

## **Recruiter Summary — IT Help Desk / Service Desk Portfolio**

Candidate: Kingsley Otoo

Target Roles: IT Help Desk / IT Support / Service Desk Analyst

Environment: Windows 11, Windows Server 2022, Active Directory

### **Profile Overview**

This portfolio demonstrates hands-on, job-ready IT Support capability through realistic Help Desk scenarios. All work was performed in a controlled Windows 11 and Active Directory lab designed to mirror real-world Service Desk operations. Each scenario follows a ticket-based workflow: issue reported, investigation, resolution, and validation.

Key Signals for Hiring Managers:

- Hands-on Windows 11 and Active Directory support experience
- Real-world incident troubleshooting using logs and policy tools
- Evidence-backed problem resolution with validation steps
- Documentation written to professional Service Desk standards

### **Core Capabilities Demonstrated**

- Windows 11 troubleshooting and user support
- Active Directory user, group, and policy management
- Group Policy enforcement and validation (gpupdate, gpresult, RSOP)
- Account lockout, permissions, and UAC troubleshooting
- Scheduled task diagnostics and log analysis
- Network drive mapping and access control
- Professional documentation and evidence collection

### **Why This Candidate Is Job-Ready**

- Thinks in tickets and incidents, not just technical tasks
- Demonstrates structured troubleshooting and root-cause analysis
- Produces documentation to professional IT standards
- Comfortable working in both standalone and domain environments
- Evidence-backed work suitable for interview deep dives

### **How to Review This Portfolio**

1. Review the Help Desk Scenarios section to assess real-world support thinking.
2. Refer to the Evidence Appendix for screenshots and validation proof.
3. Use scenarios directly as interview discussion points.

## **Windows 11 Help Desk Scenarios – IT Support Portfolio**

This portfolio presents practical Help Desk and IT Support scenarios based on a Windows 11 home lab environment. Each scenario is written in a ticket-style format to reflect real-world Service Desk workflows, including issue intake, investigation, resolution, and validation. Evidence is referenced throughout and supported by a full appendix of screenshots.

### **Environment Overview**

- Client OS: Windows 11 Pro
- Server OS: Windows Server 2022 (Active Directory)
- Virtualisation Platform: VMware Workstation
- Domain: LAB.local
- Focus: First-line and second-line IT Support scenarios

### **Support Scenario 1 — User Unable to Log In (Account Lockout)**

**Reported Issue:**

User unable to log in after multiple failed attempts.

**Investigation:**

Reviewed local security policy and Event Viewer logs.

**Resolution:**

Unlocked account and confirmed password policy settings.

**Validation:**

Successful login confirmed.

**Evidence:**

Figures 8–9

### **Support Scenario 2 — Administrative Task Blocked by UAC**

**Reported Issue:**

User could not perform administrative task.

**Investigation:**

Confirmed standard user context and UAC behaviour.

**Resolution:**

Performed task with elevated credentials.

**Validation:**

Task completed successfully.

Evidence:  
Figures 10–11

### **Support Scenario 3 — Scheduled Task Did Not Execute**

Reported Issue:  
Scheduled task failed to generate output.

Investigation:  
Reviewed Task Scheduler logs and execution context.

Resolution:  
Corrected execution settings.

Validation:  
Task ran successfully.

Evidence:  
Figures 12–20

### **Support Scenario 4 — Group Policy Not Applying**

Reported Issue:  
Expected policy not applied to user.

Investigation:  
Used gpupdate, gpresult, and RSOP.

Resolution:  
Corrected policy scope.

Validation:  
Policy applied as expected.

Evidence:  
Figures 21–37

### **Support Scenario 5 — Network Drive Missing**

Reported Issue:  
Mapped drive not visible.

Investigation:  
Checked Group Policy Preferences and permissions.

Resolution:  
Corrected access permissions.

**Validation:**  
Drive visible and accessible.

**Evidence:**  
Figures 38–40

### **Conclusion**

This portfolio demonstrates the ability to handle realistic Help Desk incidents, apply structured troubleshooting, and validate outcomes using appropriate tools.

## Evidence Appendix (Screenshots)

The following figures provide supporting evidence for the Help Desk scenarios documented in this portfolio. Figures are grouped by scenario to simplify review. Each figure includes the source filename.

# Environment & Infrastructure Evidence

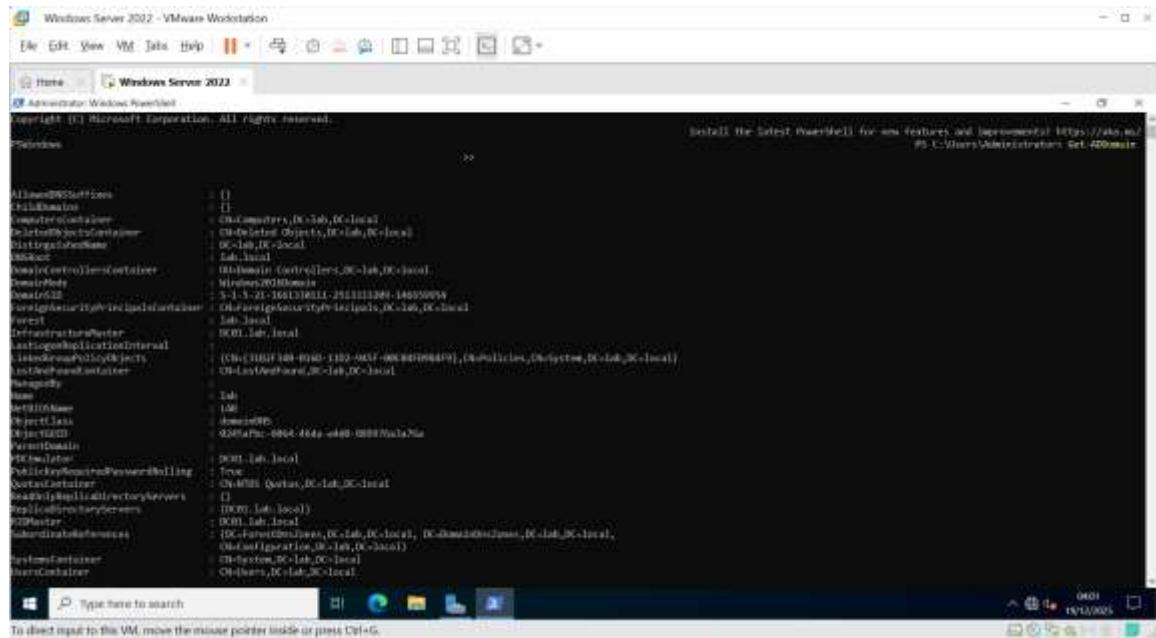


Figure 1: Screenshot evidence.

Source file: DomainControllerConfirmed.png

```
Windows Server 2022 - VMware Workstation
File Edit View VM Tabs Help || Home Windows Server 2022
Selected Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.507]
Copyright Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /flushdns

Windows IP Configuration

Adapter Name: Intel(R) Dual Band Wireless-AC 7265
    Description: Intel(R) Dual Band Wireless-AC 7265 Network Connection
    Physical Address: 00-0C-26-3E-1E-1A
    DHCP Enabled: Yes
    IP Routing Enabled: No
    WINS Proxy Enabled: No
    DNS Suffix Search List: lab.local

Internet adapter Ethernet
    Connection-specific DNS Suffix: lab.local
    Description: Intel(R) Dual Band Wireless-AC 7265 Network Connection
    Physical Address: 00-0C-26-3E-1E-1A
    DHCP Enabled: Yes
    Autoconfiguration Enabled: Yes
    Link-local IPv4 Address: 169.254.1.110(PREFERRED)
    IPv4 Address: 192.168.2.115(Preferred)
    Subnet Mask: 255.255.255.0
    Default Gateway: 192.168.2.1
    DHCPv6 IAID: 40000000
    DHCPv6 Client ID: 00-0C-26-3E-1E-1A
    DNS Servers: 127.0.0.1
    DHCPv6 Lease Ticks: Enabled

C:\Users\Administrator>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

Windows Server 2022 - VMware Workstation
File Edit View VM Tabs Help || Home Windows Server 2022
Type here to search 1245
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Figure 2: Screenshot evidence.

Source file: FixWindows11DNS.png

```
Windows Server 2022 - VMware Workstation
File Edit View VM Tabs Help || Home Windows Server 2022
Selected Administrator: Command Prompt
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.

C:\Users\Administrator>netsh http register
Windows registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.

C:\Users\Administrator>stop netsh
The Netsh service is stopping.
The Netsh service was stopped successfully.

C:\Users\Administrator>start netsh
The Netsh service is starting.
The Netsh service was started successfully.

C:\Users\Administrator>netsh http lookup <http://lab.local>
'Netsh http lookup <http://lab.local>' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>netsh http lookup <http://lab.local>
DNS request timed out.
    timeout was 2 seconds.
Server: lab.local
Address: <http://>

Name: <http://lab.local>
Address: <http://192.168.2.115>

C:\Users\Administrator>ping <http://lab.local>(a)

Pinging <http://lab.local> [8000::a4d2::209:461:b27000] with 32 bytes of data:
```

Figure 3: Screenshot evidence.

Source file: FixWindows11DNS1.png

```
C:\Windows\system32\cmd.exe [Windows Server 2022]
File Edit View VM Tabs Help < Home > Windows Server 2022 > Select Administration (Command) Prompt

C:\Windows\system32>netsh interface ipv4 show interface
"vboxnetadp0 (eth0)" is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>netsh interface ipv4 set interface
IPX request failed.
    timeout was 2 seconds.
Server: Unknown
Address: 127.00.0.1

Name: 490169.local
Address: 192.168.244.128

C:\Windows\system32>netsh interface ipv4 show interface
Ping statistics for 490169.local [490169017-490169000]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip time is 1000 microseconds.
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

Figure 4: Screenshot evidence.

Source file: FixWindows11DNS2.png

```
C:\Windows\system32\cmd.exe [Windows 11 Test]
File Edit View VM Tabs Help < Home > Windows 11 Test > Windows Server 2022 > Select Administration (Command) Prompt

C:\Windows\system32>netsh interface ipv4 show interface
Successfully claimed the IPX resolver cache.
"vboxnetadp0 (eth0)" is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>netsh interface ipv4 set interface
IPX request failed.
    timeout was 2 seconds.
Server: Unknown
Address: 127.00.0.1

Name: 490169.local
Address: 192.168.244.128

C:\Windows\system32>netsh interface ipv4 show interface
Ping statistics for 490169.local [490169017-490169000]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip time is 1000 microseconds.
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>netsh interface ipv4 set interface
IPX request failed.
    timeout was 2 seconds.
Server: Unknown
Address: 127.00.0.1

C:\Windows\system32>
```

Figure 5: Screenshot evidence.

Source file: PingDC01.png

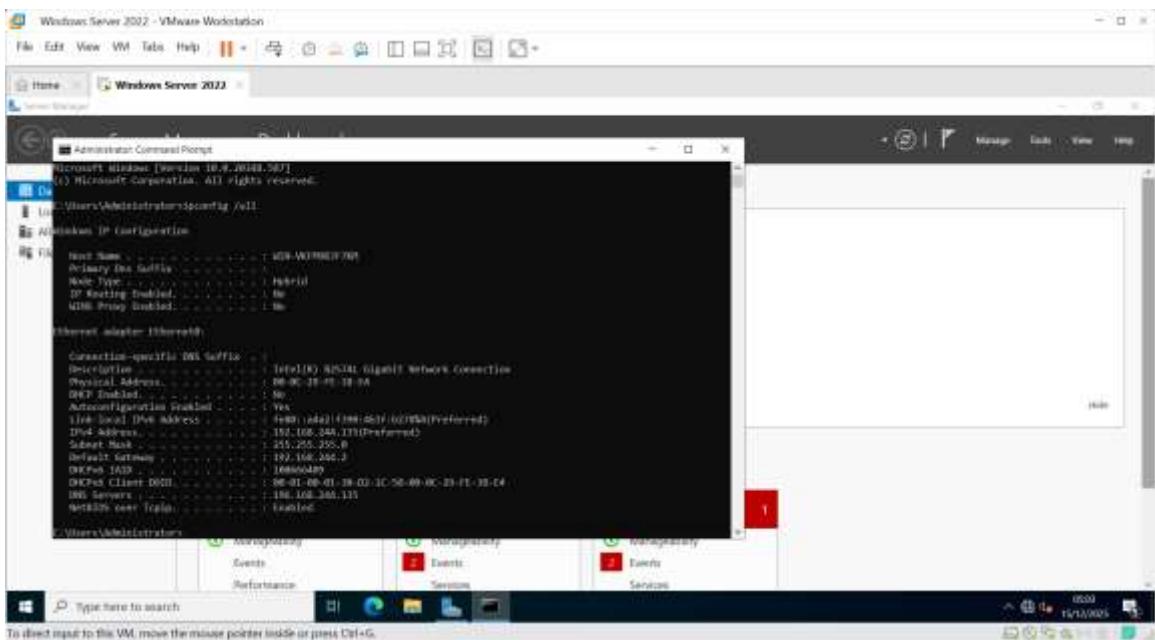


Figure 6: Screenshot evidence.

Source file: StaticIPConfig.png

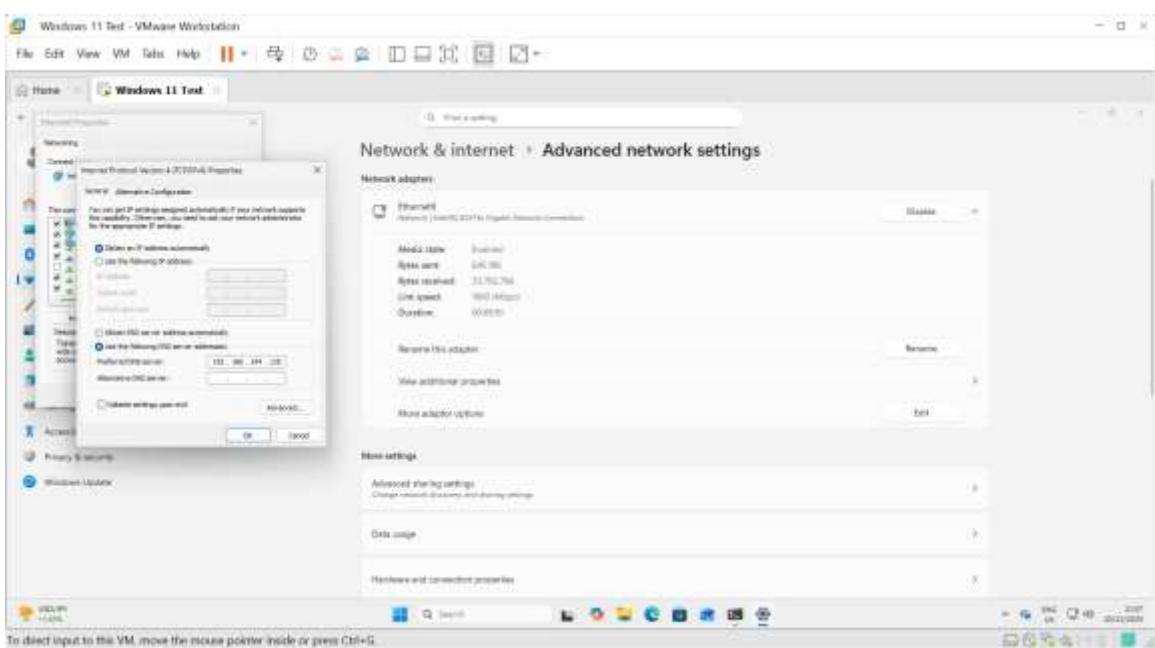


Figure 7: Screenshot evidence.

