

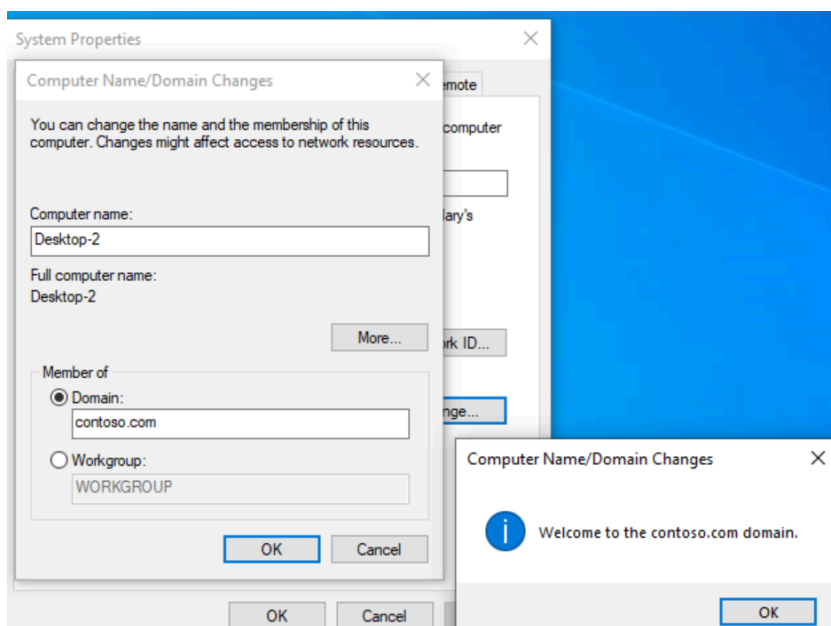
IT Onboarding Runbook (Windows AD)

Introduction

This runbook documents the standardized process for onboarding a new hire's workstation into a Windows Active Directory environment. It covers domain integration, account setup, departmental resource configuration, Group Policy application, and verification tasks

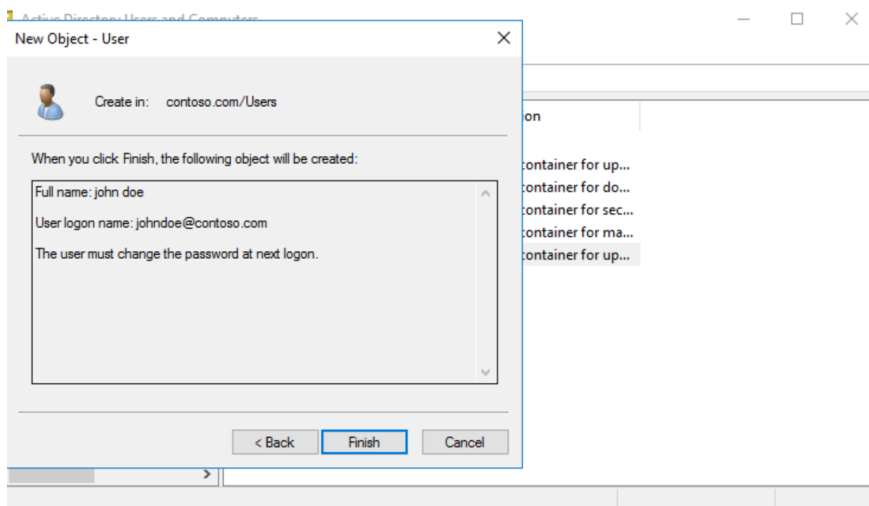
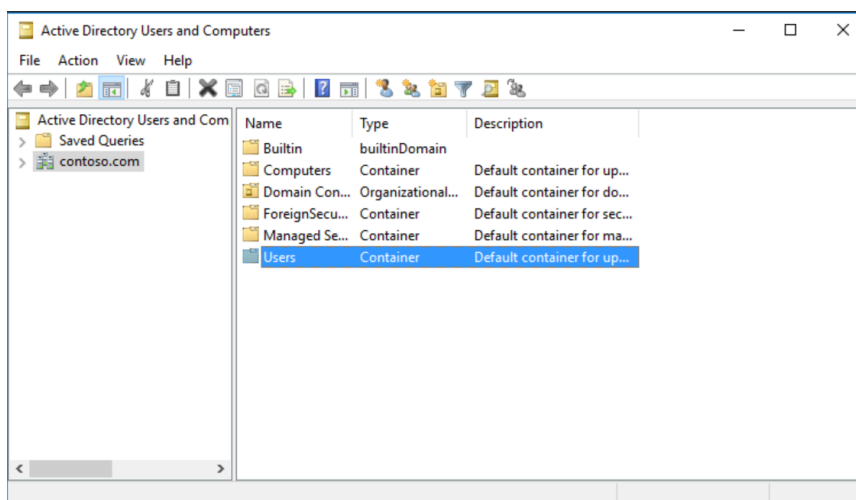
Step 1 – Join the Computer to the Domain

