Career Prep 2

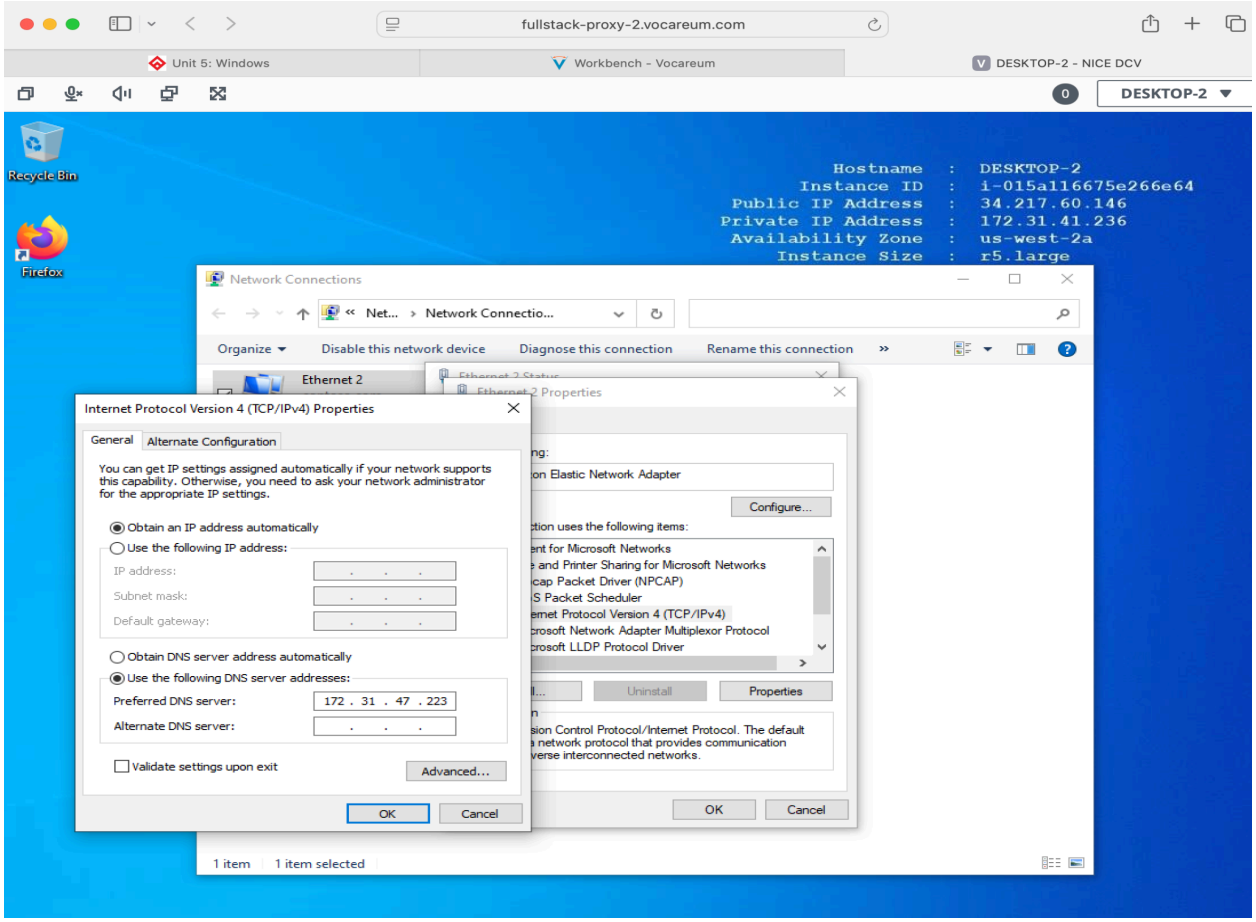
!!{My sentence formatting is not good, I ended up running my typed out responses into chat to format it. if thats not ok I'll revert and send you the rough version}!!

Join DESKTOP-2 to the Server/Domain

For this step, I configured the network settings on **DESKTOP-2** so it could communicate with the domain controller.

What I did:

- Opened **Network Connections** on DESKTOP-2.
- Right-clicked **Ethernet 2**, then opened **Properties**.
- Selected **Internet Protocol Version 4 (TCP/IPv4)**.
- Entered the **private IP address** of the server/domain controller as the preferred DNS server.

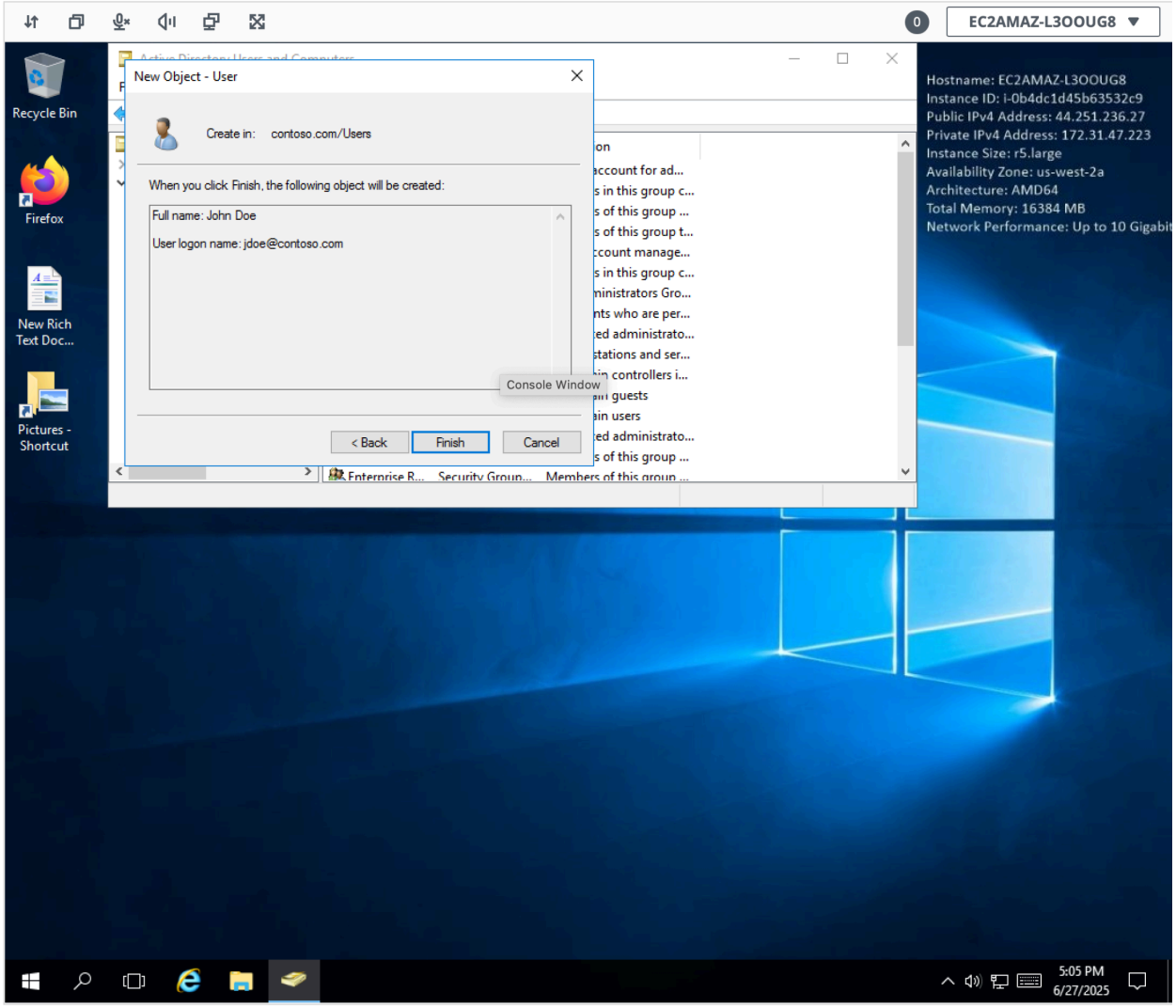


Create the User on the Server

For this step, I created the new hire's domain user account on the **server** using Active Directory.

What I did:

- Opened **Active Directory Users and Computers (ADUC)** on the **server VM**.
- Navigated to the **Users** container.
- Right-clicked and selected **New > User** to launch the new user wizard.
- Filled in the required details to create the user account for the new hire.