Source file: Win11DNSConfigured.png

## Scenario 1 — Account Lockout / Logon

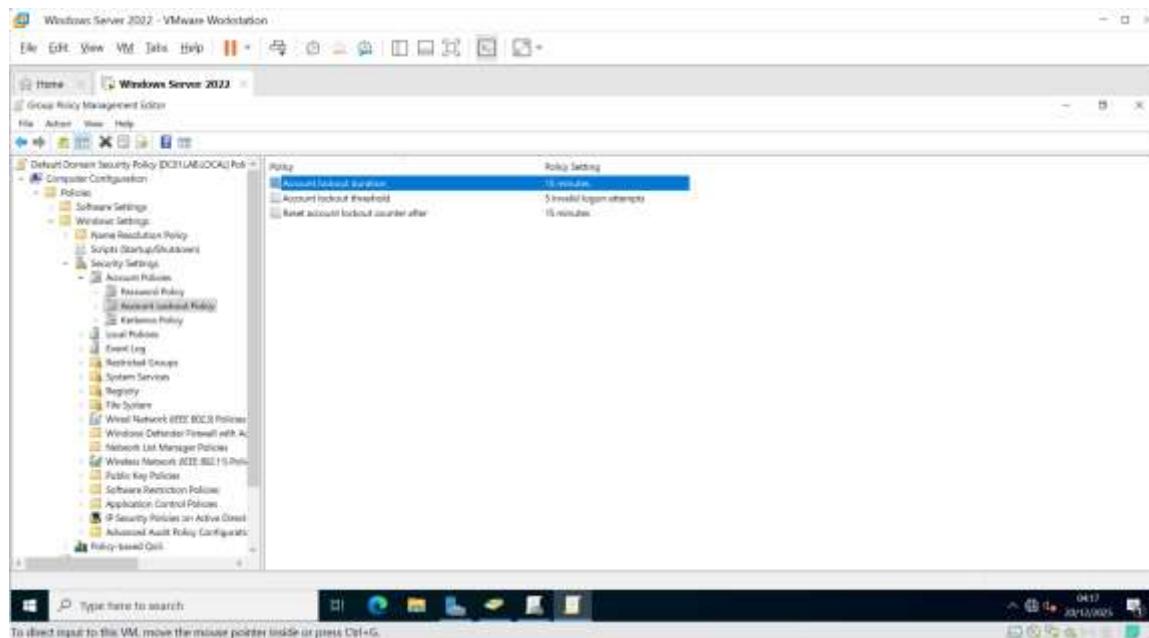


Figure 8: Account lockout policy configuration.

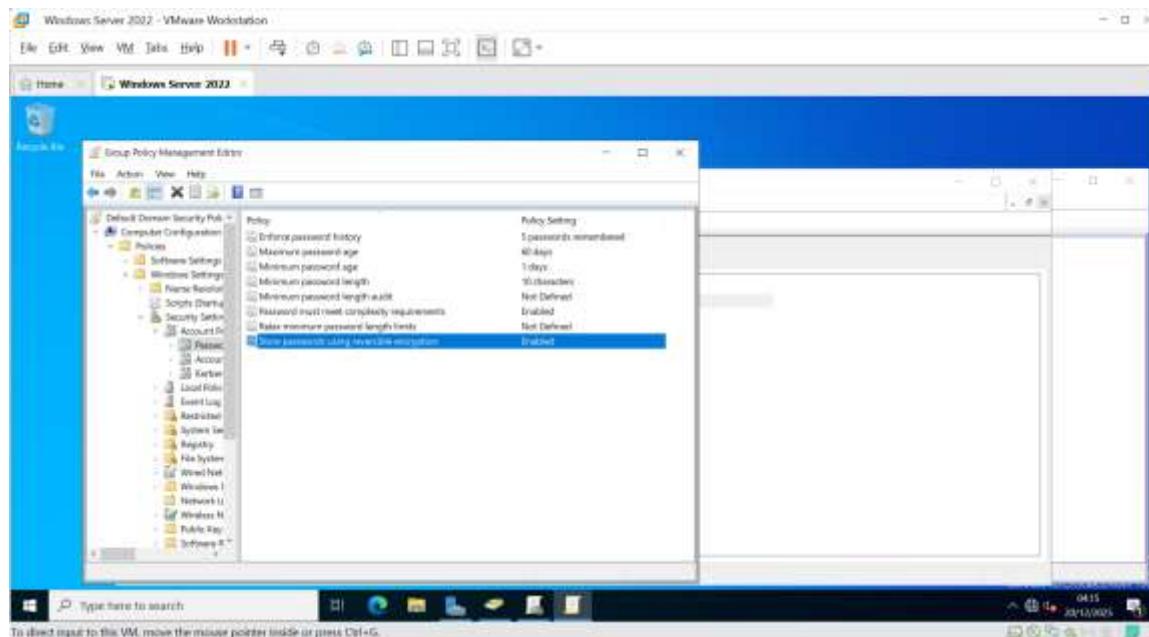


Figure 9: Screenshot evidence.

Source file: PasswordPolicyConfigured.png

## Scenario 2 — UAC / Elevation

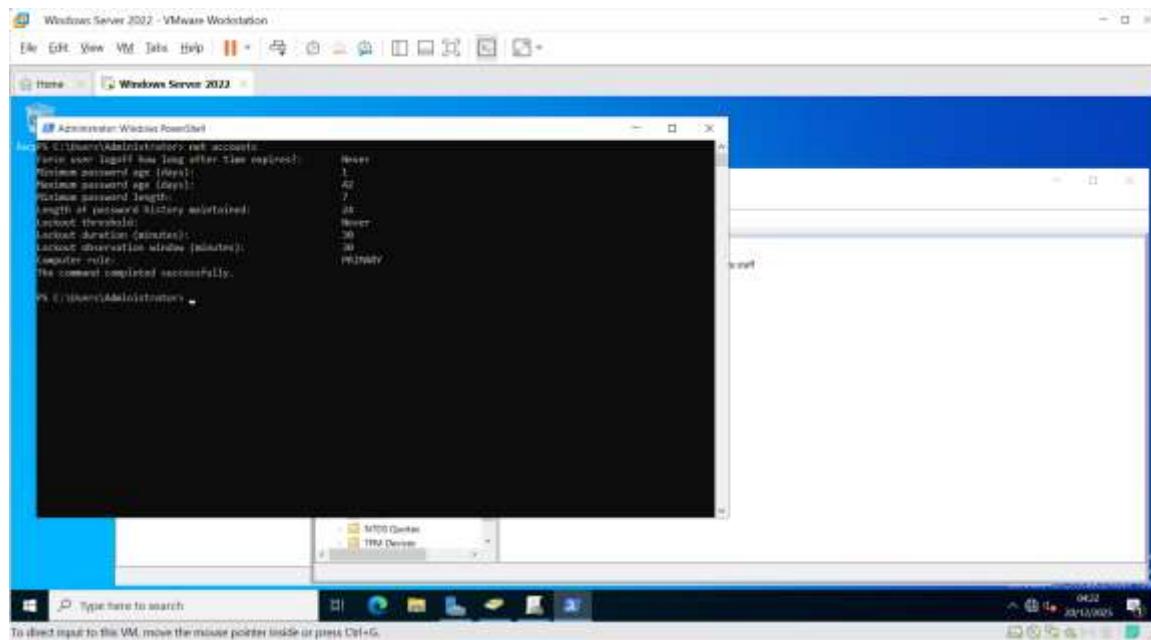


Figure 10: UAC-related policy verification.

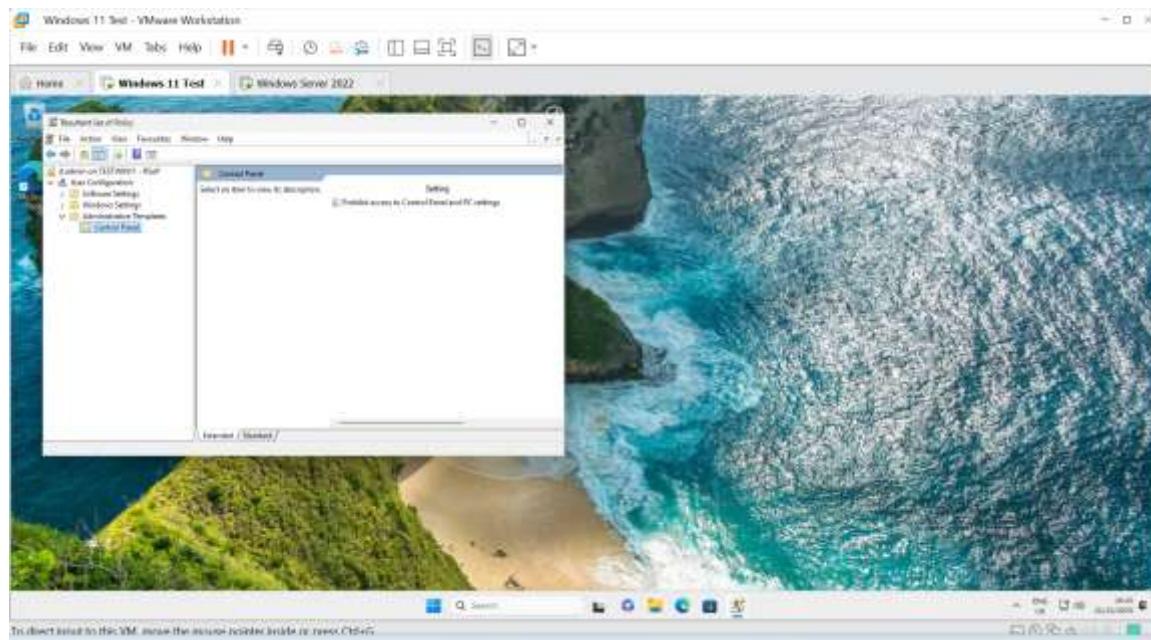


Figure 11: Screenshot evidence.

Source file: Week3\_Task3\_RSOP\_ControlPanel.png

### Scenario 3 — Scheduled Tasks / Logging

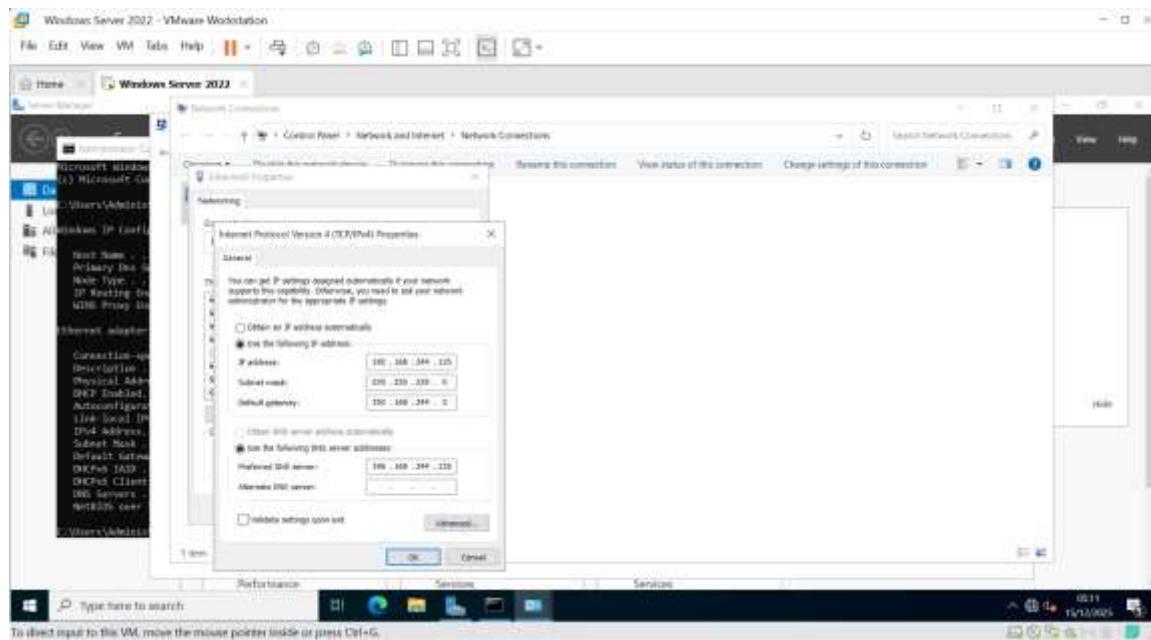


Figure 12: Task Scheduler configuration and execution context.

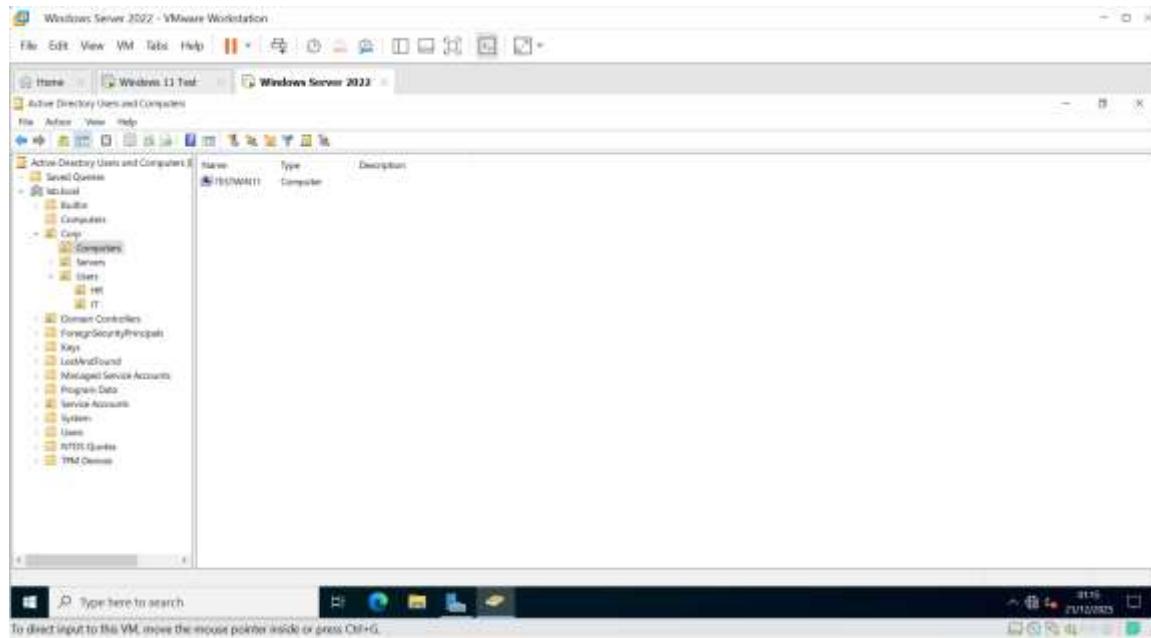


Figure 13: Screenshot evidence.

Source file: Week3\_Task2\_Computer\_In\_Correct\_OU.png

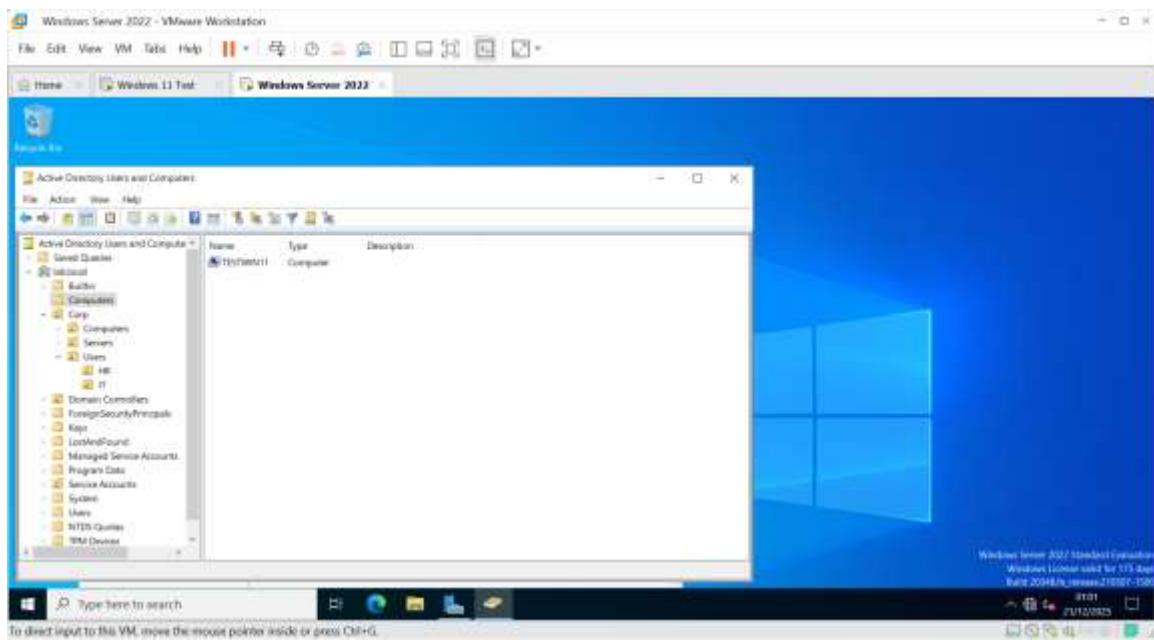


Figure 14: Screenshot evidence.

Source file: Week3\_Task2\_Computer\_In\_Default\_Container.png

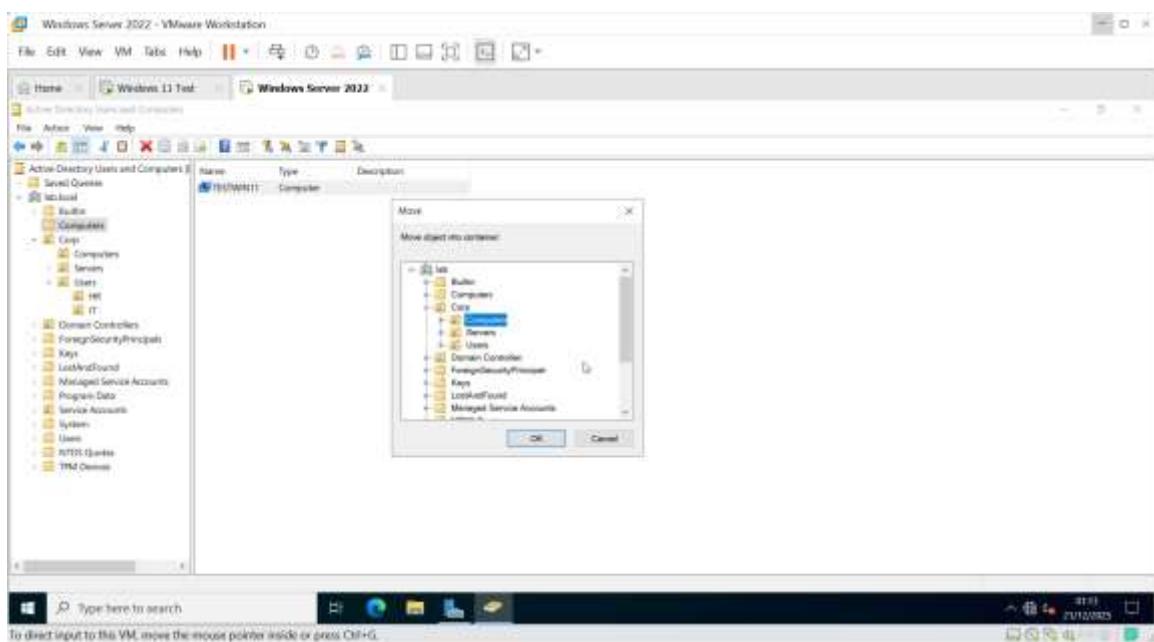


Figure 15: Screenshot evidence.

Source file: Week3\_Task2\_Computer\_Moved\_To\_Corp\_Computers.png

The screenshot shows a Windows Server 2022 desktop environment with a Command Prompt window open. The title bar of the window reads "Windows 11 Test - VMware Workstation". The Command Prompt displays the following output:

```
Windows 11 Test - VMware Workstation
File Edit View VM Tabs Help || Back Forward Stop Refresh Home Windows Server 2022

C:\Windows\system32\cmd.exe

GPO Data for LAB1\JAMESH-00-TESTM001 | Logging Mode

OS Configuration: Windows Server 2022
OS Version: 10.0.3600
Site Name: LAB
Domain Profile: N/A
Local Profile: C:\Users\JAMESH
Converted over a slow link? No

USER SETTINGS

Computer Admin (LAB1\JAMESH) | Policies: 0/0 Local
Last time Group Policy was applied: 23/12/2023 at 10:18:00
Group Policy was applied from: (K8S LAB-LOCAL)
Group Policy claim link threshold: 500 items
Domain Name: LAB
Domain Type: Windows 2008 or later

Applied Group Policy Objects:
GP - Restrict Control Panel
GP - Drive Mapping

The following GPOs were not applied because they were filtered out:
Local Group Policy
Filtering: Not Applied (Empty)

This user is a part of the following security groups:
Domain Users
Everyone
BUILTIN\Administrators
NT AUTHORITY\SYSTEM
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This organization
```

Figure 16: Screenshot evidence.

Source file: Week3\_Task3\_gpresult\_r.png

The screenshot shows a Windows 11 desktop environment with a Command Prompt window open. The title bar of the window reads "Windows 11 Test - VMware Workstation". The Command Prompt displays the following output:

```
Windows 11 Test - VMware Workstation
File Edit View VM Tabs Help || Back Forward Stop Refresh Home Windows 11 Test - VMware Workstation

C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.22621]
Copyright Microsoft Corporation. All rights reserved.

C:\Users\JAMESH\gpupdate /force
Updating policy...

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

C:\Users\JAMESH
```

Figure 17: Screenshot evidence.

Source file: Week3\_Task3\_gpupdate\_force.png

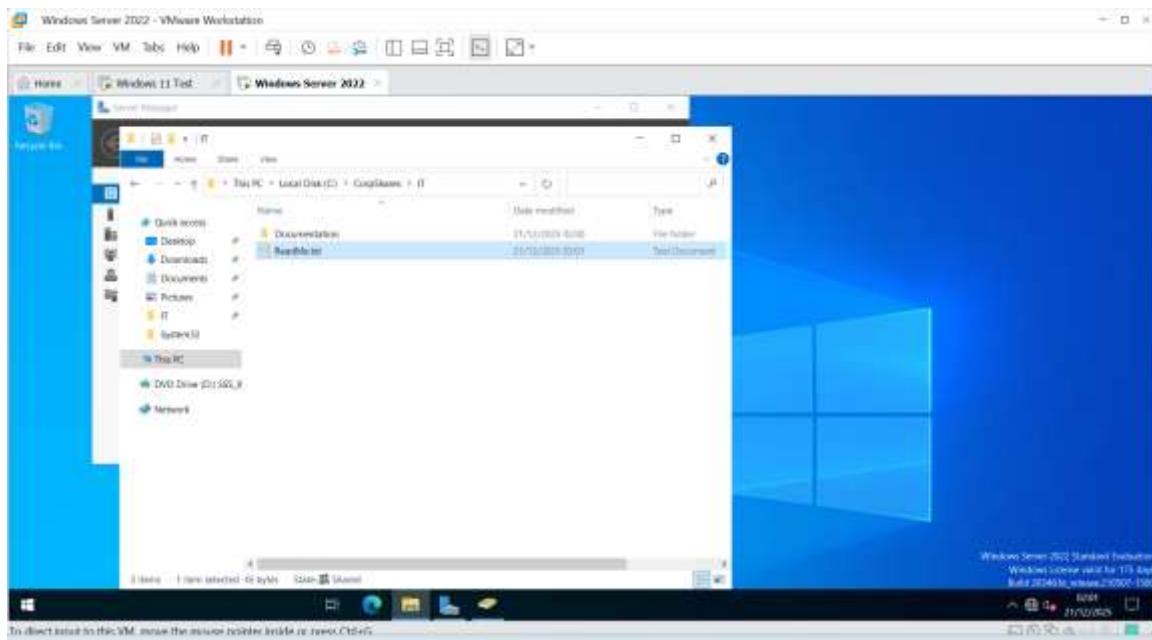


Figure 18: Screenshot evidence.

Source file: Week3\_Task3\_IT\_Share\_Content\_Created.png

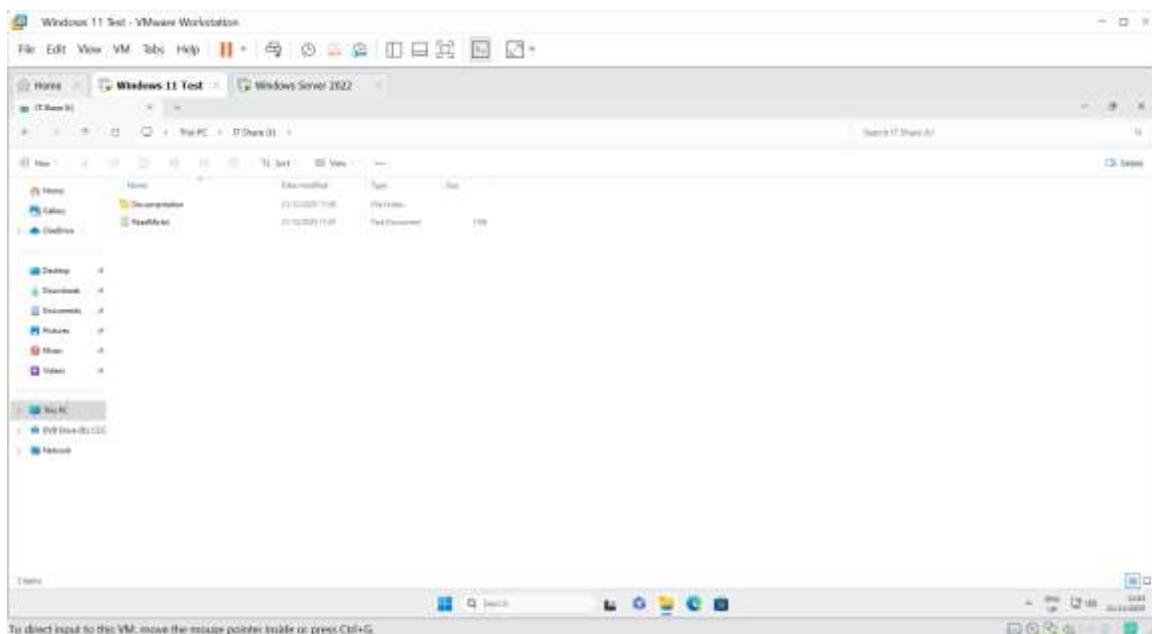


Figure 19: Screenshot evidence.

Source file: Week3\_Task3\_IT\_Share\_Content\_Visible.png

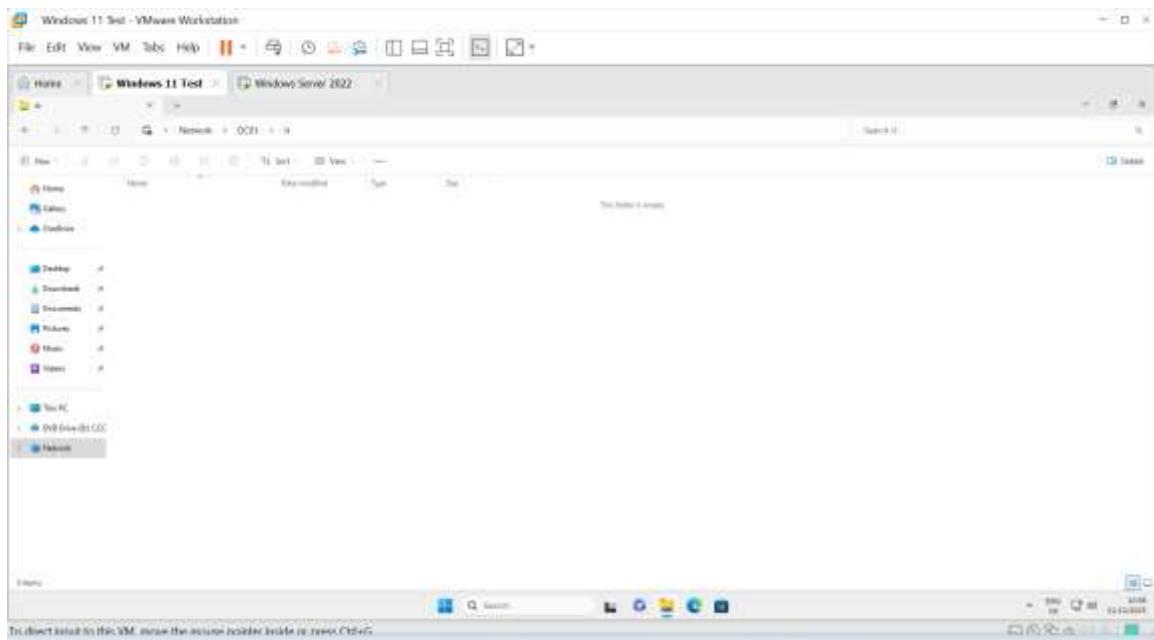


Figure 20: Screenshot evidence.

Source file: Week3\_Task3\_IT\_Share\_Empty\_Confirmed.png

#### Scenario 4 — Group Policy / Active Directory

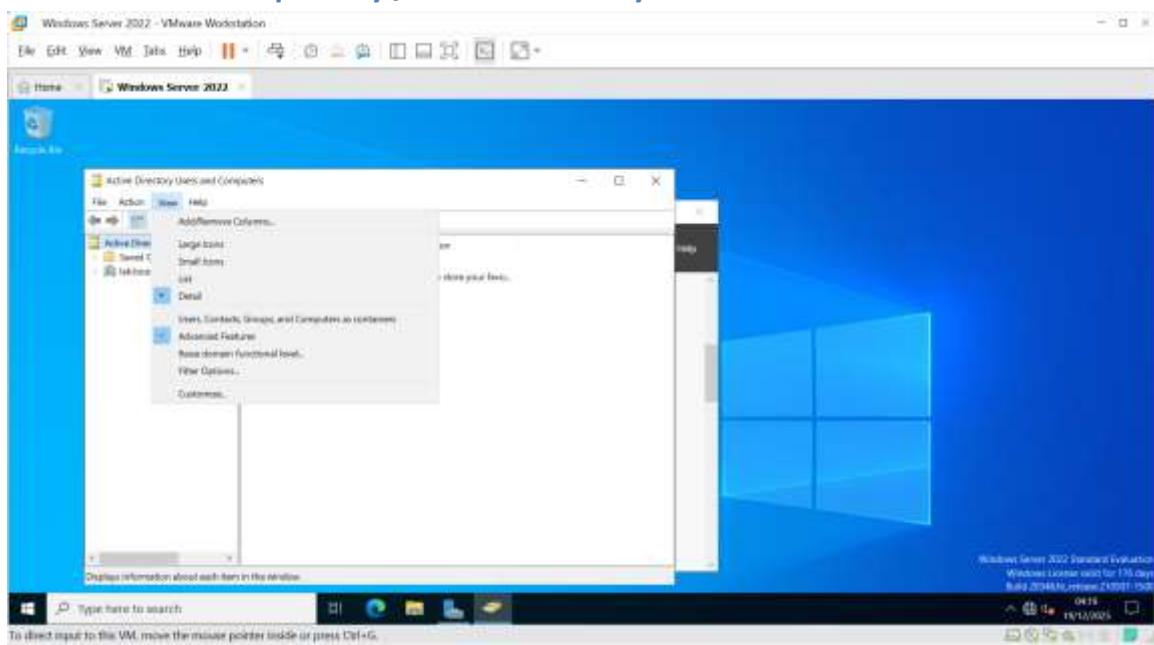


Figure 21: Active Directory Users and Computers with Advanced Features enabled.

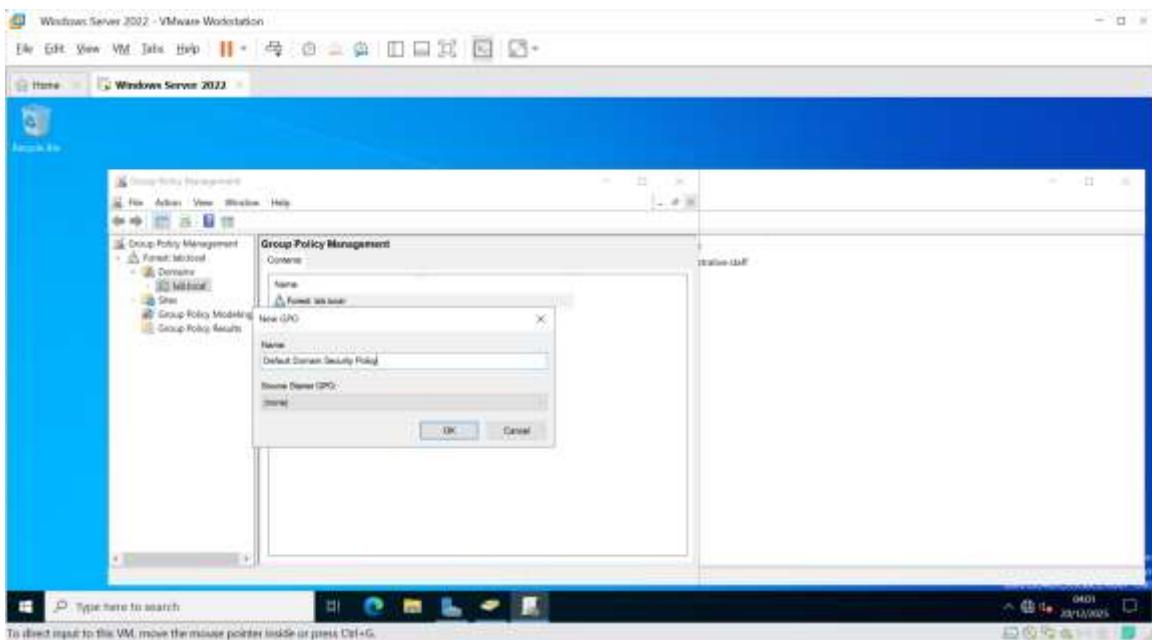


Figure 22: Screenshot evidence.

Source file: GPOCreated1.png

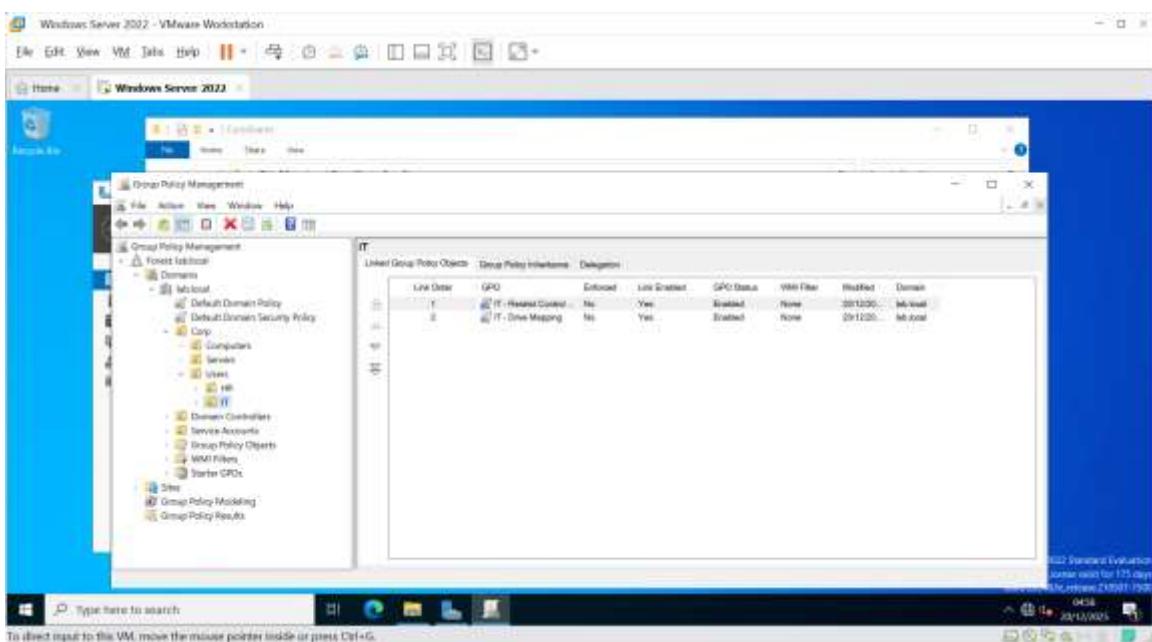


Figure 23: Screenshot evidence.

Source file: GPOCreatedDriveMapping.png

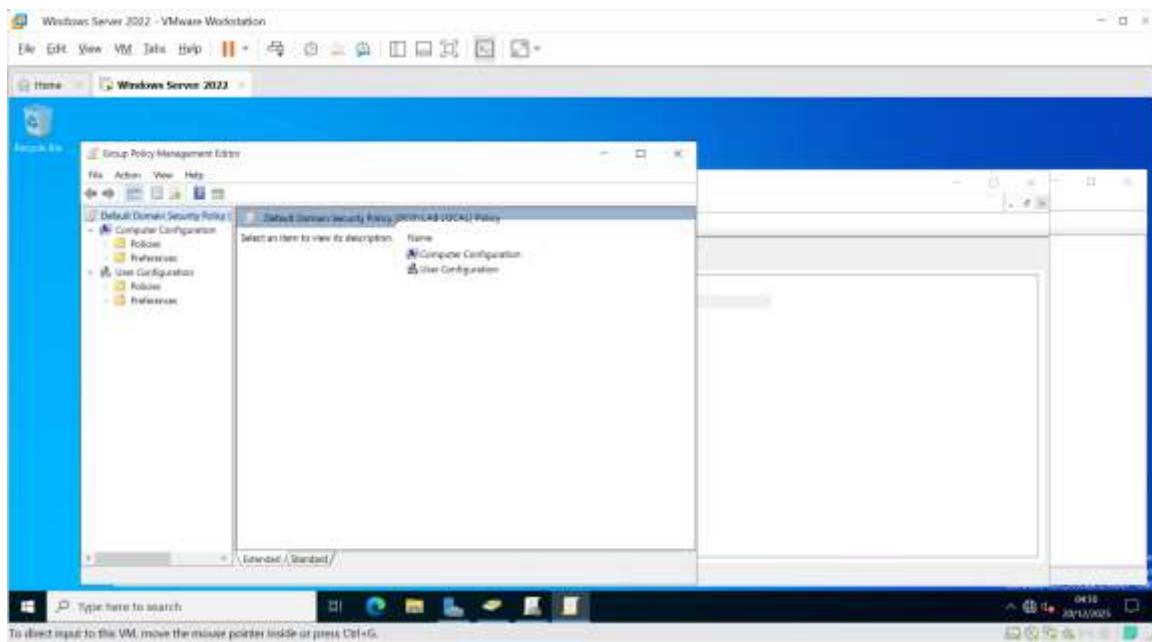


Figure 24: Screenshot evidence.

Source file: GPOEditorOpened.png

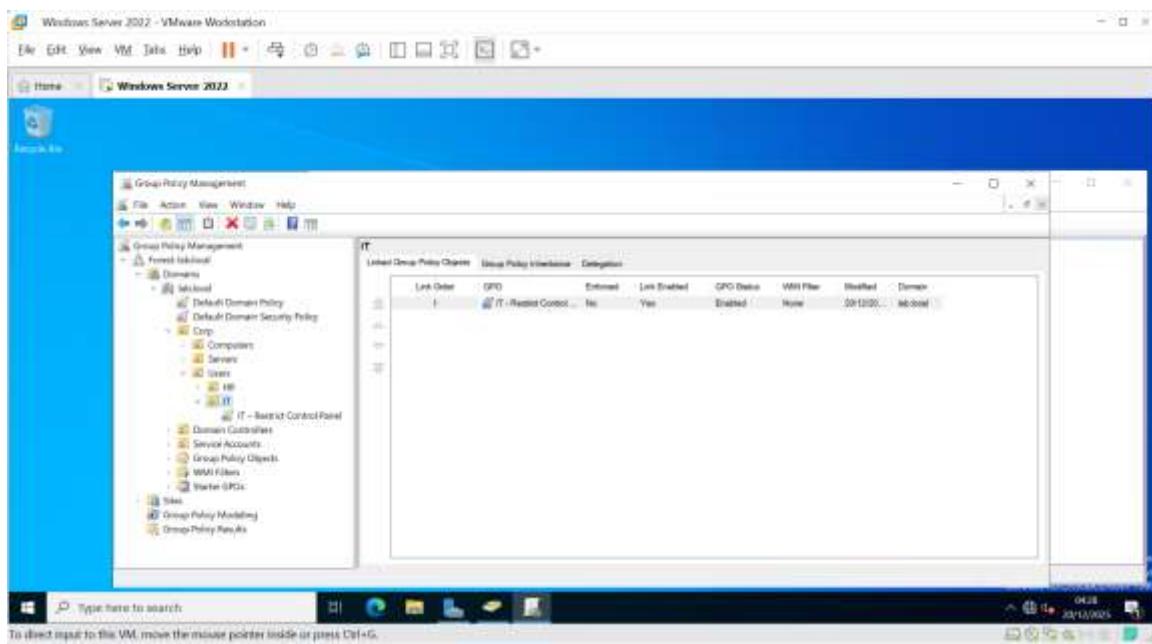


Figure 25: Screenshot evidence.

Source file: GPOLinkedITOU.png

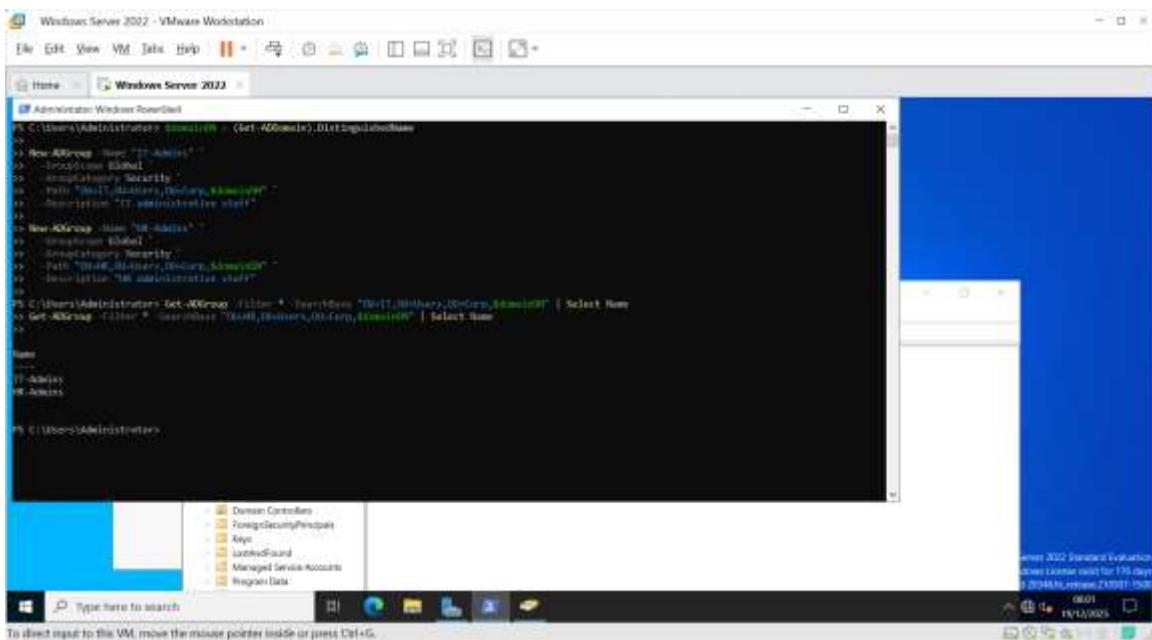


Figure 26: Screenshot evidence.

Source file: GroupsCreated.png

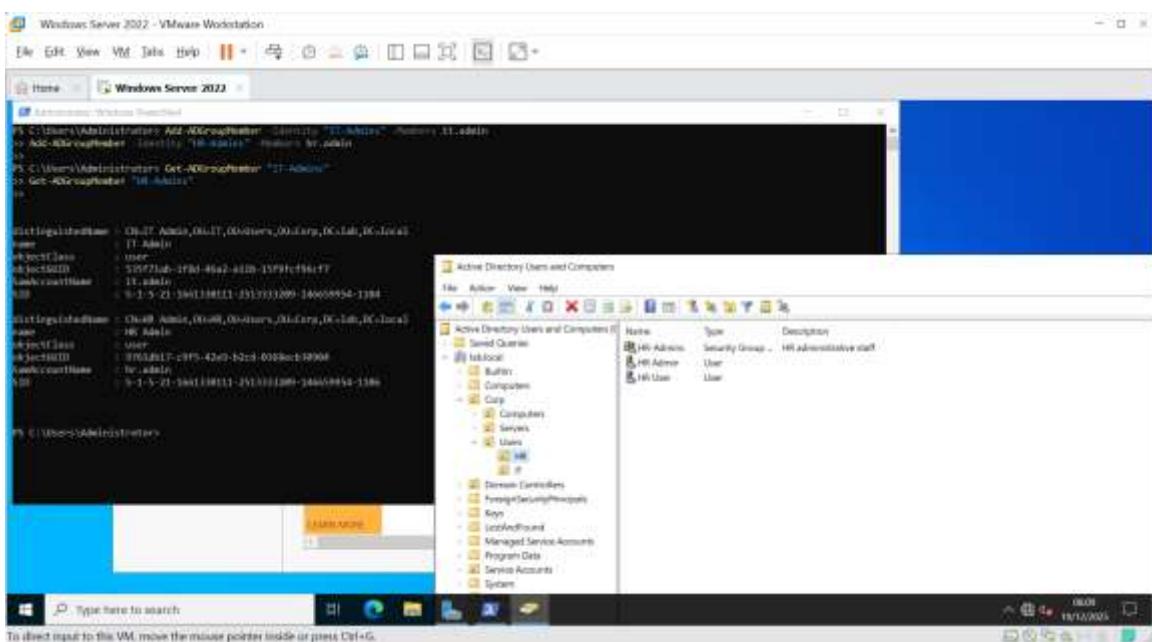


Figure 27: Screenshot evidence.

Source file: HRAdminsGroup.png

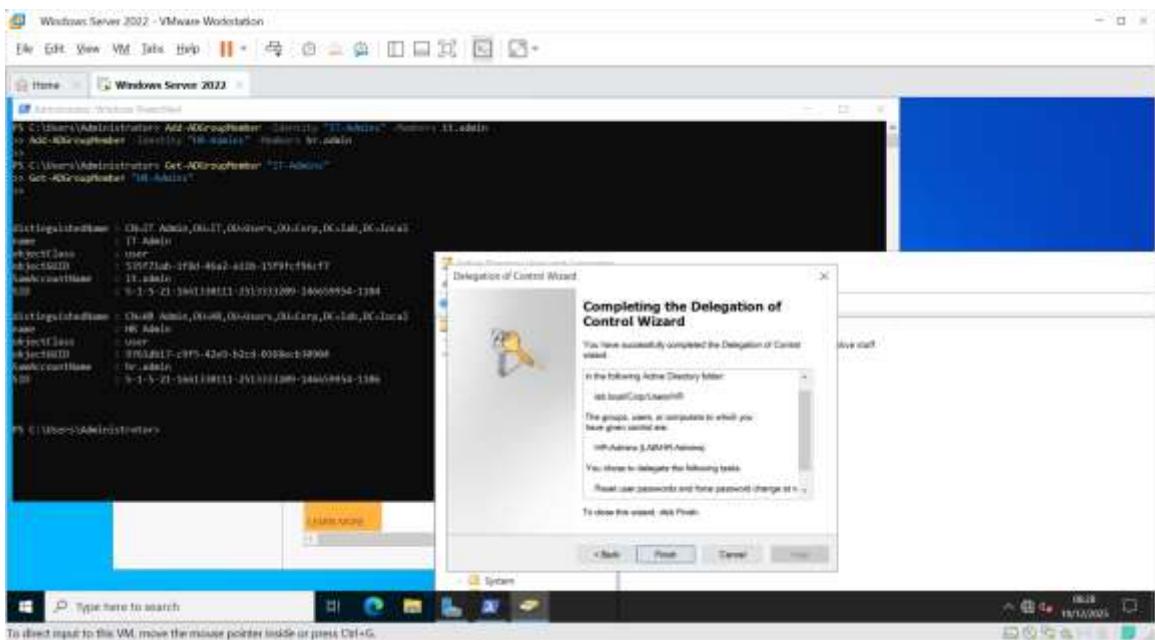


Figure 28: Screenshot evidence.

Source file: HRDelegation.png

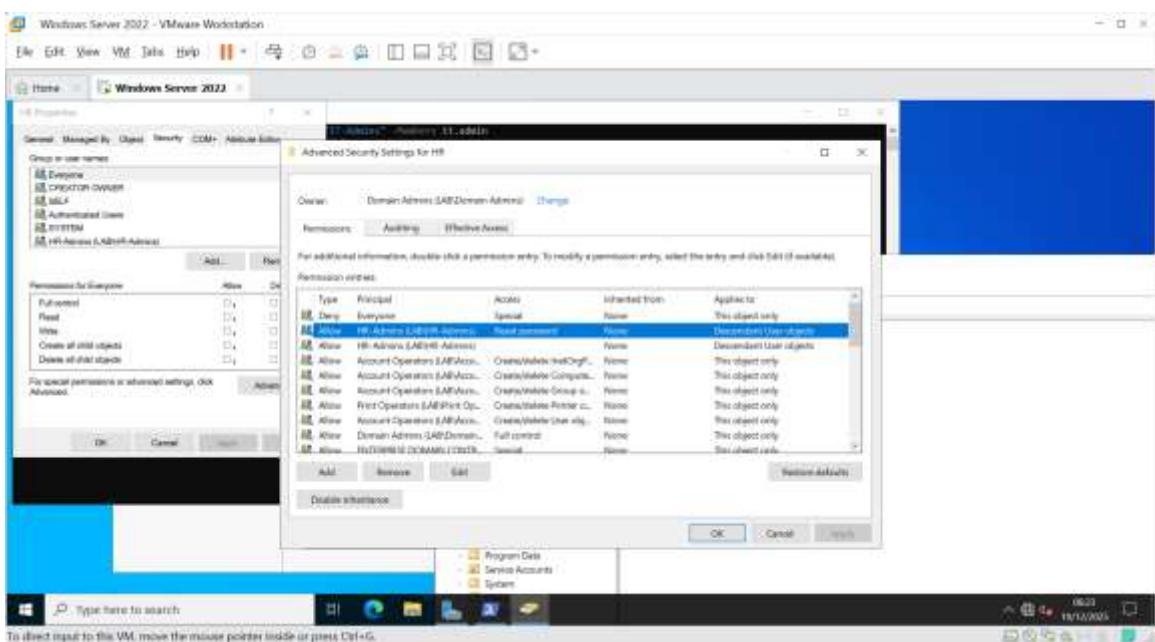


Figure 29: Screenshot evidence.

Source file: HRDelegationACL.png

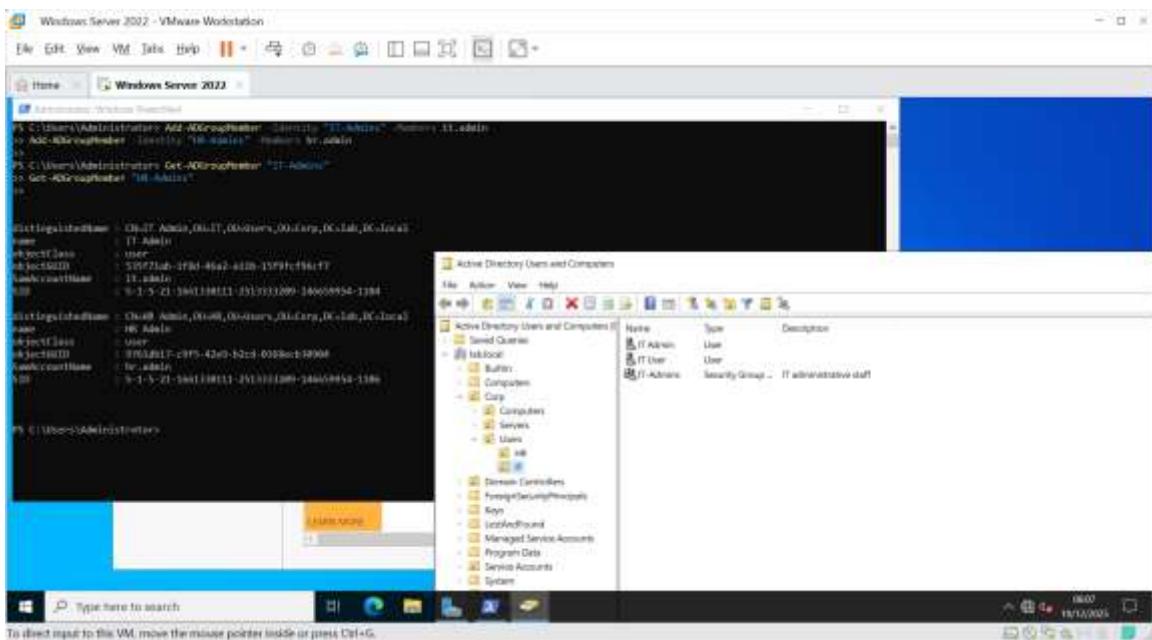


Figure 30: Screenshot evidence.

Source file: ITAdminsGroup.png

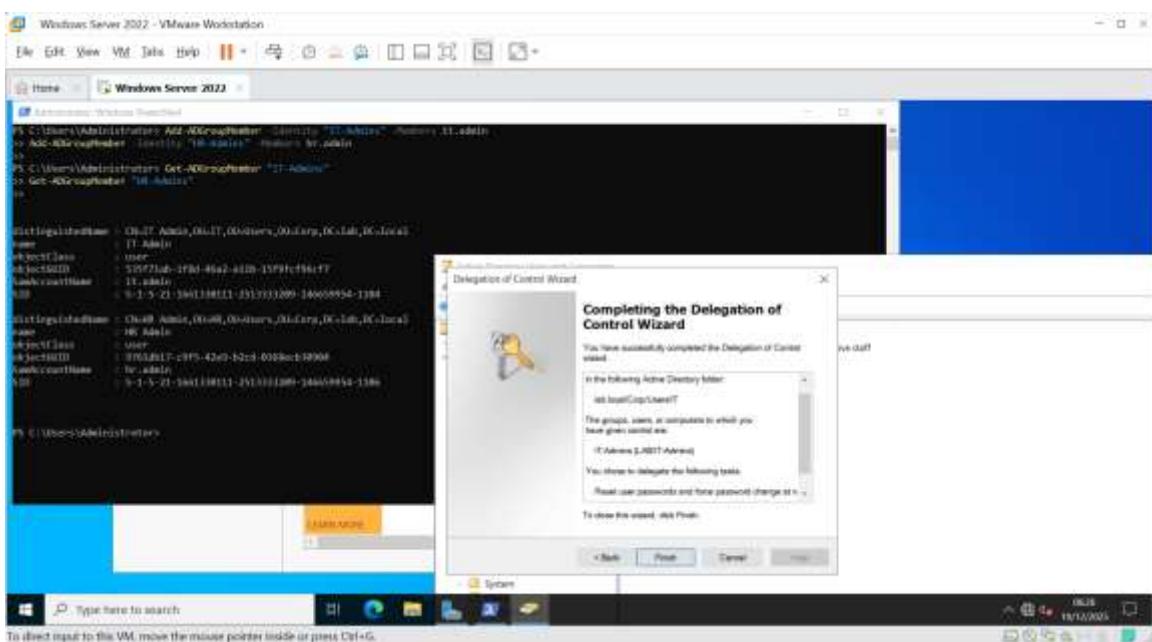


Figure 31: Screenshot evidence.

Source file: ITDelegation.png

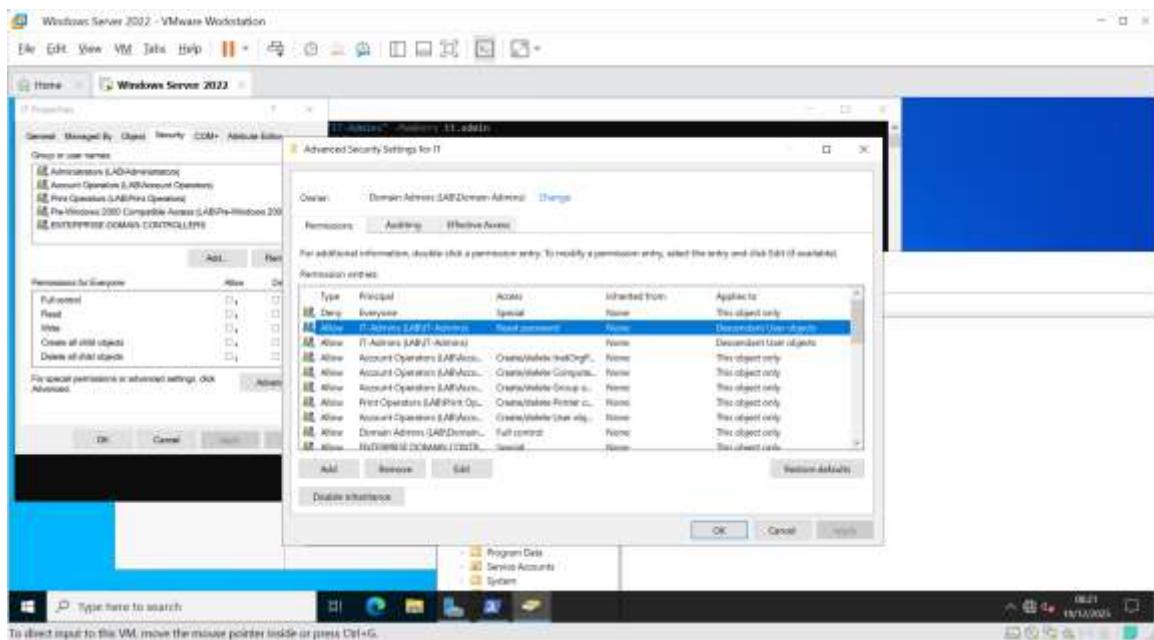


Figure 32: Screenshot evidence.

Source file: ITDelegationACL.png

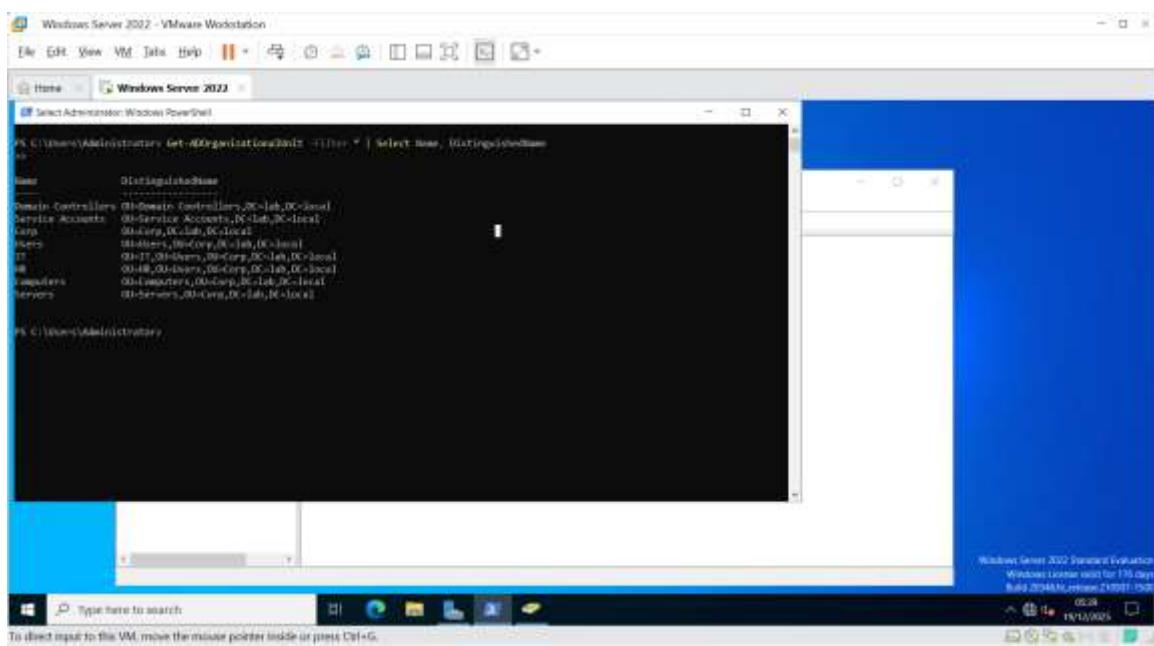


Figure 33: Screenshot evidence.

Source file: OUStructureConfirmed.png

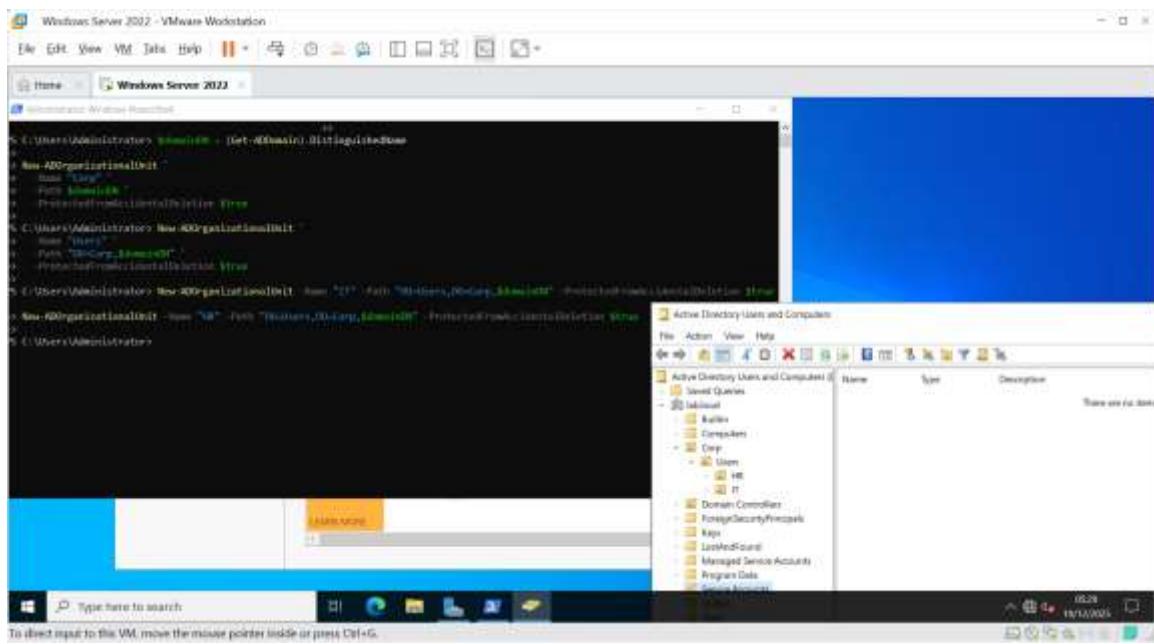


Figure 34: Screenshot evidence.

Source file: OUStructureCorrect.png

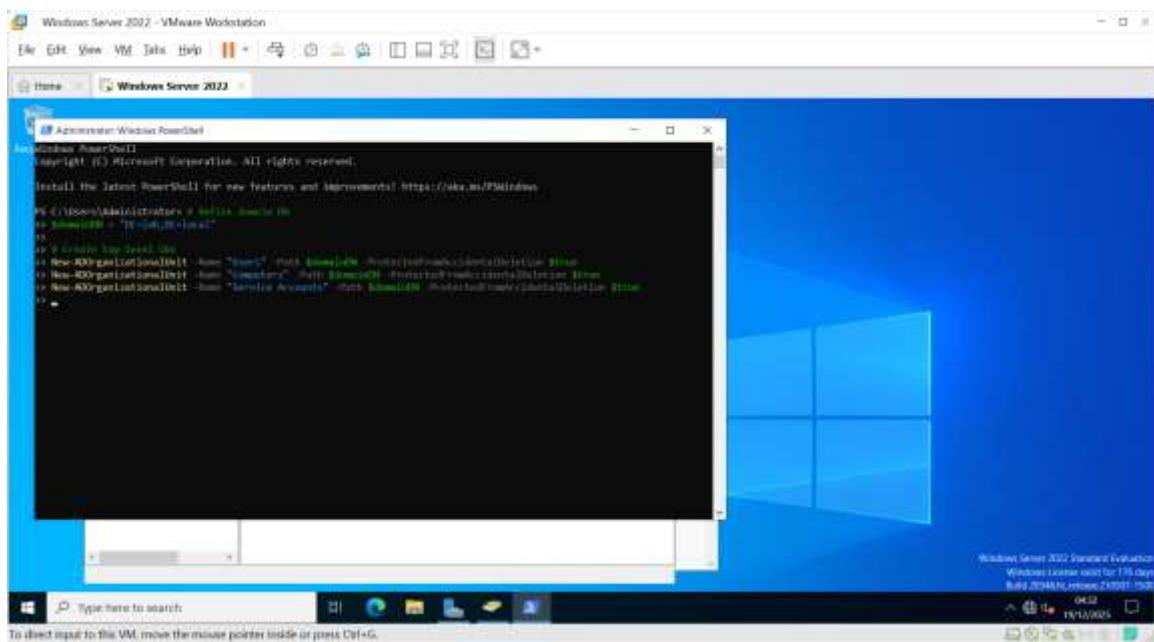


Figure 35: Screenshot evidence.

Source file: PowerShellScriptCreateTopLevelOUs.png

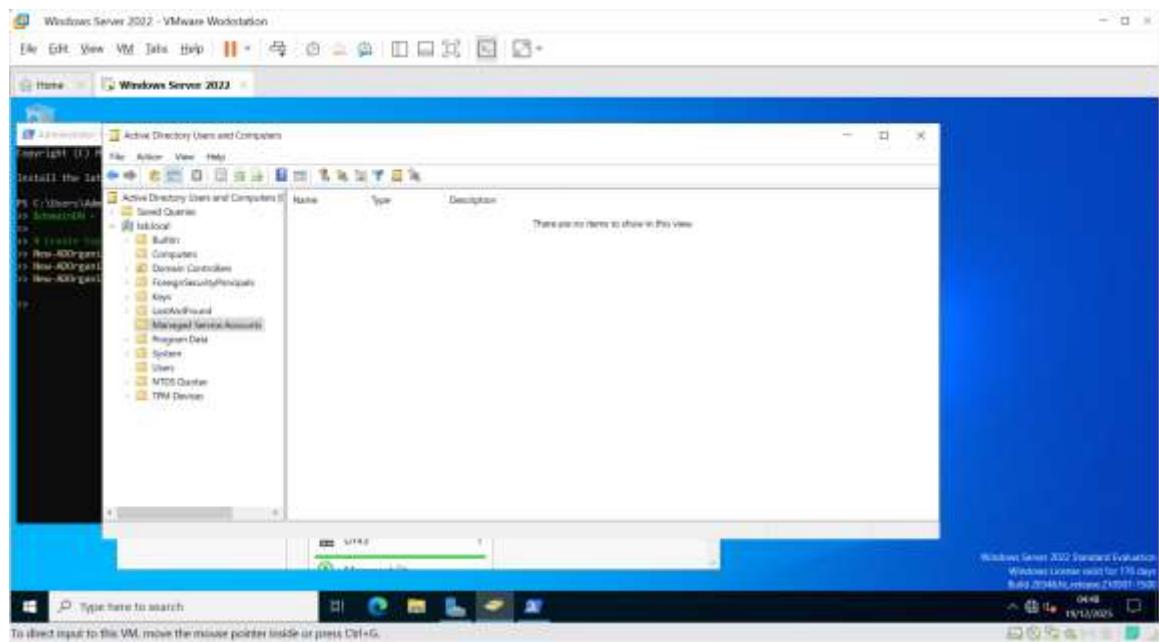


Figure 36: Screenshot evidence.

Source file: TopLevelOUs.png

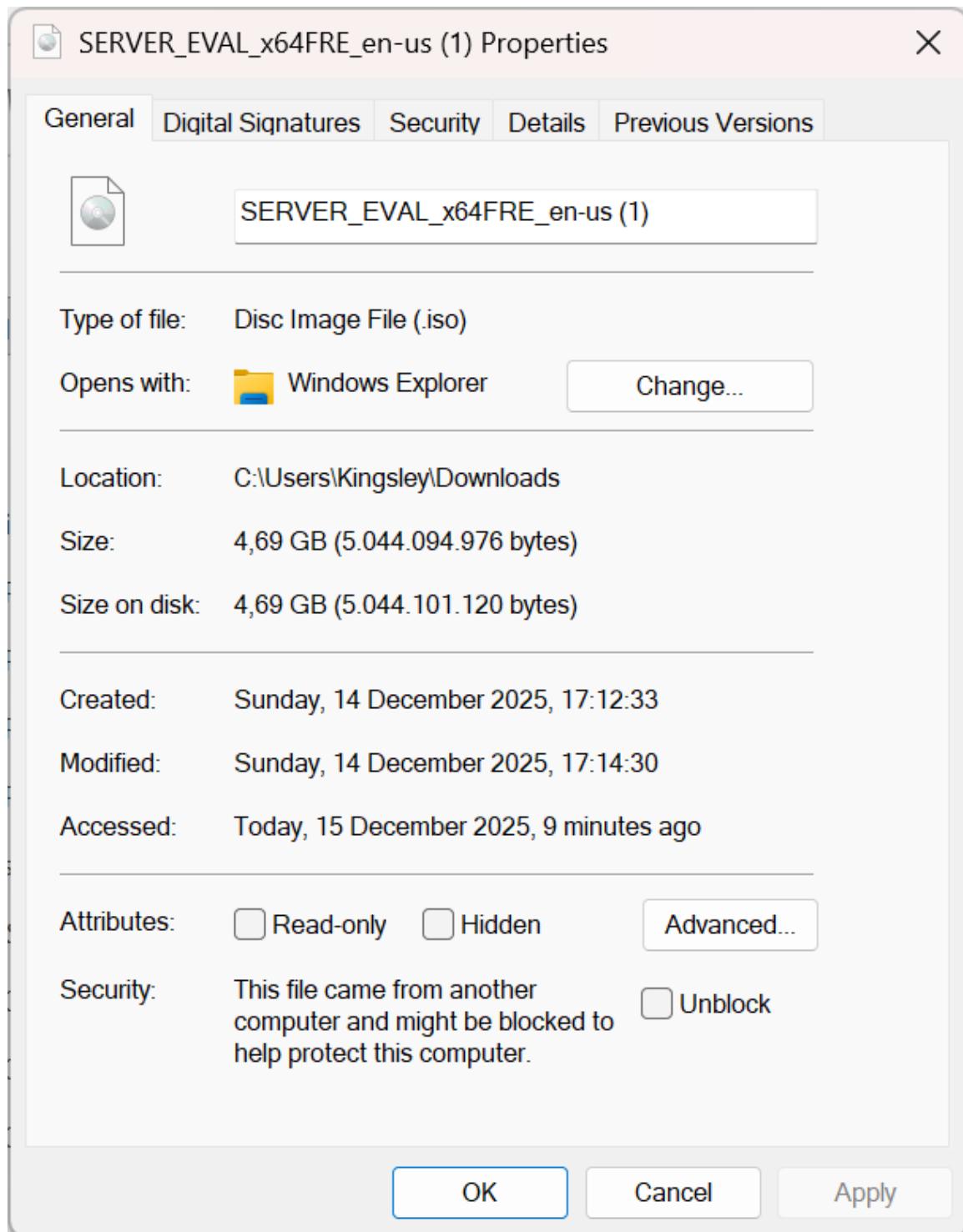


Figure 37: Screenshot evidence.

Source file: WindowsSeverisoUnblock.png

## Scenario 5 — Drive Mapping / File Access

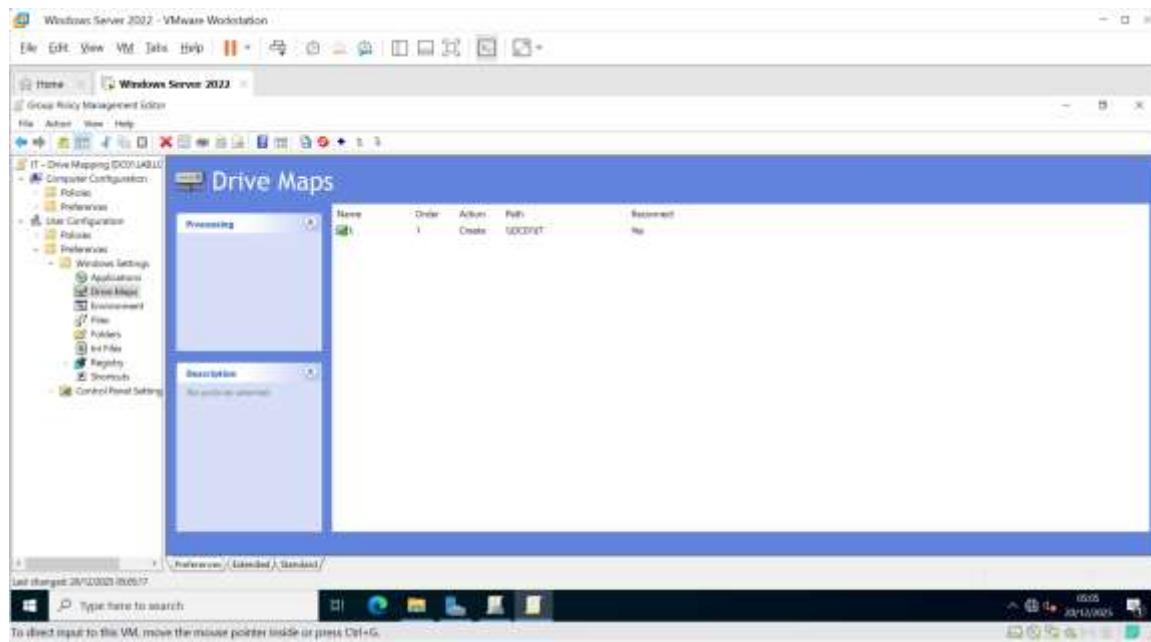


Figure 38: Group Policy drive mapping configuration.

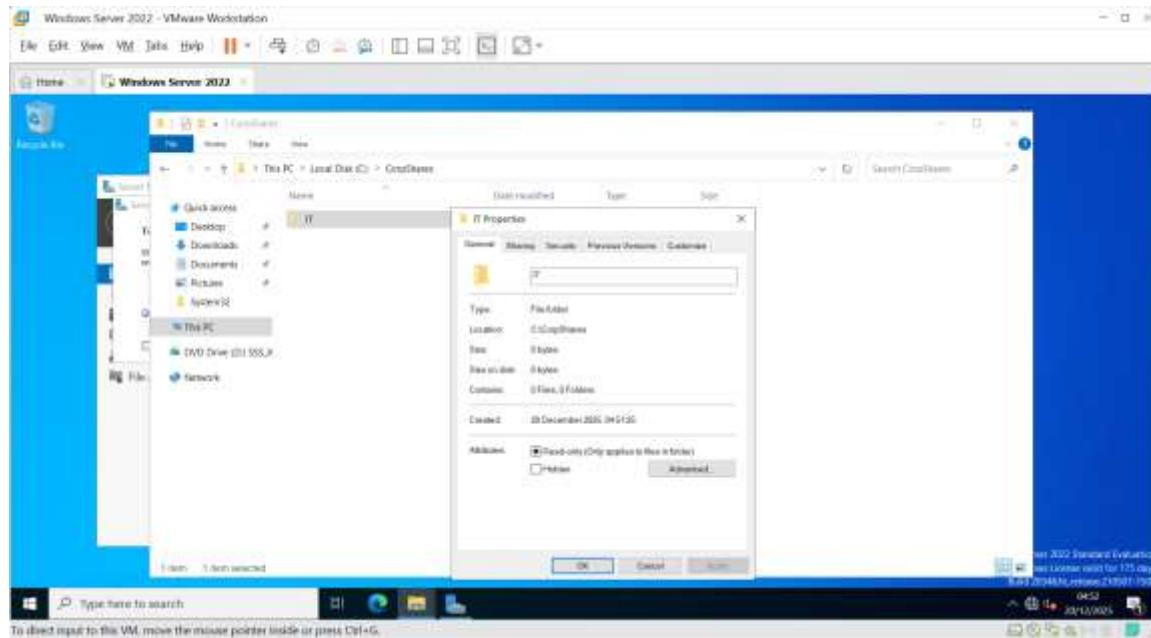


Figure 39: Screenshot evidence.

Source file: ShareFolderCreated.png

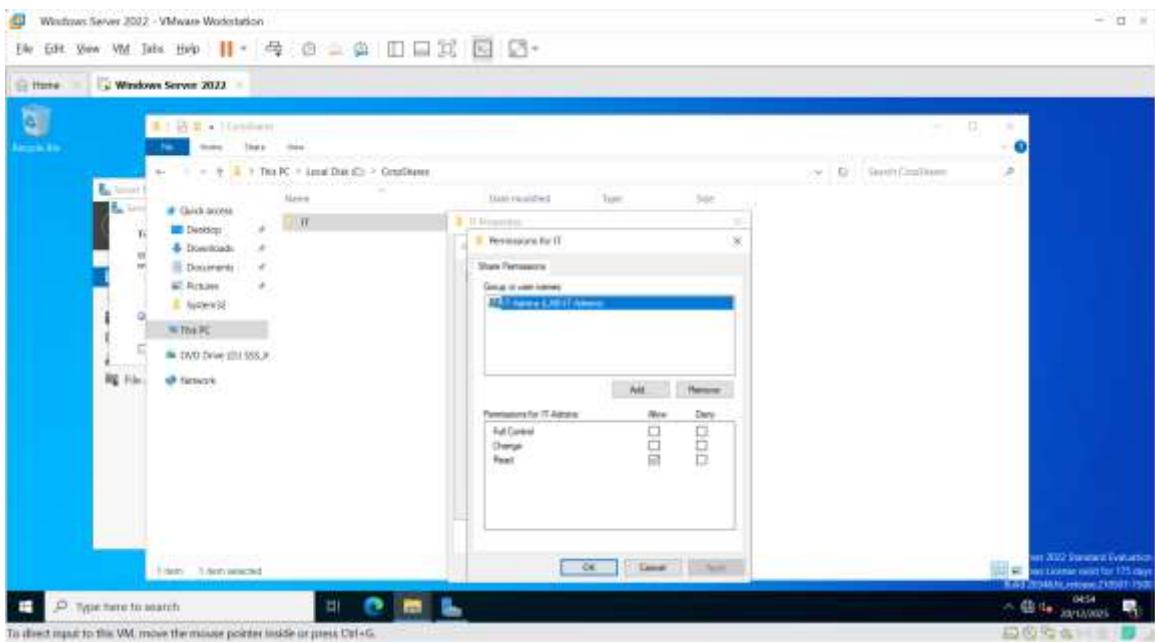


Figure 40: Screenshot evidence.

Source file: SharePermissions.png

## Additional Supporting Evidence

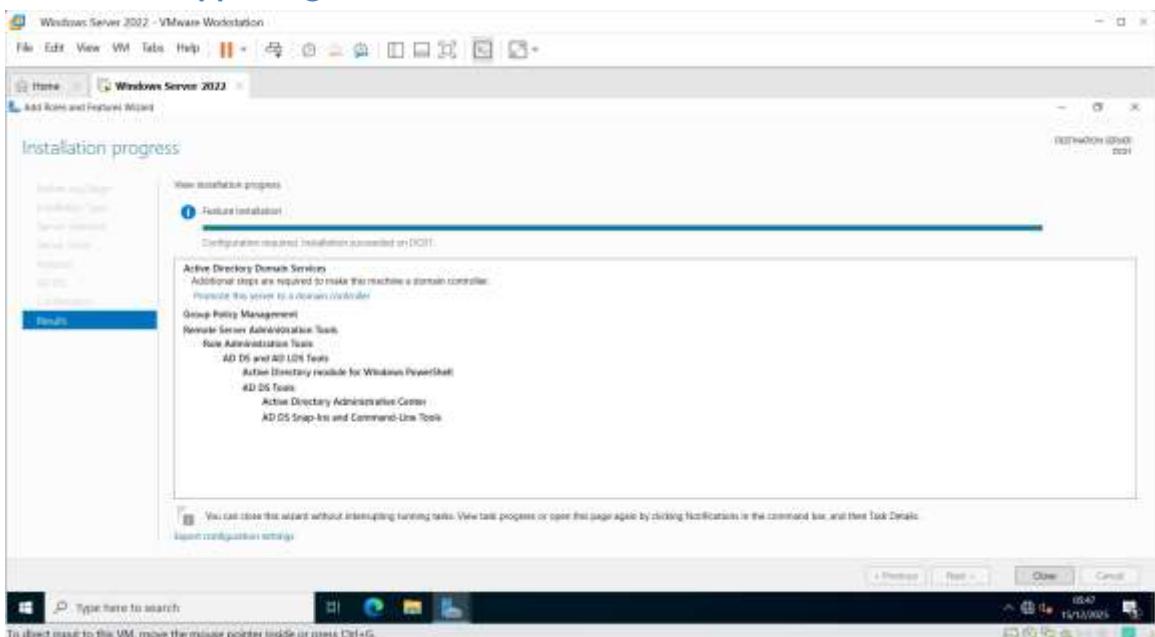


Figure 41: Screenshot evidence.

Source file: ADDSRoleInstalled.png

A screenshot of a Windows Server 2022 PowerShell window titled "Administrator: Windows PowerShell". The command entered is:

```
PS C:\Windows\Temp\WindowsPowerShell\WindowsPowerShell\v1.0\> $newUser = New-ADUser -Name "TestUser" -GivenName "Test" -SurName "User" -Path "OU=Test,OU=Users,DC=corp,DC=lab" -Enabled $true -AccountPassword (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force)
```

The output shows the creation of a new user account named "TestUser".

Figure 42: Screenshot evidence.

Source file: ADUsersCreatedPowerShell.png

A screenshot of a Windows Server 2022 PowerShell window titled "Administrator: Windows PowerShell". The command entered is:

```
PS C:\Windows\Temp\WindowsPowerShell\WindowsPowerShell\v1.0\> $newUser = Get-ADUser "TestUser" -Properties DistinguishedName | Select-Object -ExpandProperty DistinguishedName
```

The output shows the distinguished name of the newly created user account.

Figure 43: Screenshot evidence.

Source file: ADUsersVerifiedDN.png

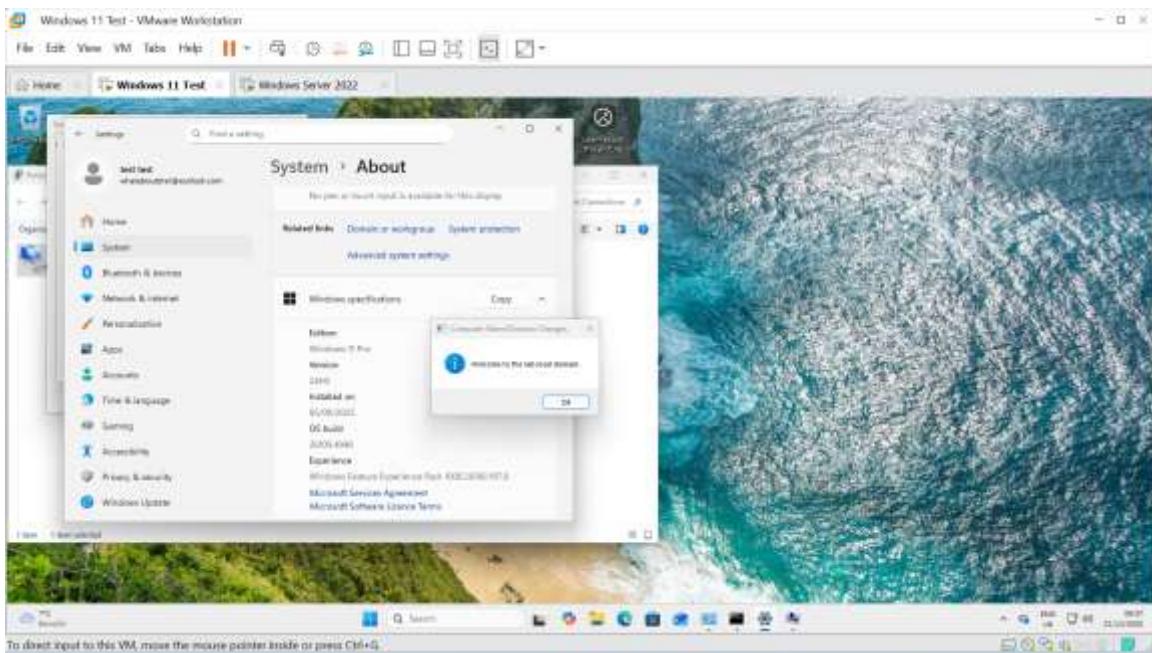


Figure 44: Screenshot evidence.