1. Log in to the workstation as a local administrator.
2. Go to **Settings** → **System** → **About** → **Rename this PC (Advanced)**.
3. Select **Member of domain**, type **contoso.com**, and click **OK**.
4. If an error says the domain controller cannot be contacted:
 - Go to **Control Panel** → **Network and Internet** → **Network Connections**.
 - Right-click your Ethernet adapter → **Properties** → select **Internet Protocol Version 4 (TCP/IPv4)**.
 - In the DNS server field, enter your domain controller's private IP (e.g., **192.168.1.10**).
5. Retry joining the domain, enter domain admin credentials, then reboot.



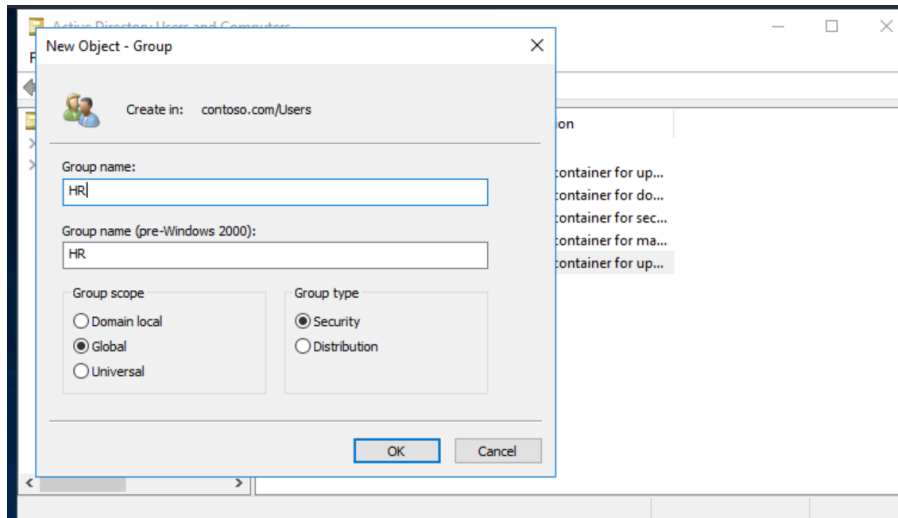
Step 2 – Create a New Hire User

1. On the server, open **Active Directory Users and Computers (ADUC)**.
2. Select the **Users** container.
3. Right-click → **New** → **User**.
4. Enter first name, last name, and logon name.
5. Set a temporary password and check **User must change password at next logon**.
6. Click **Finish**.