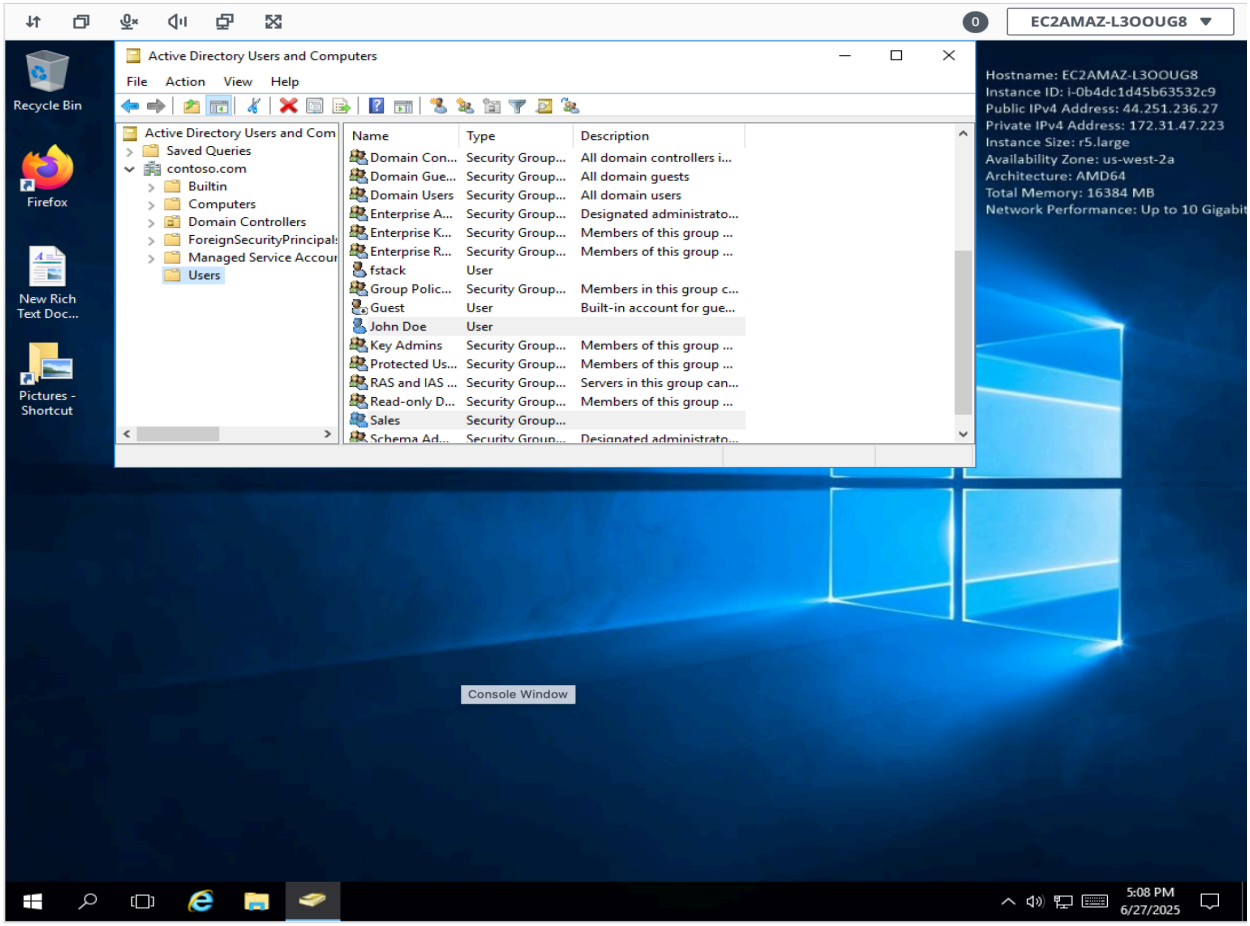
Create the Department Group

For this step, I created a **department security group** in Active Directory to help manage permissions for multiple users in the same department.

What I did:

- In **Active Directory Users and Computers (ADUC)**, I right-clicked on the **Users** container.
- Selected **New > Group**.
- Named the group `Sales`.
- Set the **Group scope** to **Global** and the **Group type** to **Security**.

- After creating the group, I double-clicked the **Sales** group, went to the **Members** tab, and added **John Doe** to the group.



Create the Department Share

For this step, I created a shared folder on the server for the **Sales** department and set proper permissions.

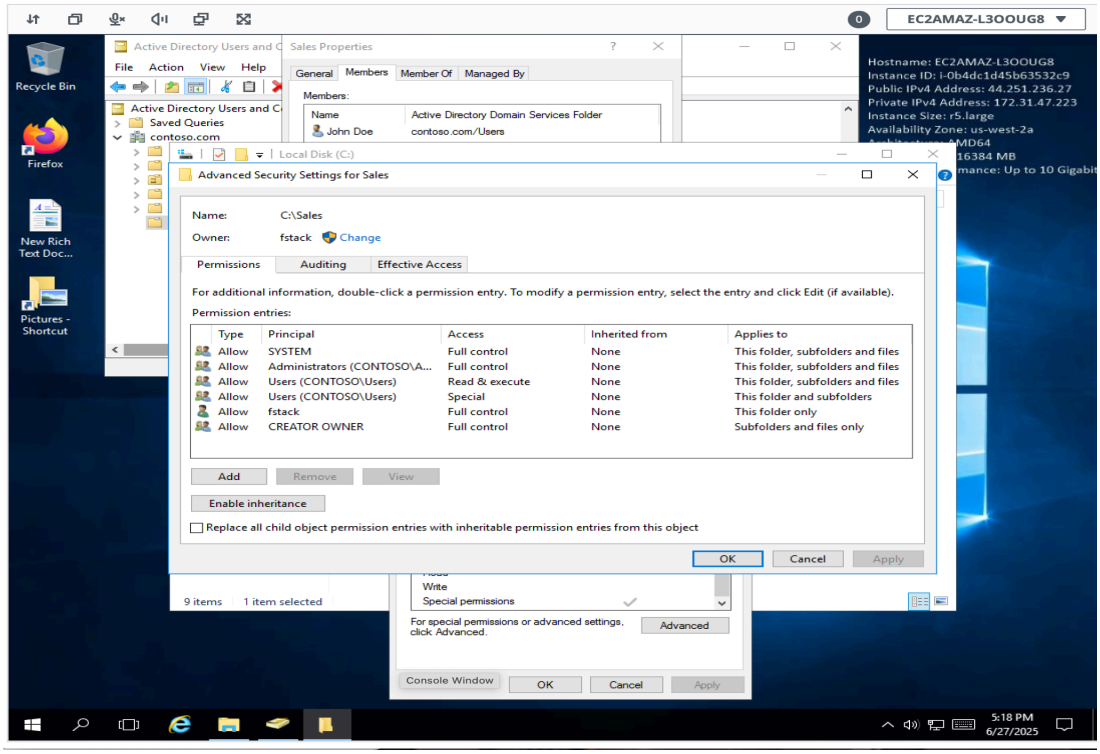
What I did:

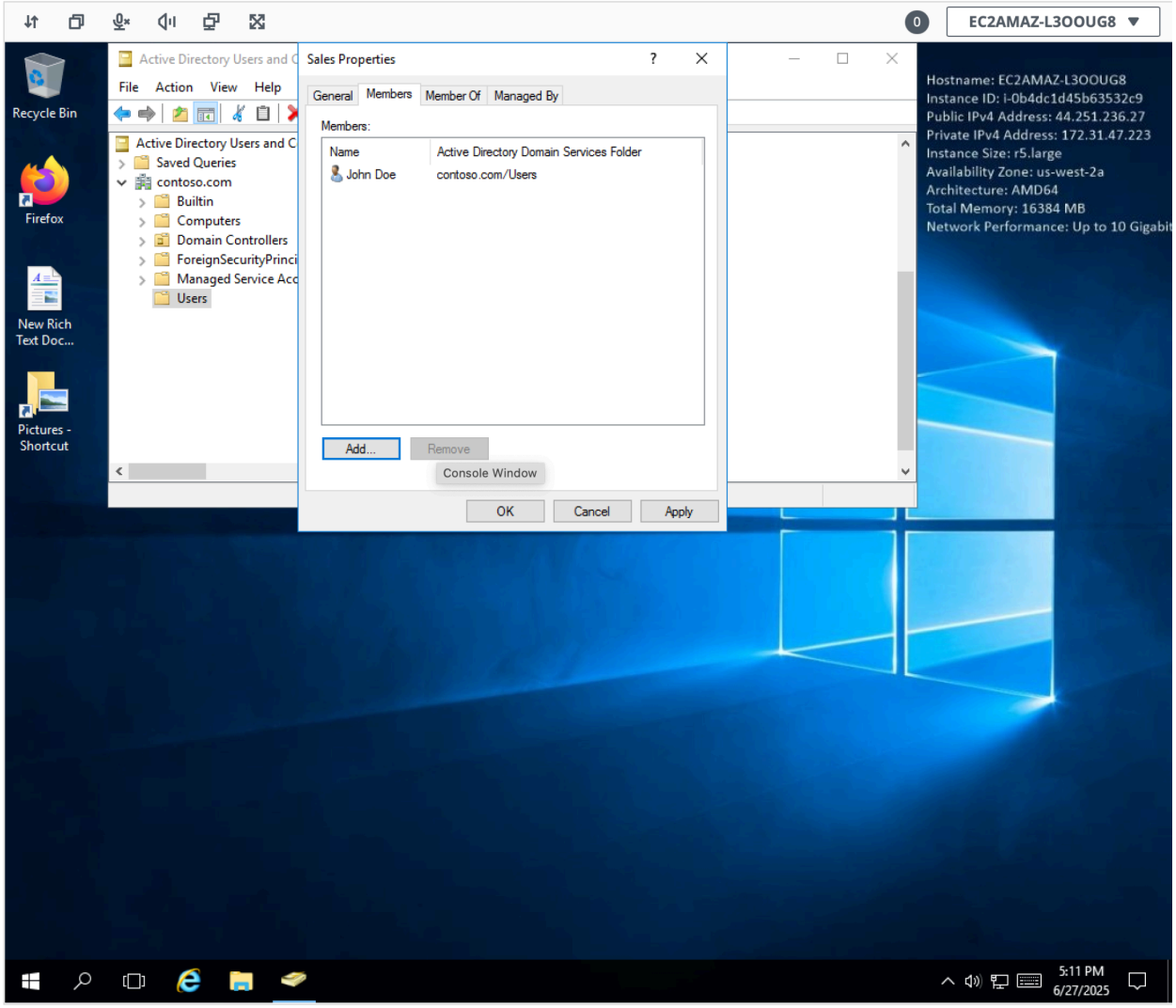
- On the **server**, I created a new folder called `Sales`.
- Right-clicked the folder → selected **Properties** → opened the **Sharing** tab.

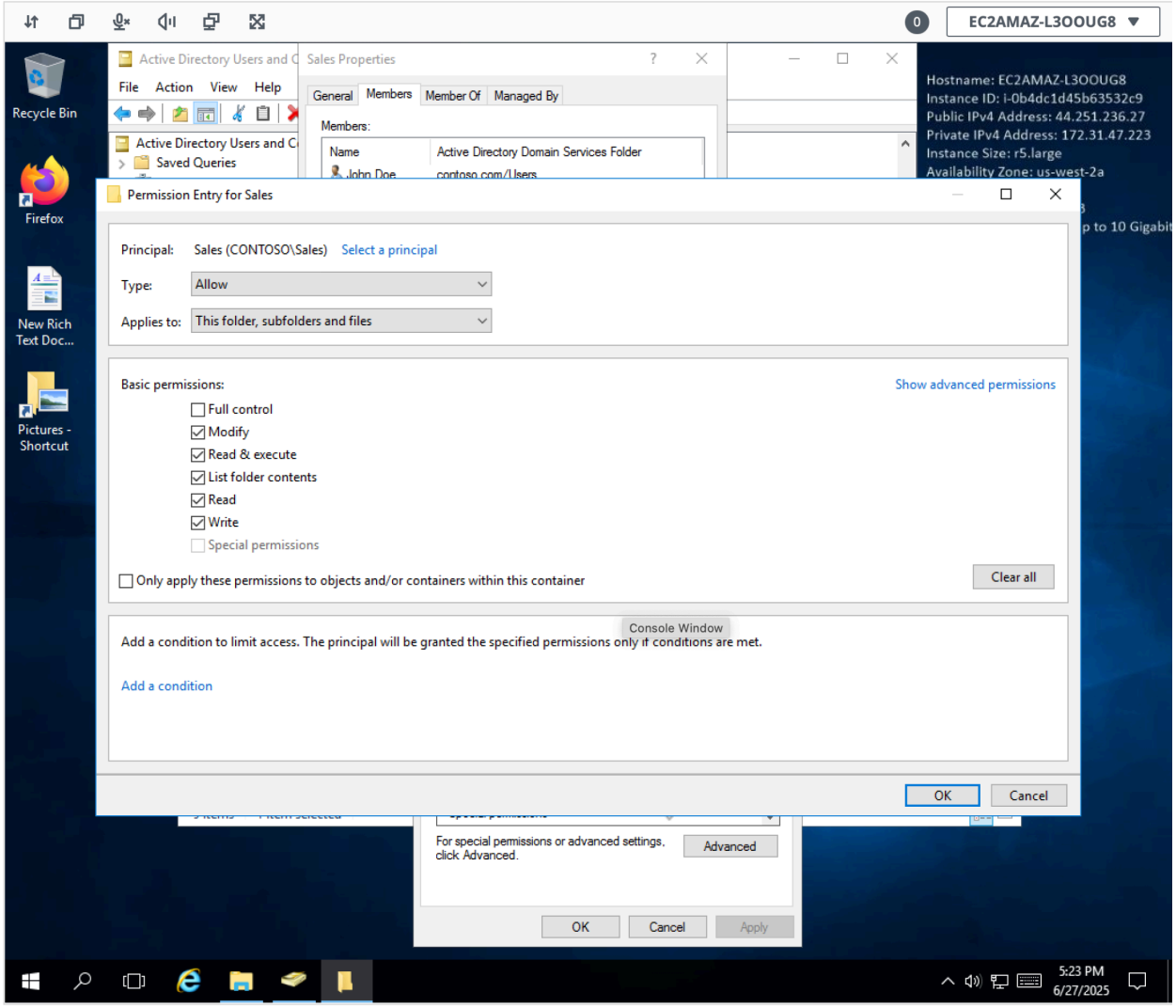
- Clicked **Advanced Sharing**, checked **Share this folder**, and named the share `Sales`.

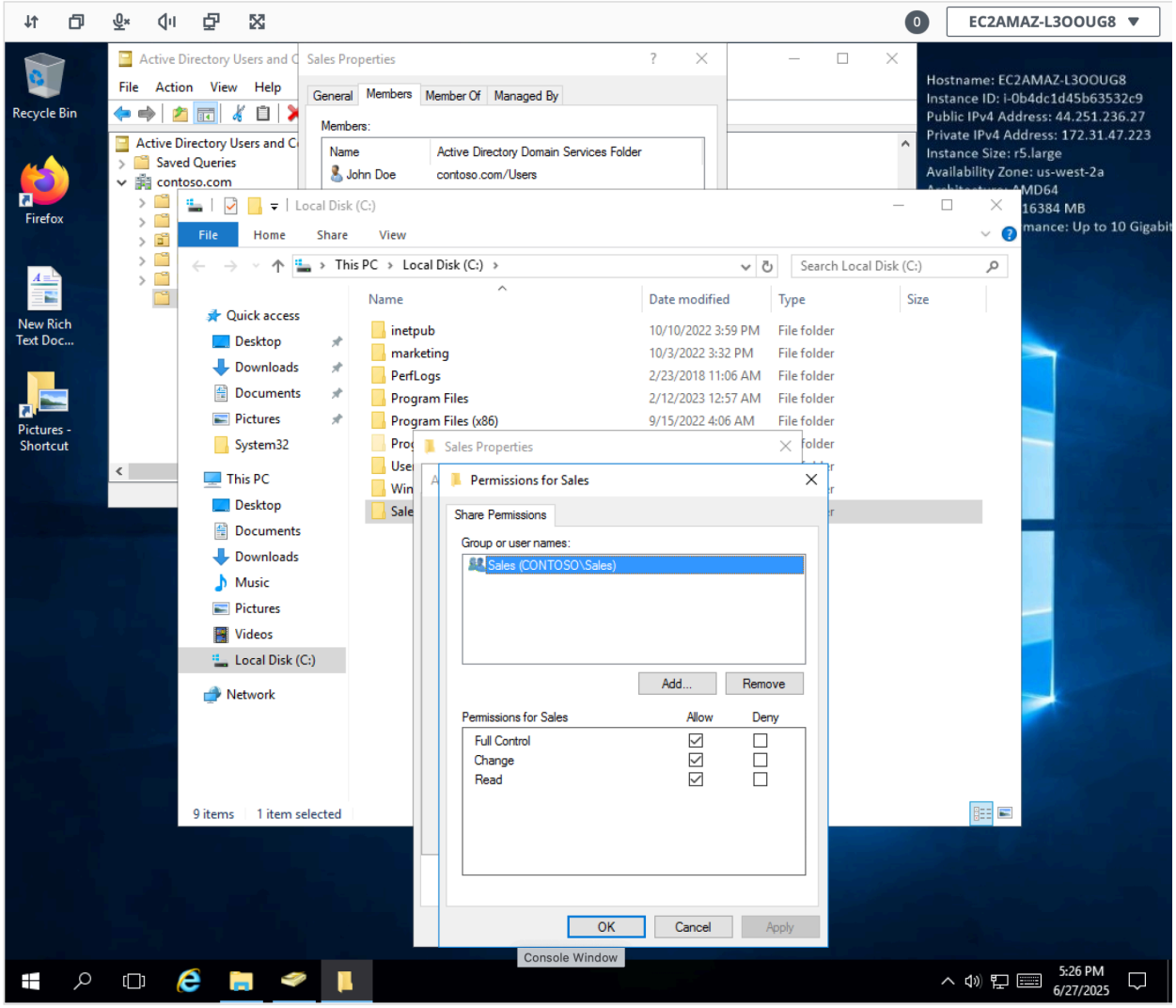
- Clicked **Permissions**, removed **Everyone**, and added the `Sales` group with **Read/Write** permissions.

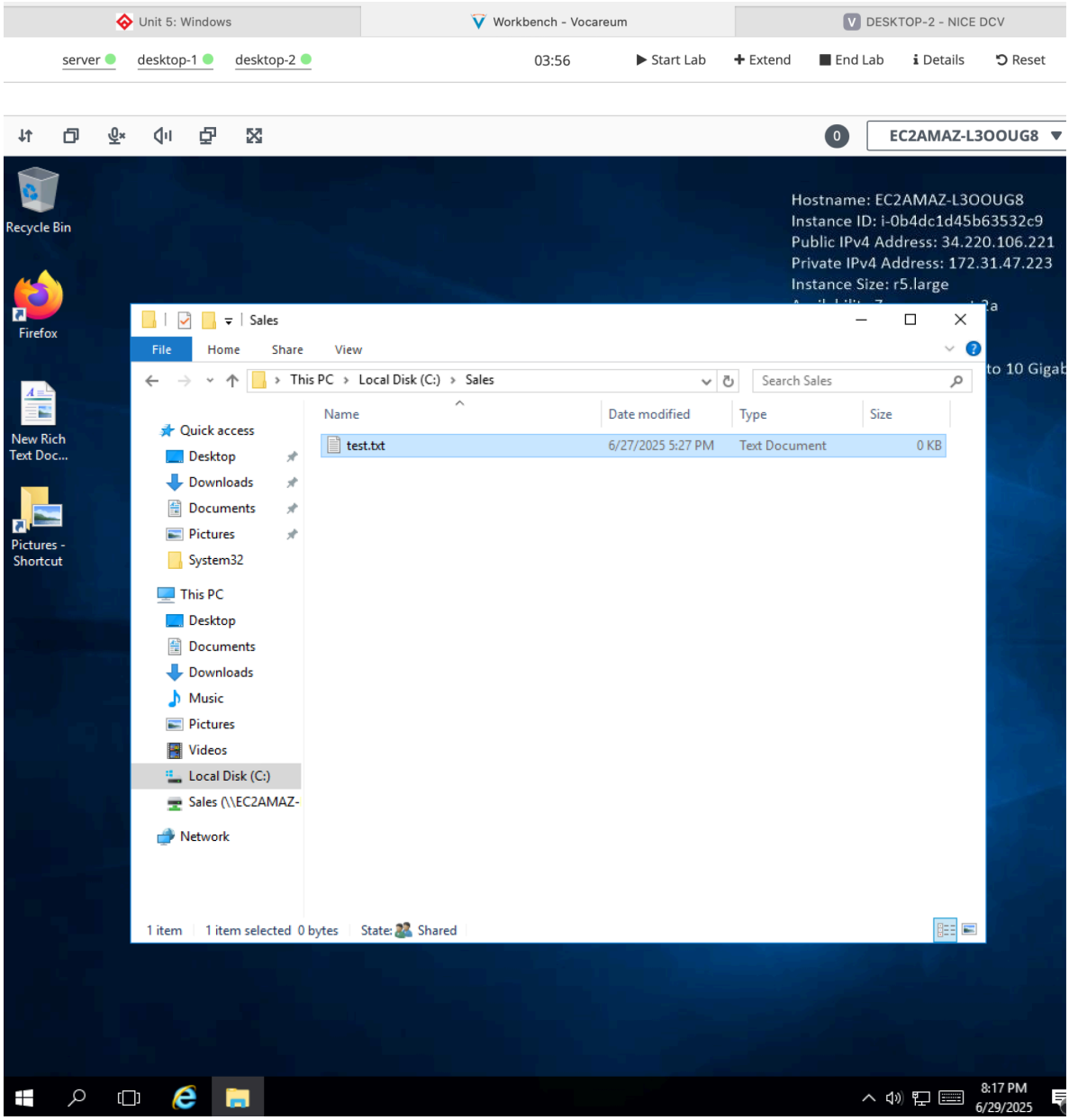
- Also went into the **Security** tab → **Permission Entry** for the Sales folder, added the `Sales` group, and granted **Modify** permissions.




EC2AMAZ-L3OOUG8
Recycle Bin
Firefox
New Rich Text Doc...
Pictures - Shortcut
Active Directory Users and C
File Action View Help
Active Directory Users and C
Saved Queries
contoso.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrinci
Managed Service Acc
Users
Sales Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
John Doe
contoso.com/Users
Add...
Remove
Console Window
OK
Cancel
Apply
Hostname: EC2AMAZ-L3OOUG8
Instance ID: i-0b4dc1d45b63532c9
Public IPv4 Address: 44.251.236.27
Private IPv4 Address: 172.31.47.223
Instance Size: r5.large
Availability Zone: us-west-2a
Architecture: AMD64
Total Memory: 16384 MB
Network Performance: Up to 10 Gigabit
5:11 PM
6/27/2025


EC2AMAZ-L3OOUG8
Recycle Bin
Firefox
New Rich Text Doc...
Pictures - Shortcut
Active Directory Users and C
File Action View Help
Active Directory Users and C
Saved Queries
Sales Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
John Doe
contoso.com/Users
Hostname: EC2AMAZ-L3OOUG8
Instance ID: i-0b4dc1d45b63532c9
Public IPv4 Address: 44.251.236.27
Private IPv4 Address: 172.31.47.223
Instance Size: r5.large
Availability Zone: us-west-2a
Permission Entry for Sales
Principal: Sales (CONTOSO\Sales) Select a principal
Type: Allow
Applies to: This folder, subfolders and files
Basic permissions:
Show advanced permissions
Full control
Modify
Read & execute
List folder contents
Read
Write
Special permissions
Only apply these permissions to objects and/or containers within this container
Clear all
Console Window
Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.
Add a condition
OK
Cancel
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
5:23 PM
6/27/2025


EC2AMAZ-L3OOUG8
Recycle Bin
Firefox
New Rich Text Doc...
Pictures - Shortcut
Active Directory Users and C
File Action View Help
Saved Queries
contoso.com
Sales Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
John Doe
contoso.com/Users
Hostname: EC2AMAZ-L3OOUG8
Instance ID: i-0b4dc1d45b63532c9
Public IPv4 Address: 44.251.236.27
Private IPv4 Address: 172.31.47.223
Instance Size: r5.large
Availability Zone: us-west-2a
Local Disk (C:)
File Home Share View
This PC › Local Disk (C:) ›
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Date modified
Type
Size
inetpub
10/10/2022 3:59 PM
File folder
marketing
10/3/2022 3:32 PM
File folder
PerfLogs
2/23/2018 11:06 AM
File folder
Program Files
2/12/2023 12:57 AM
File folder
Program Files (x86)
9/15/2022 4:06 AM
File folder
9 items
1 item selected
Sales Properties
Permissions for Sales
Share Permissions
Group or user names:
Sales (CONTOSO\Sales)
Add...
Remove
Permissions for Sales
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
Console Window
5:26 PM
6/27/2025