Source file: DomainJoinSuccess.png

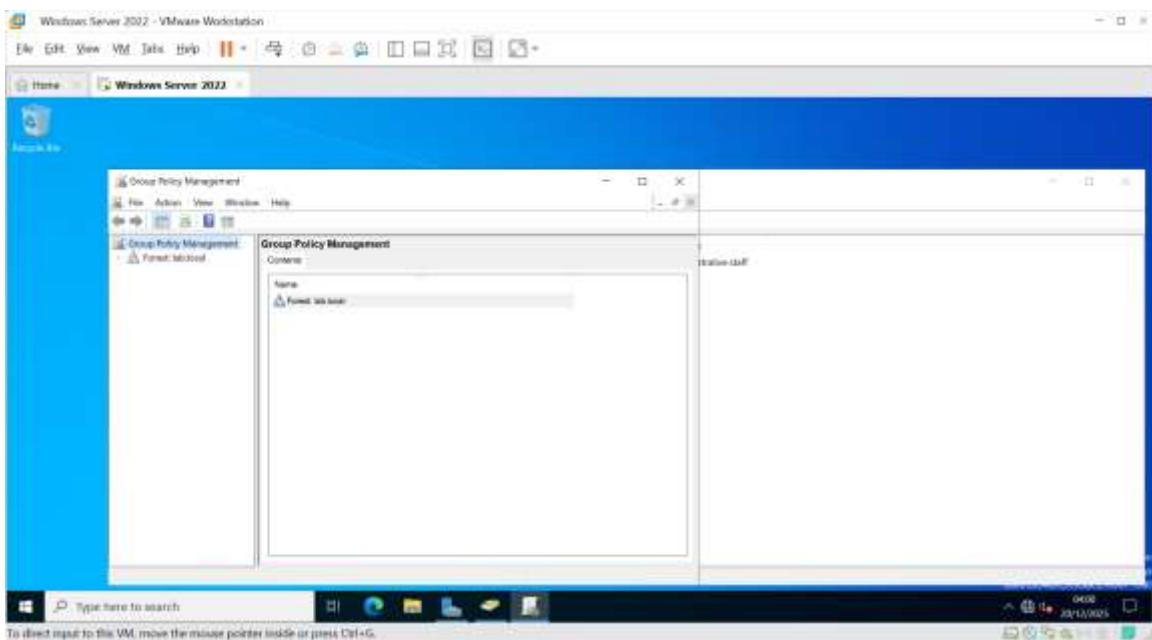


Figure 45: Screenshot evidence.

Source file: GPMCOpened.png

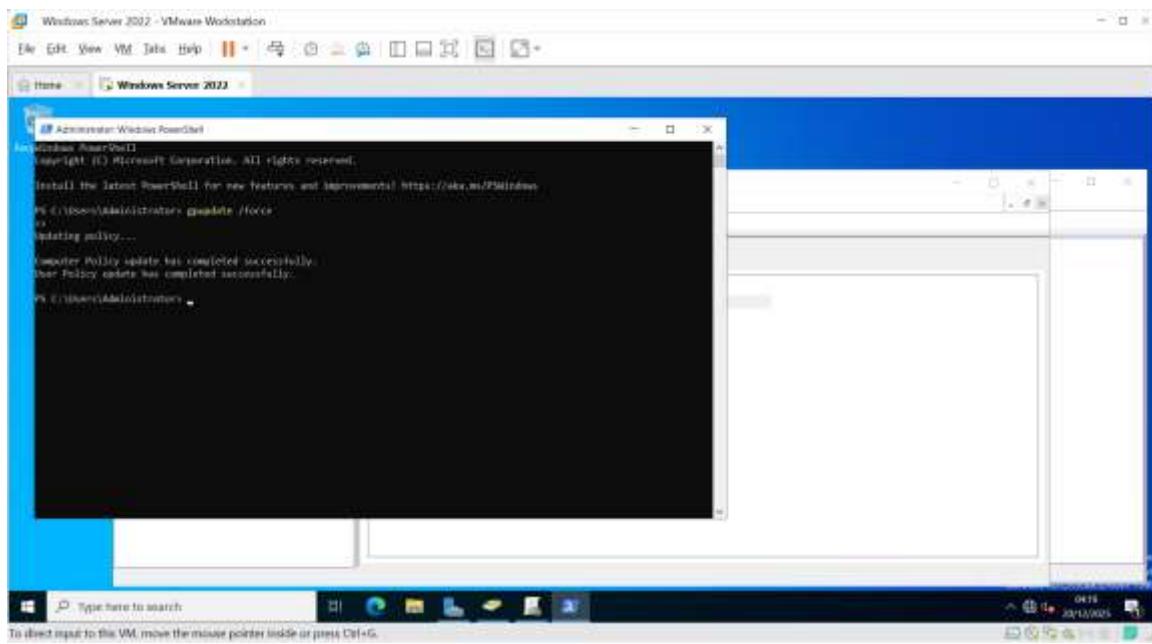


Figure 46: Screenshot evidence.

Source file: gpupdateforce.png

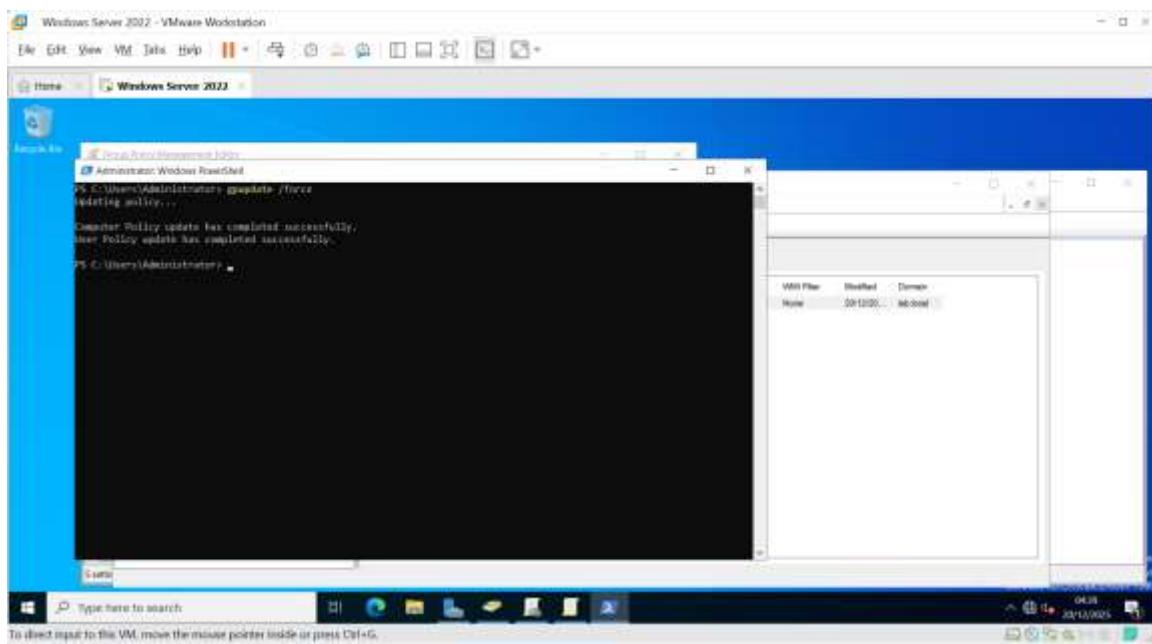


Figure 47: Screenshot evidence.

Source file: gpupdateforce1.png

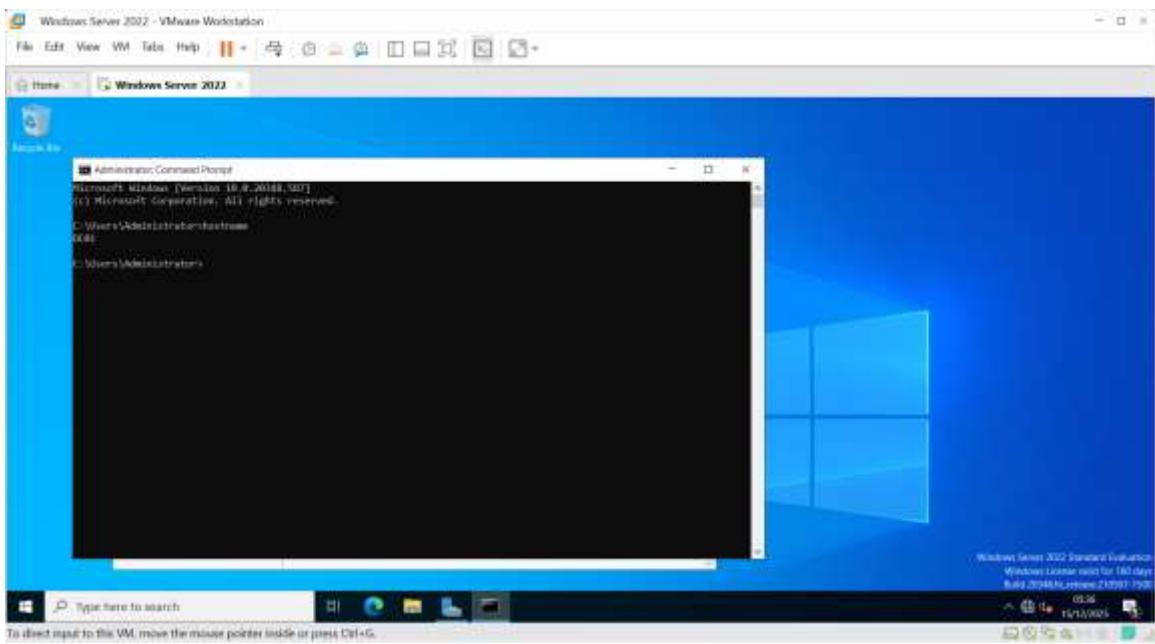


Figure 48: Screenshot evidence.

Source file: ServerRenamed.png

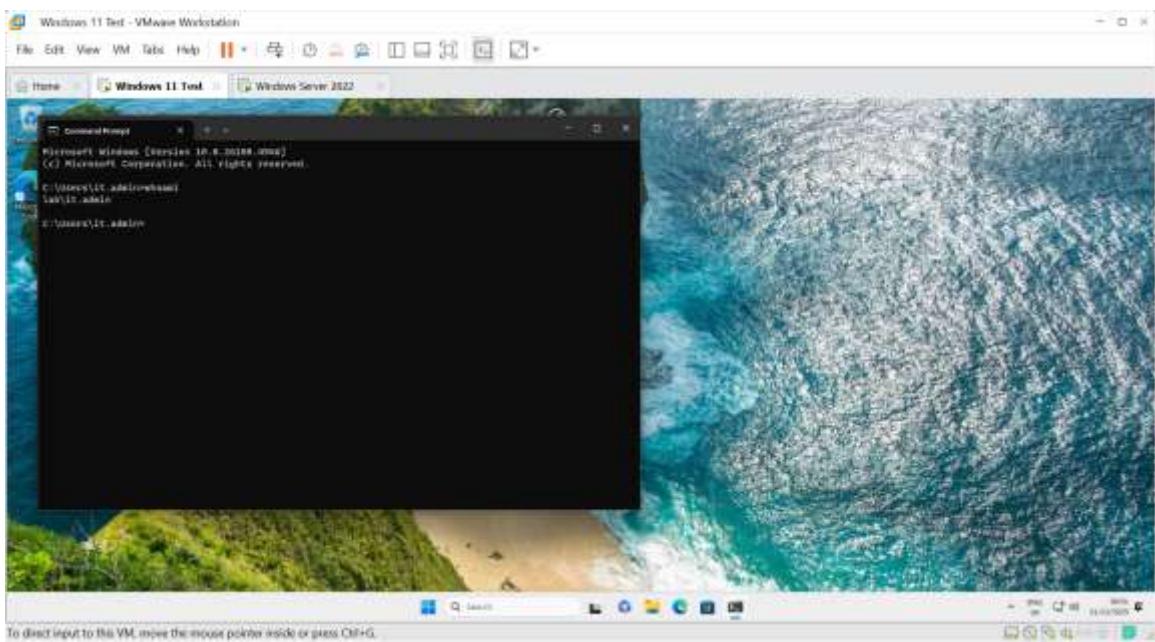


Figure 49: Screenshot evidence.

Source file: whoamiVerified.png

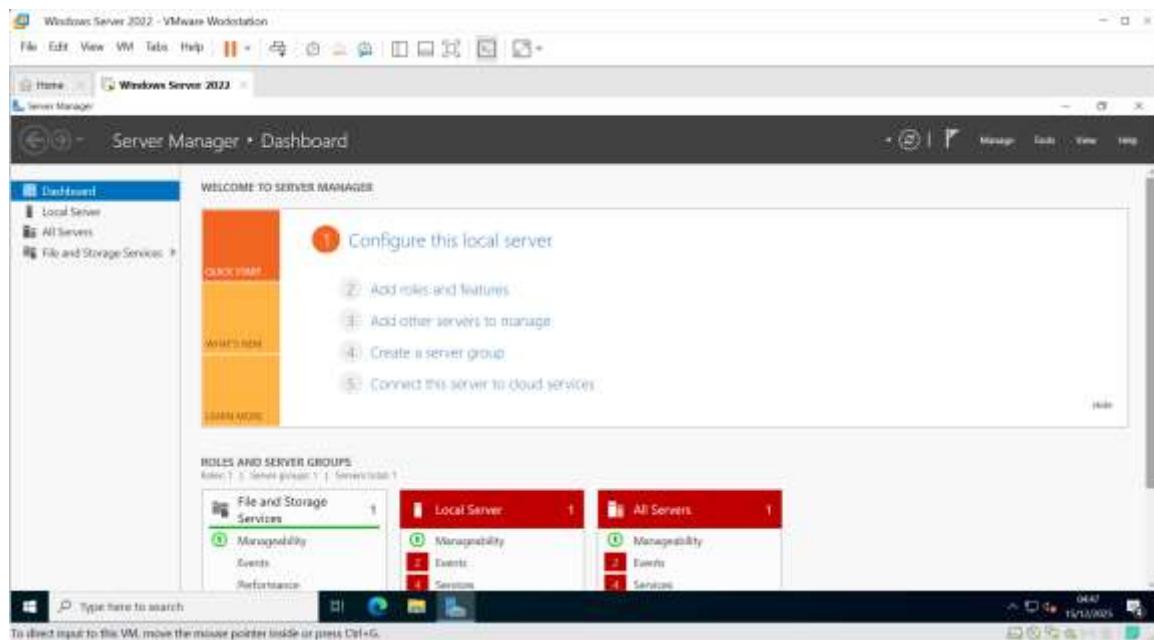


Figure 50: Screenshot evidence.

Source file: WindowsServer2022Installed.png

Tools Used:

- Event Viewer
- Task Scheduler
- Active Directory Users and Computers (ADUC)
- Group Policy Management Console (GPMC)
- gpupdate / gpresult / RSOP
- PowerShell (basic administration)
- VMware Workstation