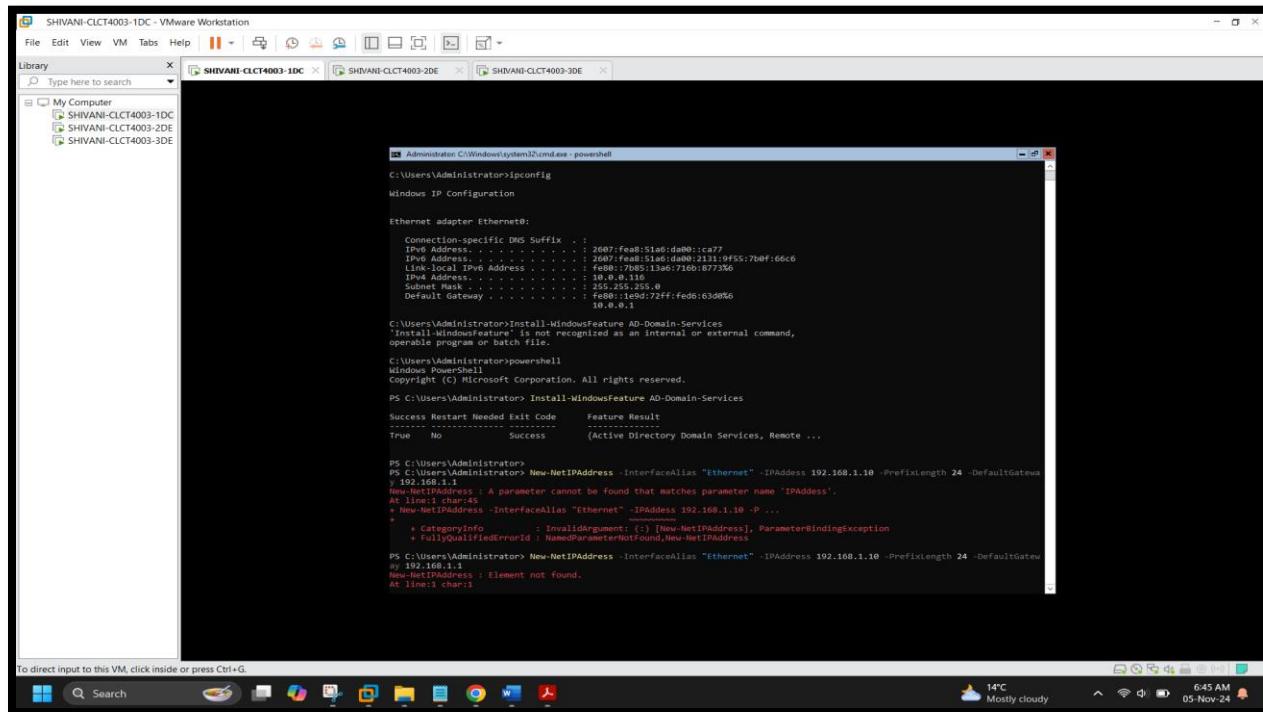
~~~~~

Paste your screenshots here

# Windows Server Security

## 1) INSTALL A DOMAIN CALLED YOURNAME.LOCAL ON SERVER CORE

[Screenshot 1: Successfully Installed domain name shivani. Local Server Core]



The screenshot shows a Windows Server Core desktop environment with a single open command prompt window. The title bar says "Administrator: C:\Windows\system32\cmd.exe - powershell". The command history shows the following steps:

```
C:\Users\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . : CLCT4003-1DC
  IPv4 Address . . . . . : 10.0.0.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.0.1

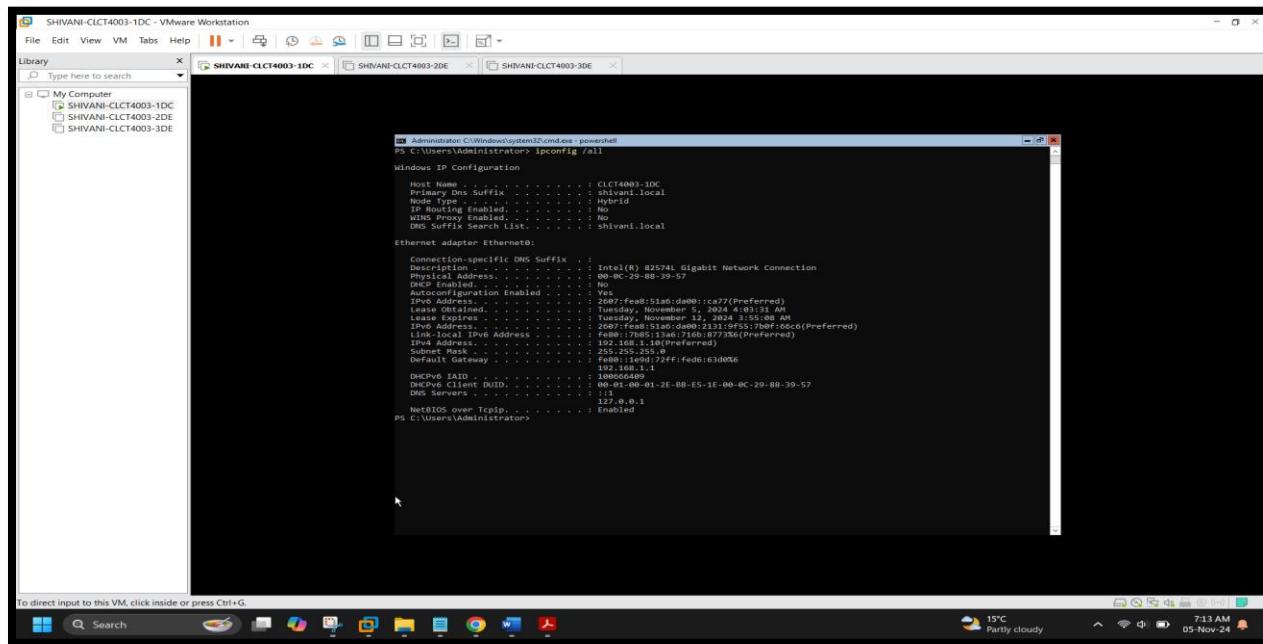
C:\Users\Administrator>Install-WindowsFeature AD-Domain-Services
'Install-WindowsFeature' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Install-WindowsFeature AD-Domain-Services
Success Restart Needed Exit Code Feature Result
----- ----- -----
True No Success (Active Directory Domain Services, Remote ...)

PS C:\Users\Administrator>New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.1.10 -PrefixLength 24 -DefaultGateway 192.168.1.1
New-NetIPAddress : A parameter cannot be found that matches parameter name 'IPAddres'.
At line:1 char:45
+ New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.1.10 -P ...
+                 ^ CategoryInfo          : InvalidArgument: (:) [New-NetIPAddress], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,New-NetIPAddress
PS C:\Users\Administrator>New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.1.10 -PrefixLength 24 -DefaultGateway
192.168.1.1
New-NetIPAddress : Element not found.
At line:1 char:1
```

[Screenshot 2: IP Configuration Details for CLCT4003-1DC]



The screenshot shows a Windows Server Core desktop environment with a single open command prompt window. The title bar says "Administrator: C:\Windows\system32\cmd.exe - powershell". The command history shows the following steps:

```
PS C:\Users\Administrator> ipconfig /all
Windows IP Configuration

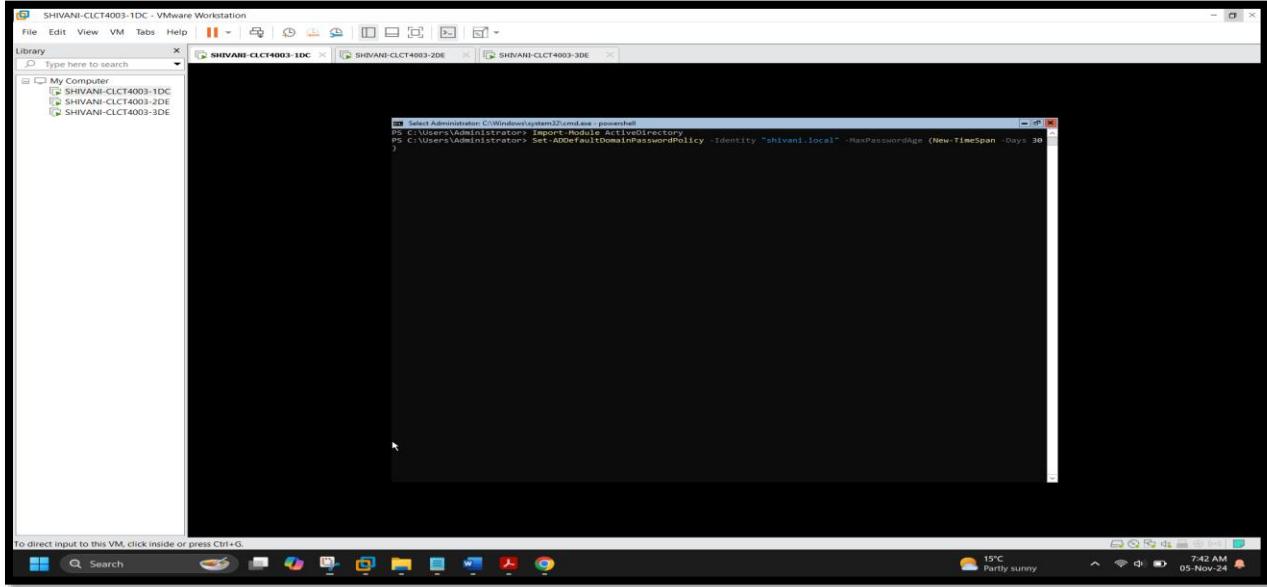
Host Name . . . . . : CLCT4003-1DC
Primary Dns Suffix . . . . . : shivani.local
Node Type . . . . . : Hybrid
Is Gated . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : shivani.local

Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . : Intel(R) Dual Band Wireless-AC 7265
  Physical Address . . . . . : 00-8C-29-88-39-57
  DHCP Enabled . . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  IPv6 Address . . . . . : fe80::1e9d:72ff:fed6:163d%6(Preferred)
    Lease Obtained . . . . . : Tuesday, November 13, 2024 3:55:08 AM
    Lease Expires . . . . . : Tuesday, November 13, 2024 3:55:08 AM
  IPv4 Address . . . . . : 192.168.1.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0(Preferred)
    Default Gateway . . . . . : 192.168.1.1
  DHCPv6 IID . . . . . : 00-01-00-01-2E-8B-E5-1E-00-8C-29-88-39-57
  DHCPv6 Client DUID . . . . . : 00-01-00-01-2E-8B-E5-1E-00-8C-29-88-39-57
  DNS Servers . . . . . : 127.0.0.1
  NetBIOS over Tcpip . . . . . : Enabled
```

# Windows Server Security

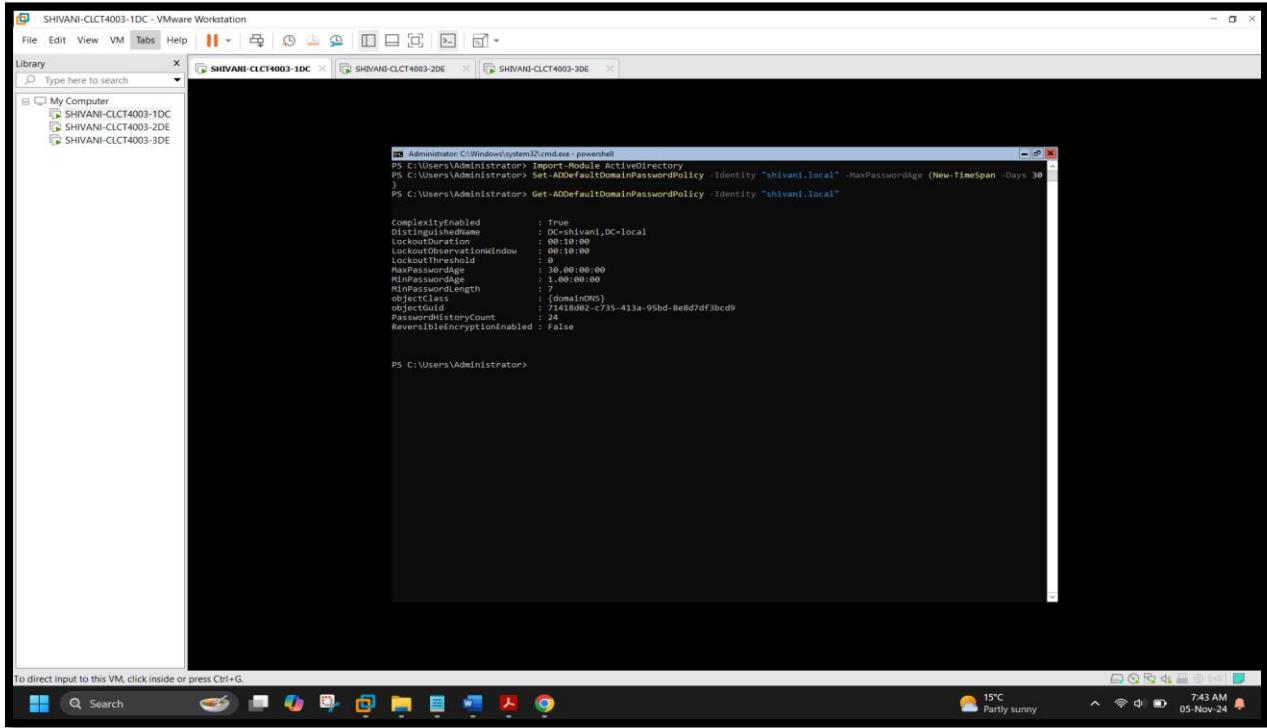
## 2) CONFIGURE GROUP POLICY AND ENFORCE PASSWORD CHANGE TO 30 DAYS

[Screenshot 3: Configuring Group Policy and Enforcing password changing to 30 days]



```
Set-ADDefaultDomainPasswordPolicy -Identity "shivani.local" -MaxPasswordAge (New-TimeSpan -Days 30)
```

[Screenshot 4: Verify the Group Policy and Enforcing password changing to 30 days]



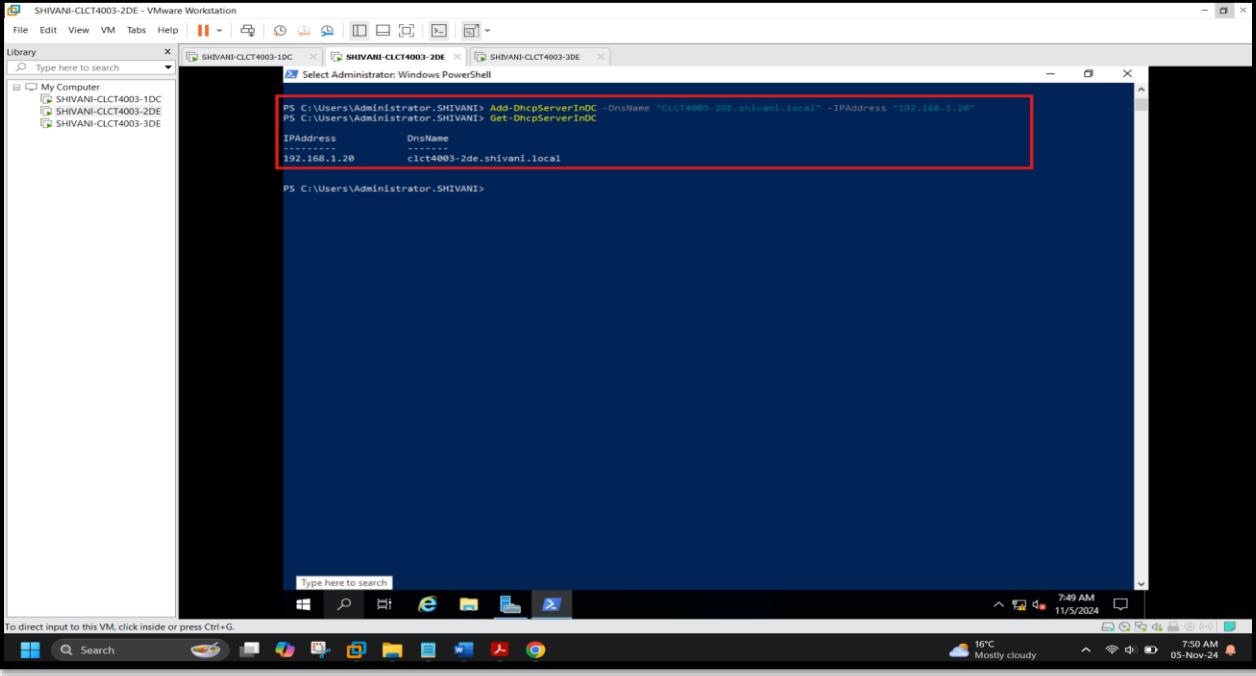
```
Get-ADDefaultDomainPasswordPolicy
```

| Property                    | Value                                    |
|-----------------------------|------------------------------------------|
| ComplexityEnabled           | : True                                   |
| DistinguishedName           | : DC=shivani,DC=local                    |
| Enabled                     | : True                                   |
| LockoutObservationWindow    | : 00:10:00                               |
| LockoutThreshold            | : 0                                      |
| MaxPasswordAge              | : 30.00:00:00                            |
| MinPasswordAge              | : 1.00:00:00                             |
| MinPasswordLength           | : 7                                      |
| objectGUID                  | : {domainGUID}                           |
| objectSID                   | : {1418d992-c735-413a-95bd-8e8d2df3bcd9} |
| PasswordHistoryCount        | : 24                                     |
| ReversibleEncryptionEnabled | : False                                  |

# Windows Server Security

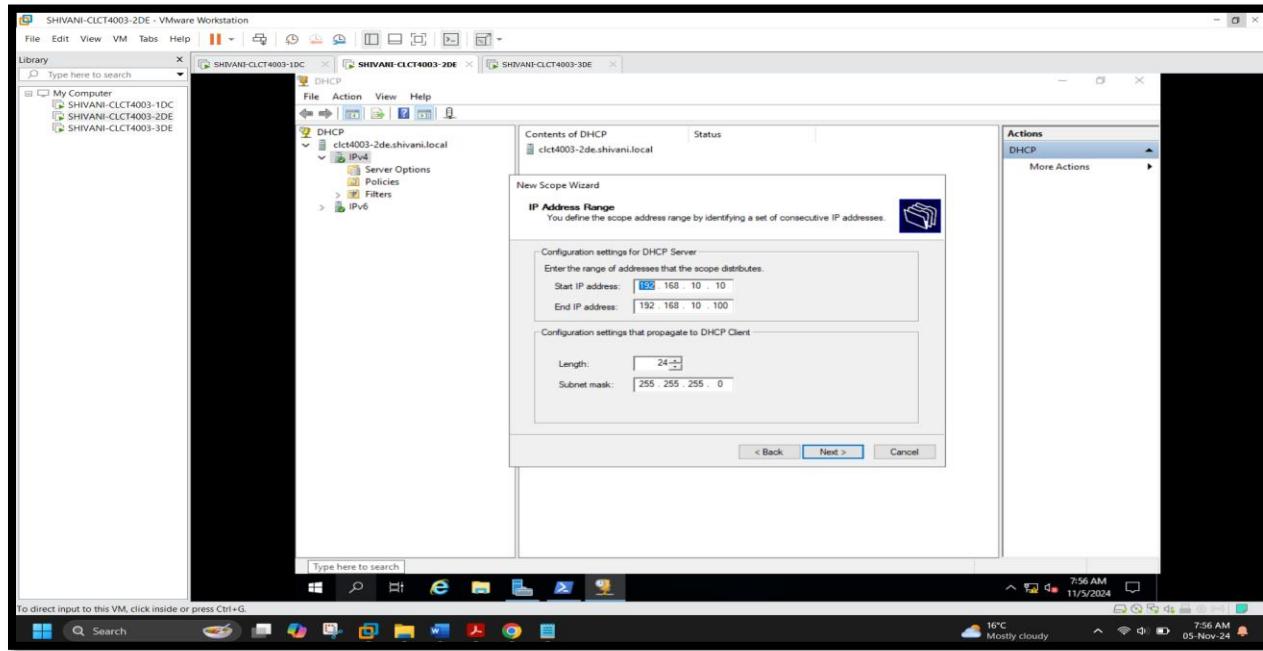
## 3) INSTALL DHCP SERVER

[Screenshot 5: Installing and authorizing the DHCP server has been completed successfully]



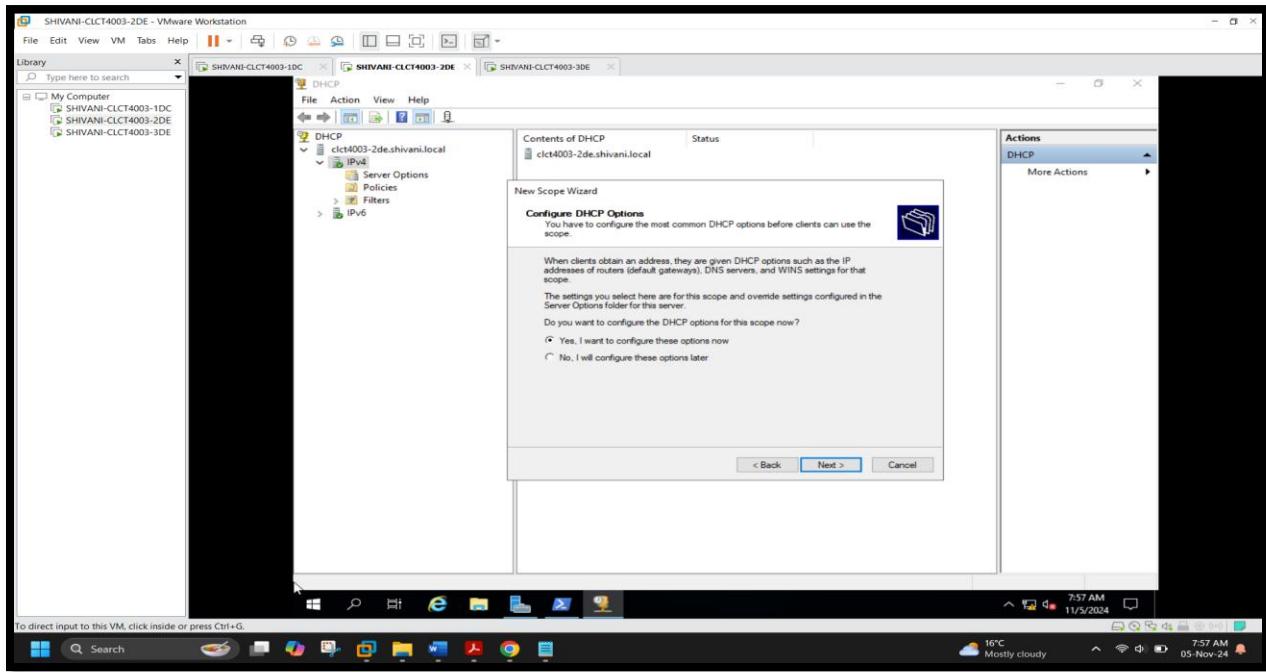
The screenshot shows a Windows PowerShell window titled "Select Administrator: Windows PowerShell". The command PS C:\Users\Administrator.SHIVANI> Add-DhcpServerInDc -DnsName "CLCT4003-2de.shivani.local" -IpAddress "192.168.1.20" was run, followed by PS C:\Users\Administrator.SHIVANI> Get-DhcpServerInDC. The output shows a table with columns "IP Address" and "Dns Name", containing one row with IP 192.168.1.20 and DnsName clict4003-2de.shivani.local. The entire command and output area is highlighted with a red box.