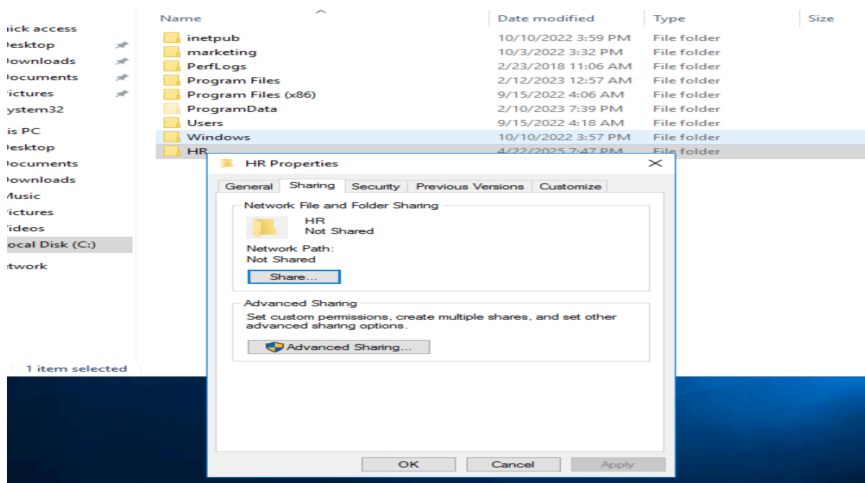
Step 3 – Create Department Group and Add User

1. In ADUC, right-click **Users** → **New** → **Group**.
2. Name it after the department (e.g., Sales).
3. Right-click the new hire's user → **Add to a group...** → enter the group name.



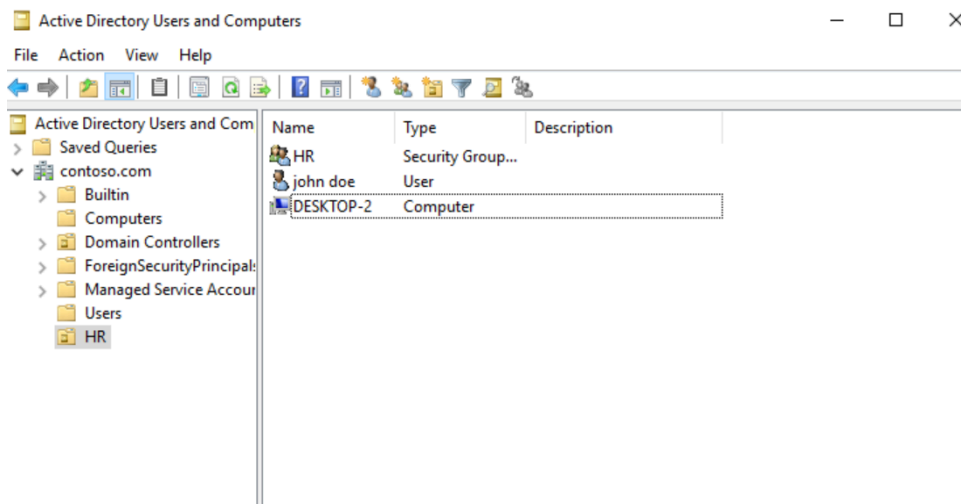
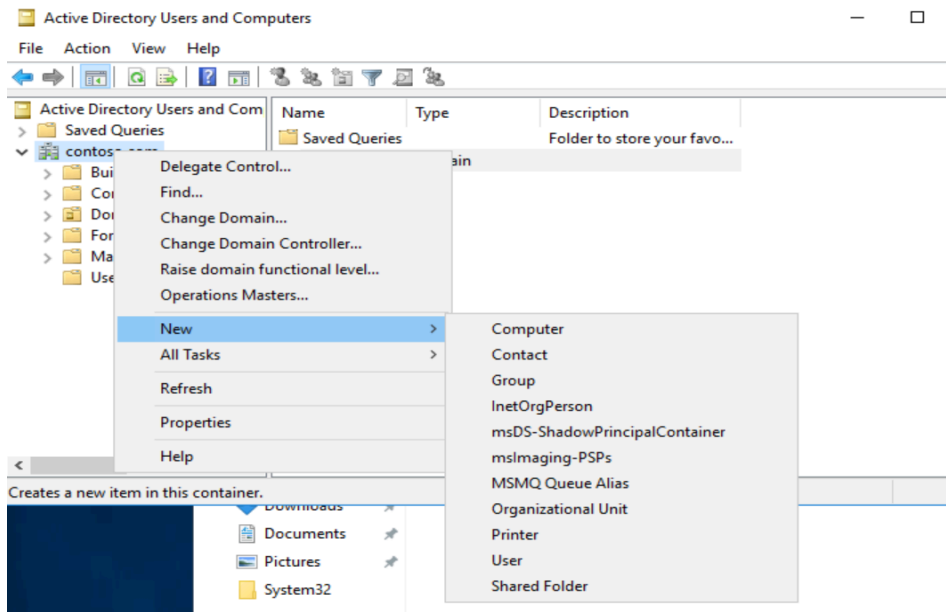
Step 4 – Create Departmental Share