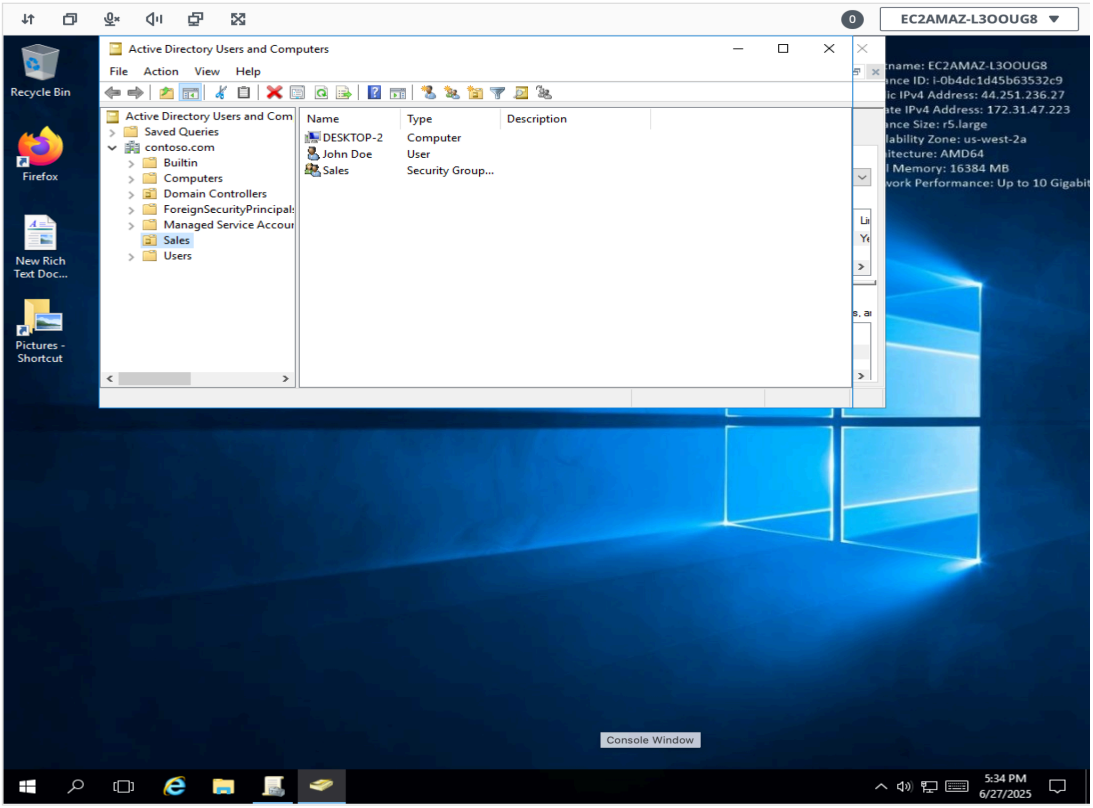

Unit 5: Windows
Workbench - Vocareum
DESKTOP-2 - NICE DCV
server
desktop-1
desktop-2
03:56
Start Lab
Extend
End Lab
Details
Reset
EC2AMAZ-L3OOUG8
Recycle Bin
Firefox
New Rich Text Doc...
Pictures - Shortcut
Hostname: EC2AMAZ-L3OOUG8
Instance ID: i-0b4dc1d45b63532c9
Public IPv4 Address: 34.220.106.221
Private IPv4 Address: 172.31.47.223
Instance Size: r5.large
Sales
File
Home
Share
View
This PC › Local Disk (C:) › Sales
Search Sales
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Sales (\\EC2AMAZ-
Network
Name
Date modified
Type
Size
test.txt
6/27/2025 5:27 PM
Text Document
0 KB
1 item
1 item selected 0 bytes
State: Shared
8:17 PM
6/29/2025

Create the OU (Organizational Unit) & Move Objects

For this step, I created an Organizational Unit (OU) for the Sales department in Active Directory and organized all related objects inside it.

What I did:

- **Opened Active Directory Users and Computers (ADUC).**
- **Found the domain `contoso.com`, right-clicked it, and selected New > Organizational Unit.**
- **Named the new OU `Sales`.**
- **Moved the following objects into the Sales OU:**
  - **The `John Doe` user account**
  - **The `Sales` group**
  - **The DESKTOP-2 computer object**



Create & Configure the GPO (Group Policy Object)

For this step, I created and configured a Group Policy Object (GPO) to apply security and management settings to the Sales department's workstations.

What I did:

- Opened Group Policy Management on the server.
- Right-clicked the Sales OU, selected Create a GPO in this domain, and named it `Sales-Workstation-Policy`.
- Right-clicked the new GPO and chose Edit to configure the settings.

Configured the following policies:

Startup Message:
I navigated to Security Options and set:

- Interactive Logon: Message title for users attempting to log on
- Interactive Logon: Message text for users attempting to log on
  This displays a message reminding users: "Do not install unauthorized programs."

Block CMD:
I disabled access to the Command Prompt to prevent unauthorized command execution.

Disable Run Command:
I disabled the Run command from the Start Menu to limit ways users can bypass restrictions.

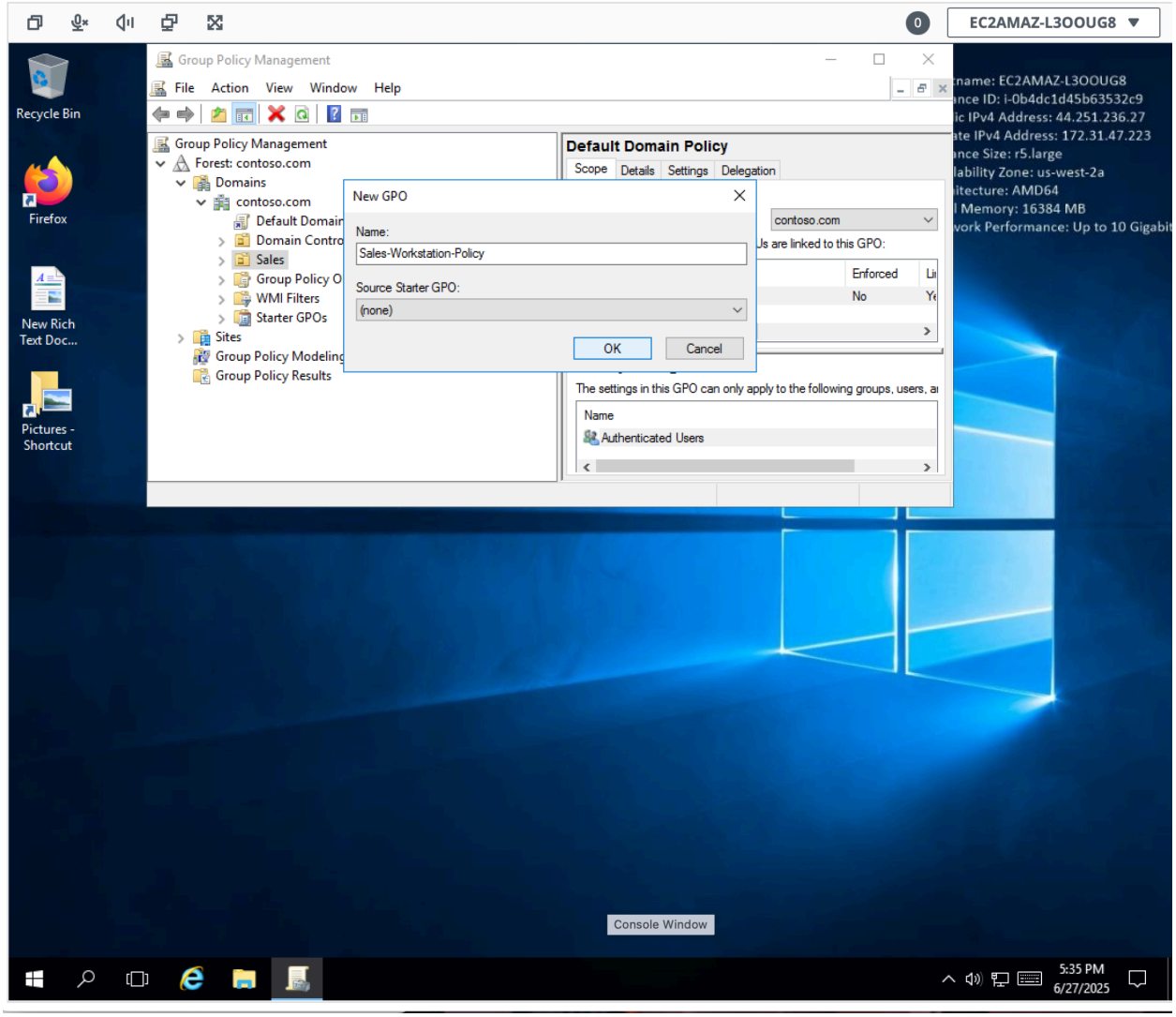
Map Drive Script:
I opened PowerShell as Administrator and wrote the logon script to automatically map a shared drive:

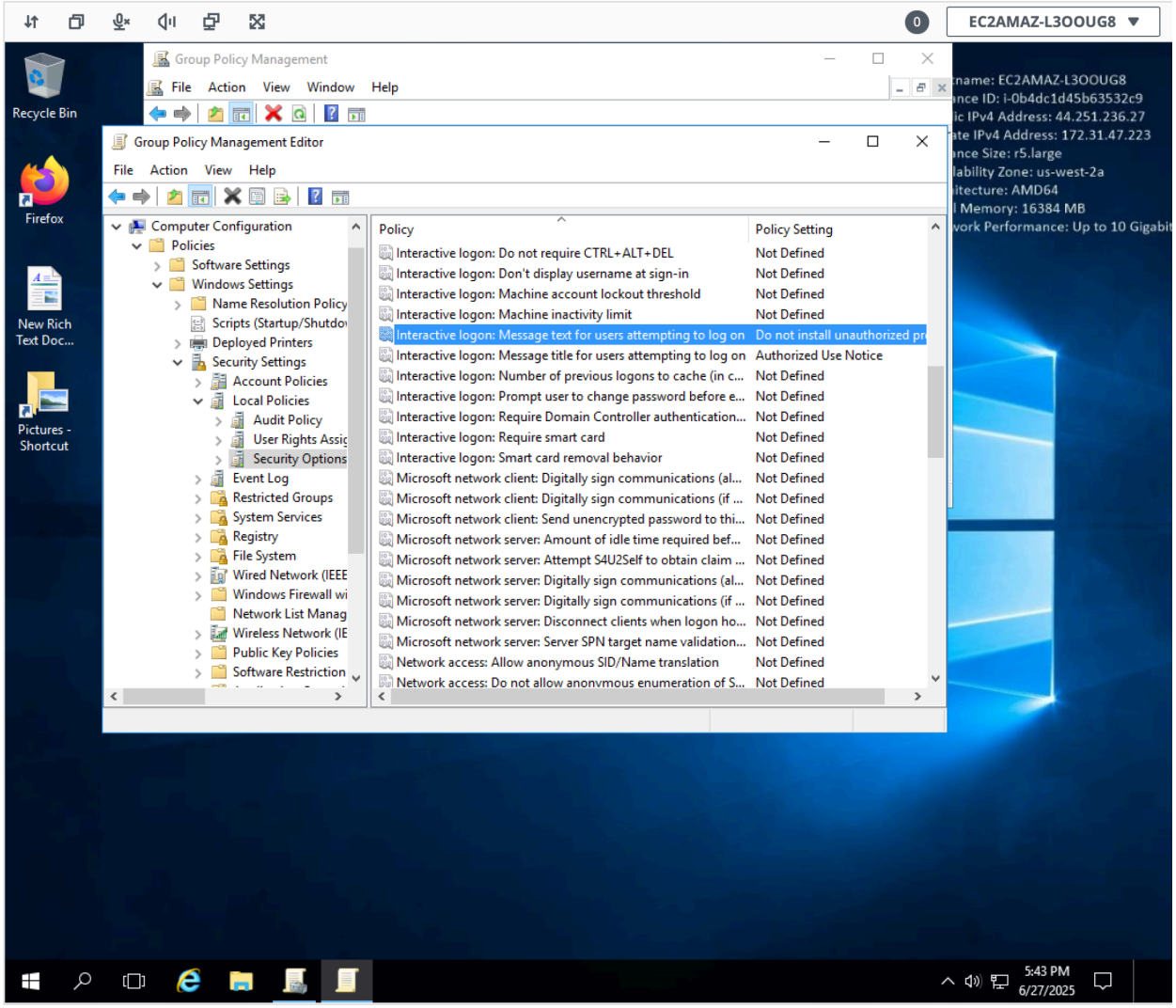
```
'New-PSDrive -Name "Z" -PSProvider "FileSystem" -Root "\\EC2AMAZ-L3O0UG8\Sales"
-Persist' | Out-File -FilePath 'C:\Windows\SYSVOL\sysvol\contoso.com\scripts\MapDrive.ps1'
-Encoding utf8
```

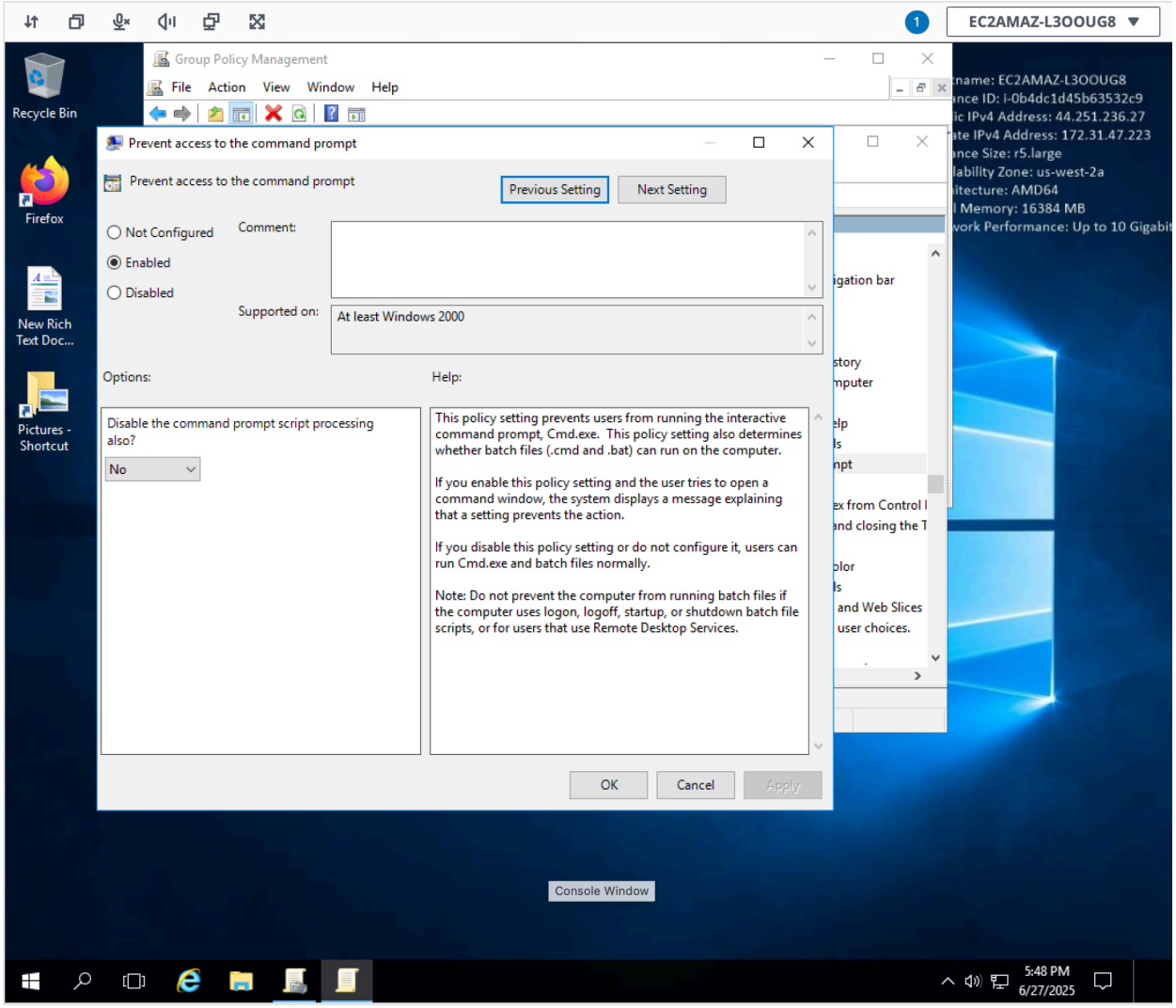
Because Group Policy Logon Scripts require a .bat or .cmd file, I created a wrapper script:

```
'@echo off
powershell.exe -ExecutionPolicy Bypass -File
\\EC2AMAZ-L3O0UG8\SYSVOL\contoso.com\scripts\MapDrive.ps1' | Out-File -FilePath
"C:\Windows\SYSVOL\sysvol\contoso.com\scripts\MapDriveWrapper.bat" -Encoding ascii
```