[Screenshot 6: Creating and Defining IP Address Range for New DHCP Scope]

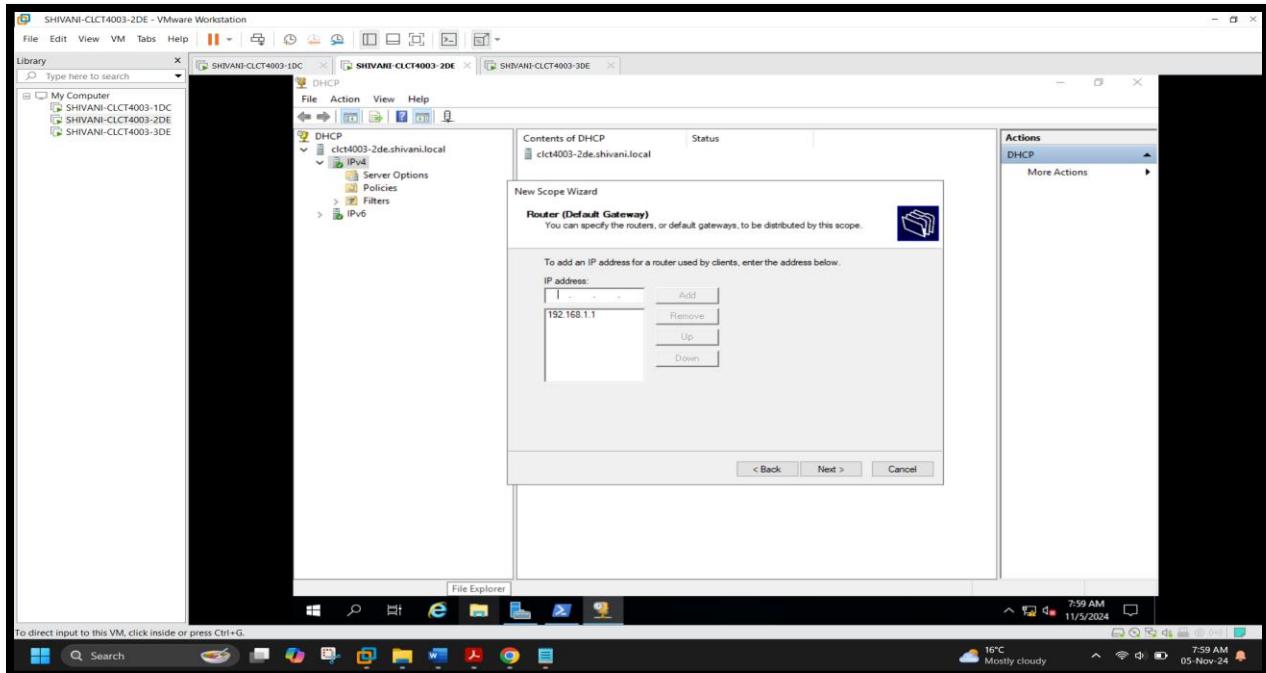


# Windows Server Security

[Screenshot 7: Adding Default Gateway in DHCP Scope]

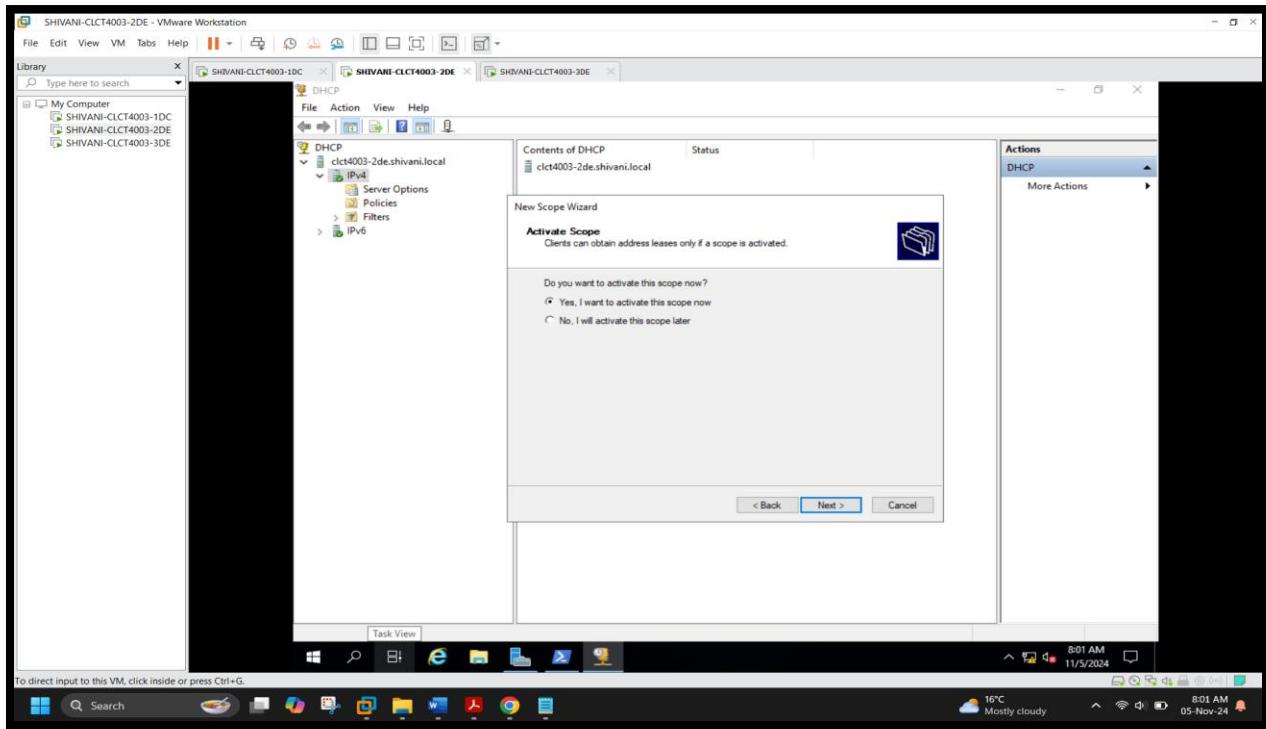


[Screenshot 8: Activating the New DHCP Scope]

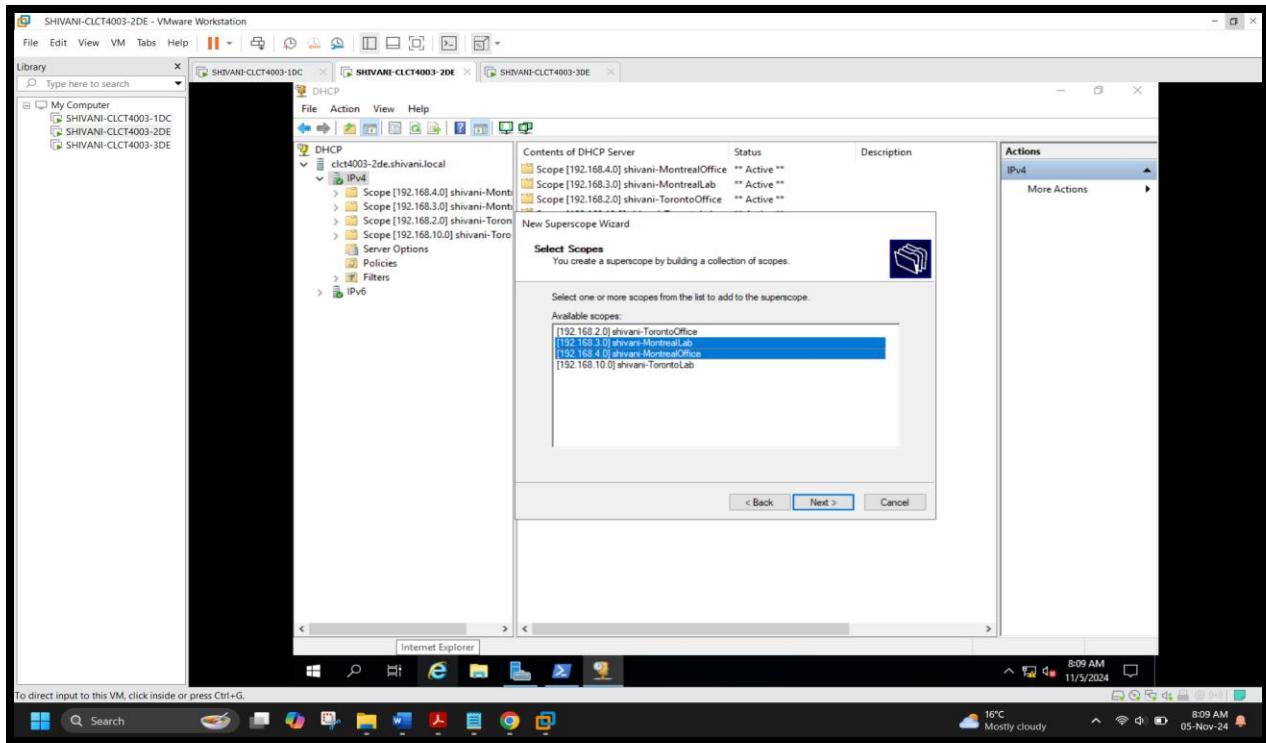


# Windows Server Security

[Screenshot 9: Activating the New scope Wizard]

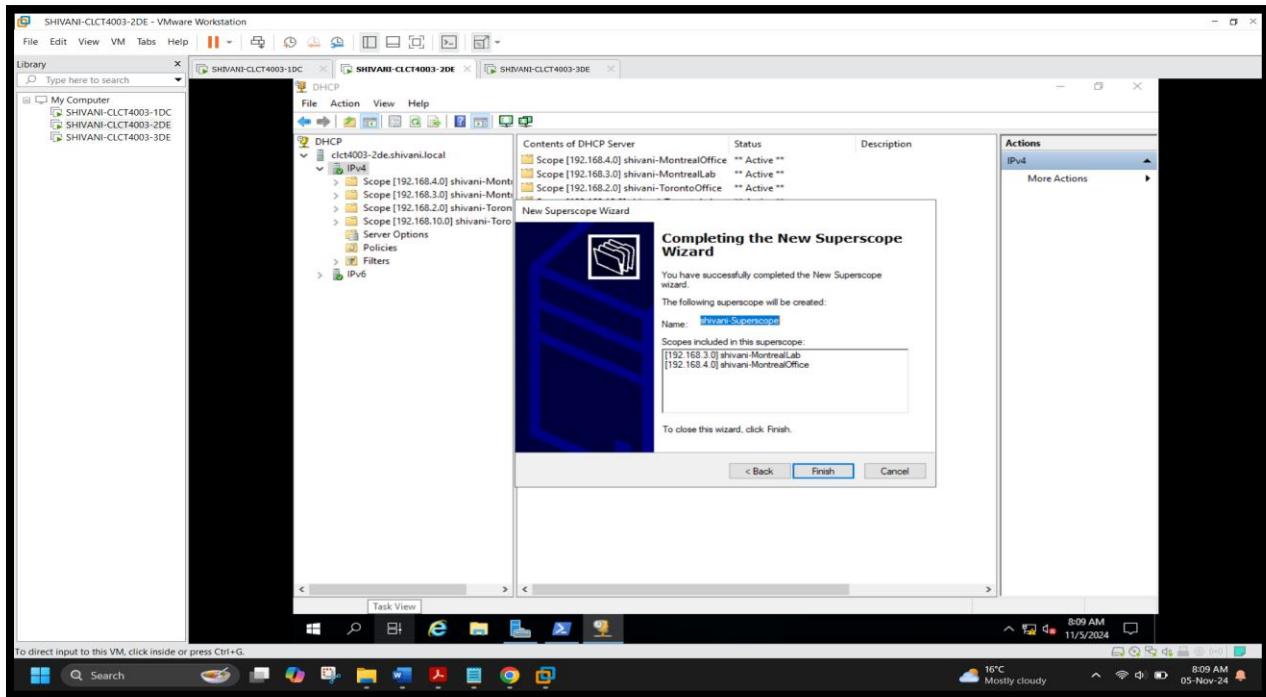


[Screenshot 10: Selecting Superscope]

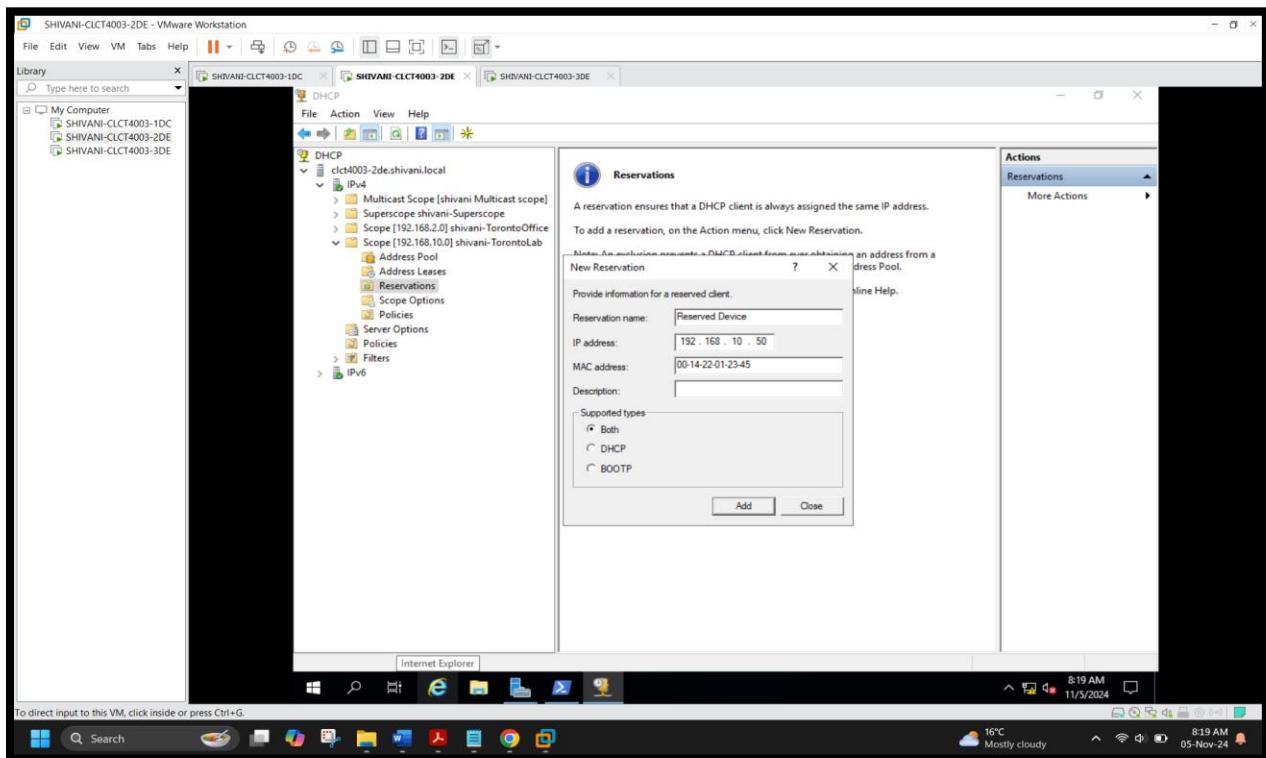


# Windows Server Security

[Screenshot 11: SuperScope Created]

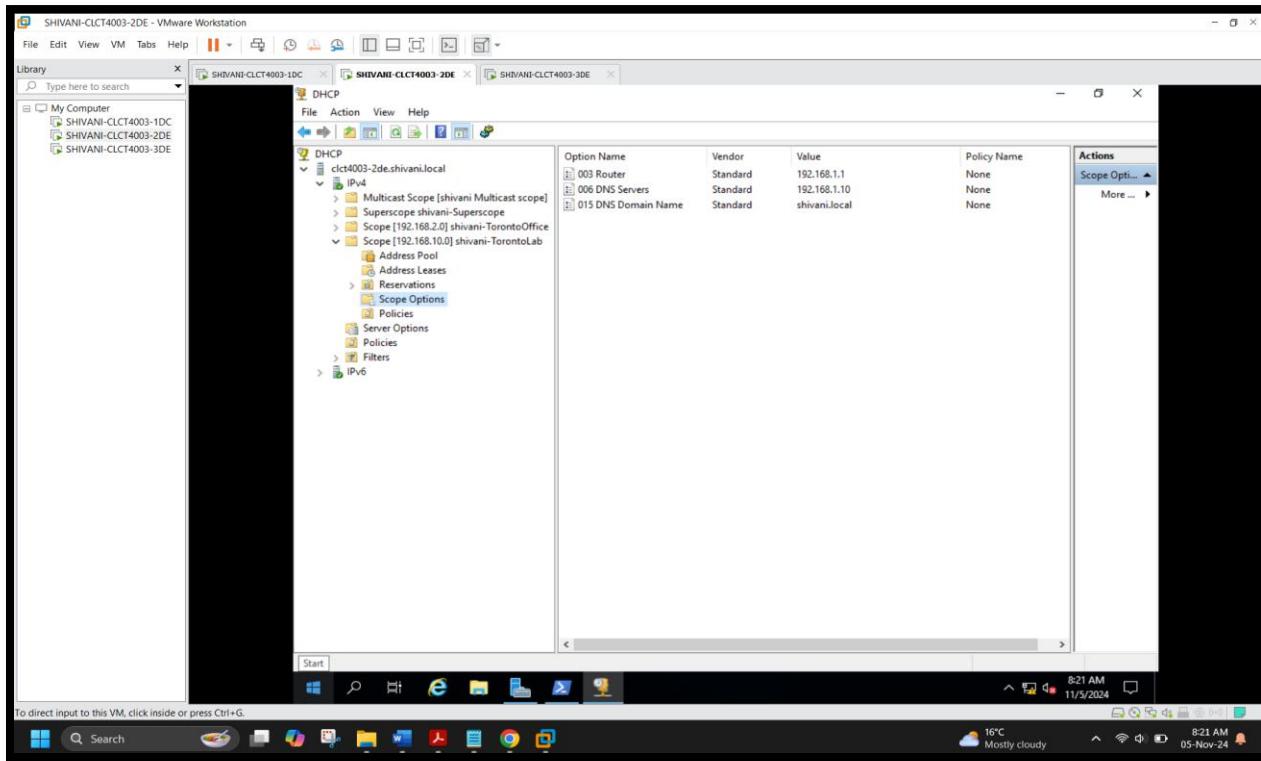


[Screenshot 12: Created reservation]

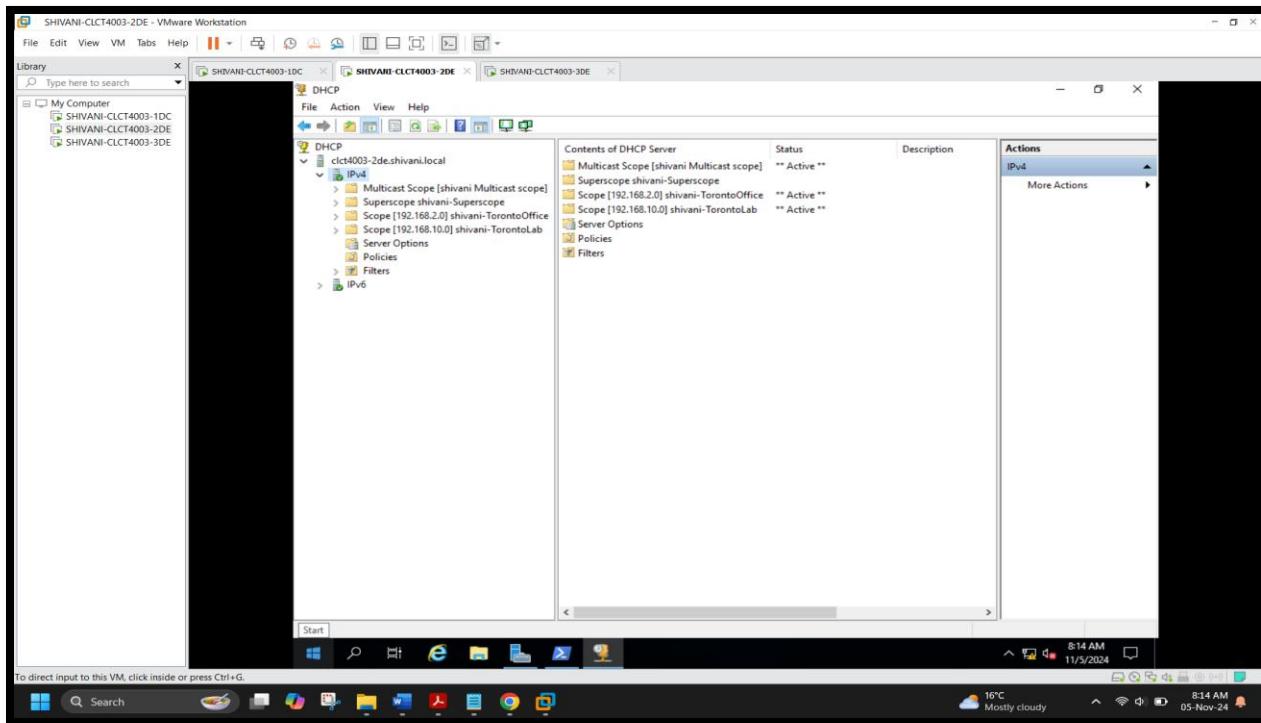


# Windows Server Security

[Screenshot 13: Configured Scope Options]



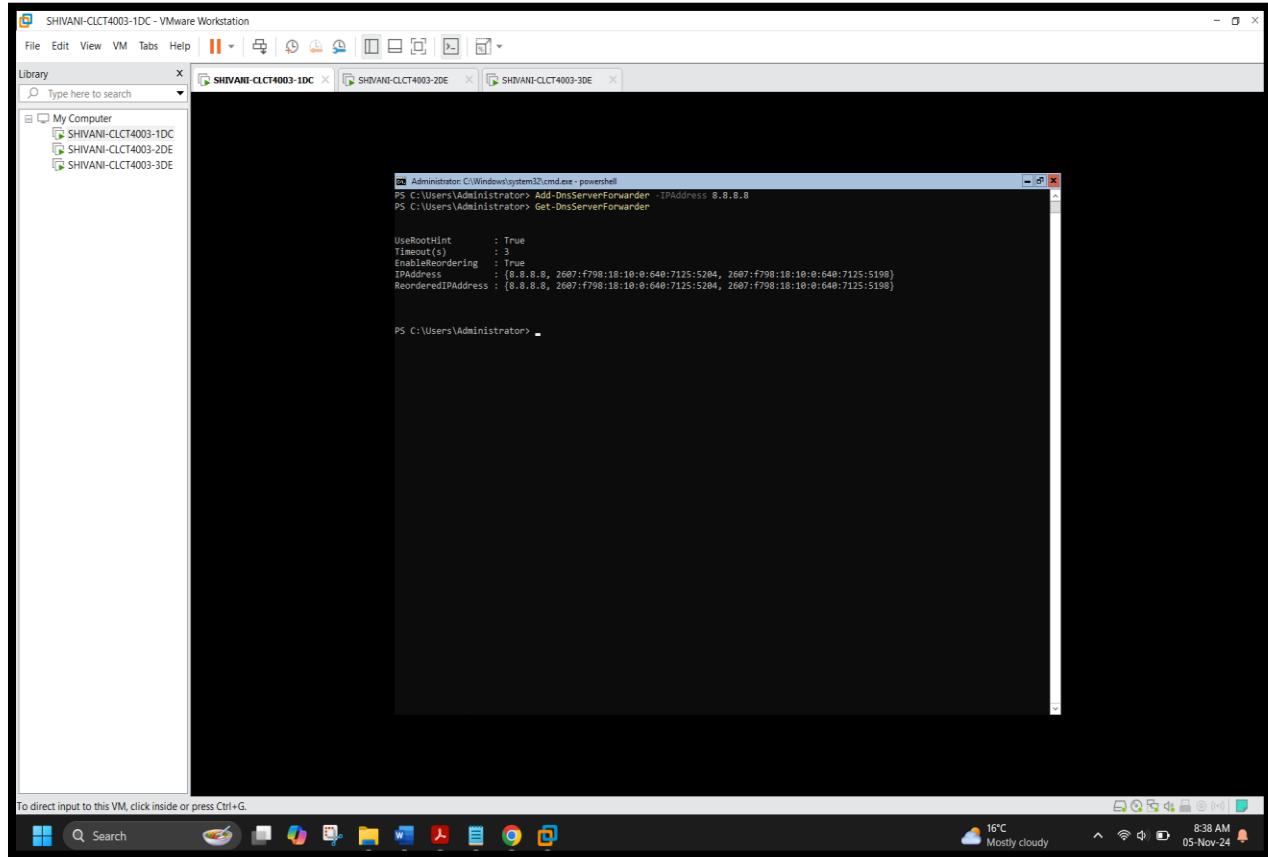
[Screenshot 14: Created 4 DHCP Scopes]



# Windows Server Security

## 4) ON YOUR DOMAIN DNS SERVER, CREATE FORWARDER AND FORWARD ALL REQUESTS TO 8.8.8.8

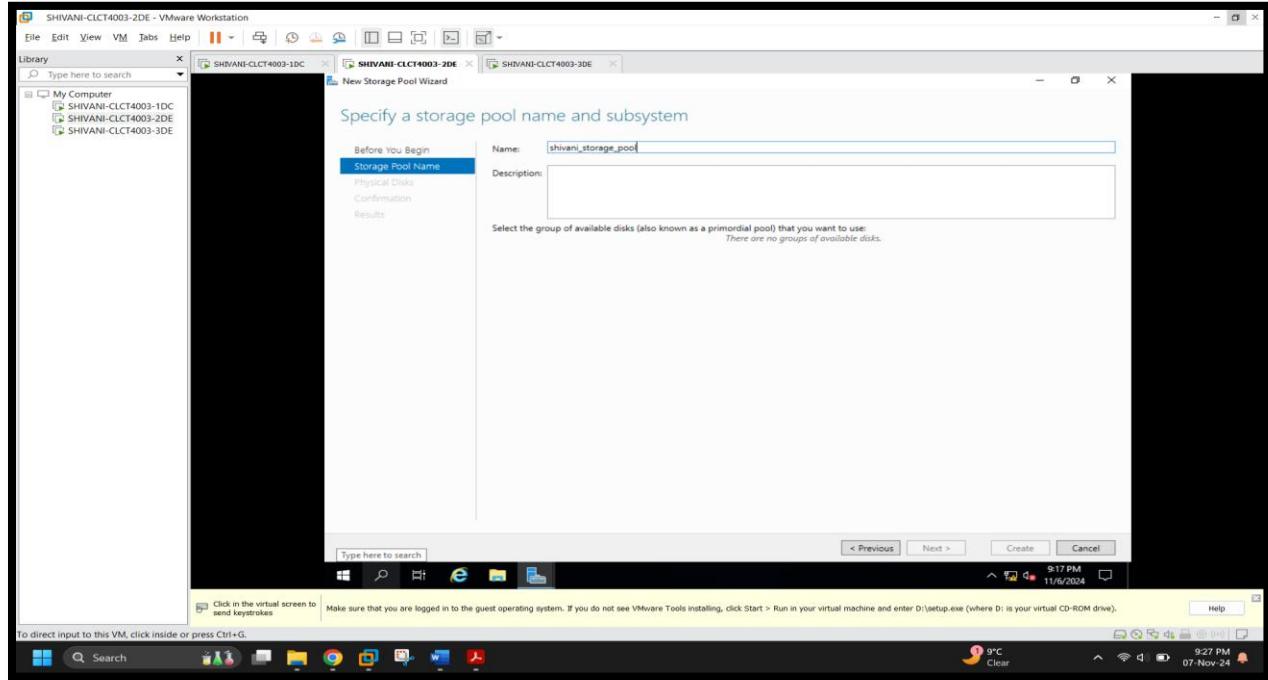
[Screenshot 15: Configured DNS Forwarder to 8.8.8.8 on Domain DNS Server on DC]



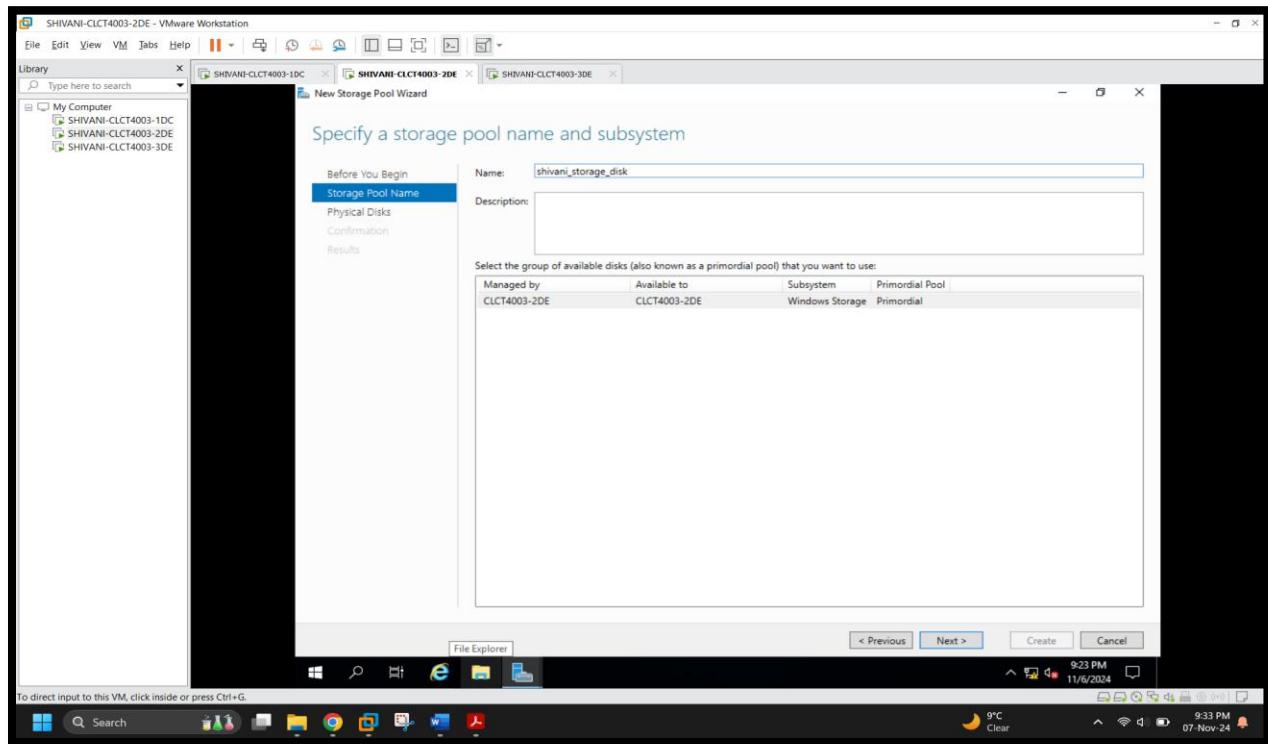
# Windows Server Security

## 5) CREATE A STORAGE POOL AND A VIRTUAL DISK

[Screenshot 16: Specifying storage pool name and subsystem as "shivani\_storage\_pool"]

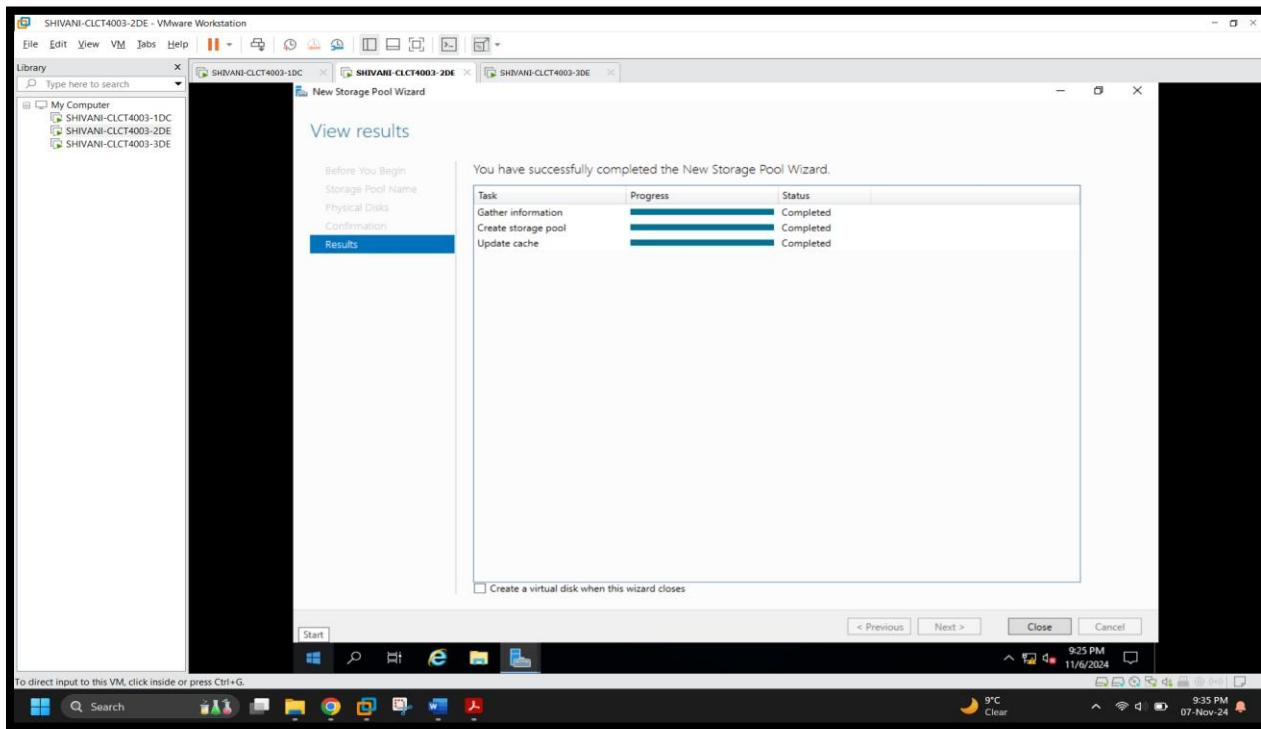


[Screenshot 17: Adding physical disks to the storage pool]

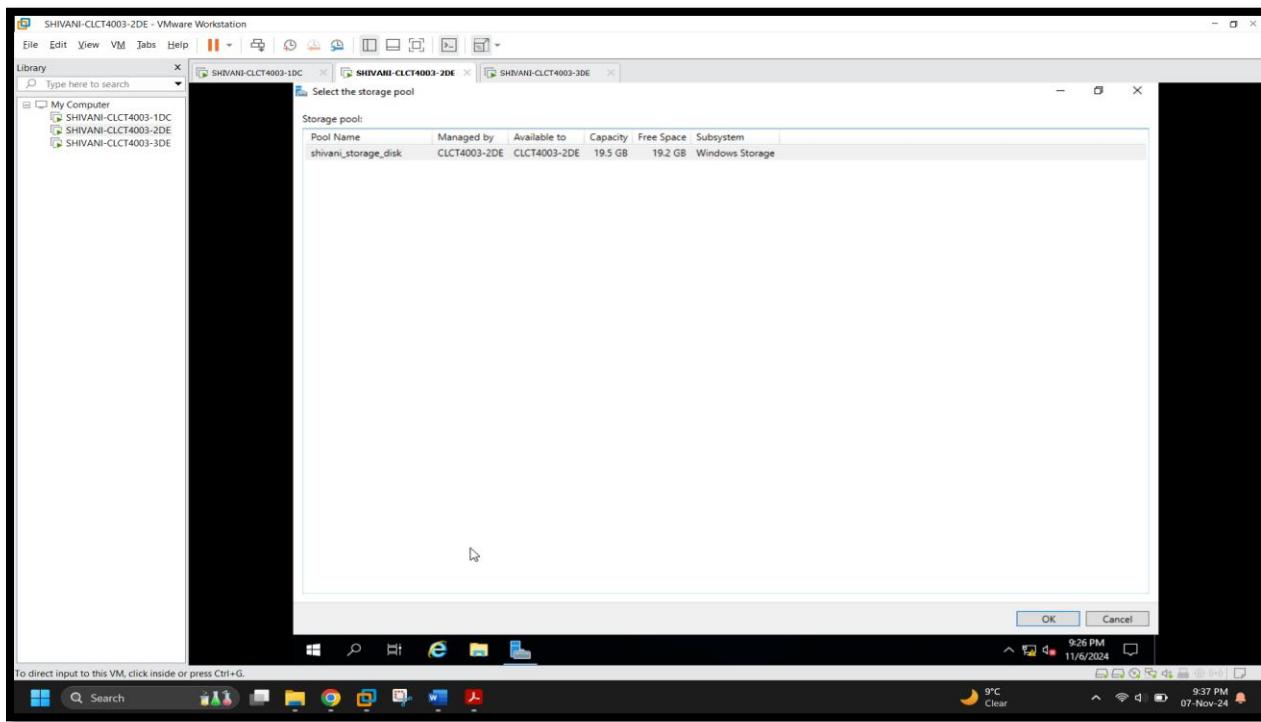


# Windows Server Security

[Screenshot 18: Successfully created the storage pool]

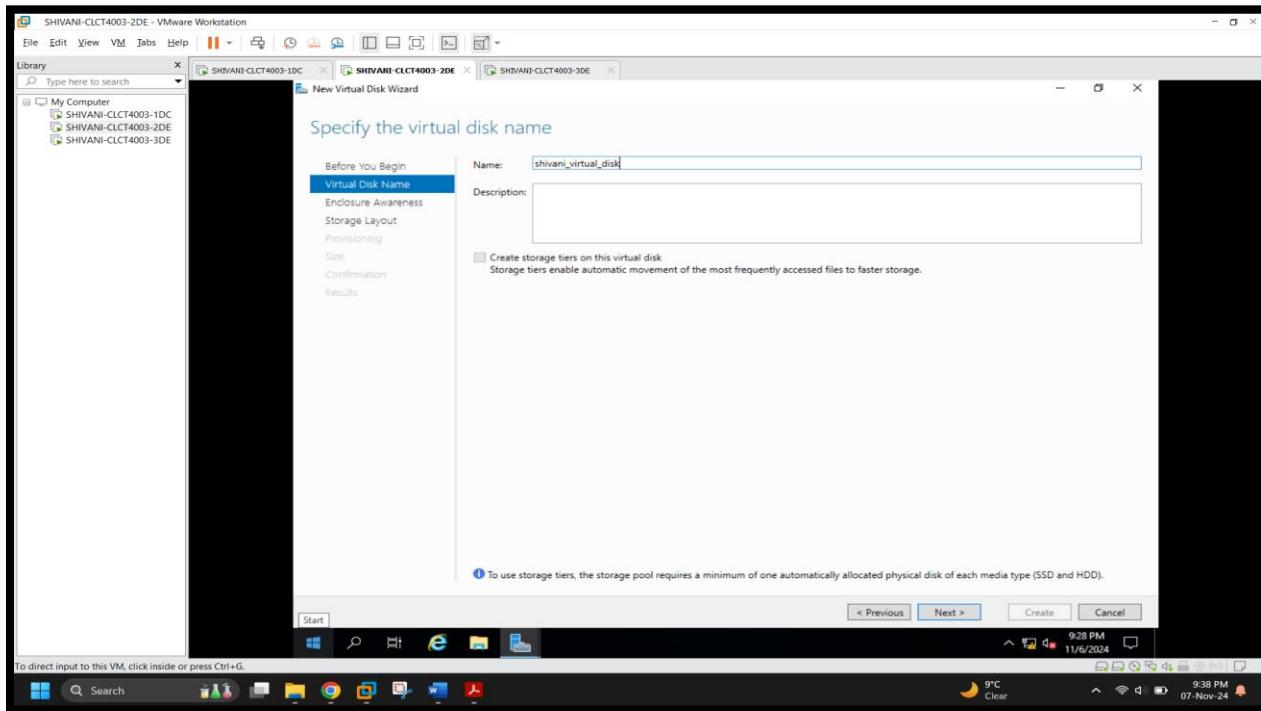


[Screenshot 19: Viewing the created storage pool with available space]

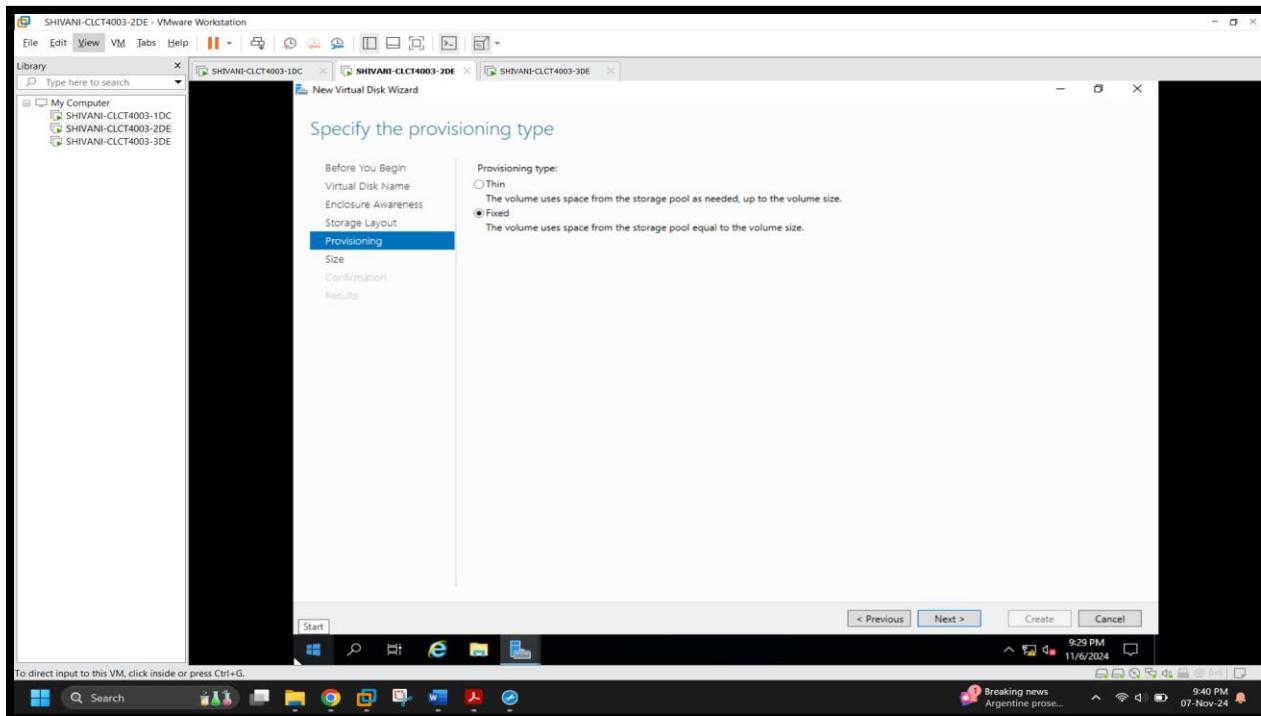


# Windows Server Security

[Screenshot 20: Specifying virtual disk name as "shivani\_virtual\_disk"]

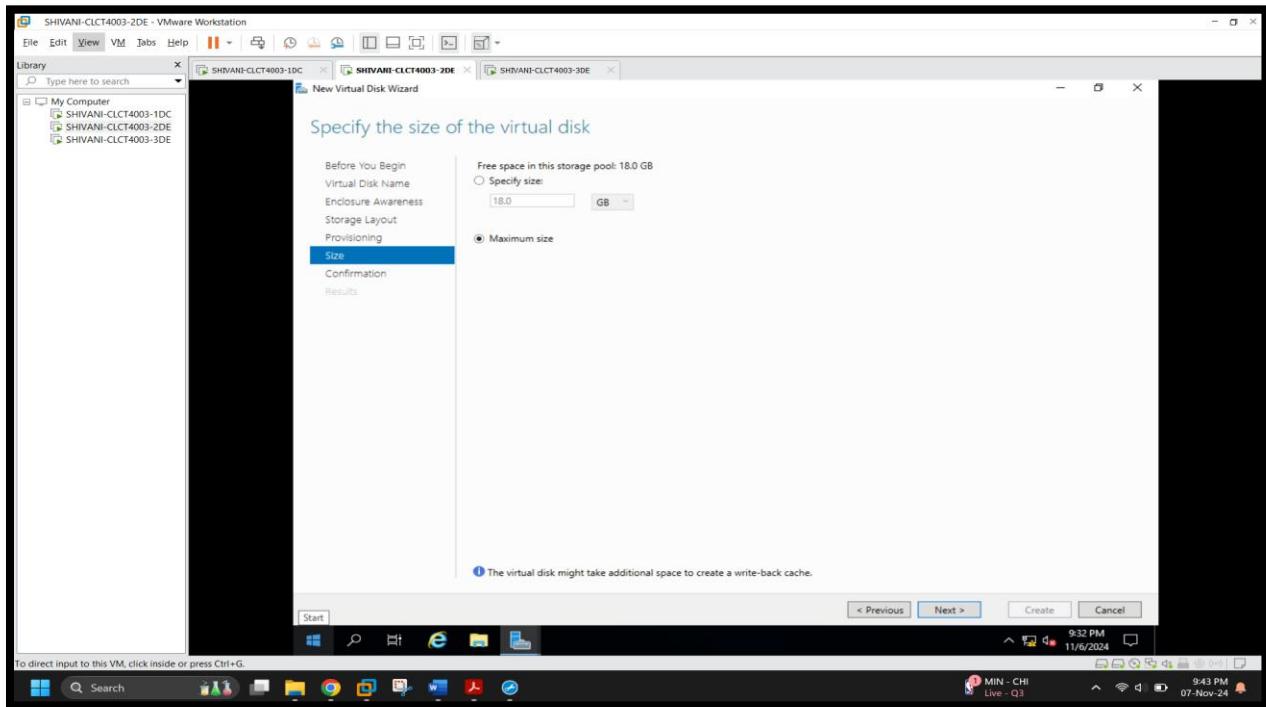


[Screenshot 21: Choosing the provisioning type for the virtual disk]

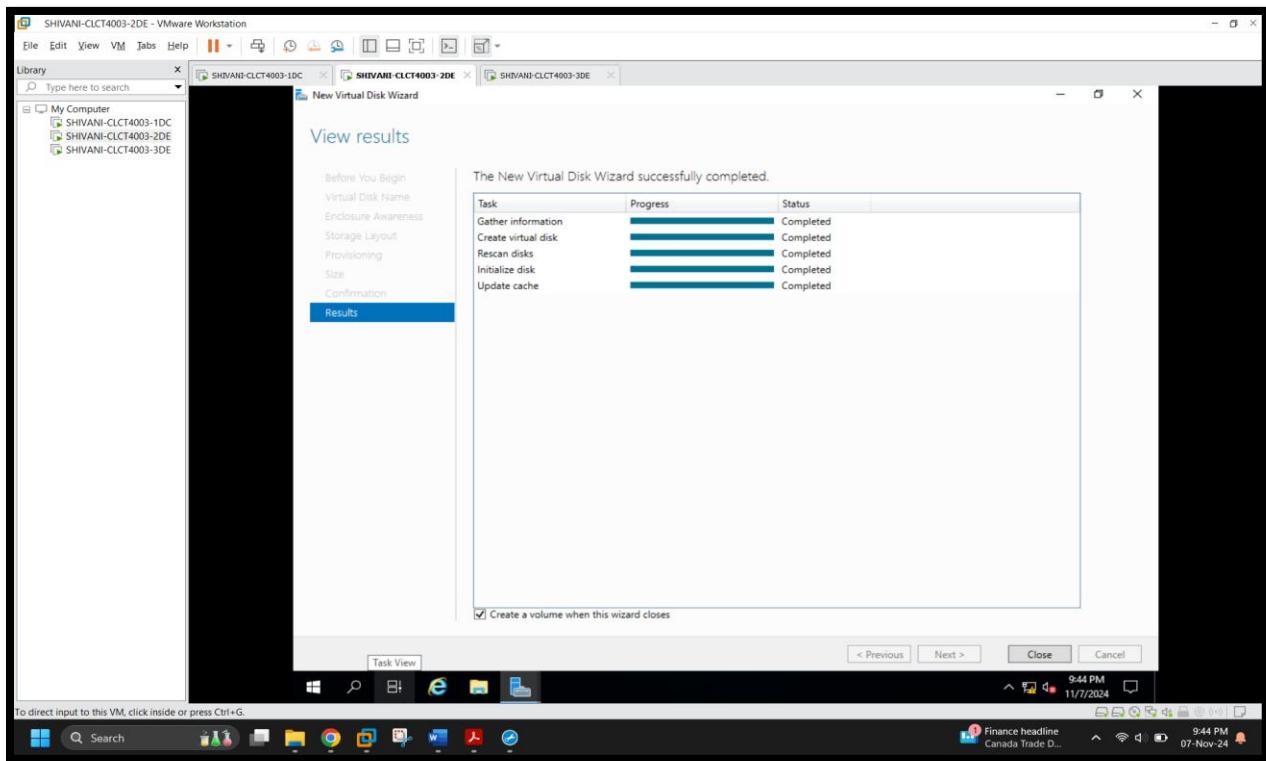


# Windows Server Security

[Screenshot 22: Specifying the size of the virtual disk]

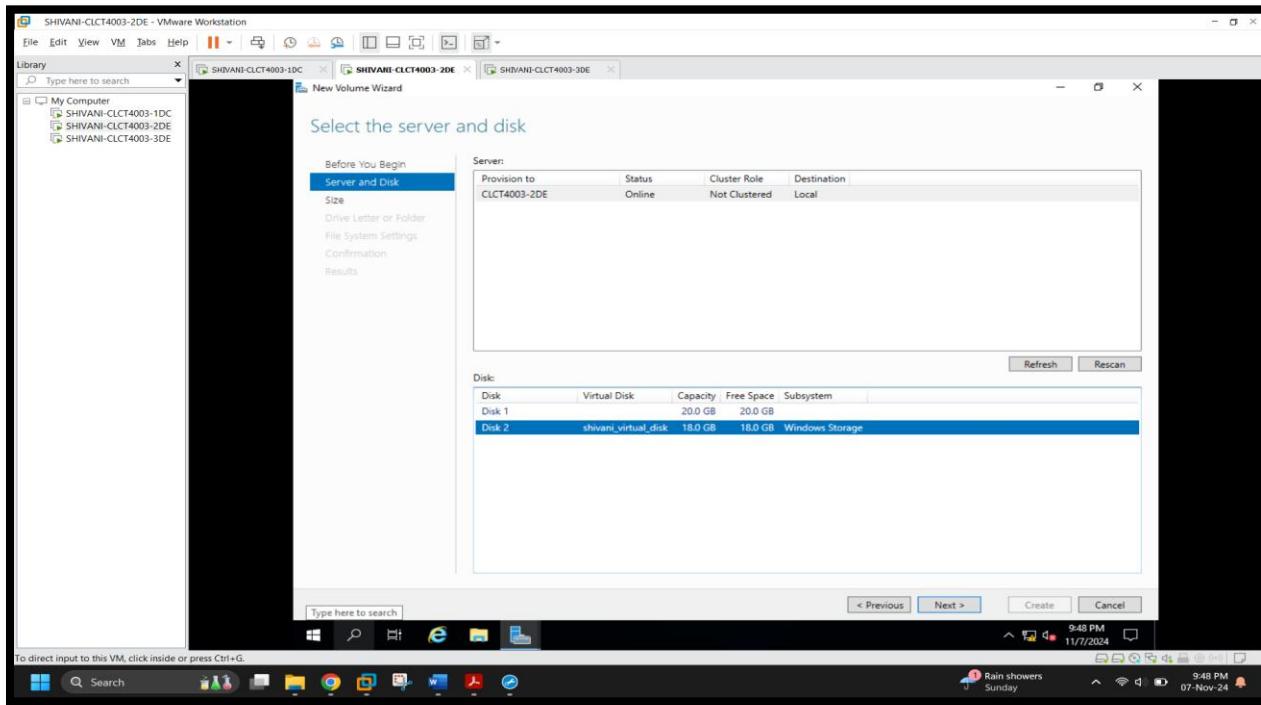


[Screenshot 23: Successfully completed virtual disk creation in the wizard]

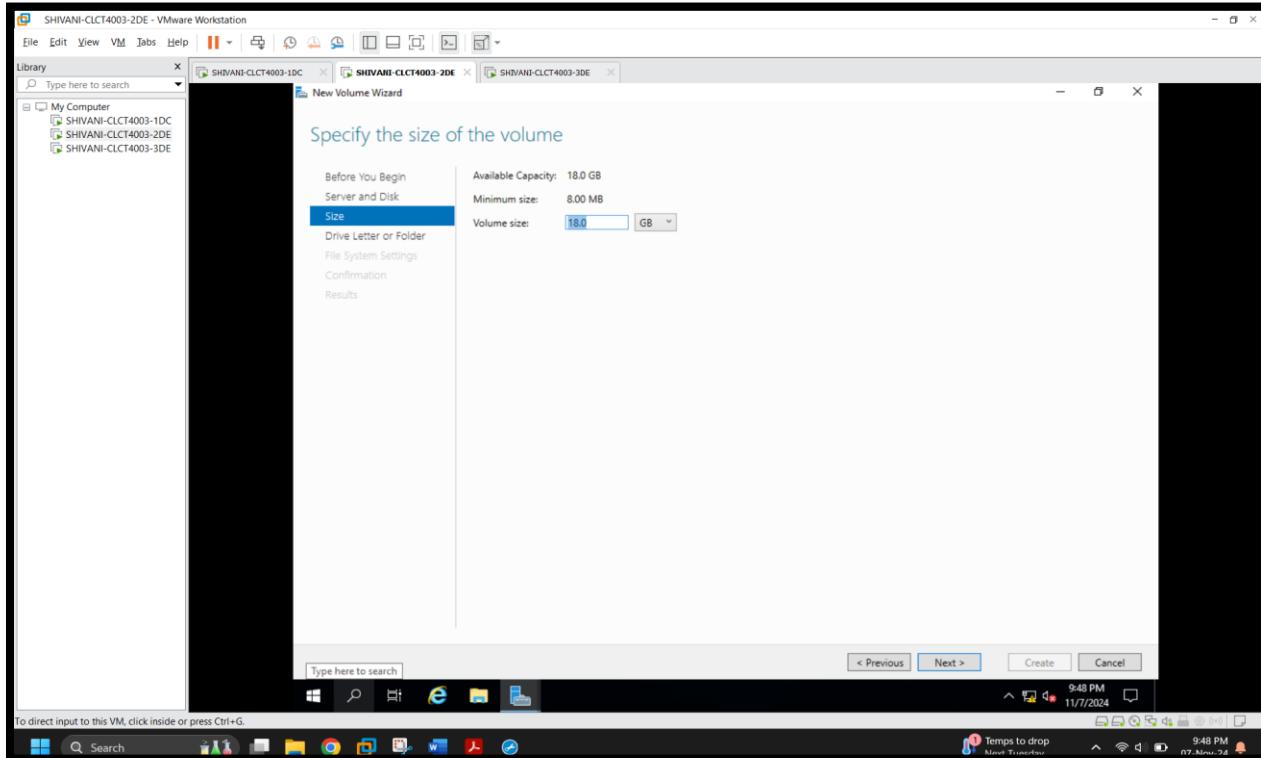


# Windows Server Security

[Screenshot 24: Selecting server and disk for new volume on CLCT4003-2DE.]

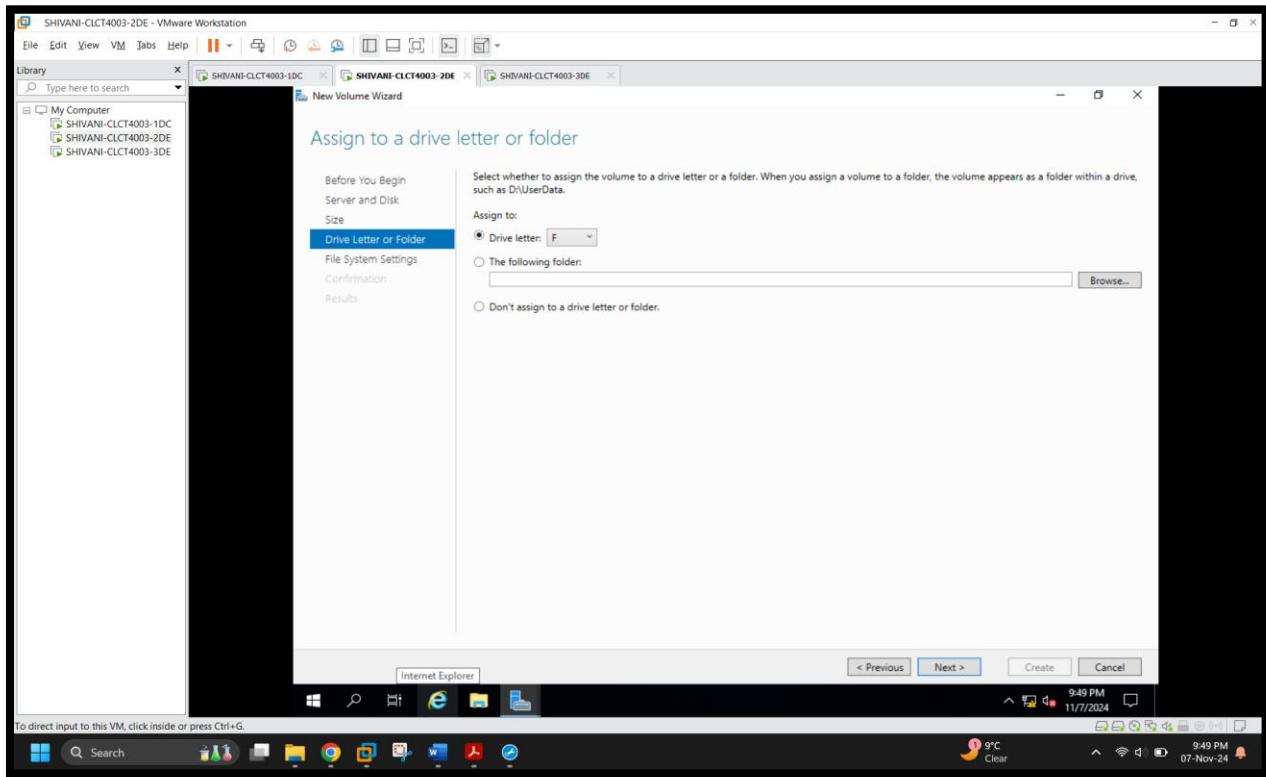


[Screenshot 25: Specifying volume size as 18 GB.]

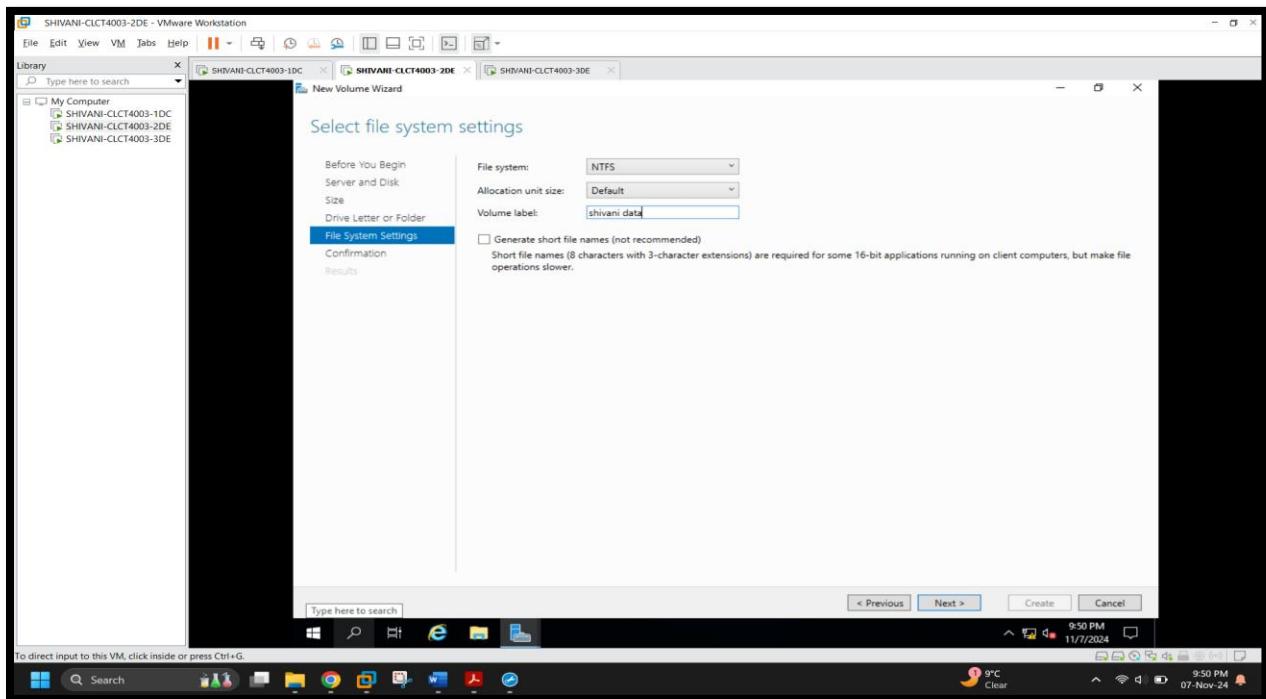


# Windows Server Security

[Screenshot 26: Assigning drive letter to the new volume.]

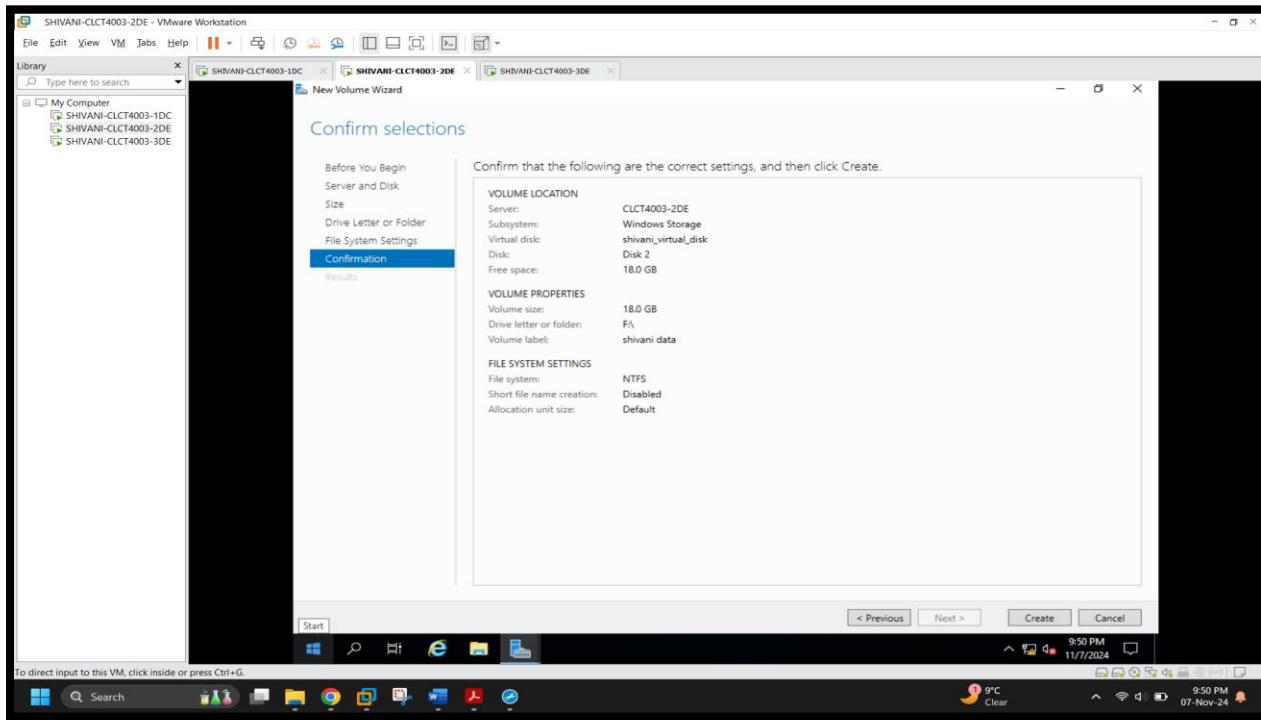


[Screenshot 27: Setting NTFS file system and volume label.]

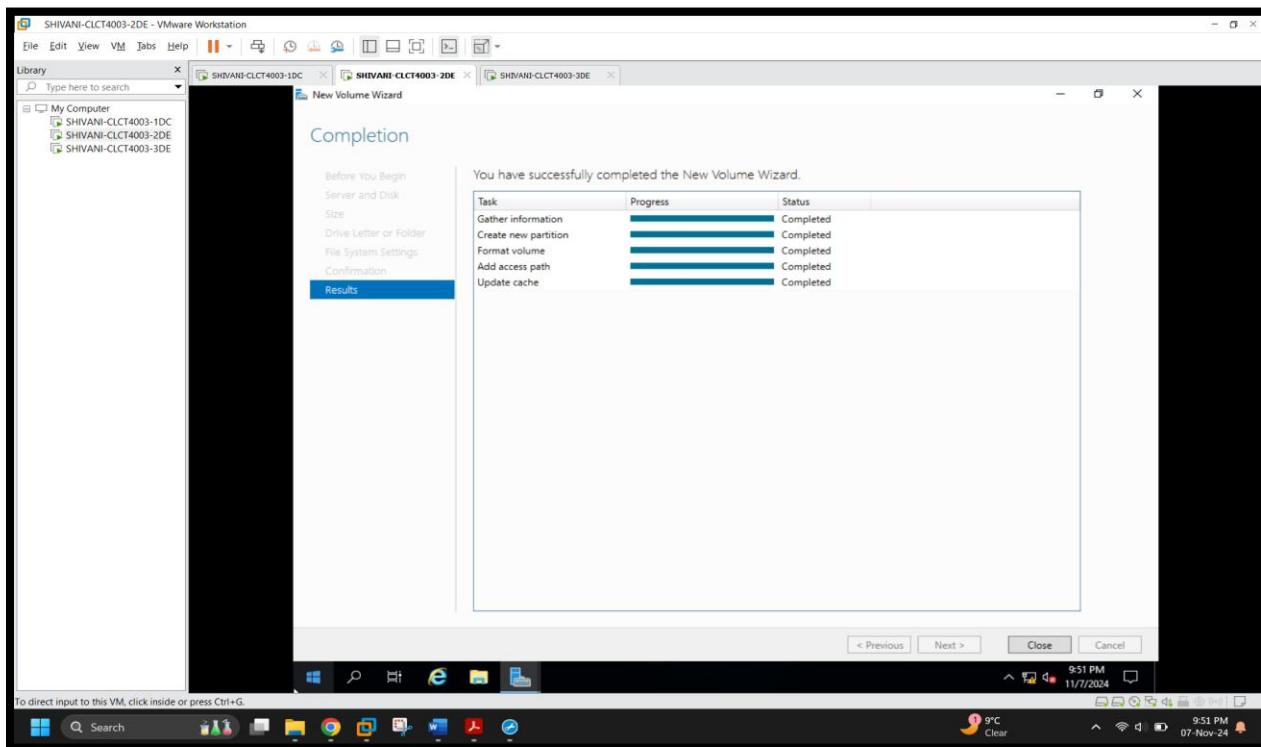


# Windows Server Security

[Screenshot 28: Confirming settings for volume creation.]

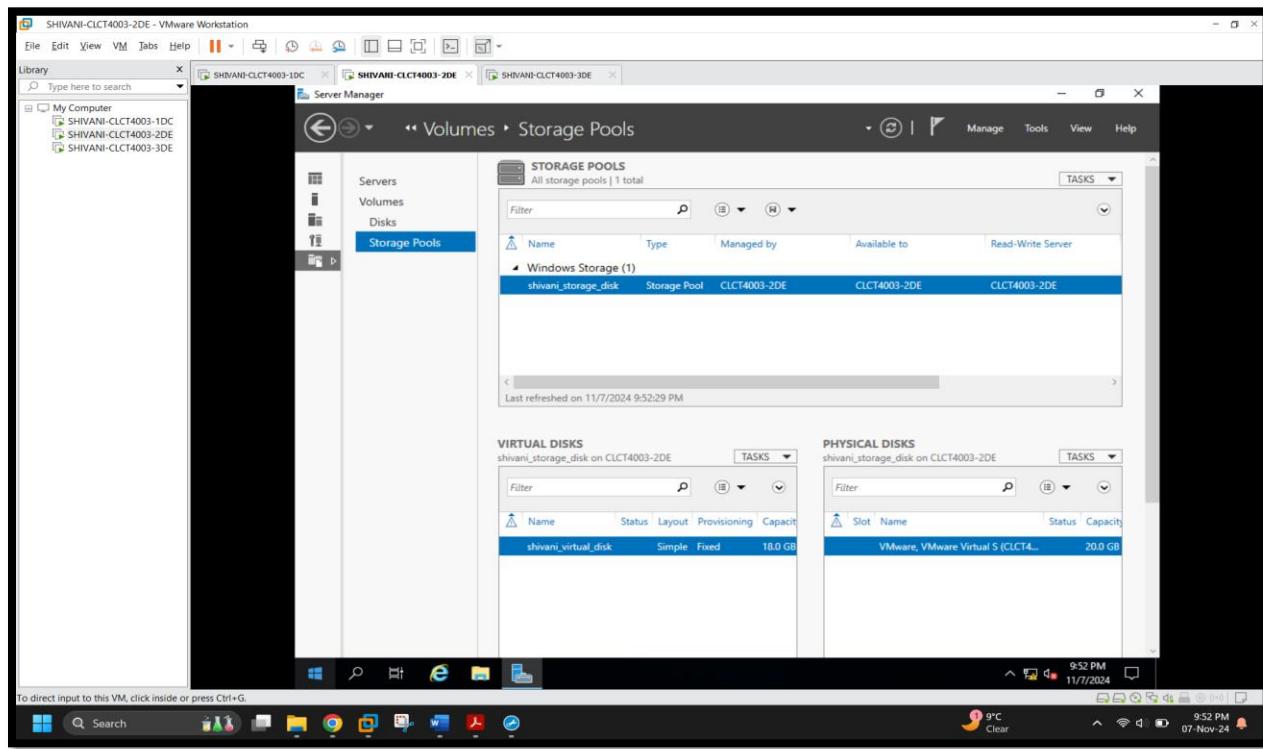


[Screenshot 29: Volume creation completed successfully.]

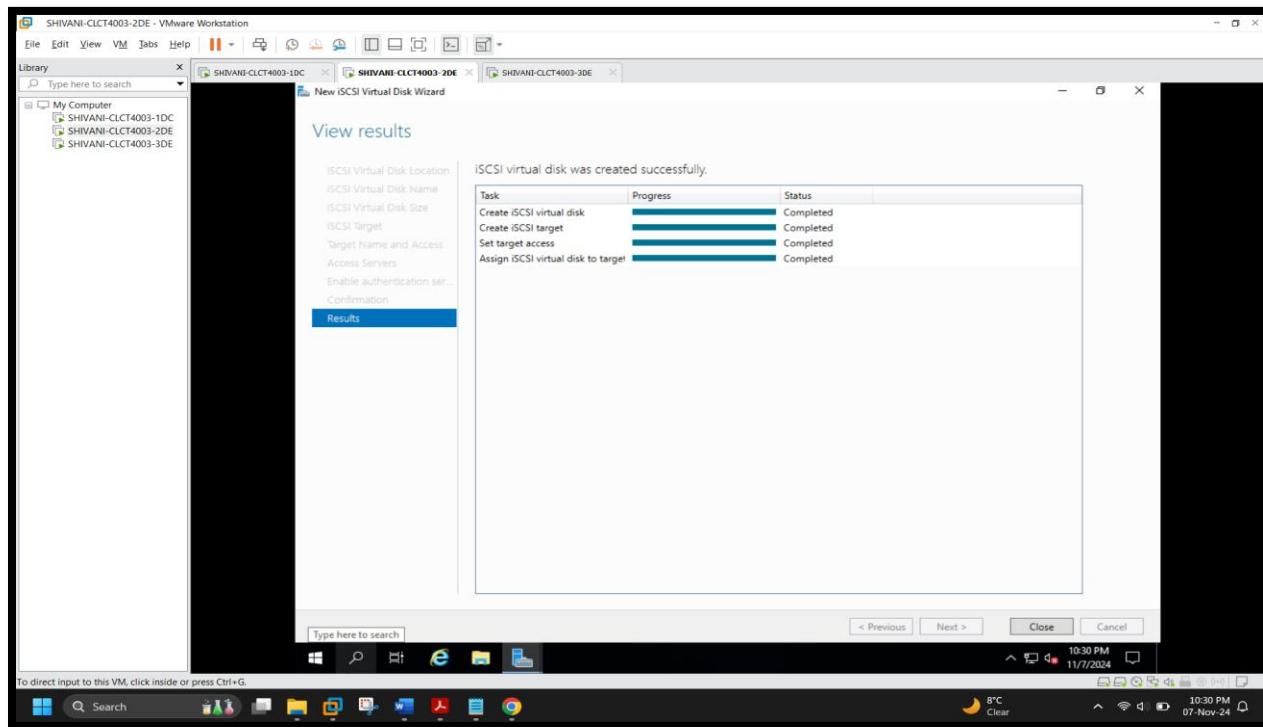


# Windows Server Security

[Screenshot 30: New storage pool and virtual disk displayed in Server Manager.]



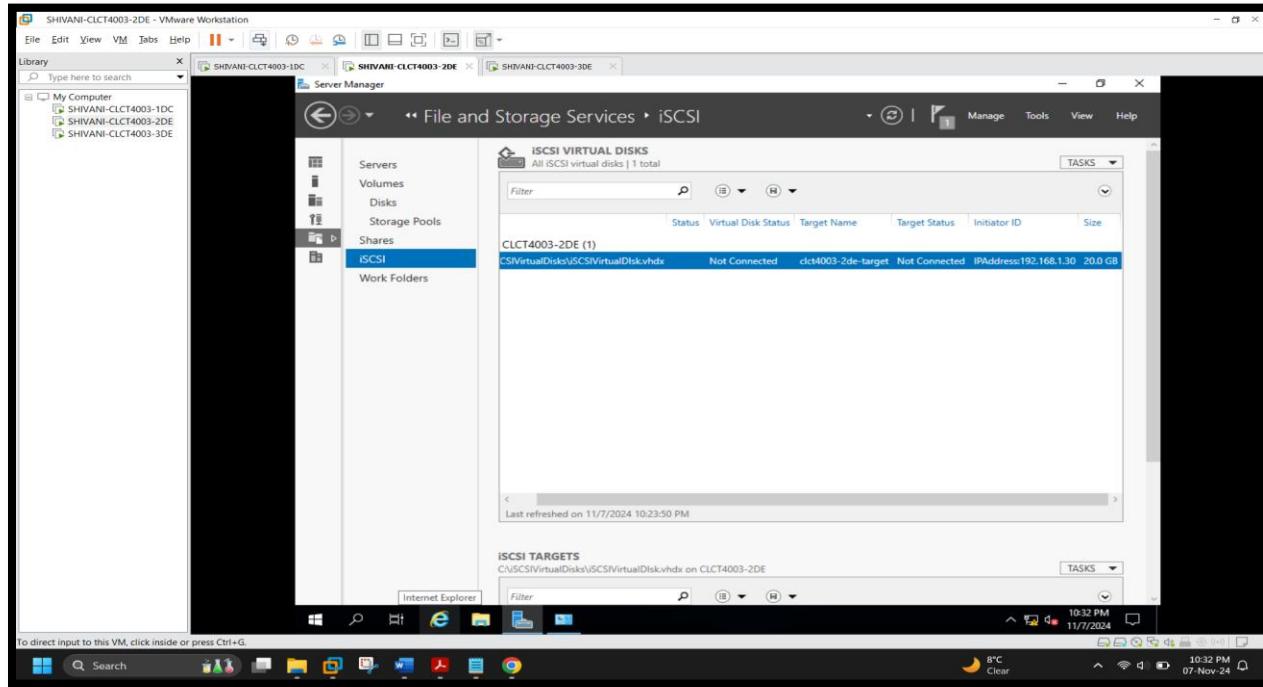
[Screenshot 31: iSCSI Virtual Disk Created successfully]



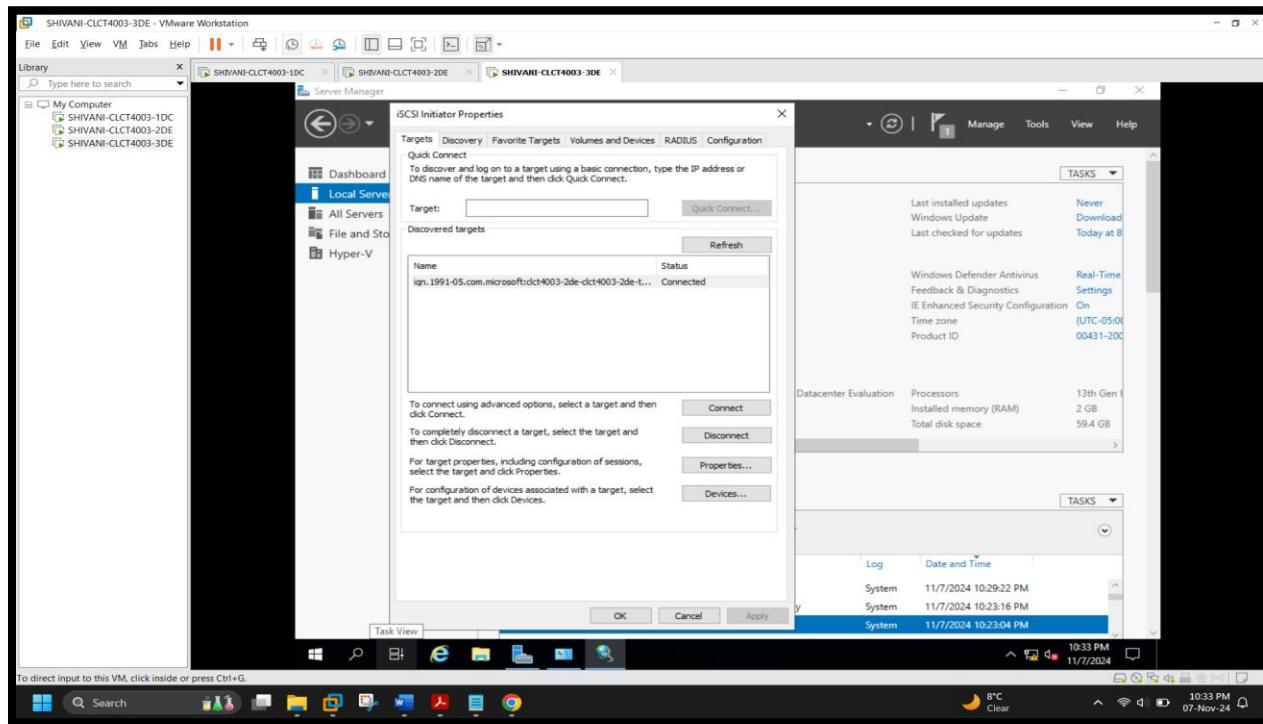
# Windows Server Security

## 6) CREATE AN iSCSI DISK ON SERVER 2 AND ATTACH IT TO SERVER 3

[Screenshot 32: Overview of iSCSI Virtual Disks in Server Manager of Node 2]

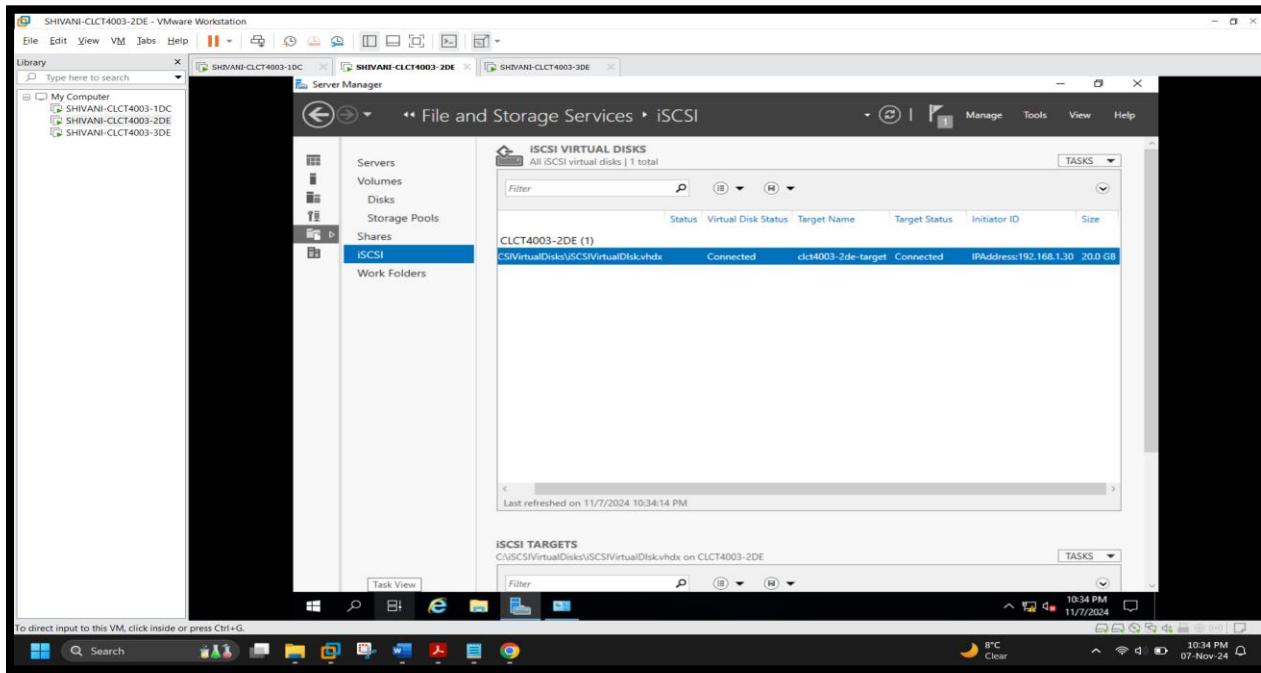


[Screenshot 33: iSCSI Initiator Properties Showing Connected Target]

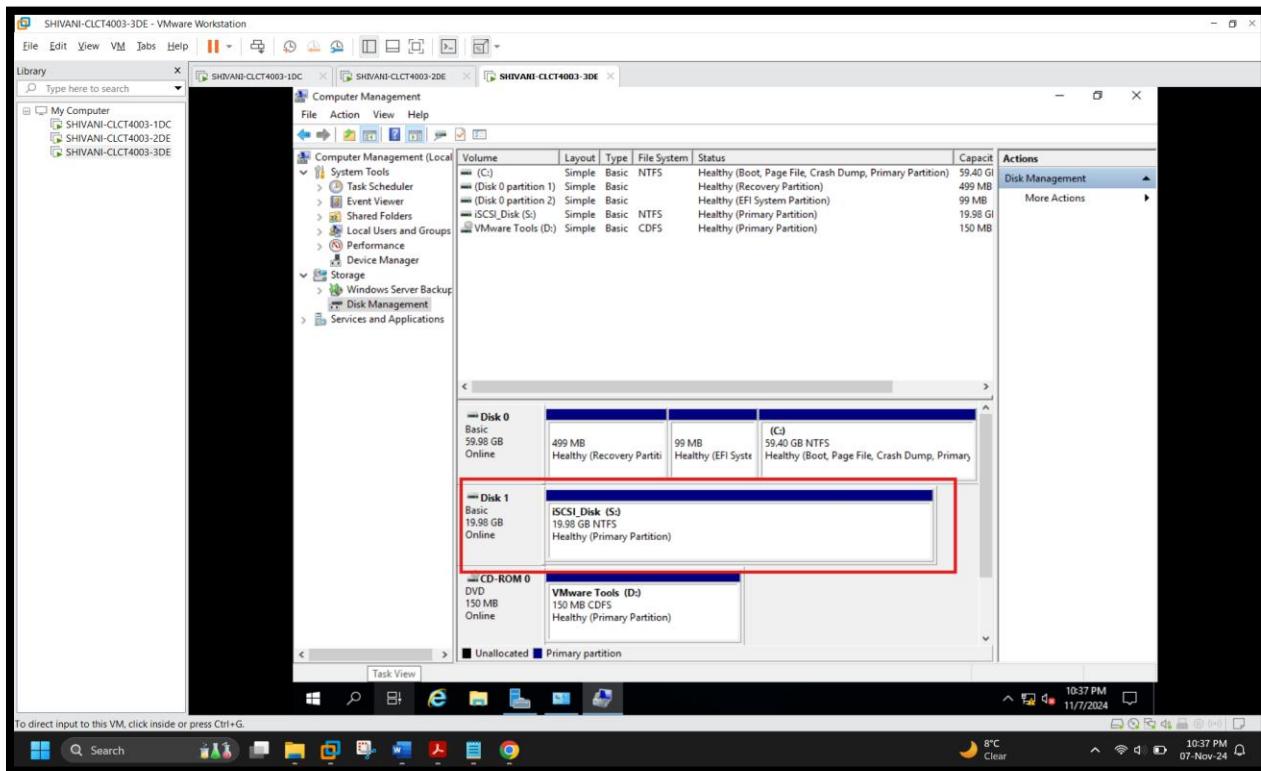


# Windows Server Security

[Screenshot 34: iSCSI Virtual Disk Connection Status]



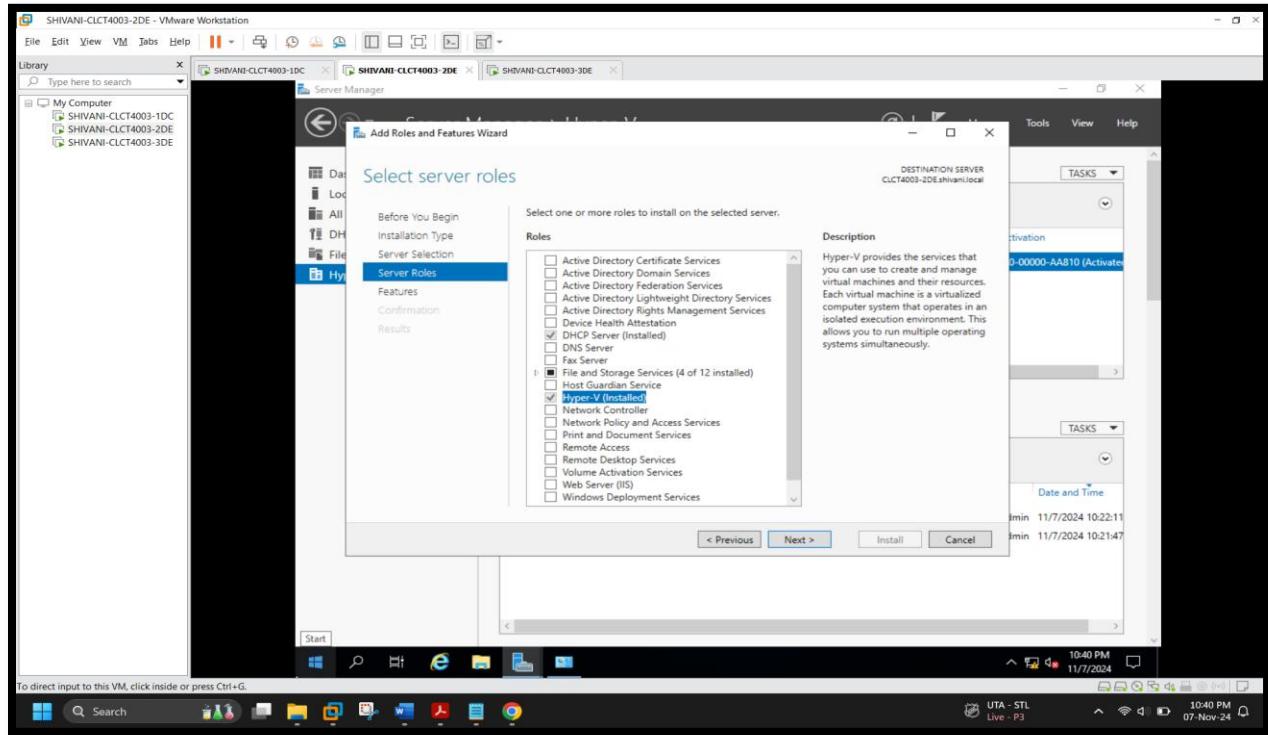
[Screenshot: 35: Disk Has been attached, created, available and Initialized on Node 3 from Node 2]



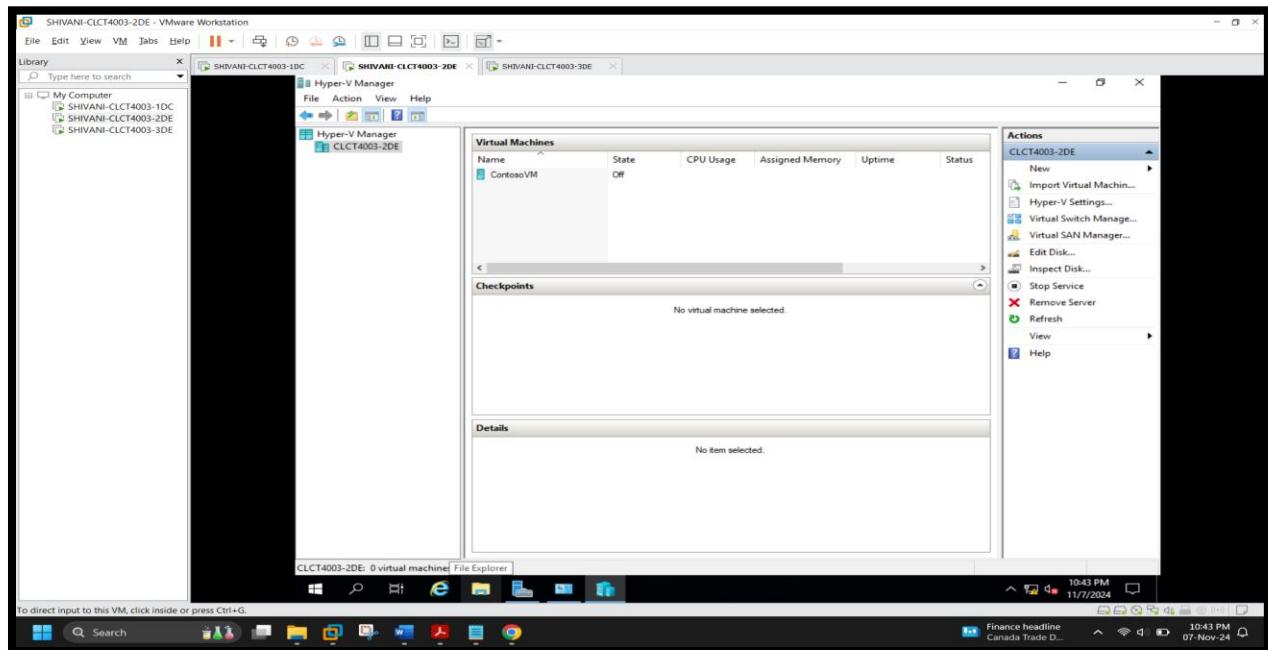
# Windows Server Security

## 7) INSTALL HYPER-V ROLE ON SERVER 2 AND CREATE A VIRTUAL MACHINE

[Screenshot 36: Installed Hyper V Role on Server 2]



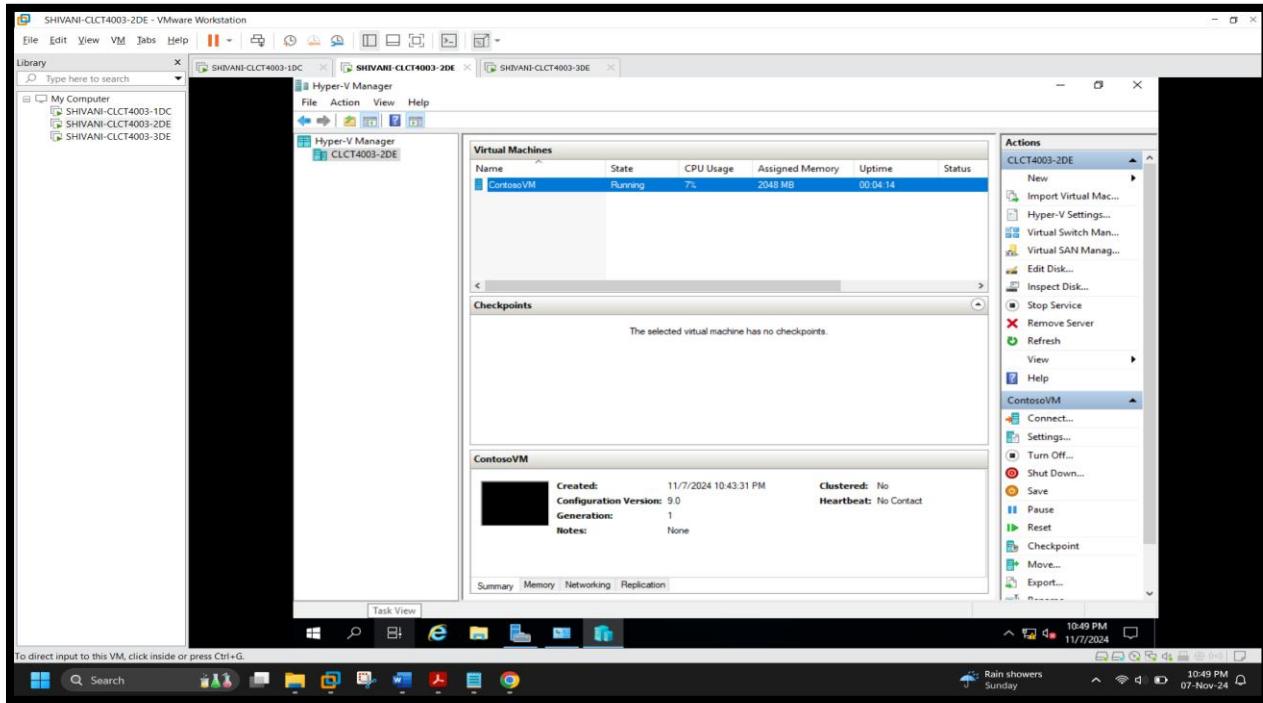
[Screenshot 37: Created New Virtual Machine on CLCT4003-2DE]



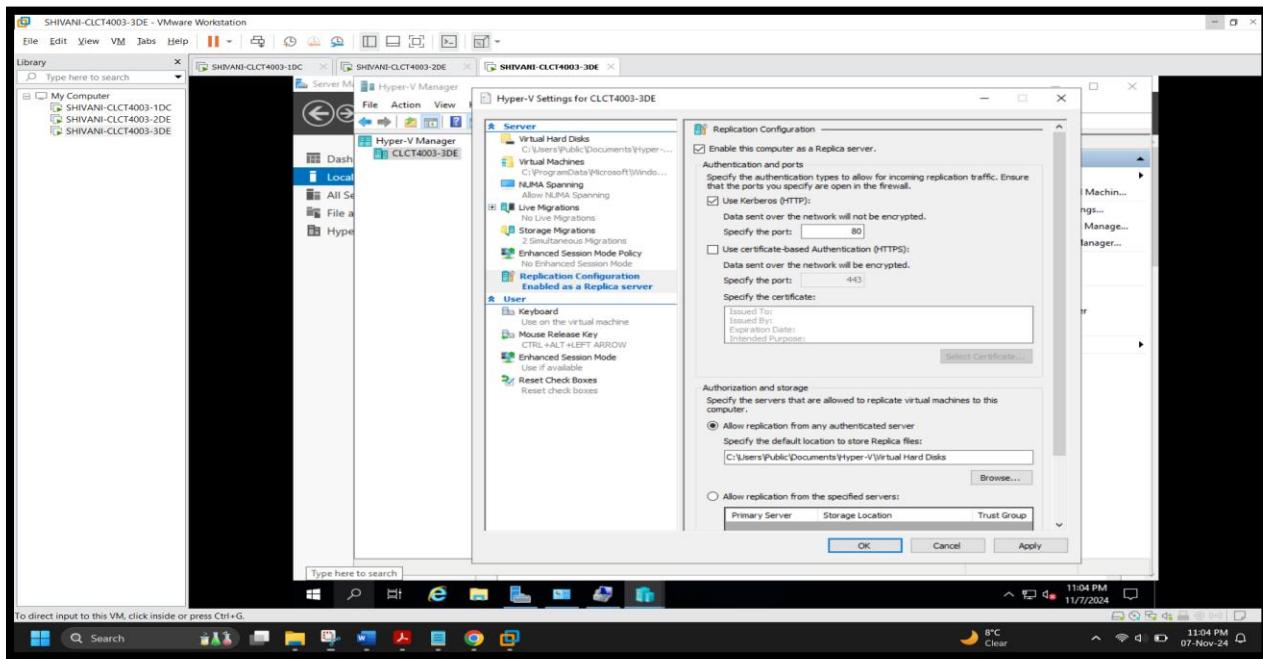
# Windows Server Security

## 8) INSTALL HYPER-V ROLE ON SERVER 3 AND CONFIGURE HYPER-V REPLICA

[Screenshot 38: "ContosoVM" Running Status in Hyper-V Manager]

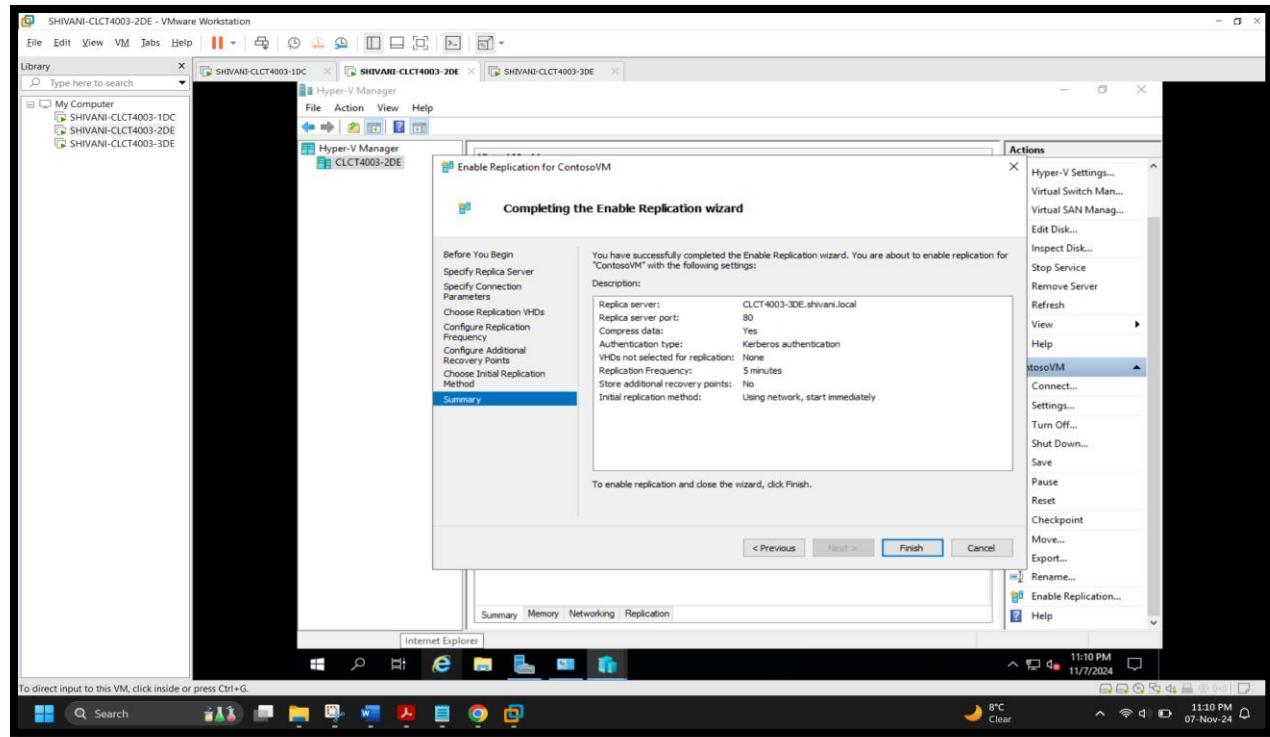


[Screenshot 39: Configuring CLCT4003-3DE as a Replica server in Hyper-V settings]

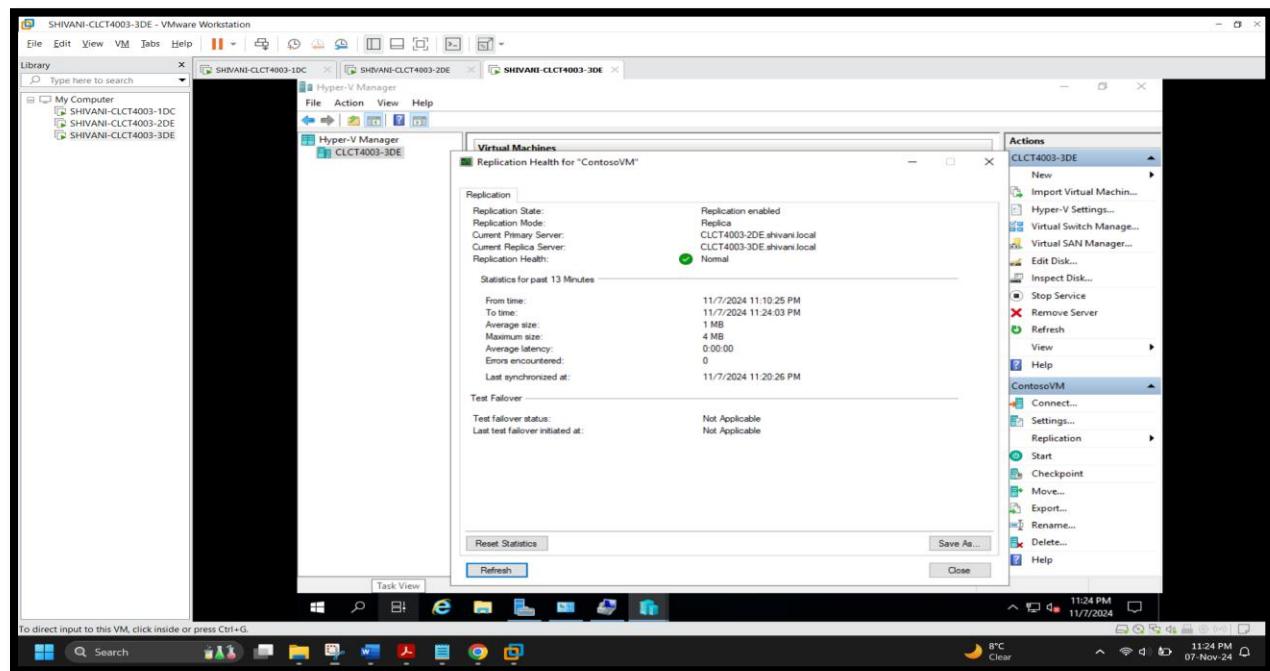


# Windows Server Security

[ Screenshot 40: Completing the Enable Replication for "ContosoVM" on Server 2 with replication settings]

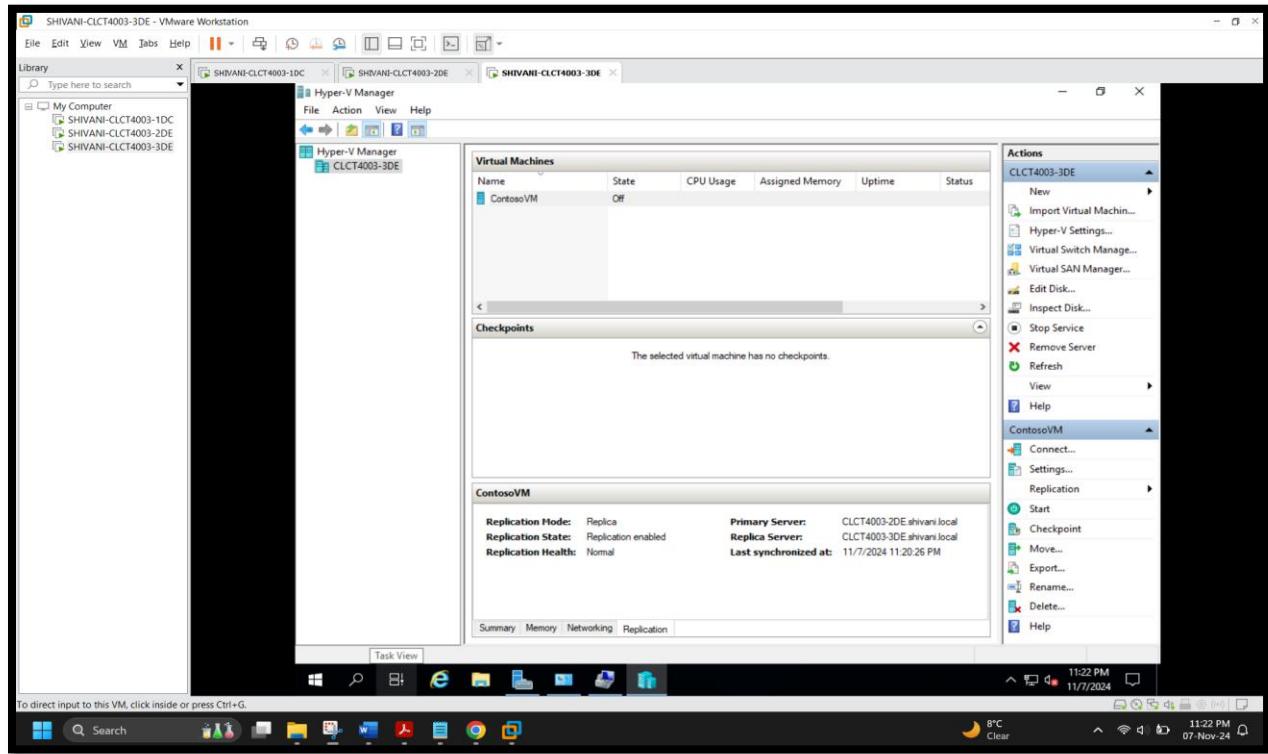


[ Screenshot 41: Replication Health for "ContosoVM" showing replication enabled, with status and statistics on Server 3]



# Windows Server Security

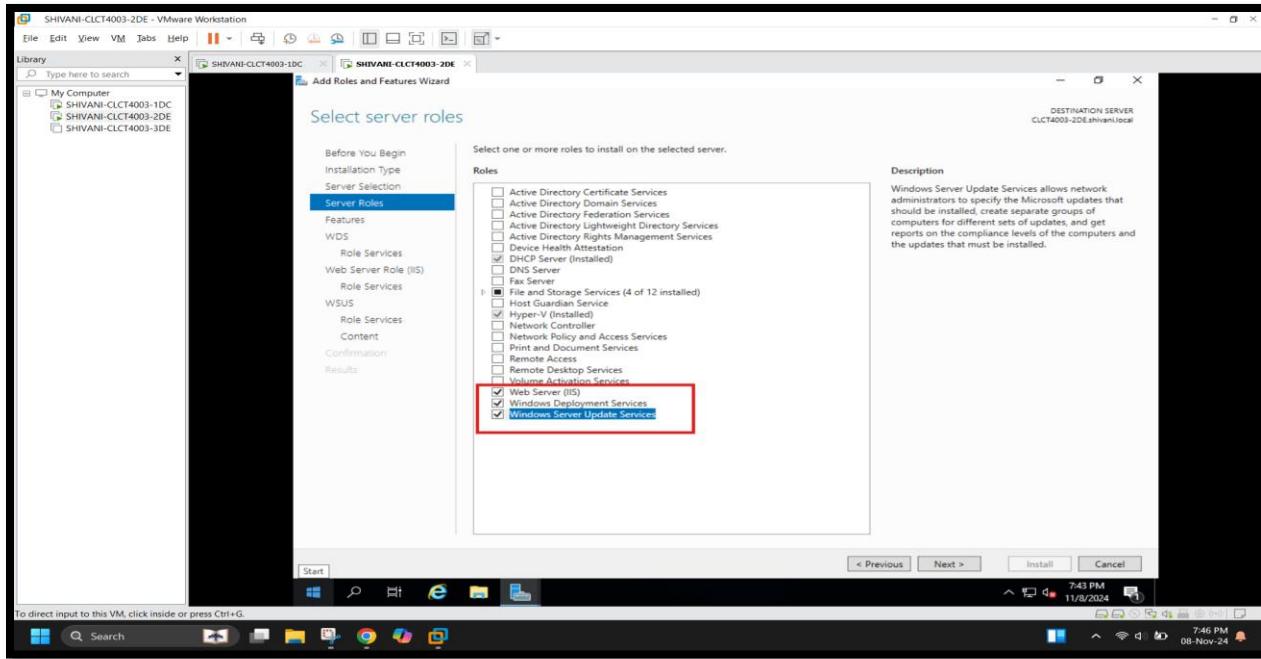
[Screenshot 42: ContosoVM with replication mode and replication health details on Server 3]



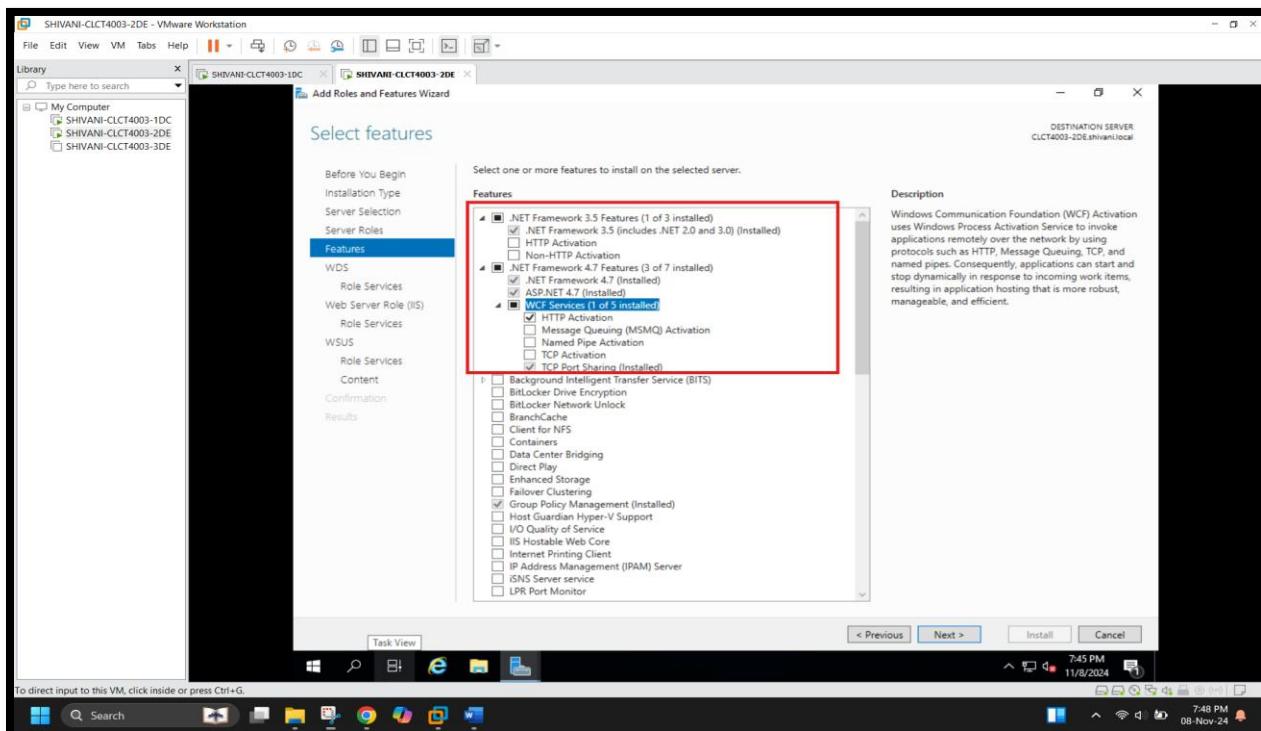
# Windows Server Security

## 9) INSTALL AND CONFIGURE WDS

[Screenshot 43: Installed Server Roles for WDS and WSUS]

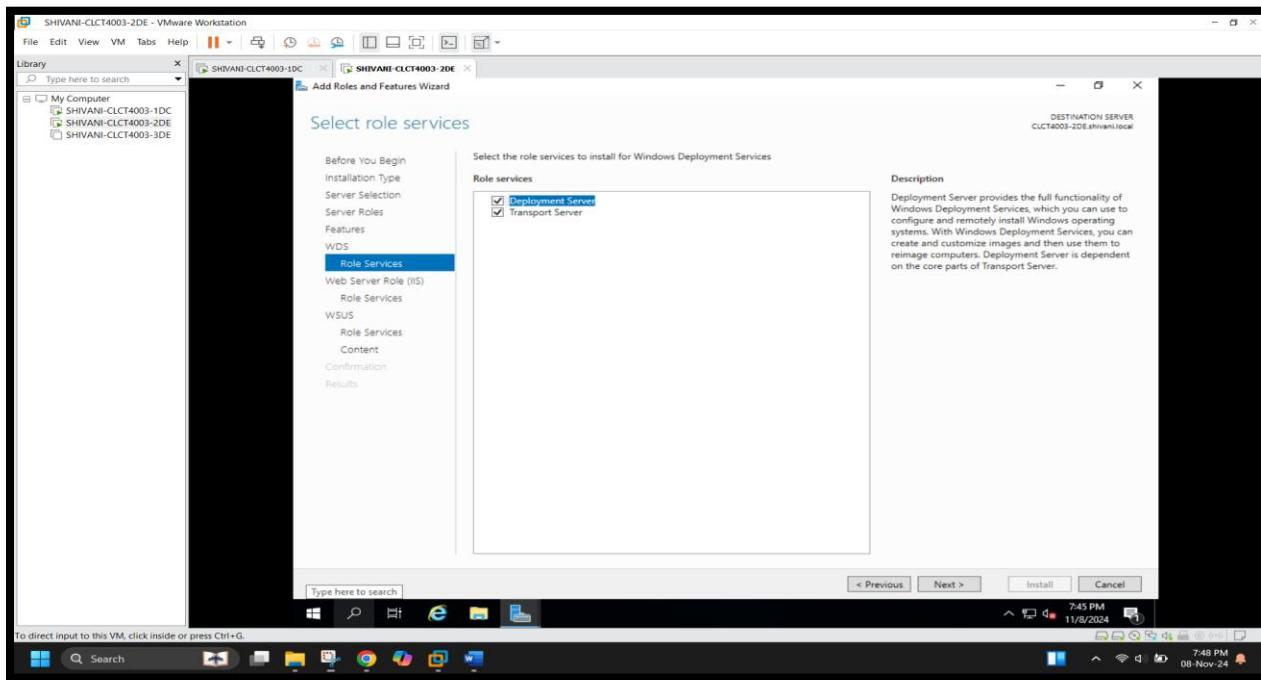


[Screenshot 44: Selecting Features such as .Net framework]

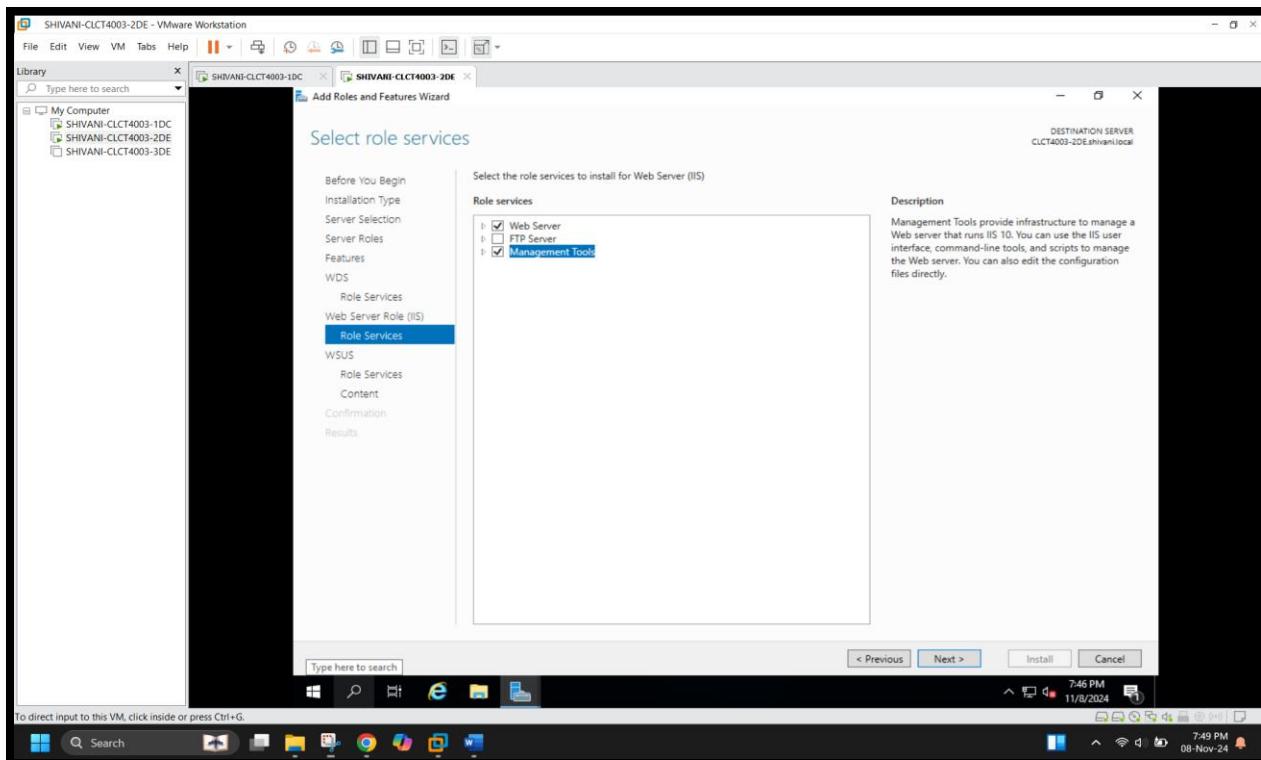


# Windows Server Security

[Screenshot 45: Selecting Roles on WDS]

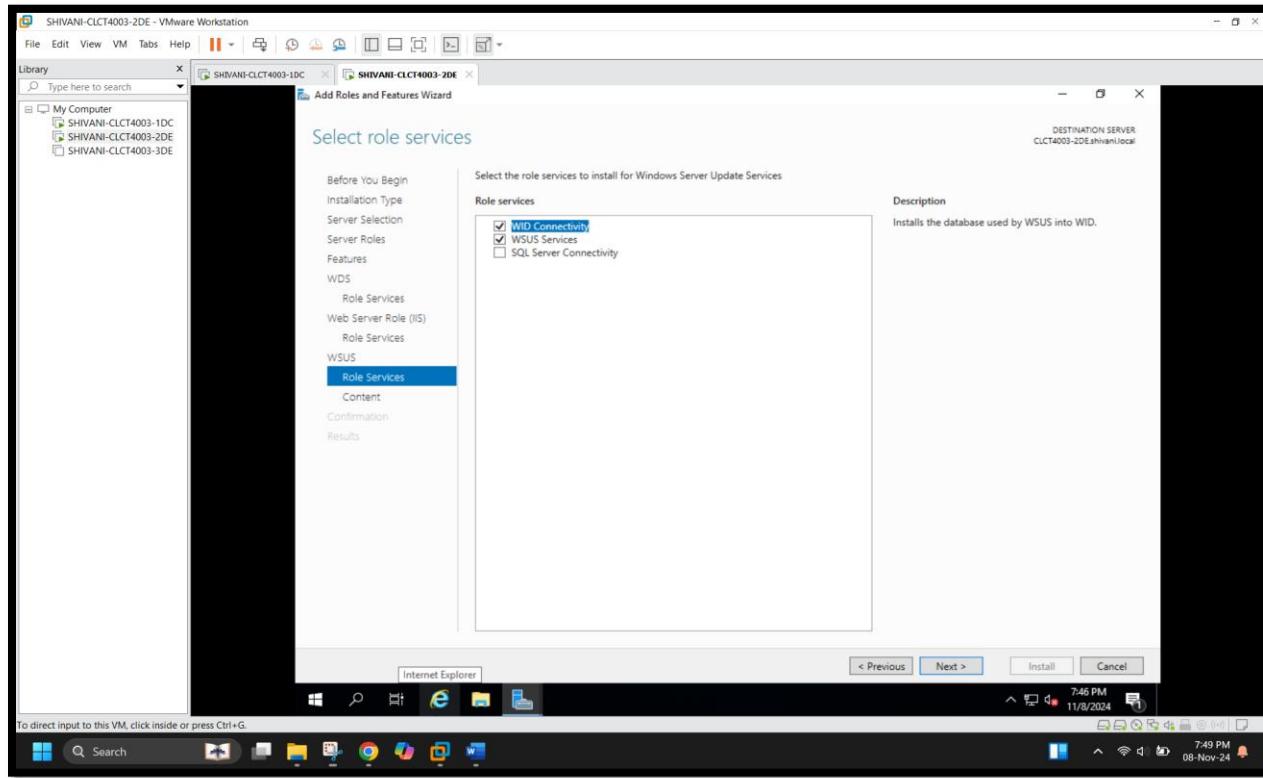


[Screenshot 46: Selecting Roles Services on Web Server IIS]

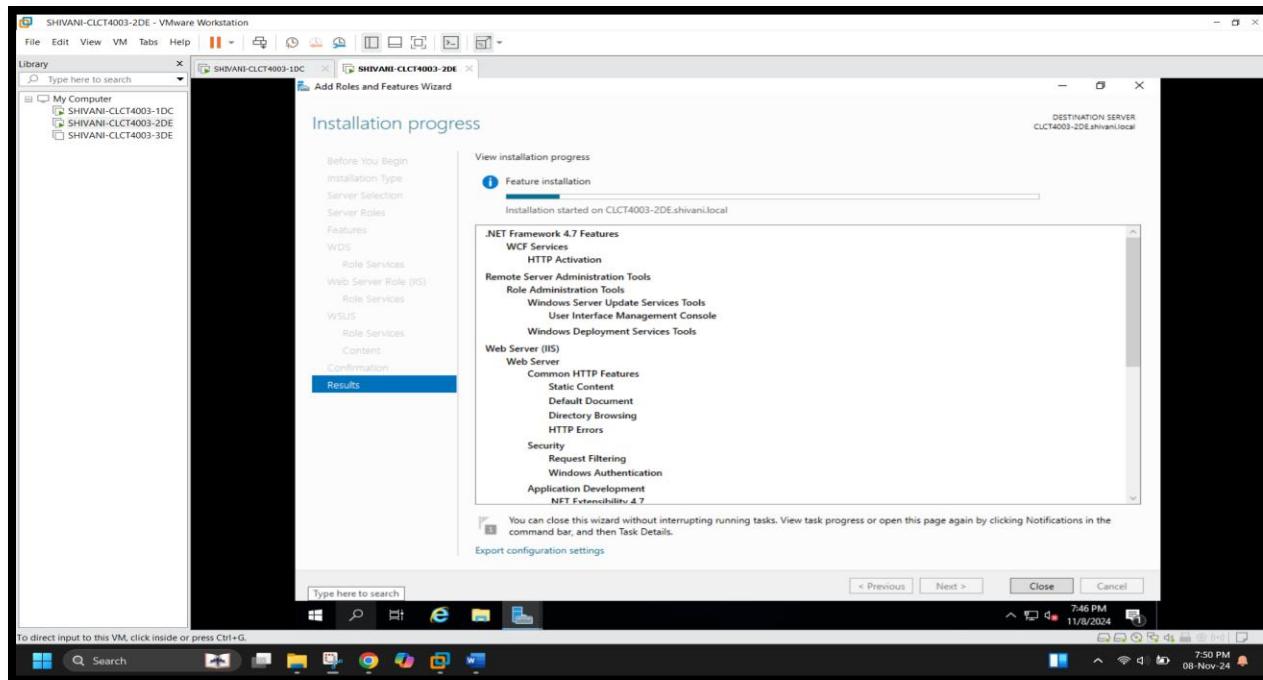


# Windows Server Security

[Screenshot 47: Selecting Role Services such as WID connectivity and WSUS Services on WDS]

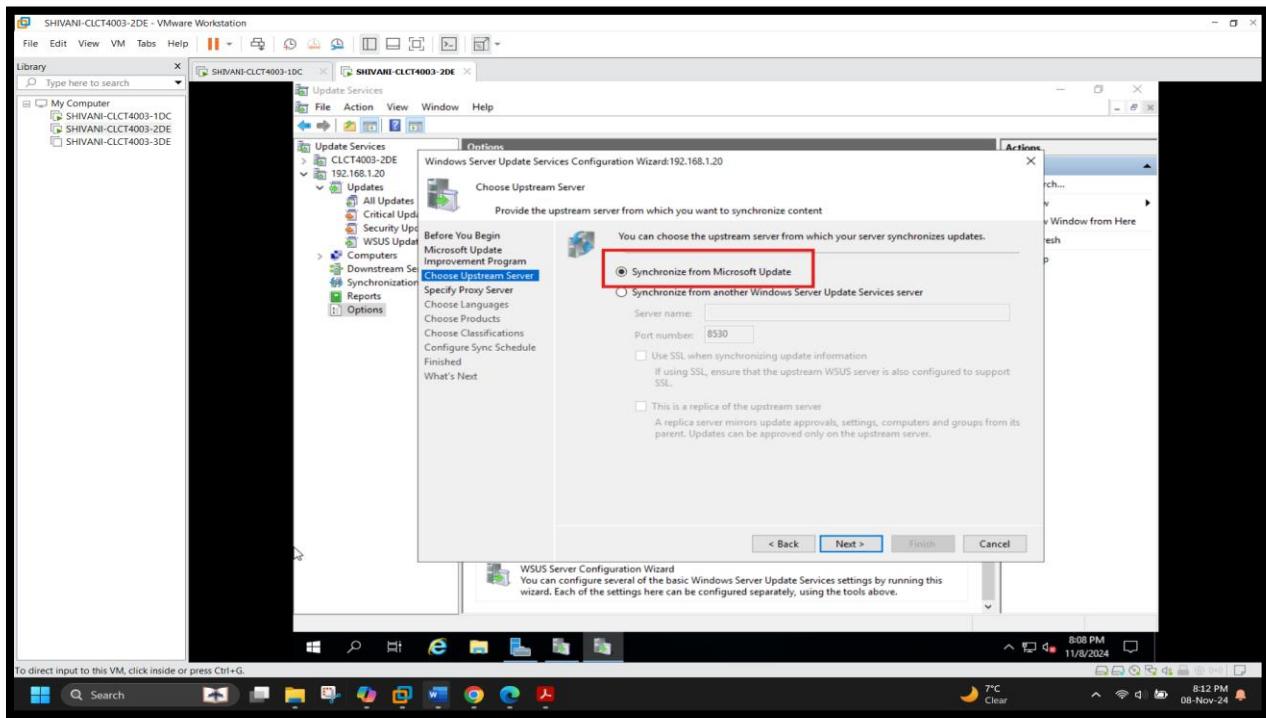


[Screenshot 48: Installed WDS and WSUS on Server 2]

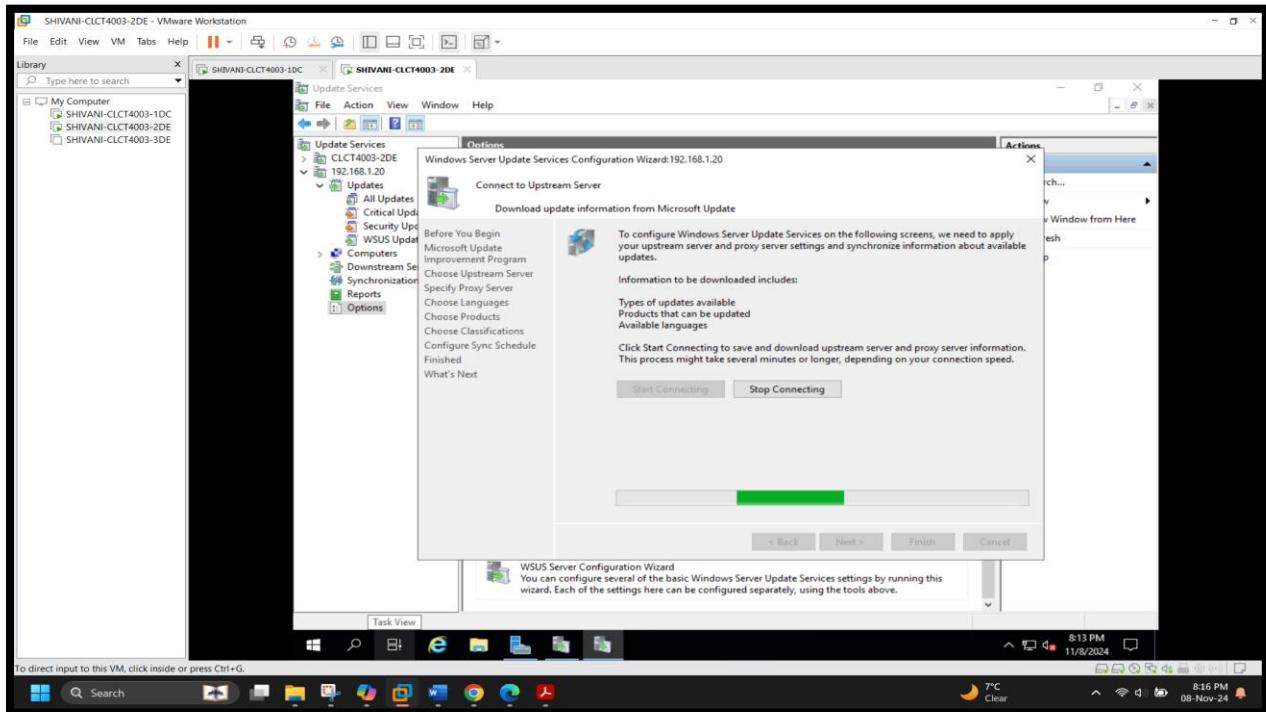


# Windows Server Security

[ Screenshot 49: Selecting Upstream Server ]

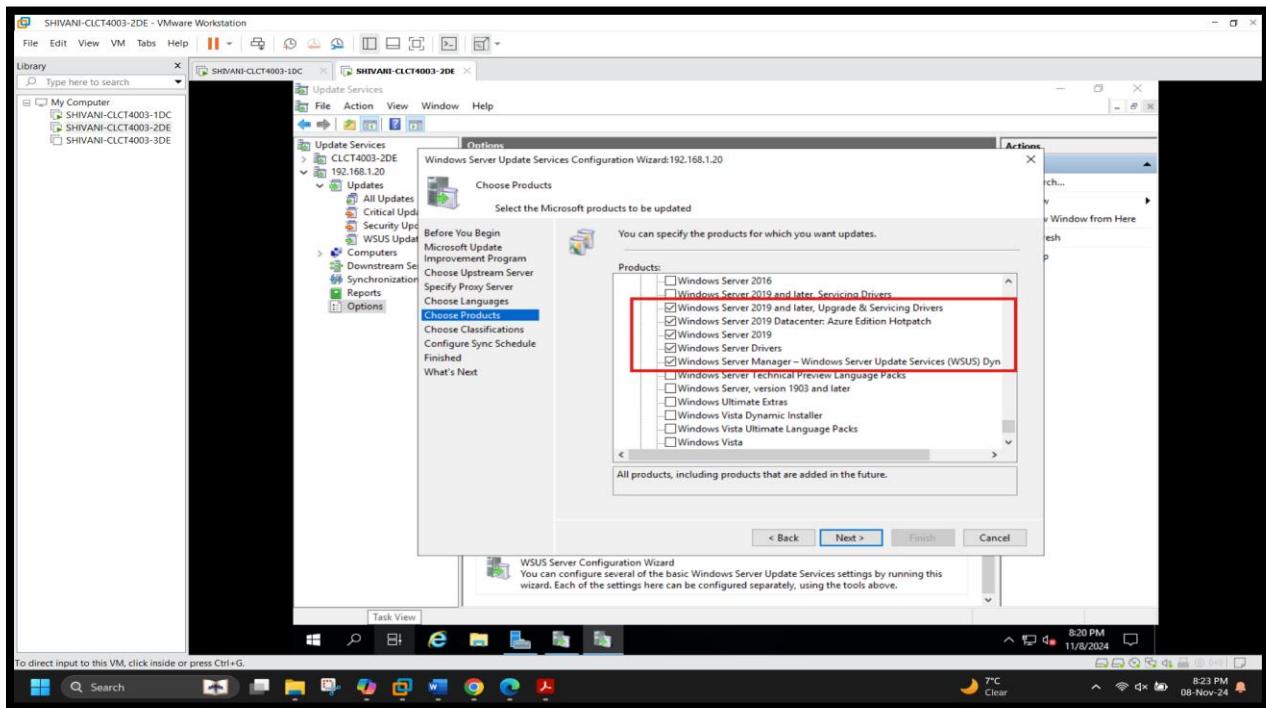


[ Screenshot 50: Connecting Server ]

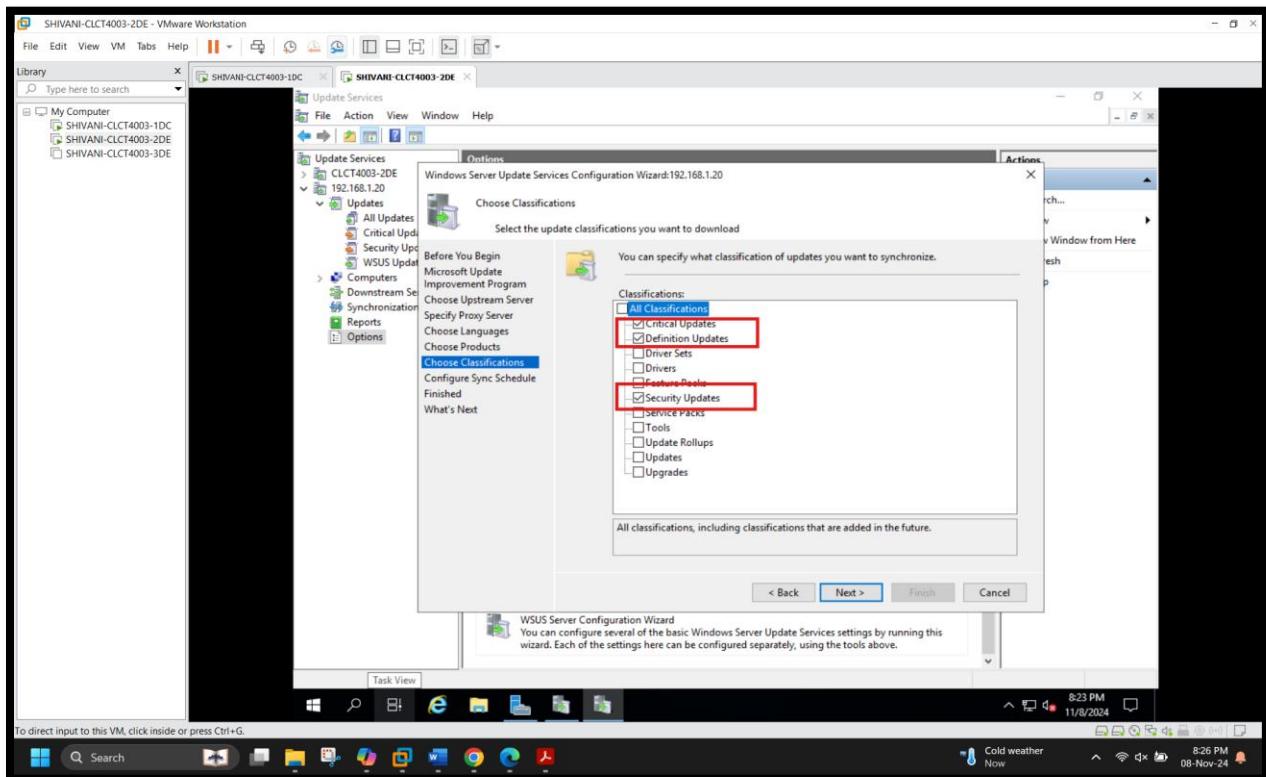


# Windows Server Security

[ Screenshot 51: Selecting Products ]

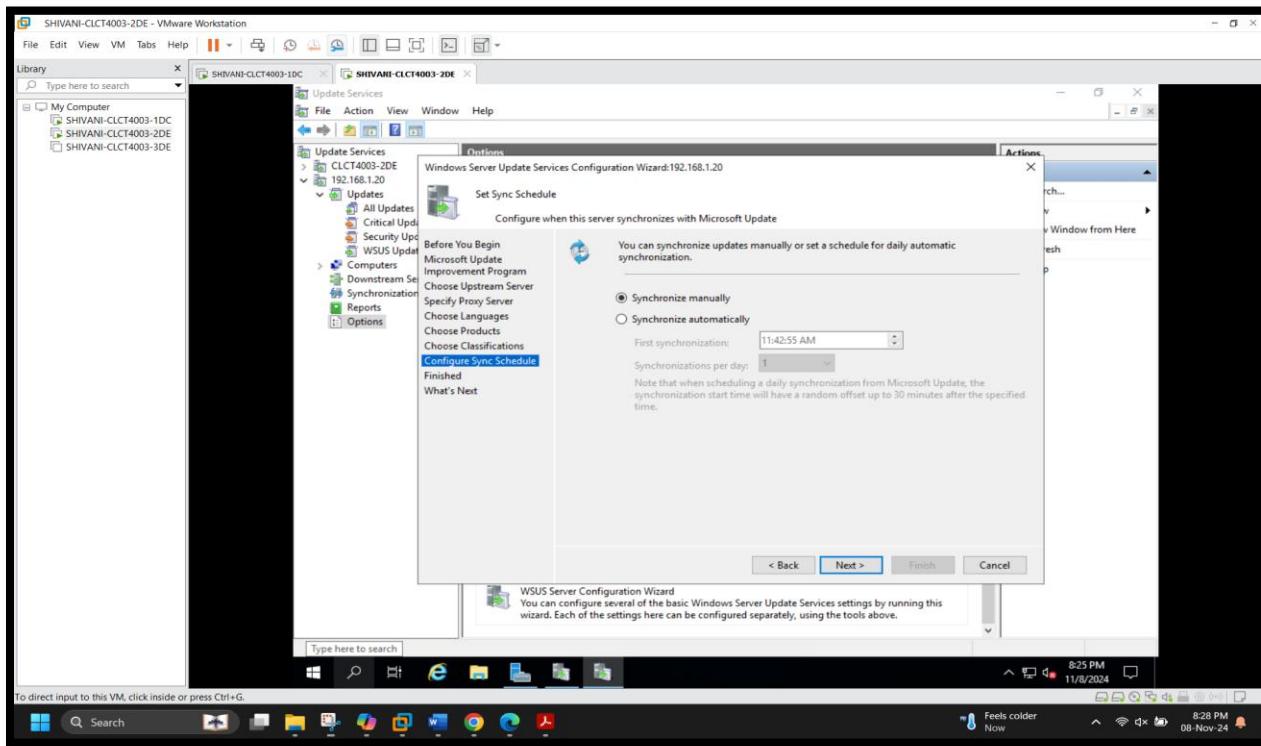


[ Screenshot 52:Selecting Classification for Updates]

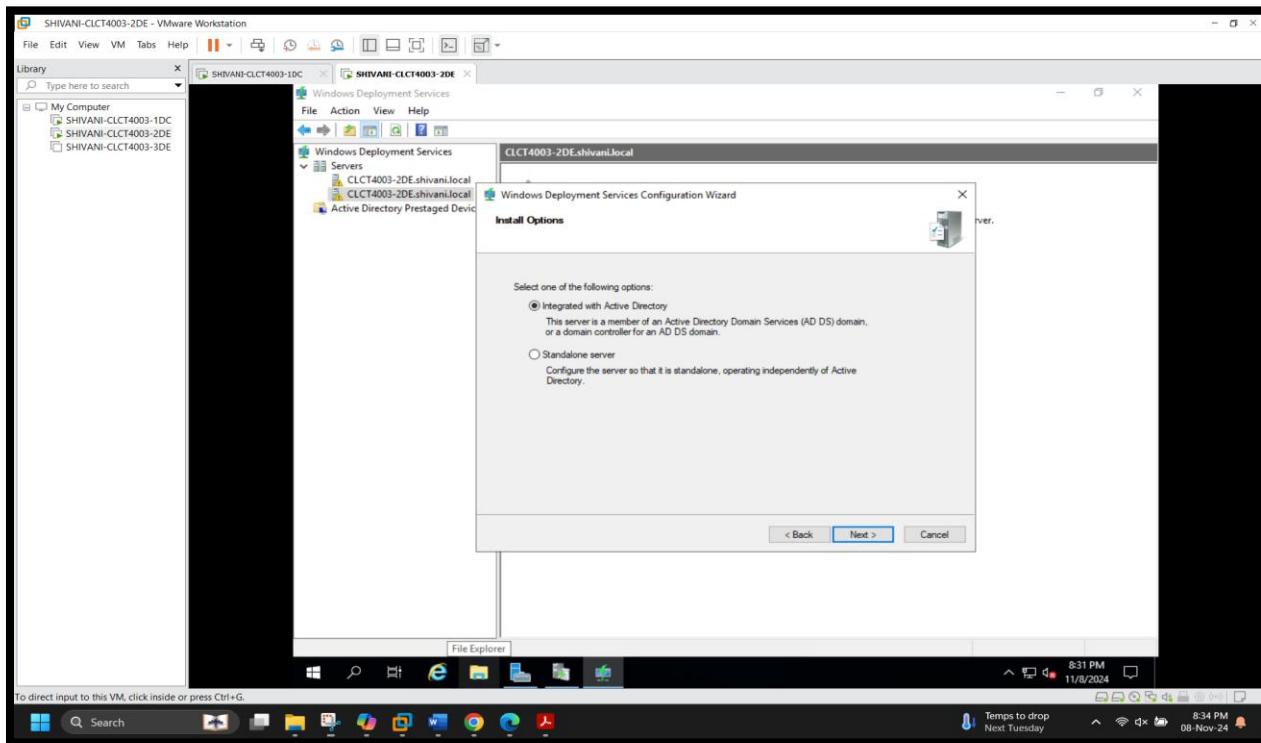


# Windows Server Security

[ Screenshot 53: Selecting Synchronization for Updates]

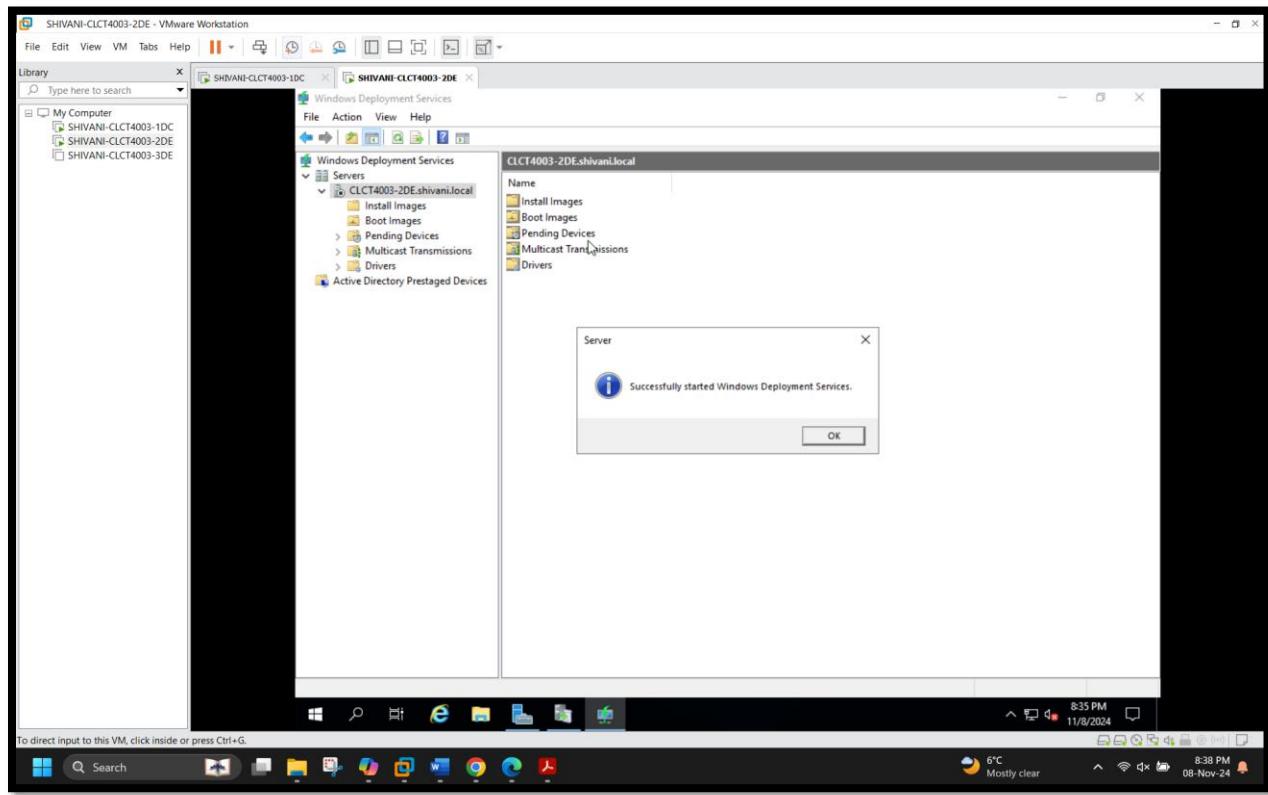


[Screenshot 54: Configuring WDS ]



# Windows Server Security

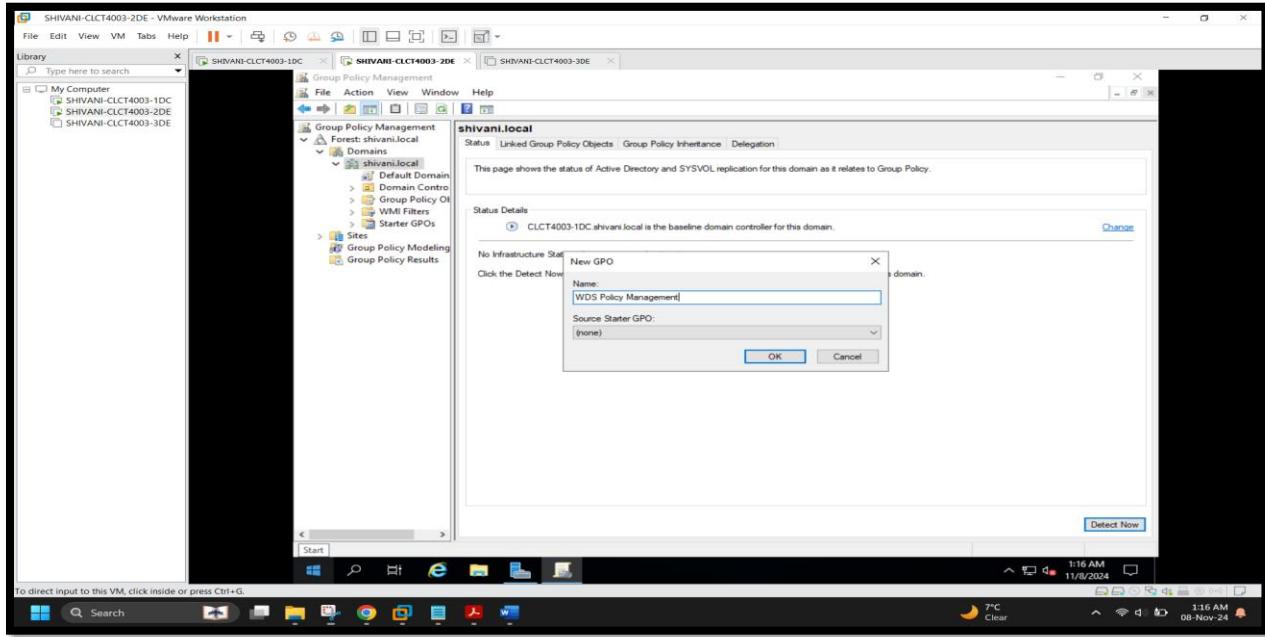
[Screenshot 55: WDS Setup Completed]



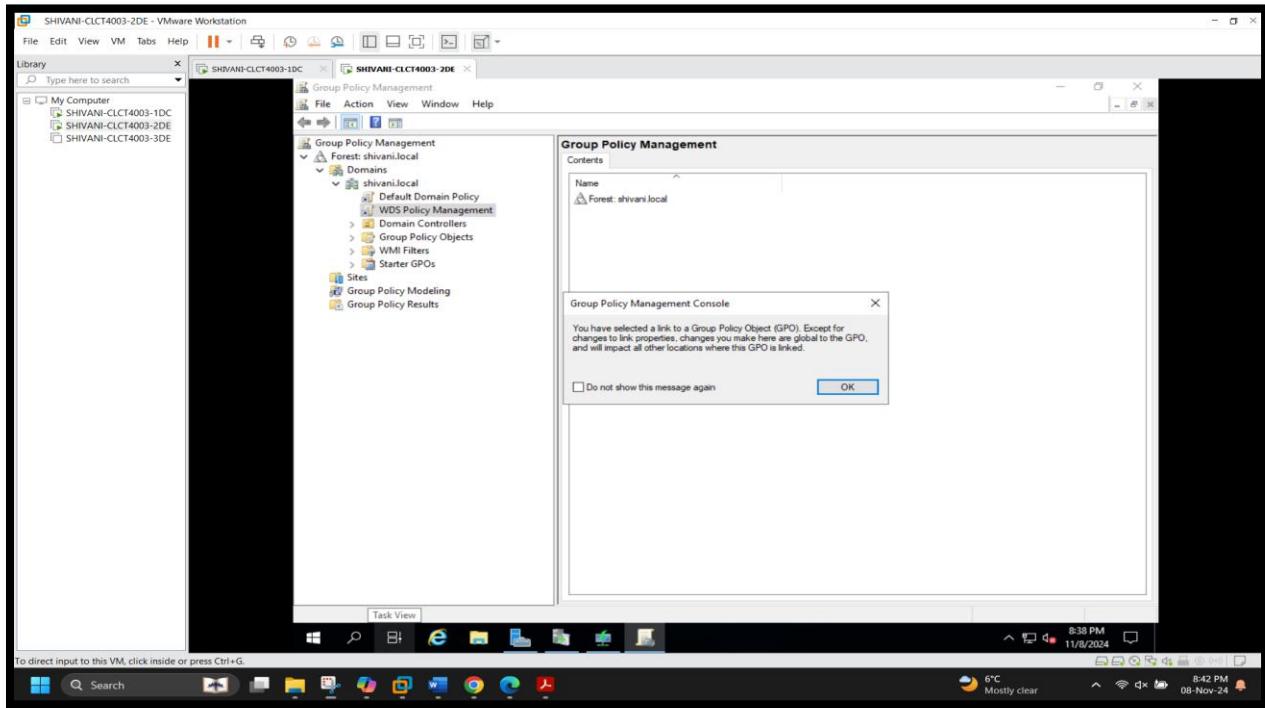
# Windows Server Security

## A) ENFORCE WDS SETTINGS TO CLIENTS USING GROUP POLICY AND REMOVE PAUSE OPTION.

[ Screenshot 56 : Creating New Group Policy Object for WDS Management ]

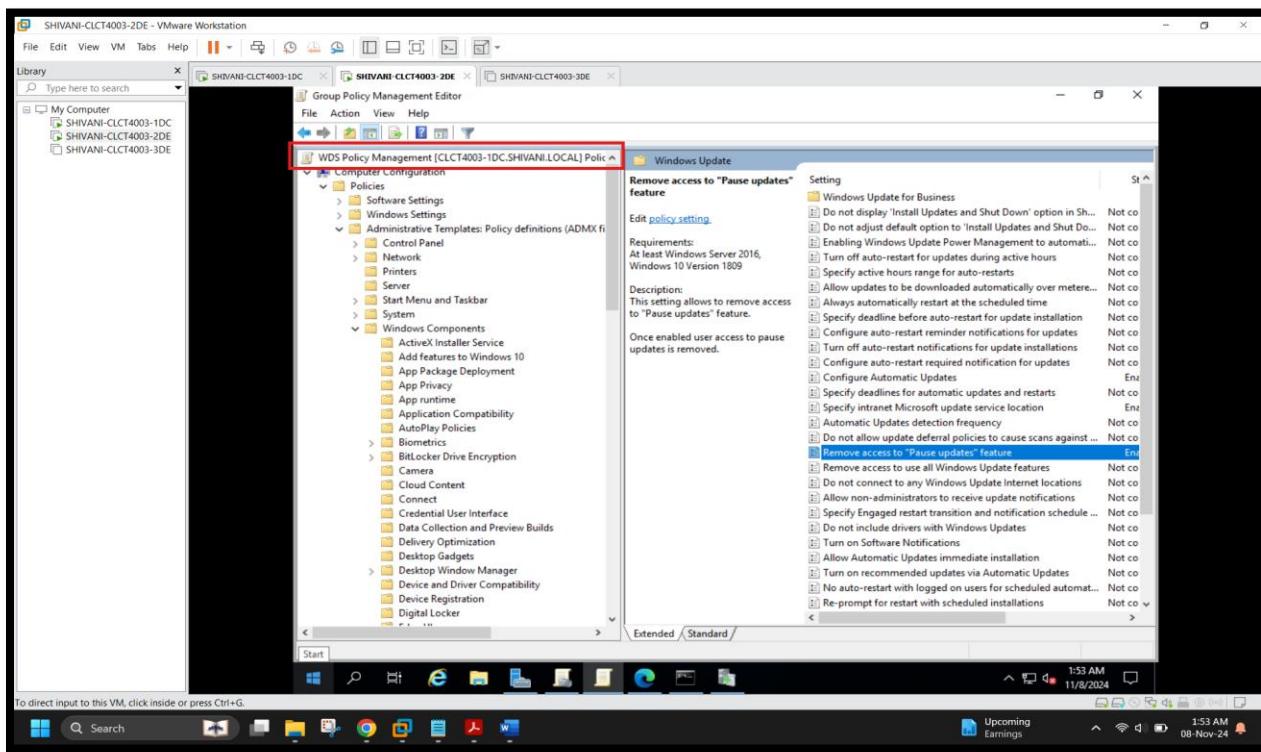


[Screenshot 57: WDS Group Policy is created and linked to GPO]

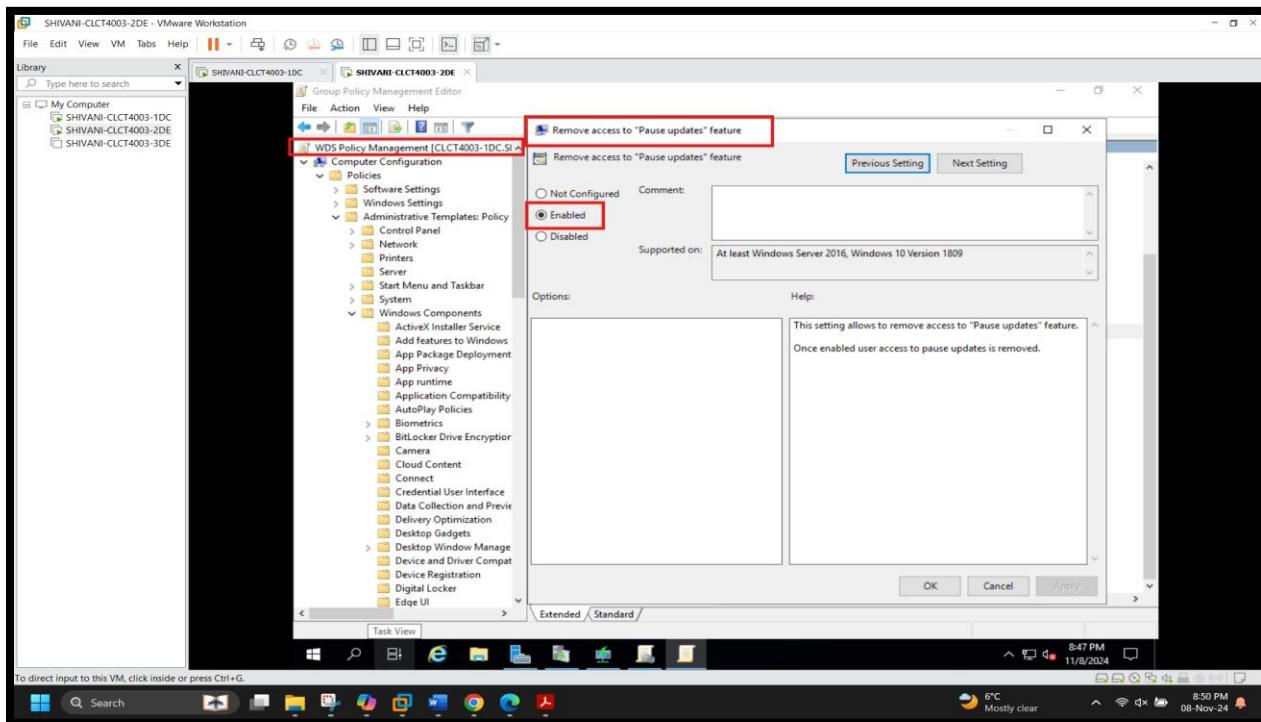


# Windows Server Security

[Screenshot 58 : WDS Policy Created ]



a) [Screenshot 59: Enforce WDS settings to clients using group policy and selected remove pause option]



# Windows Server Security

[ Screenshot 60 : Updating GPO Policy]