1. On the server, create **C:\Shares\Sales**.
2. Right-click folder → **Properties** → **Sharing** → **Advanced Sharing**.
3. Share with the department group (Allow: Read, Change).
4. In **Security** tab, grant the group **Modify**.
5. Create **test.txt** inside.



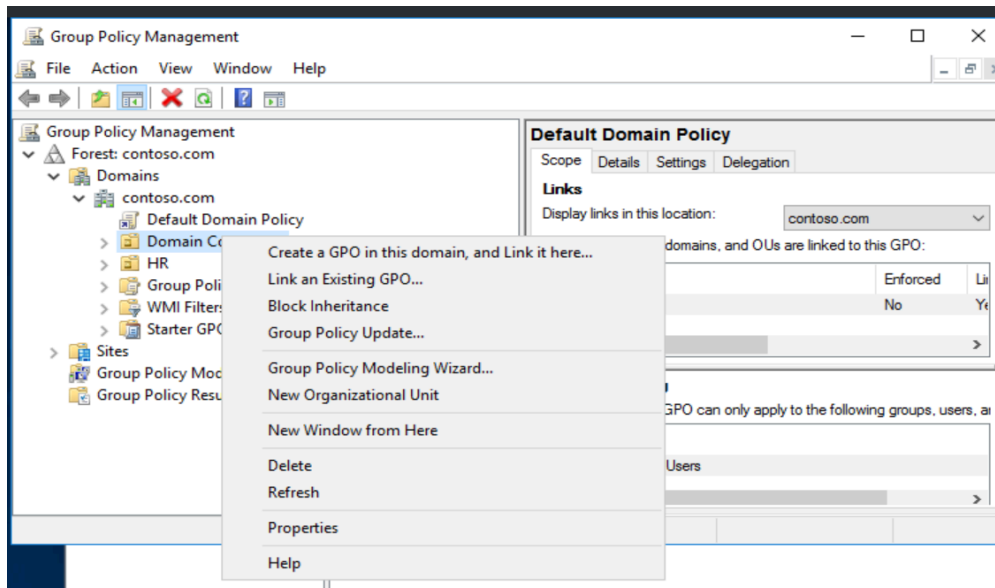
Step 5 – Create OU and Move Objects

1. In ADUC, right-click domain root → **New** → **Organizational Unit** → name it after the department.
2. Move the new hire's user, group, and computer objects into the OU.

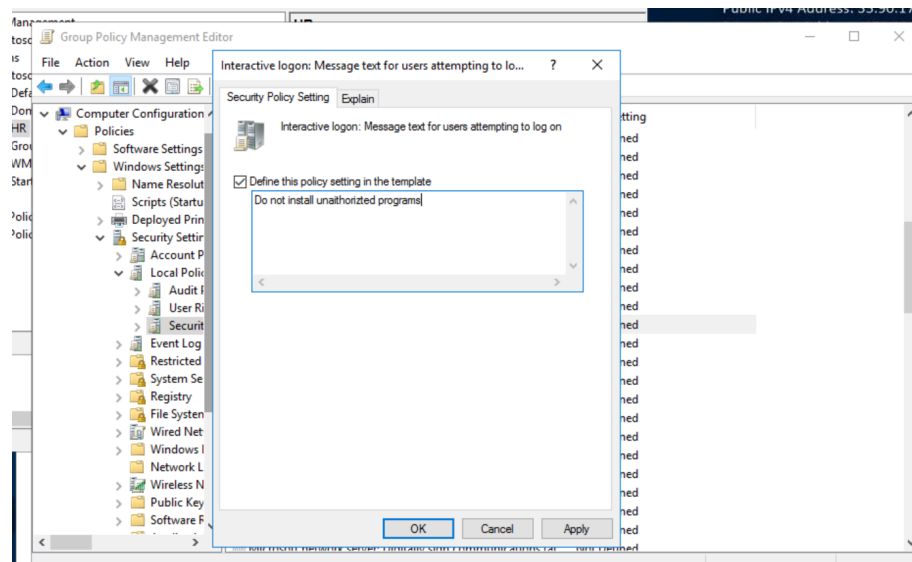


Step 6 – Apply GPO to OU

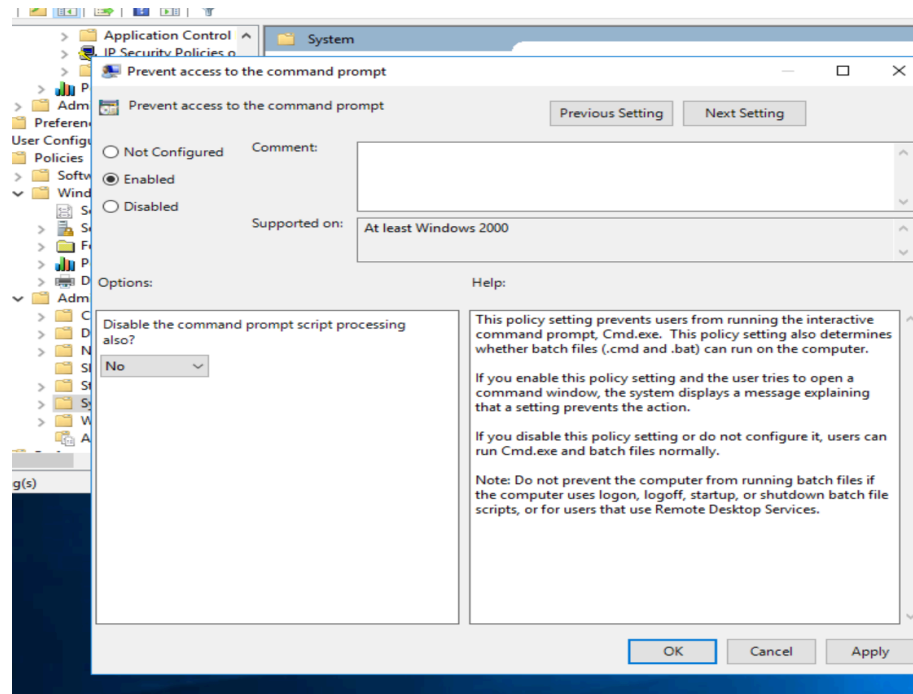
1. In **Group Policy Management**, create and link a new GPO to the OU.



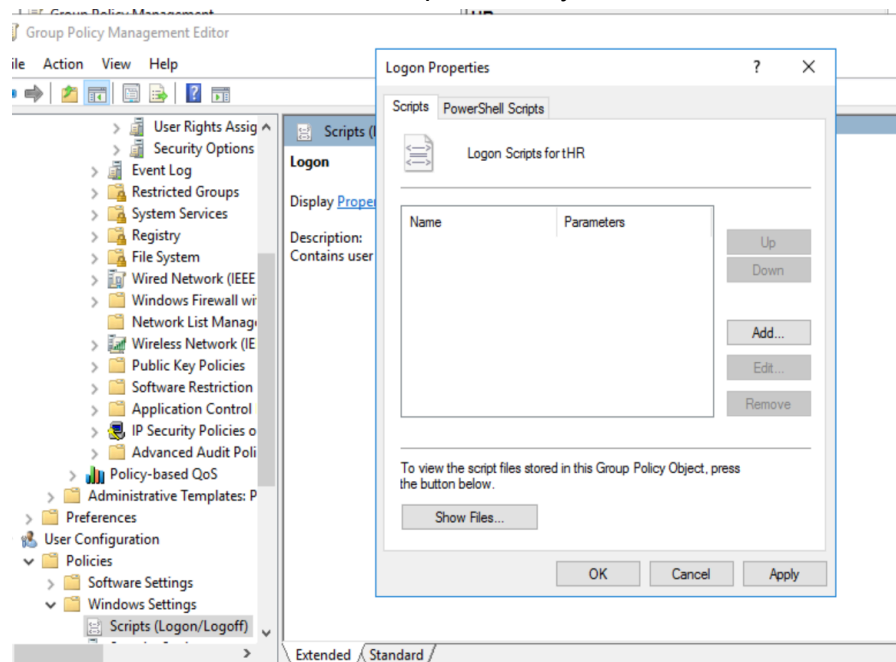
2. Edit the GPO to configure:
 - **Startup message:** Computer Config → Policies → Windows Settings → Security Settings → Local Policies → Security Options → set Interactive logon message.



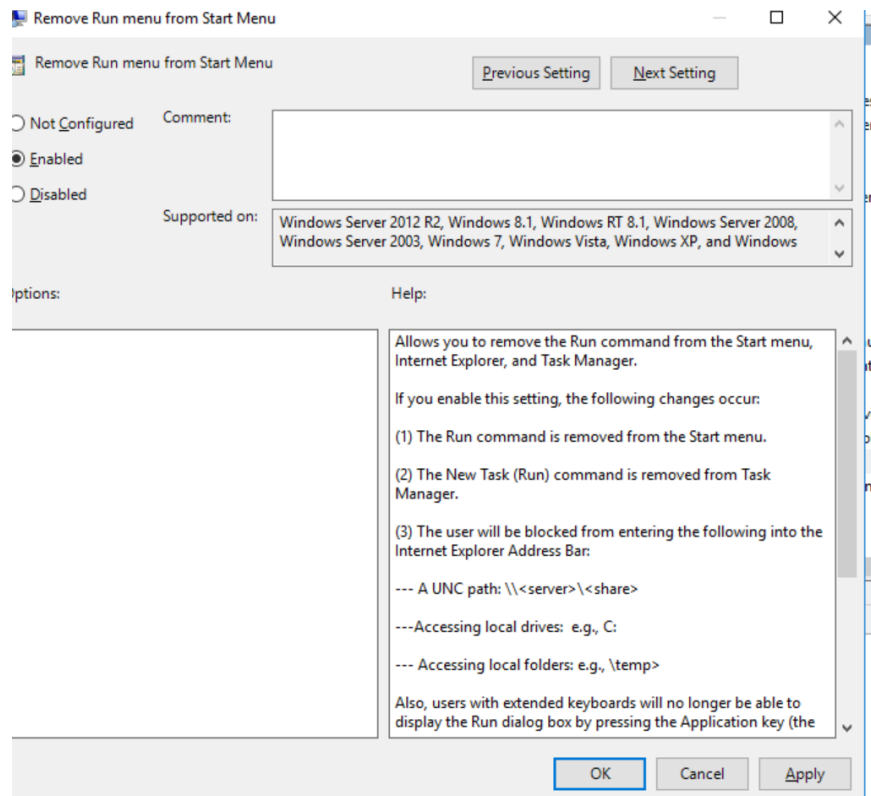
- **Disable Command Prompt:** User Config → