

# Windows Server Security

---

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.

## 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.

~~~~~

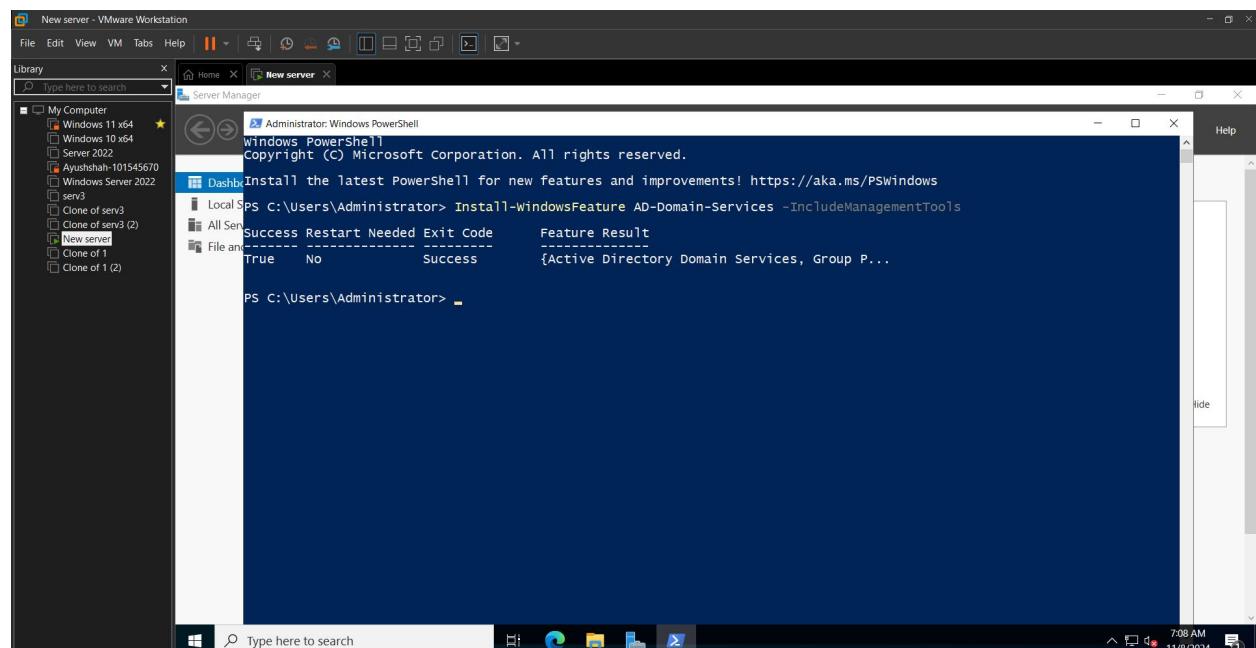
Paste your screenshots here

I have attached all screenshots step by step and covered all the topics

# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.

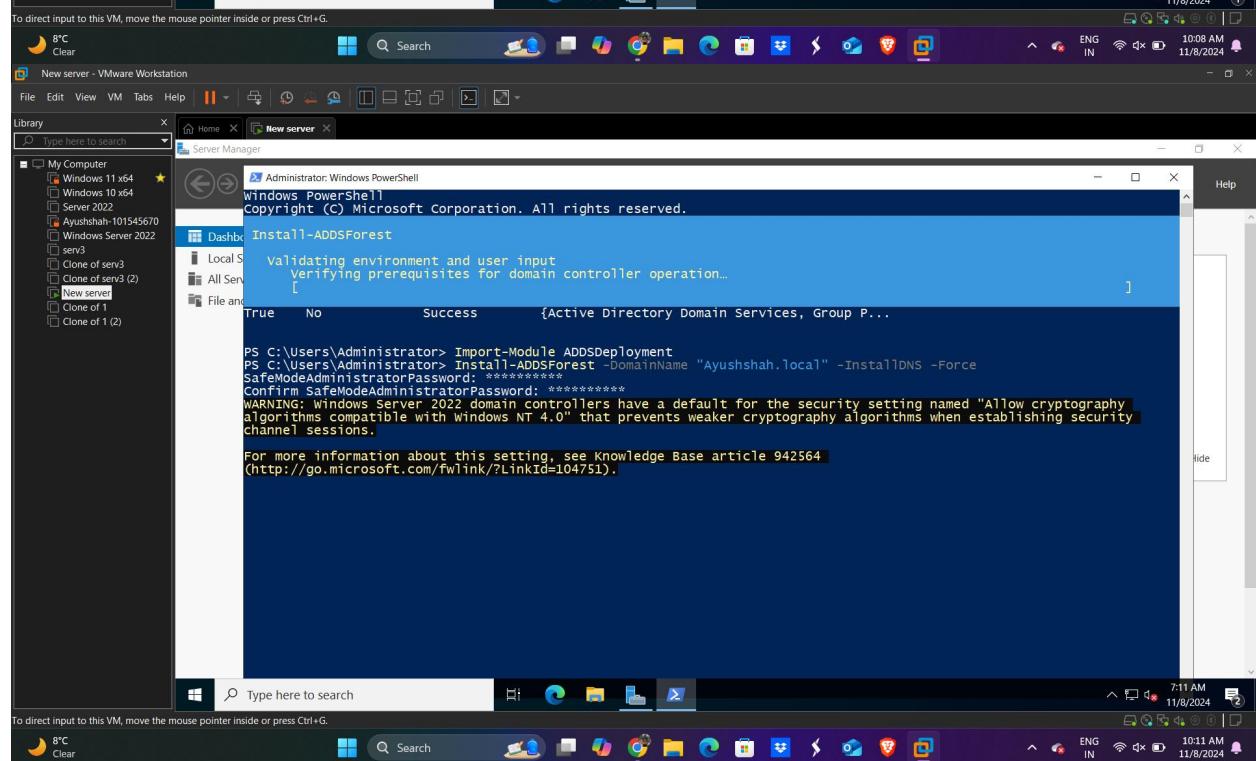


```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code Feature Result
True No Success {Active Directory Domain Services, Group P...}

PS C:\Users\Administrator>
```

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

Install-ADDSForest
    validating environment and user input
    Verifying prerequisites for domain controller operation...
    []

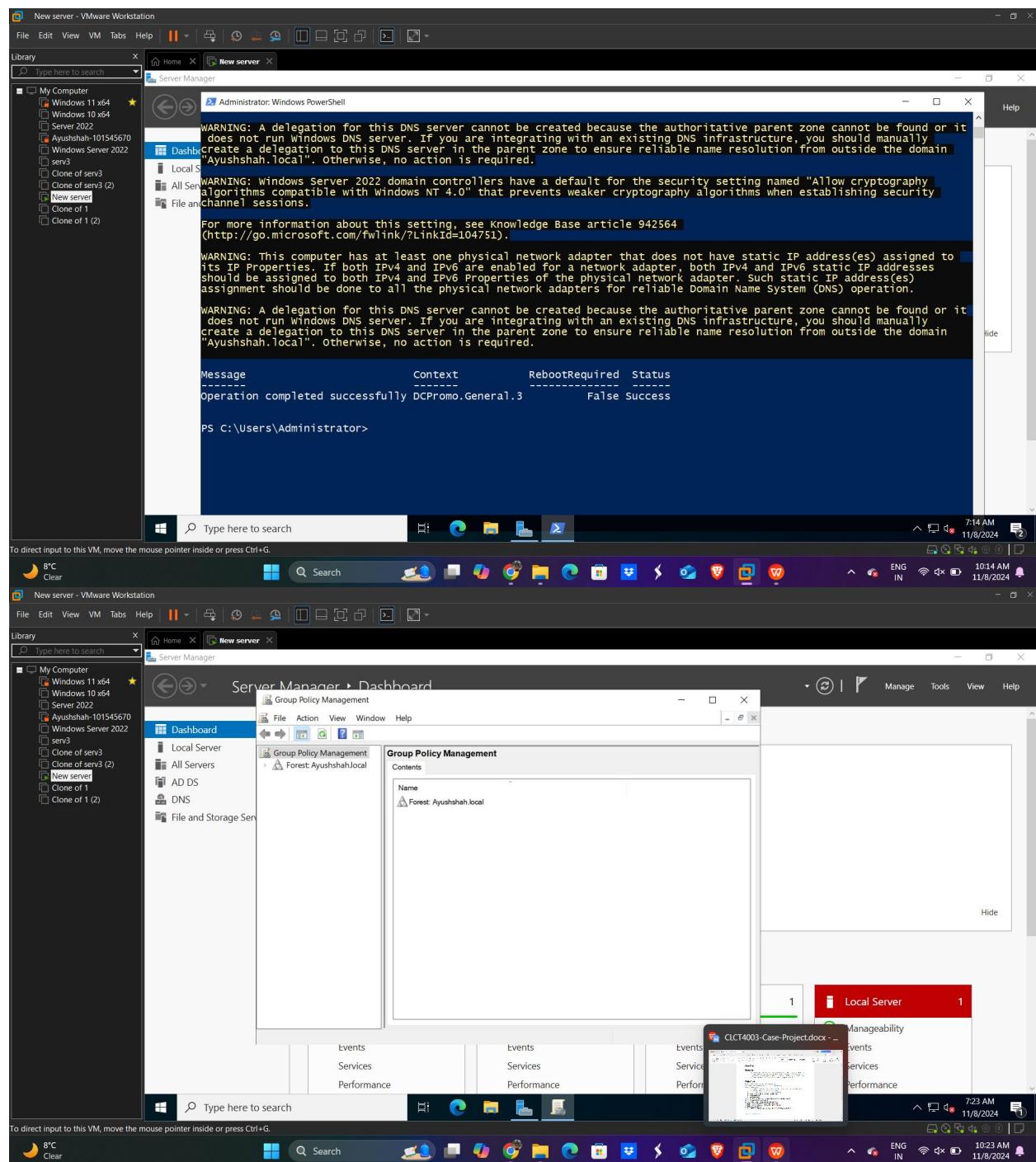
PS C:\Users\Administrator> Import-Module ADDSDeployment
PS C:\Users\Administrator> Install-ADDSForest -DomainName "Ayushshah.local" -InstallDNS -Force
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****
WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).
```

# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

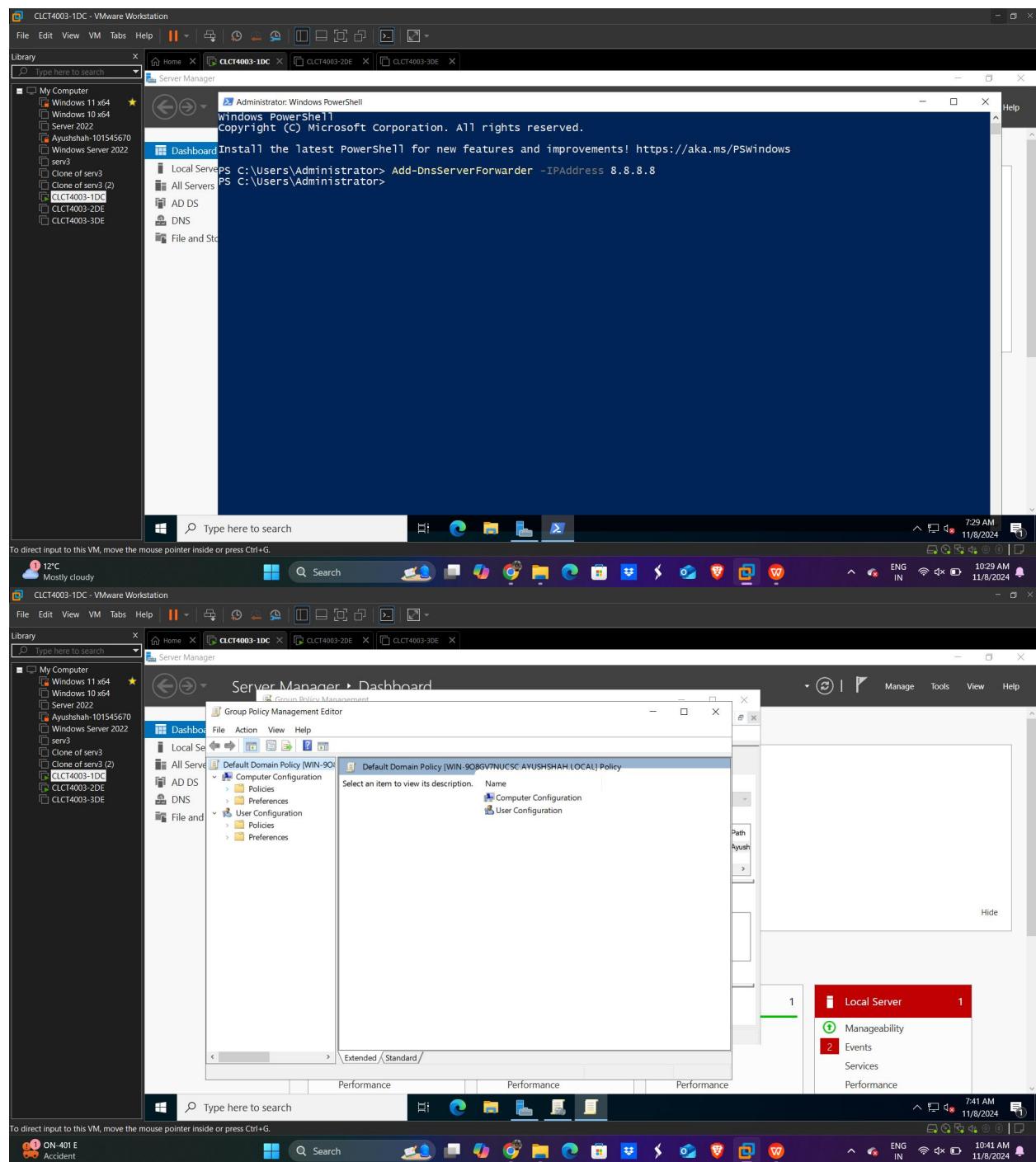
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

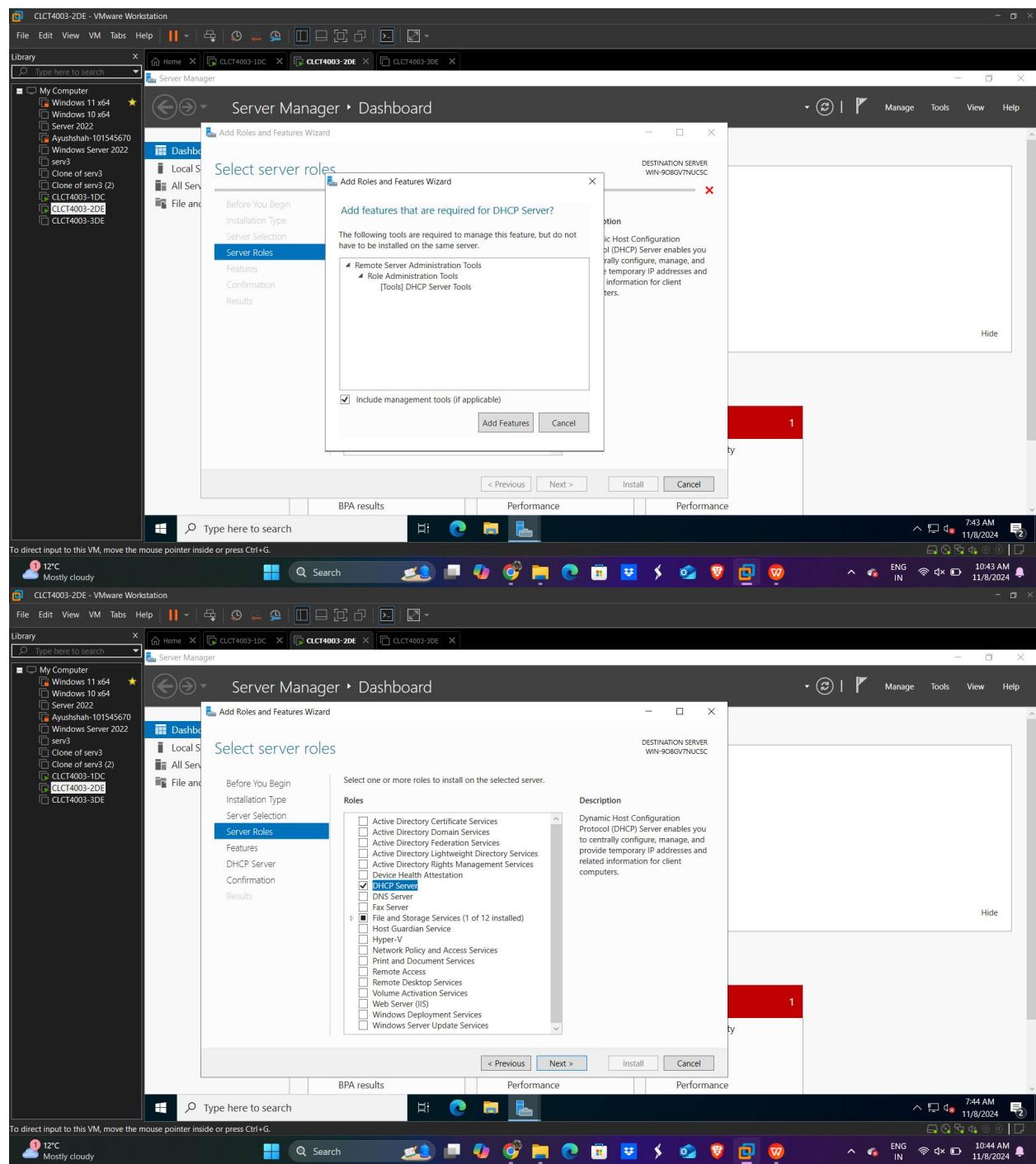
Term: Fall 2024.