I then linked this .bat file in the GPO under:
User Configuration → Windows Settings → Scripts (Logon)




EC2AMAZ-L3OOUG8
Recycle Bin
Firefox
New Rich Text Doc...
Pictures - Shortcut
Group Policy Management
File Action View Window Help
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdo
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assig
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE
Windows Firewall wi
Network List Manag
Wireless Network (IE
Public Key Policies
Software Restriction
Policy
Policy Setting
Interactive logon: Do not require CTRL+ALT+DEL
Not Defined
Interactive logon: Don't display username at sign-in
Not Defined
Interactive logon: Machine account lockout threshold
Not Defined
Interactive logon: Machine inactivity limit
Not Defined
Interactive logon: Message text for users attempting to log on
Do not install unauthorized pr
Interactive logon: Message title for users attempting to log on
Authorized Use Notice
Interactive logon: Number of previous logons to cache (in c...
Not Defined
Interactive logon: Prompt user to change password before e...
Not Defined
Interactive logon: Require Domain Controller authentication...
Not Defined
Interactive logon: Require smart card
Not Defined
Interactive logon: Smart card removal behavior
Not Defined
Microsoft network client: Digitally sign communications (al...
Not Defined
Microsoft network client: Digitally sign communications (if ...
Not Defined
Microsoft network client: Send unencrypted password to thi...
Not Defined
Microsoft network server: Amount of idle time required bef...
Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim ...
Not Defined
Microsoft network server: Digitally sign communications (al...
Not Defined
Microsoft network server: Digitally sign communications (if ...
Not Defined
Microsoft network server: Disconnect clients when logon ho...
Not Defined
Microsoft network server: Server SPN target name validation...
Not Defined
Network access: Allow anonymous SID/Name translation
Not Defined
Network access: Do not allow anonymous enumeration of S...
Not Defined
5:43 PM
6/27/2025


EC2AMAZ-L3OOUG8
Group Policy Management
File Action View Window Help
Recycle Bin
Firefox
New Rich Text Doc...
Pictures - Shortcut
Prevent access to the command prompt
Prevent access to the command prompt
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Disable the command prompt script processing also?
No
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.
If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.
If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.
Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.
OK
Cancel
Apply
Console Window
5:48 PM
6/27/2025

server desktop-1 desktop-2 02:33 ▶ Start Lab + Extend ■ End Lab ℹ Details ↺ Reset

EC2AMAZ-L3OOUG8

Administrator: Windows PowerShell

```
PS C:\Windows\system32> 'New-PSDrive -Name "Z" -PSProvider "FileSystem" -Root "\\EC2AMAZ-L3OOUG8\Sales
ile -FilePath "MapDrive.ps1" -Encoding utf8
PS C:\Windows\system32> 'New-PSDrive -Name "Z" -PSProvider "FileSystem" -Root "\\EC2AMAZ-L3OOUG8\Sales
ile -FilePath "\\EC2AMAZ-L3OOUG8\SYSVOL\contoso.com\scripts\MapDrive.ps1" -Encoding utf8
Out-File : The network path was not found.
At line:1 char:92
+ ... -Persist' | Out-File -FilePath "\\EC2AMAZ-L3OOUG8\SYSVOL\contoso.com\ ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OpenError: (:) [Out-File], IOException
    + FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCommand

PS C:\Windows\system32>
PS C:\Windows\system32> 'New-PSDrive -Name "Z" -PSProvider "FileSystem" -Root "\\EC2AMAZ-L3OOUG8\Sales
ile -FilePath "\\EC2AMAZ-L3OOUG8\SYSVOL\contoso.com\scripts\MapDrive.ps1" -Encoding utf8
Out-File : The network path was not found.
At line:1 char:92
+ ... -Persist' | Out-File -FilePath "\\EC2AMAZ-L3OOUG8\SYSVOL\contoso.com\ ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OpenError: (:) [Out-File], IOException
    + FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCommand

PS C:\Windows\system32> 'New-PSDrive -Name "Z" -PSProvider "FileSystem" -Root "\\EC2AMAZ-L3OOUG8\Sales
ile -FilePath "\\EC2AMAZ-L3OOUG8\SYSVOL\sysvol\contoso.com\scripts\MapDrive.ps1" -Encoding utf8
Out-File : The network path was not found.
At line:1 char:92
+ ... -Persist' | Out-File -FilePath "\\EC2AMAZ-L3OOUG8\SYSVOL\sysvol\conto ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OpenError: (:) [Out-File], IOException
    + FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCommand

PS C:\Windows\system32> 'New-PSDrive -Name "Z" -PSProvider "FileSystem" -Root "\\EC2AMAZ-L3OOUG8\Sales
ile -FilePath "C:\Windows\SYSVOL\sysvol\contoso.com\scripts\MapDrive.ps1" -Encoding utf8
PS C:\Windows\system32>
```

stname: EC2AMAZ-L3OOUG8

ripts Search scripts

Date m

rive 6/29/2

1 item 1 item selected

Console Window

server desktop-1 desktop-2 02:32 ▶ Start Lab + Extend ■ End Lab ℹ Details ↺ Reset

0 EC2AMAZ-L3OOUG8

Administrator: Windows PowerShell

```
PS C:\Windows\system32> New-PSDrive -Name "Z" -PSProvider "FileSystem" -Root "\\EC2AMAZ-L3OOUG8\Sales
ile -FilePath "MapDrive
PS C:\Windows\system32>
ile -FilePath "\\EC2AMA
Out-File : The network
At line:1 char:92
+ ... -Persist' | Out-F
+                 ~~~~~
    + CategoryInfo
    + FullyQualifiedErr

PS C:\Windows\system32>
PS C:\Windows\system32>
ile -FilePath "\\EC2AMA
Out-File : The network
At line:1 char:92
+ ... -Persist' | Out-F
+                 ~~~~~
    + CategoryInfo
    + FullyQualifiedErr

PS C:\Windows\system32>
ile -FilePath "\\EC2AMA
Out-File : The network
At line:1 char:92
+ ... -Persist' | Out-F
+                 ~~~~~
    + CategoryInfo
    + FullyQualifiedErr

PS C:\Windows\system32>
ile -FilePath "C:\Windo
PS C:\Windows\system32>
```

stname: EC2AMAZ-L3OOUG8

scripts

File Home Share View

« Windows › SYSVOL › sysvol › contoso.com › scripts

Search scripts

Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network

Name	Date modified	Type	Size
MapDrive	6/29/2025 9:37 PM	Windows PowerS...	1 KB

1 item State: Shared

1 item 1 item selected

Console Window

server desktop-1 desktop-2 02:58 ▶ Start Lab ✚ Extend ■ End Lab ℹ Details ↺ Reset

EC2AMAZ-L3OOUG8

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> @echo off powershell.exe -ExecutionPolicy Bypass -File \\EC2AMAZ-L3OOUG8\SYSVOL\contoso.com\scri
pts\MapDrive.ps1
At line:1 char:7
+ @echo off powershell.exe -ExecutionPolicy Bypass -File \\EC2AMAZ-L300 ...
+       ~~~
Unexpected token 'off' in expression or statement.
At line:1 char:1
+ @echo off powershell.exe -ExecutionPolicy Bypass -File \\EC2AMAZ-L300 ...
+ ~~~~~
The splatting operator '@' cannot be used to reference variables in an expression. '@echo' can be used only as an
argument to a command. To reference variables in an expression use '$echo'.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : UnexpectedToken

PS C:\Windows\system32> '@echo off powershell.exe -ExecutionPolicy Bypass -File \\EC2AMAZ-L3OOUG8\SYSVOL\contoso.com\scr
Out-File -FilePath "C:\Windows\SYSVOL\sysvol\contoso.com\scripts\MapDriveWrapper.bat" -Encoding ascii
PS C:\Windows\system32>
```

Console Window

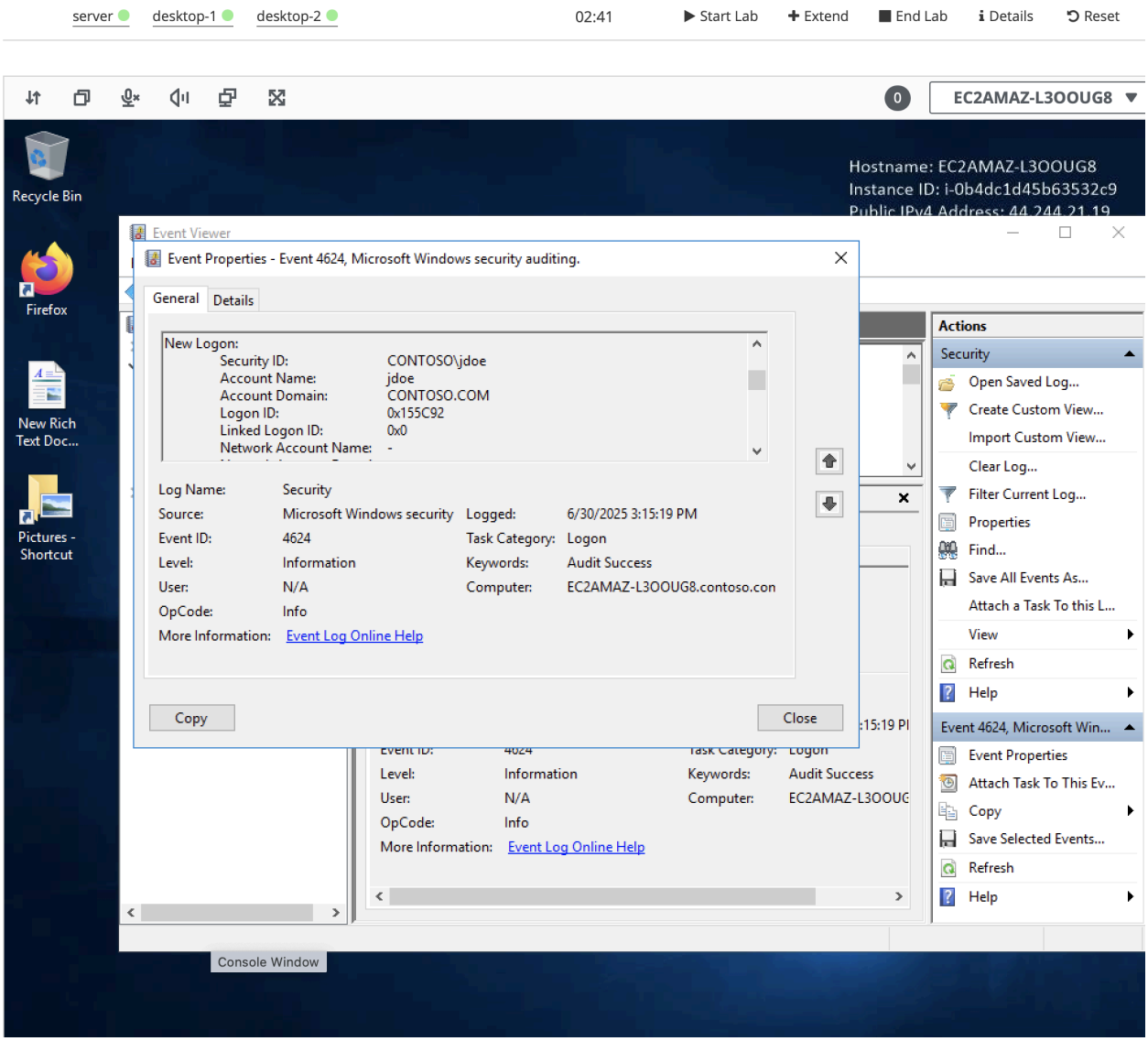
-L3OOUG8
d45b63532c9
44.244.21.19
172.31.47.223
e
west-2a
4 MB
e: Up to 10 Gigab

Verify Successful Logon in Event Viewer

For this step, I confirmed that the new user account successfully logged in by checking the Event Viewer.

What I did:

- Opened **Event Viewer** on the server.
- Clicked **Windows Logs**, then selected **Security**.
- Filtered for **Event ID 4624** (successful logon events).
- Verified that `CONTOSO\jdoe` appeared in the log as having successfully logged in.



Generate Installed Programs Report

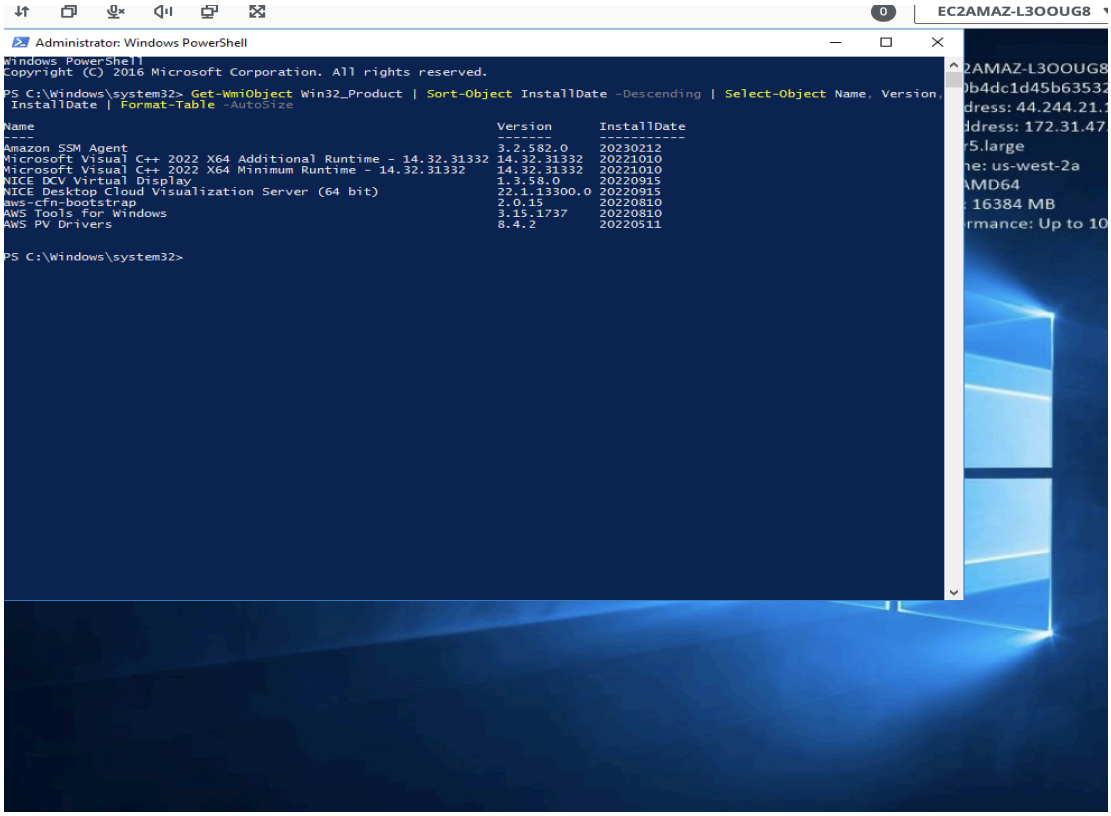
For this step, I ran a PowerShell command to generate a report of the most recently installed programs on the server.

What I did:

- Opened **PowerShell** on the server.
- Used the following command to list all installed MSI-based programs, sorted by the install date from newest to oldest:

  Get-WmiObject Win32_Product |
  Sort-Object InstallDate -Descending |
  Select-Object Name, Version, InstallDate |
  Format-Table -AutoSize

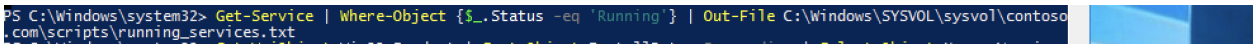
  This output shows the software name, version, and installation date in a clear, readable table.



Generate Running Services Report

For this step, I used PowerShell to create a report listing all currently running services on the server.

What I did:

- Opened **PowerShell** on the server.
- Ran the following command to get all services with a status of **Running** and saved the output to a text file in the `SYSVOL\scripts` folder:

Get-Service | Where-Object {$_.Status -eq 'Running'} | Out-File "C:\Windows\SYSVOL\sysvol\contoso.com\scripts\running_services.txt"