The screenshot shows the Windows Server 2022 Group Policy Management Editor. The left navigation pane shows 'My Computer' with several servers listed under 'All Servers'. The main pane displays the 'Default Domain Policy (WIN-...)'. Under 'Computer Configuration / Policies / Windows Settings / Security Settings / Account Policies / Passwords', the 'Maximum password age' setting is highlighted. The current value is '30 days'. Other settings visible include 'Enforce password history' (24 passwords remembered), 'Minimum password length' (7 characters), and 'Store passwords using reversible encryption' (Disabled).

# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

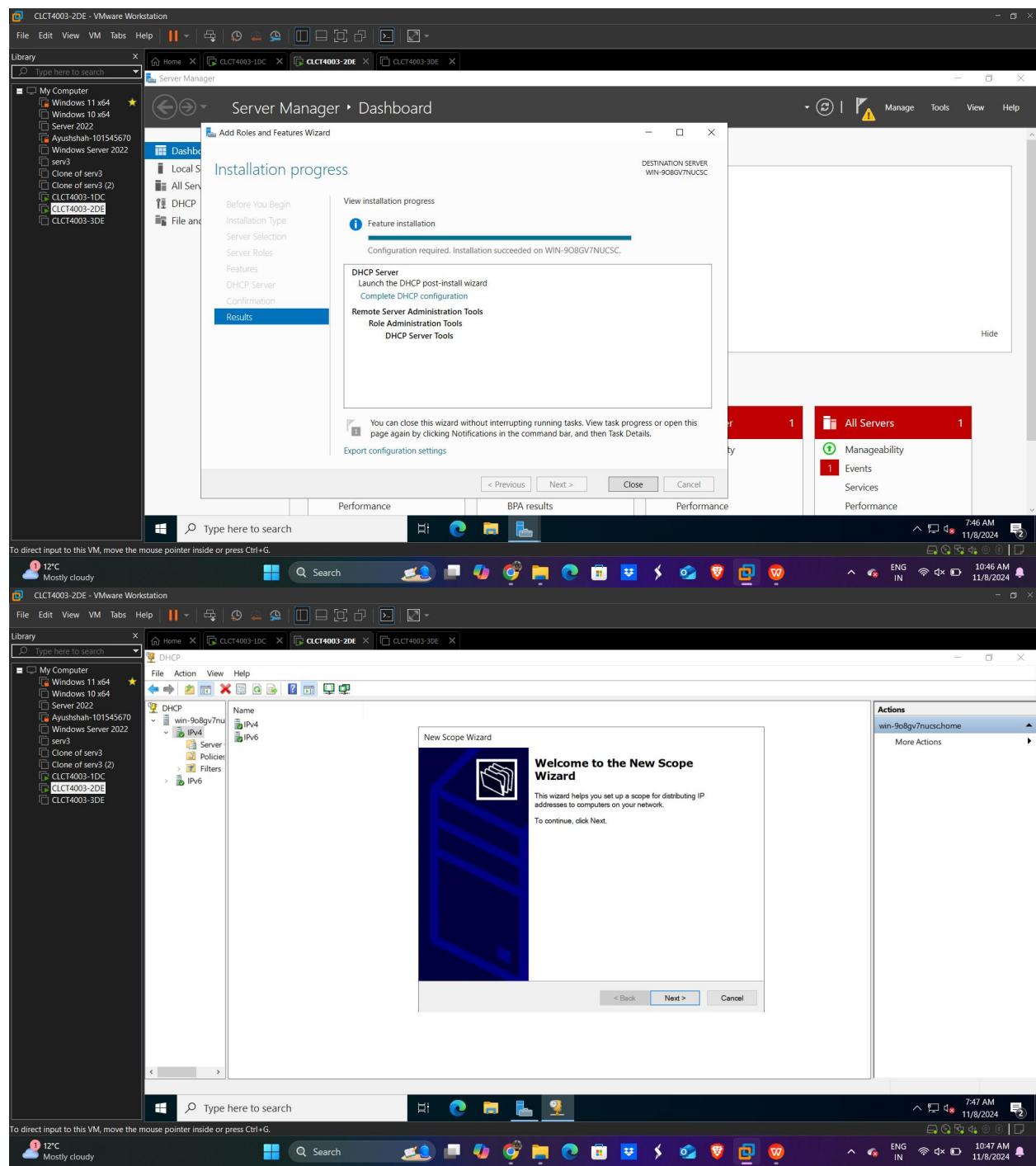
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

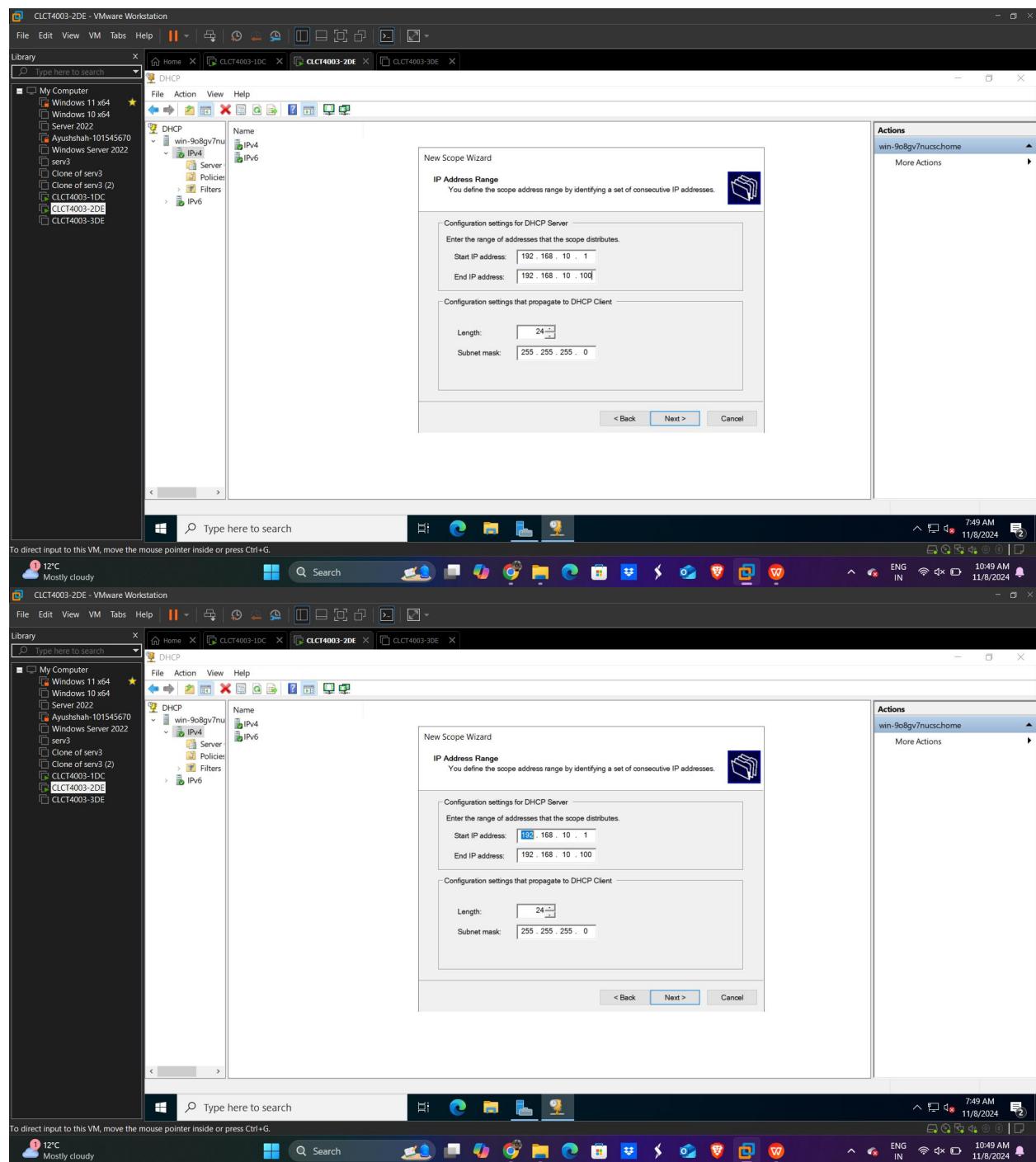
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

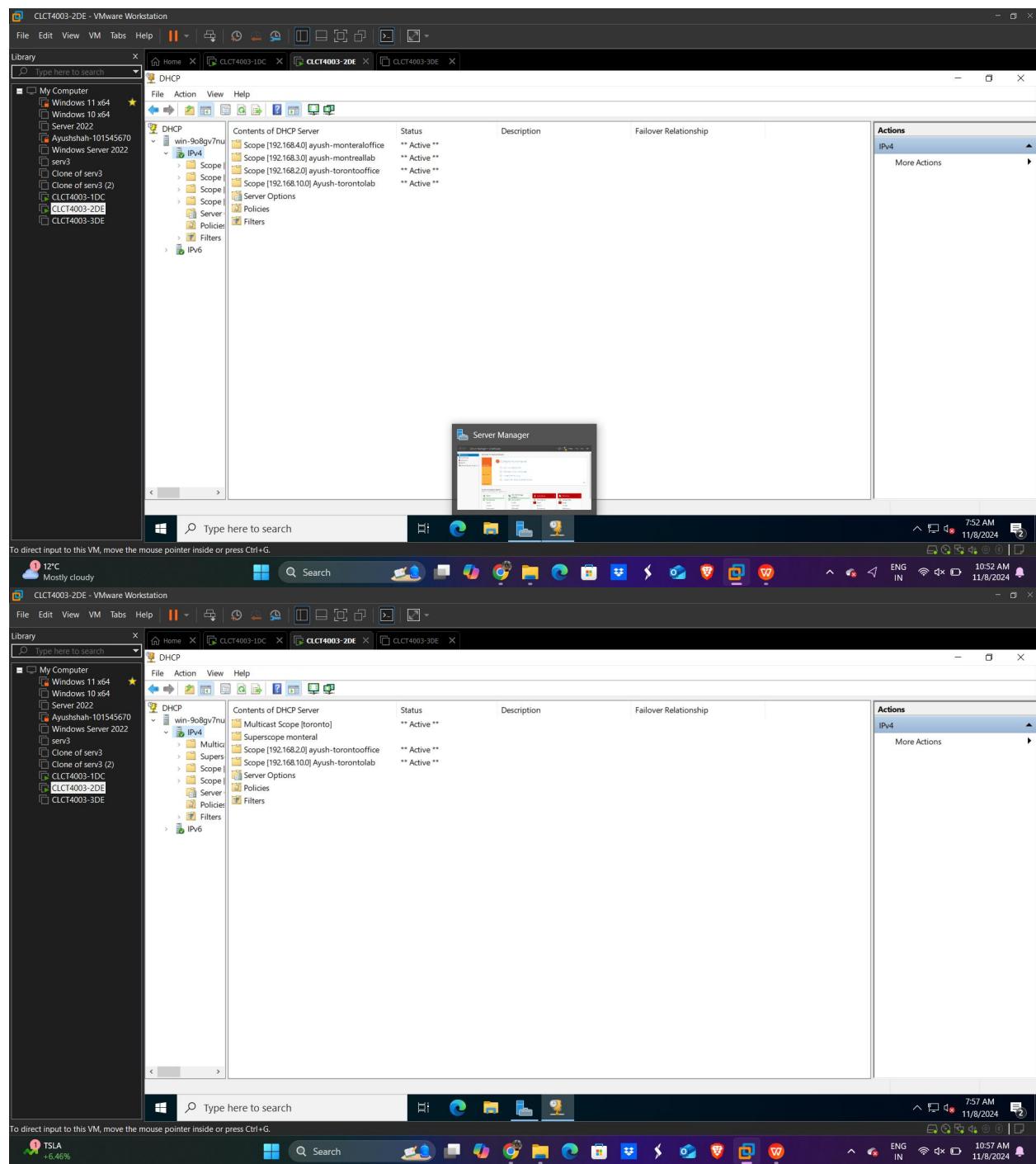
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

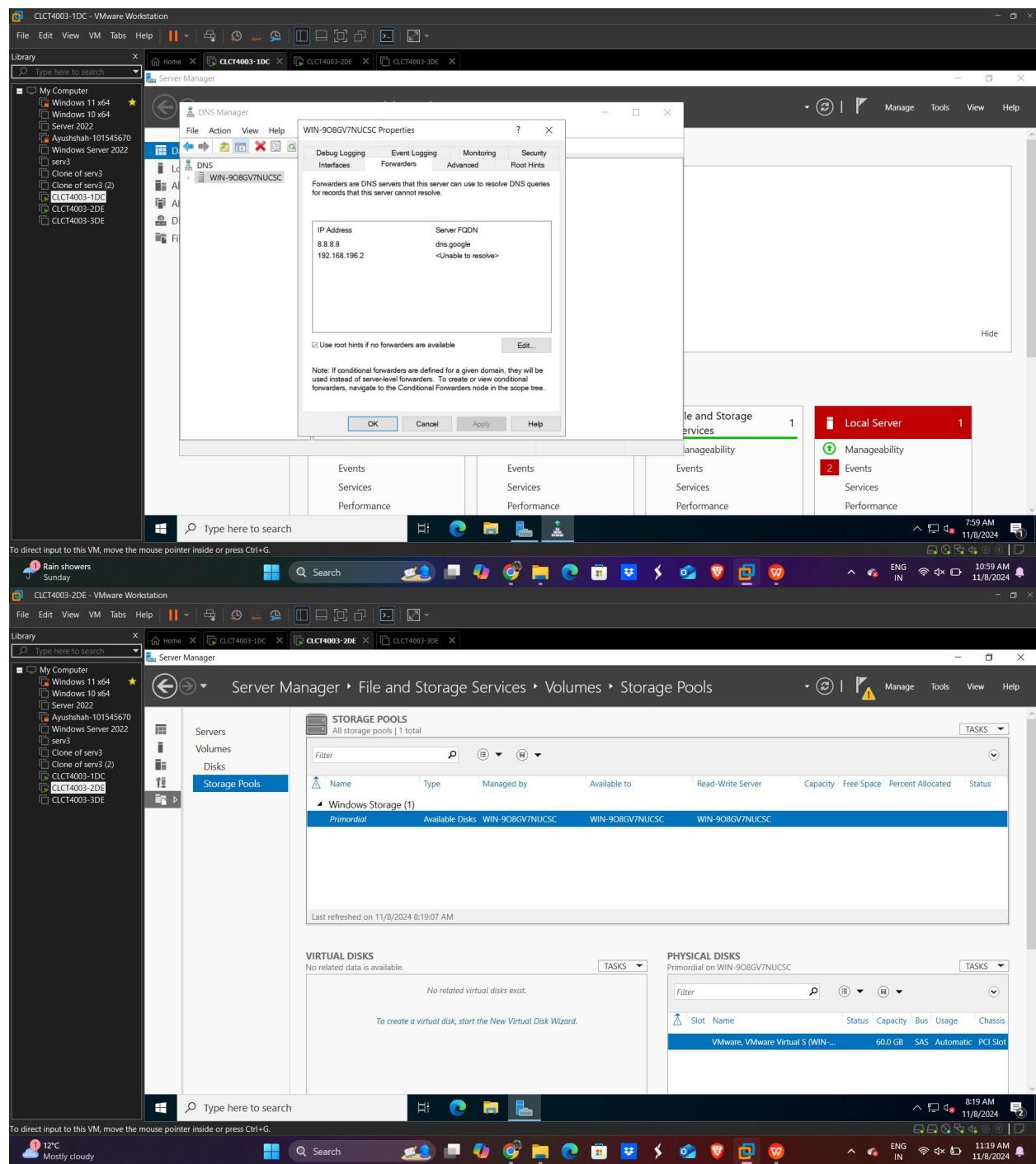
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

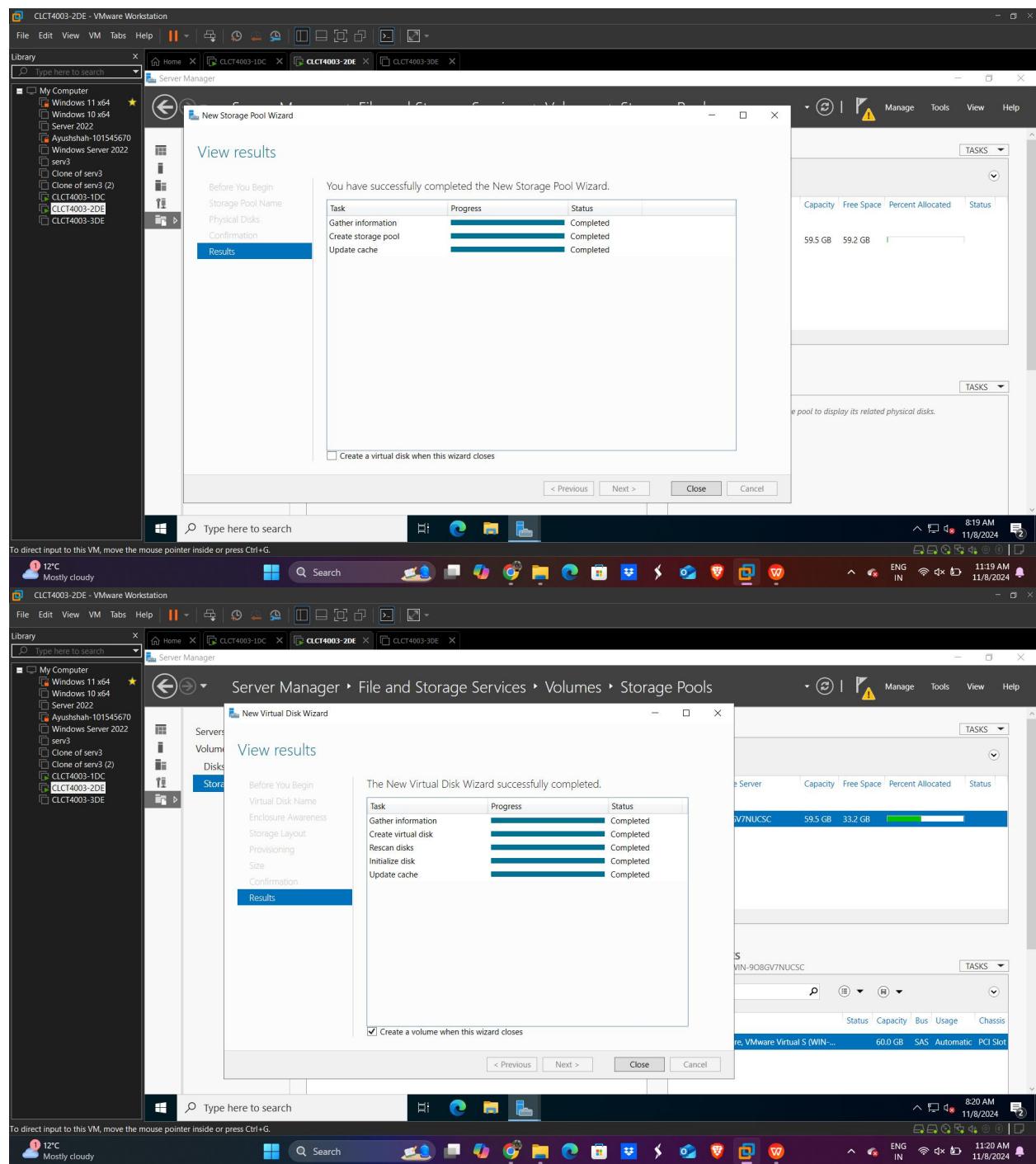
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

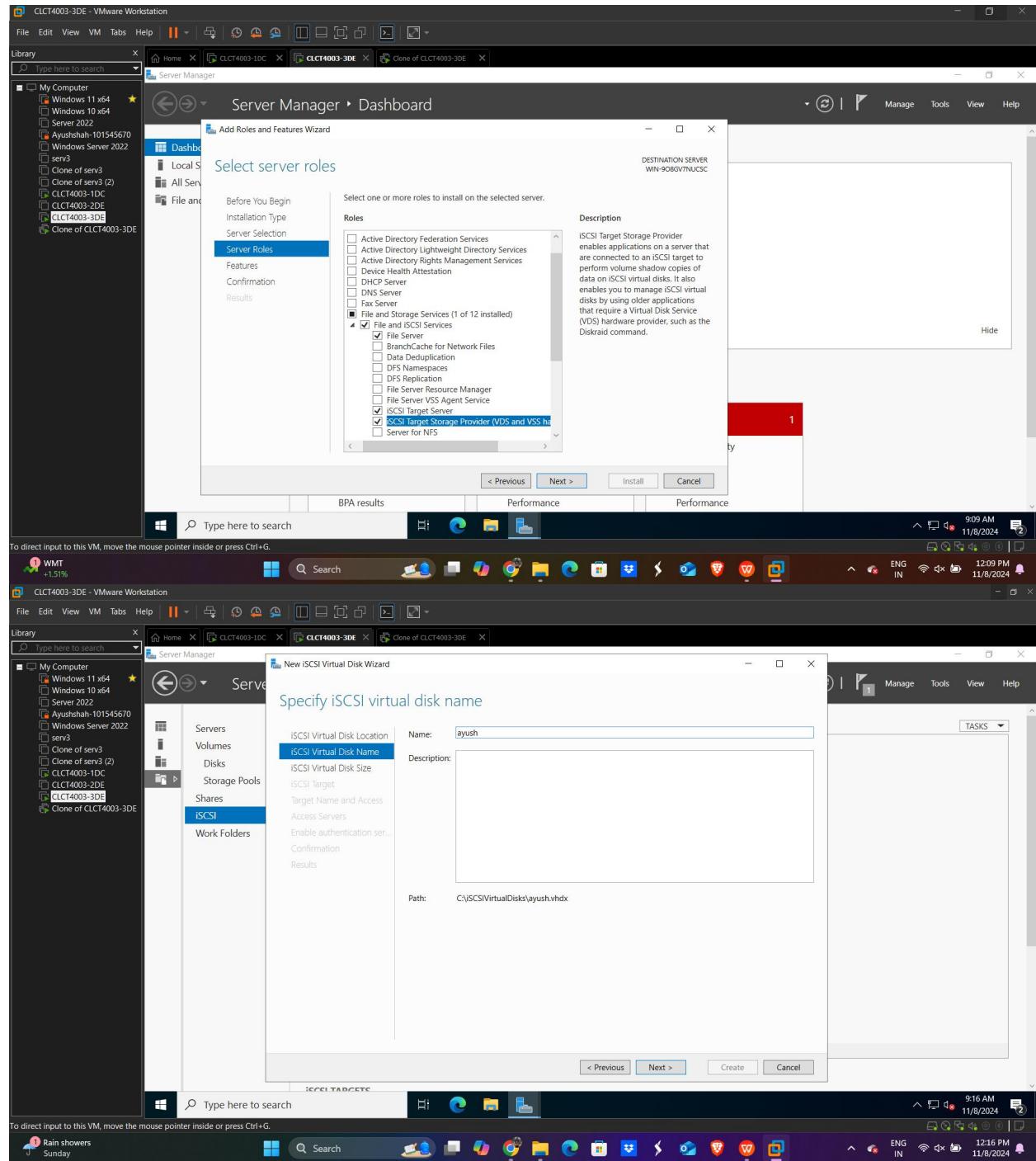
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

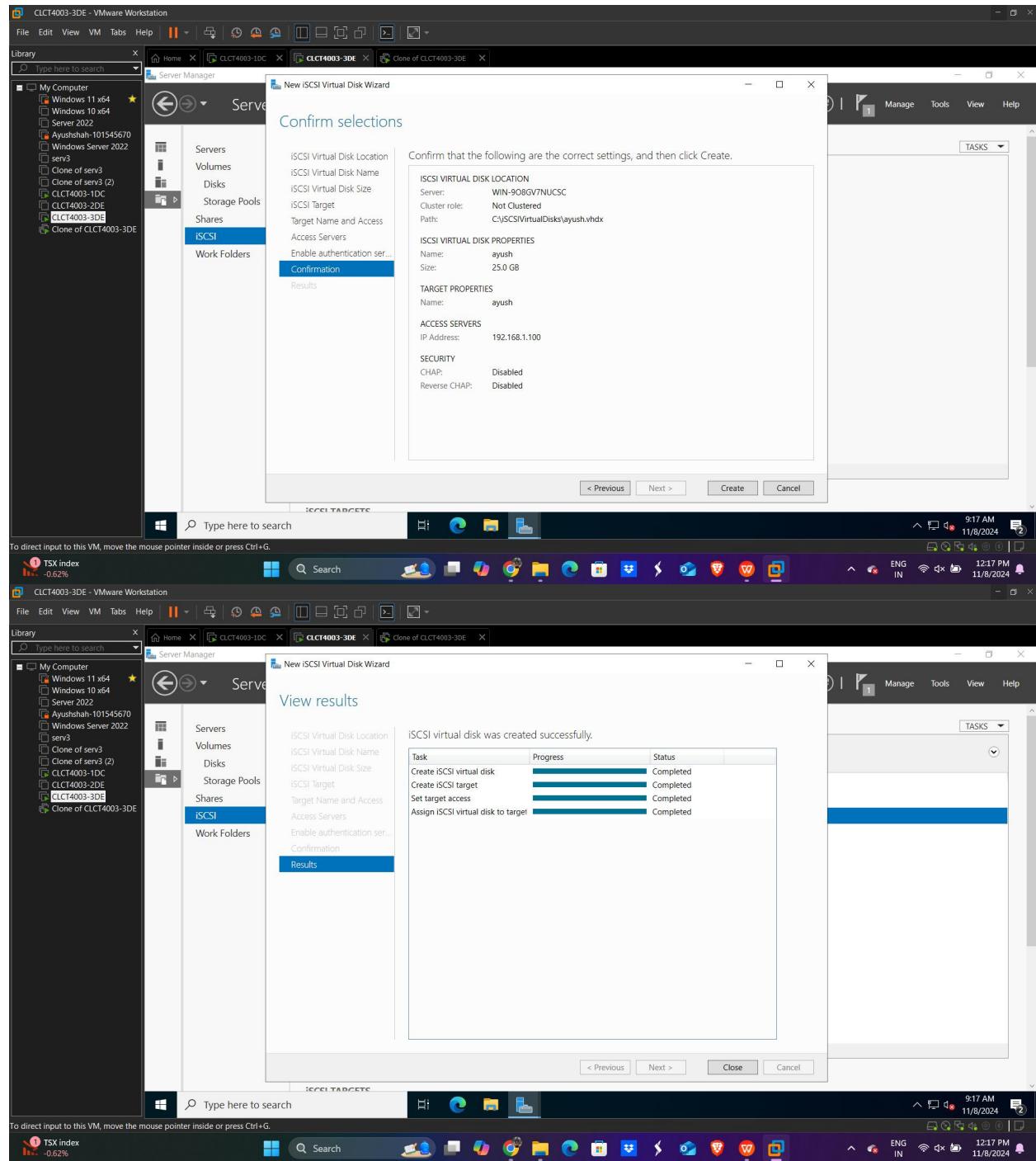
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.

The screenshot displays two separate Windows Server 2022 environments running in VMware Workstation. Both VMs have the same configuration: Windows Server 2022, IP address 192.168.1.100, and a single iSCSI virtual disk named 'ayush.vhdx' located at C:\SCSI\VirtualDisks\ayush.vhdx. The disks are both 'Not Connected'.

**VMware Workstation Interface:**

- Top Bar:** File, Edit, View, VM, Tabs, Help, etc.
- Left Sidebar:** Library, My Computer, Dashboard, Local Server, All Servers, File and Folders.
- Central Window:** iSCSI Initiator Properties dialog box. It shows a 'Targets' tab with 'Target' set to '192.168.1.100' and a 'Discovery' tab showing a discovered target 'ayush'. Buttons include 'Quick Connect...', 'Refresh', 'Connect', 'Disconnect', 'Properties...', and 'Devices...'. A note says: 'To connect using advanced options, select a target and then click Connect. To completely disconnect a target, select the target and then click Disconnect. For target properties, including configuration of sessions, select the target and click Properties. For configuration of devices associated with a target, select the target and then click Devices.'
- Right Side:** Server Manager dashboard with sections for local server, features, and server group.
- Bottom Taskbar:** Shows the date and time (11/8/2024), system status (12°C, mostly cloudy), and various application icons.

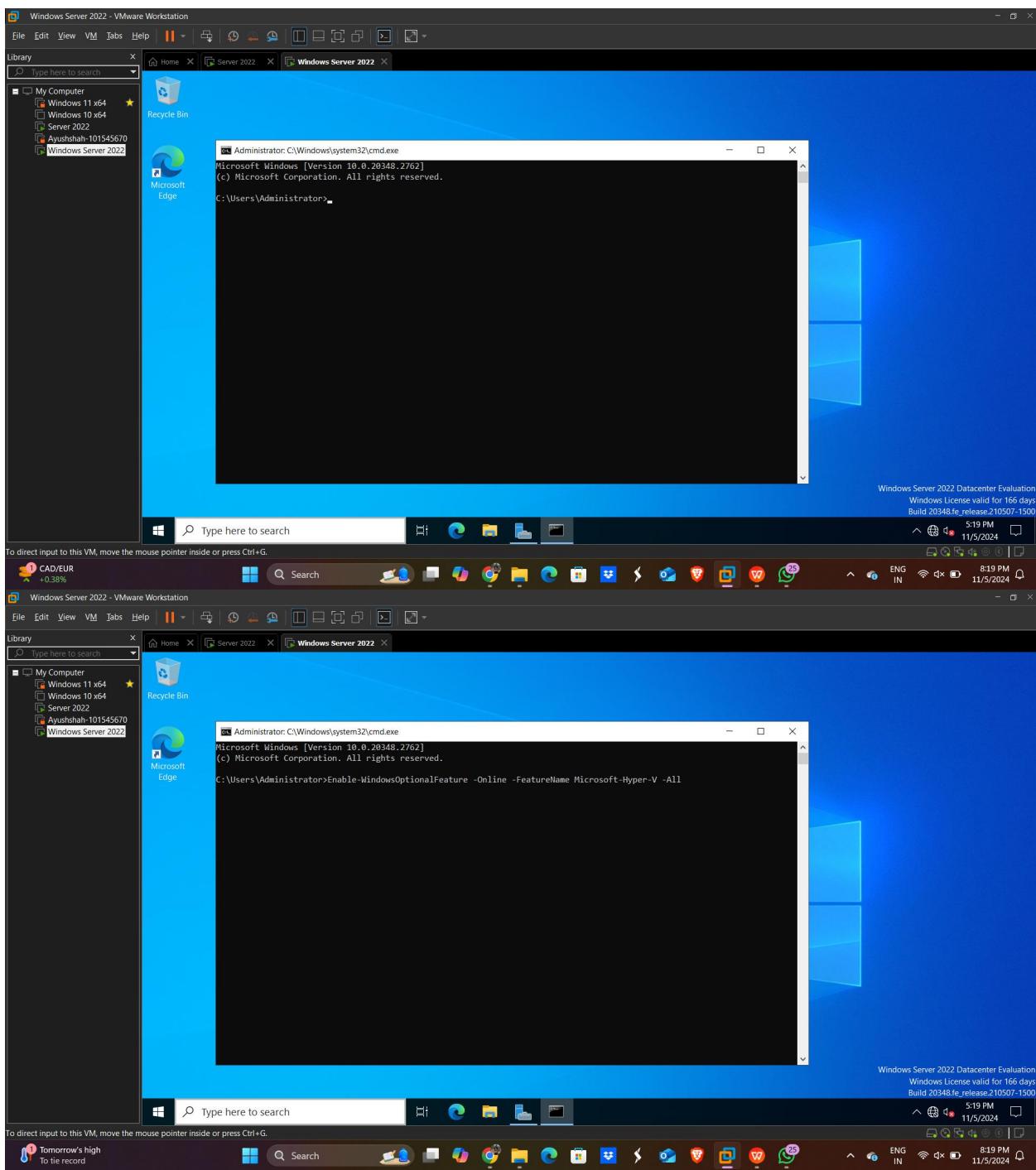
**Server Manager Interface:**

- Top Bar:** File, Edit, View, VM, Tabs, Help, etc.
- Left Sidebar:** Library, My Computer, Servers, Volumes, Disks, Storage Pools, Shares, iSCSI, Work Folders.
- Central Window:** File and Storage Services > iSCSI > iSCSI VIRTUAL DISKS. It lists one virtual disk: WIN-9Q8GV7NUCSC (1) at C:\SCSI\VirtualDisks\ayush.vhdx.
- Bottom Taskbar:** Shows the date and time (11/8/2024), system status (12°C, mostly cloudy), and various application icons.

# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

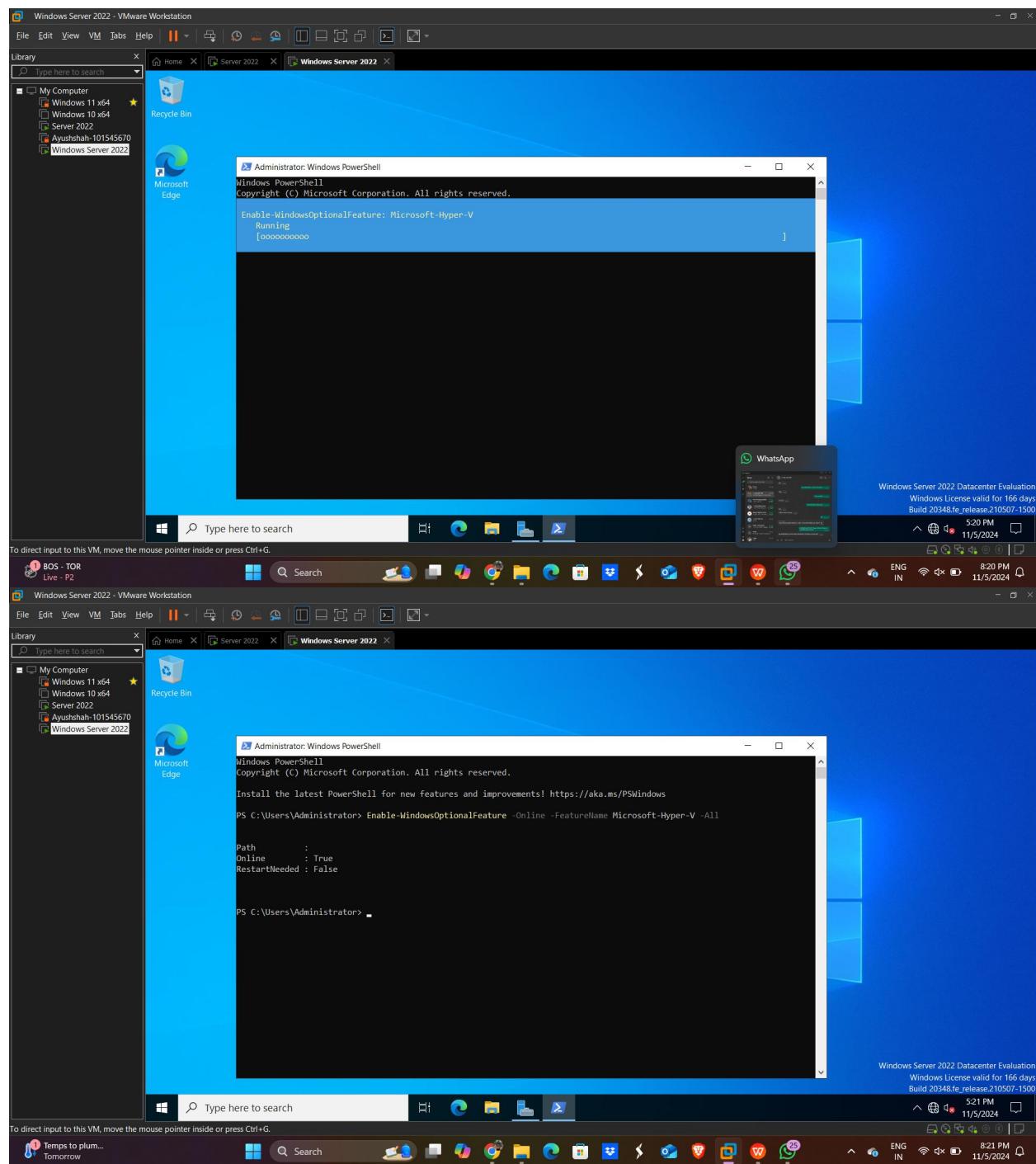
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

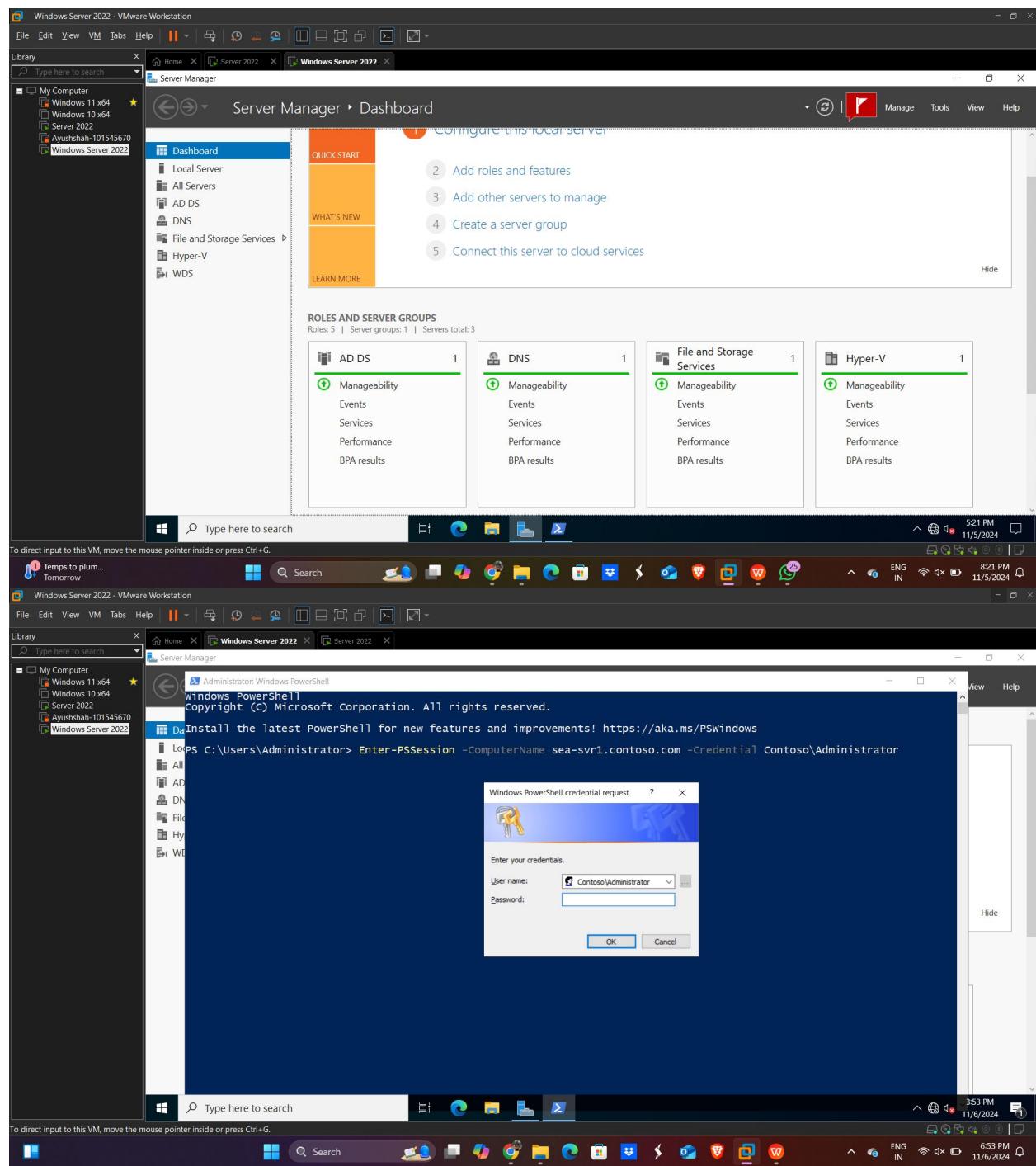
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

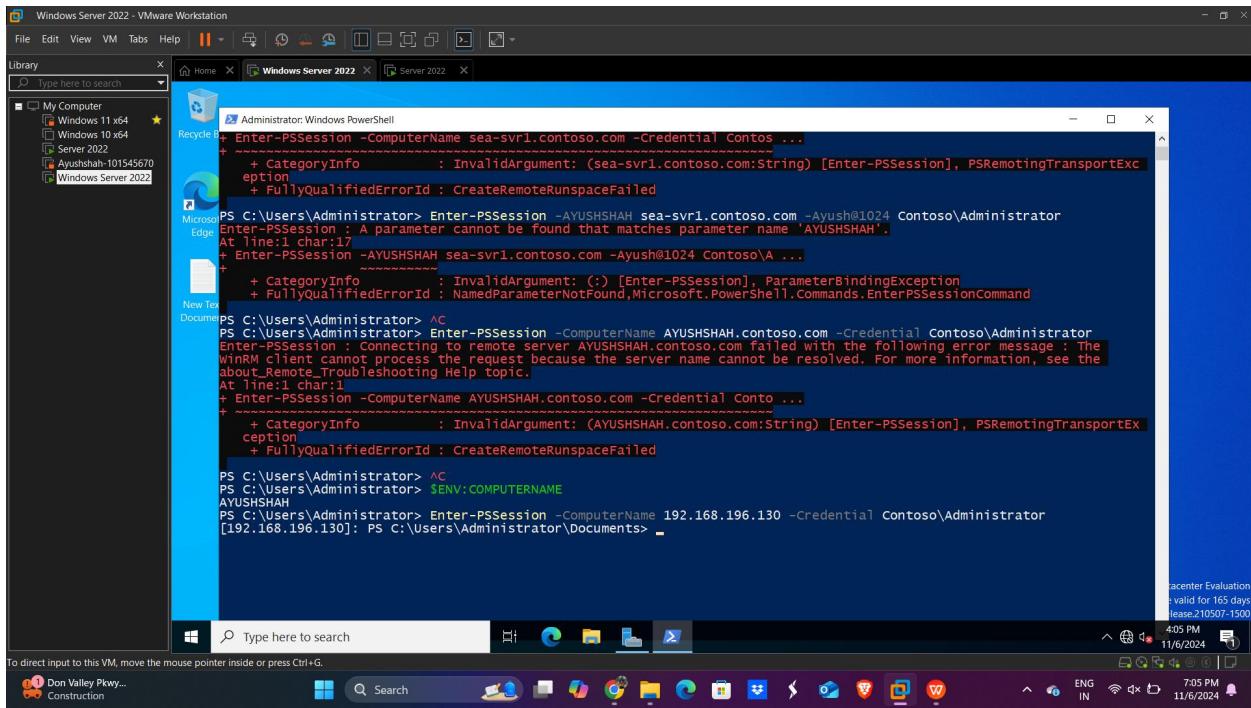
Term: Fall 2024.



# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.



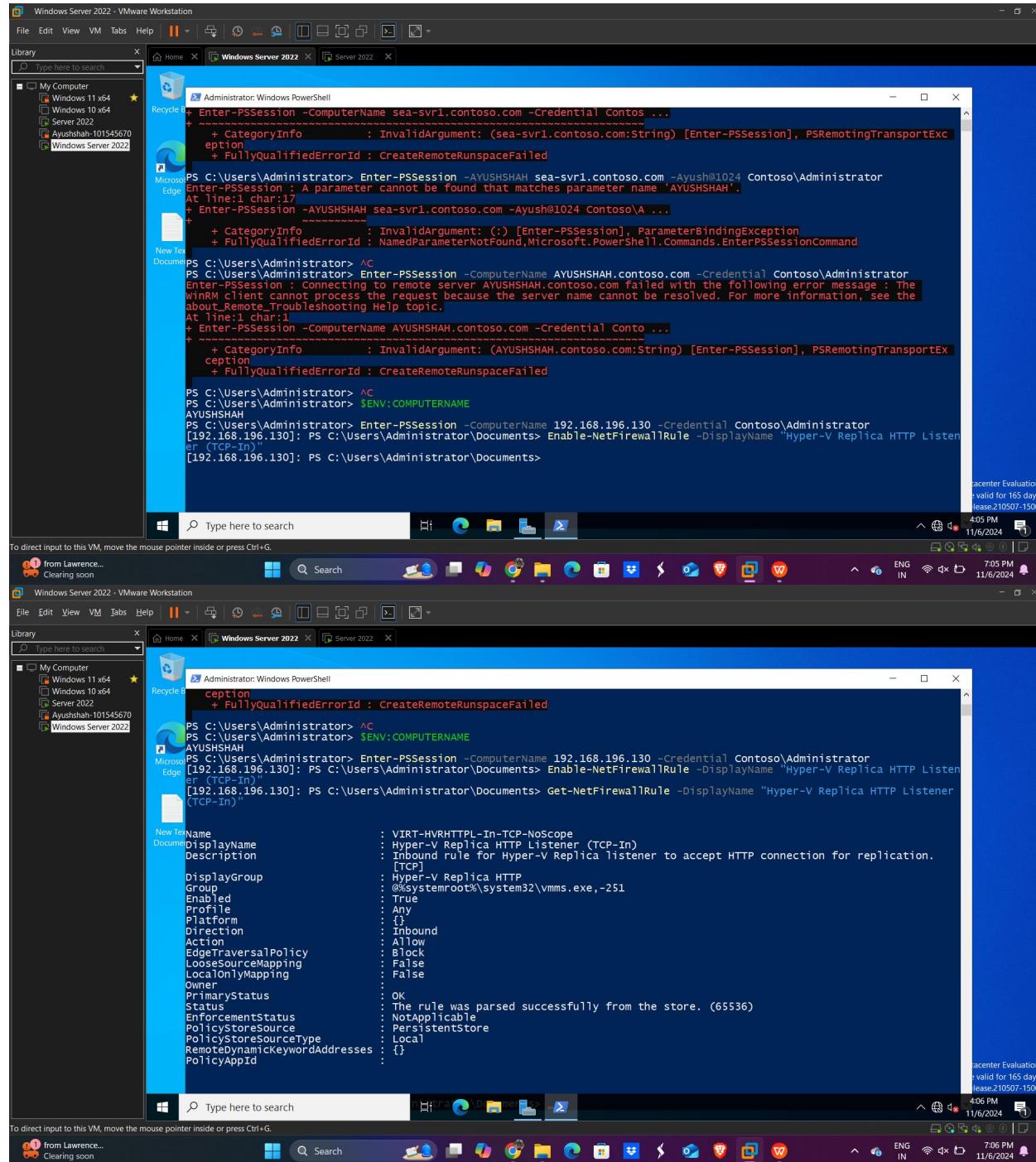
The screenshot shows a Windows Server 2022 PowerShell window titled "Administrator: Windows PowerShell". The user is attempting to establish a remote session using the `Enter-PSSession` cmdlet. The first attempt fails because the computer name is specified as a URL (sea-svrl.contoso.com) instead of a standard host name. The second attempt fails because the user does not have the correct credentials for the remote machine. The third attempt fails because the user does not have the correct credentials for the remote machine. The fourth attempt succeeds by specifying the IP address (192.168.196.130) instead of the host name. The PowerShell window is running on a Windows Server 2022 desktop interface.

```
+ Enter-PSSession -ComputerName sea-svrl.contoso.com -Credential Contoso ...
+ CategoryInfo          : InvalidArgument: (sea-svrl.contoso.com:String) [Enter-PSSession], PSRemotingTransportException
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed
PS C:\Users\Administrator> Enter-PSSession -AYUSHSHAH sea-svrl.contoso.com -Ayush@1024 Contoso\Administrator
Enter-PSSession : A parameter cannot be found that matches parameter name 'AYUSHSHAH'.
At line:1 char:17
+ Enter-PSSession -AYUSHSHAH sea-svrl.contoso.com -Ayush@1024 Contoso\A ...
+ CategoryInfo          : InvalidArgument: () [Enter-PSSession], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.EnterPSSessionCommand
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> Enter-PSSession -ComputerName AYUSHSHAH.contoso.com -Credential Contoso\Administrator
Enter-PSSession : Connecting to remote server AYUSHSHAH.contoso.com failed with the following error message : The WinRM client cannot process the request because the server name cannot be resolved. For more information, see the about_Remote_Troubleshooting Help topic.
At line:1 char:17
+ Enter-PSSession -ComputerName AYUSHSHAH.contoso.com -Credential Conto ...
+ CategoryInfo          : InvalidArgument: (AYUSHSHAH.contoso.com:String) [Enter-PSSession], PSRemotingTransportException
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> $ENV:COMPUTERNAME
AYUSHSHAH
PS C:\Users\Administrator> Enter-PSSession -ComputerName 192.168.196.130 -Credential Contoso\Administrator
[192.168.196.130]: PS C:\Users\Administrator\Documents> -
```

# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.



The screenshot shows two windows of a Windows Server 2022 VM in VMware Workstation. Both windows are titled "Administrator: Windows PowerShell".

The top window displays several PowerShell commands related to remote sessions:

```
+ Enter-PSSession -ComputerName sea-svrl.contoso.com -Credential Contoso ...
+ CategoryInfo          : InvalidArgument: (sea-svrl.contoso.com:String) [Enter-PSSession], PSRemotingTransportException
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed
PS C:\Users\Administrator> Enter-PSSession -AYUSHSHAH sea-svrl.contoso.com -Ayush@1024 Contoso\Contoso\Contoso
Enter-PSSession : A parameter cannot be found that matches parameter name 'AYUSHSHAH'.
At line:1 char:17
+ Enter-PSSession -AYUSHSHAH sea-svrl.contoso.com -Ayush@1024 Contoso\A ...
+ CategoryInfo          : InvalidArgument: () [Enter-PSSession], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.EnterPSSessionCommand
PS C:\Users\Administrator> AC
PS C:\Users\Administrator> $ENV:COMPUTERNAME
AYUSHSHAH
PS C:\Users\Administrator> Enter-PSSession -ComputerName 192.168.196.130 -Credential Contoso\Contoso\Contoso
[192.168.196.130]: PS C:\Users\Administrator\Documents> Enable-NetFirewallRule -DisplayName "Hyper-V Replica HTTP Listener (TCP-In)"
[192.168.196.130]: PS C:\Users\Administrator\Documents>
```

The bottom window shows the configuration of a NetFirewallRule:

```
cepition
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed
PS C:\Users\Administrator> AC
PS C:\Users\Administrator> $ENV:COMPUTERNAME
AYUSHSHAH
PS C:\Users\Administrator> Enter-PSSession -ComputerName 192.168.196.130 -Credential Contoso\Contoso\Contoso
[192.168.196.130]: PS C:\Users\Administrator\Documents> Enable-NetFirewallRule -DisplayName "Hyper-V Replica HTTP Listener (TCP-In)"
[192.168.196.130]: PS C:\Users\Administrator\Documents> Get-NetFirewallRule -DisplayName "Hyper-V Replica HTTP Listener (TCP-In)"

Name          : VIRT-HVRHTTPPL-In-TCP-NoScope
DisplayName   : Hyper-V Replica HTTP Listener (TCP-In)
Description   : Inbound rule for Hyper-V Replica listener to accept HTTP connection for replication.
LTCPIPPort    : 443
Protocol      : TCP
Enabled       : True
Profile       : Any
Inbound       : {}
Action        : Allow
EdgeTraversalPolicy : NotApplicable
LooseSourceMapping : PersistentStore
LocalOnlyMapping : Local
Owner         : 
PrimaryStatus : OK
Status        : The rule was parsed successfully from the store. (65536)
EncryptionStatus : 
PolicyStoreResource : 
PolicyStoreSourceType : 
RemoteDynamicKeywordAddresses : 
PolicyApplid : {}
```

# Windows Server Security

Student Name: Ayush Shah  
Student ID: 101545670

Term: Fall 2024.

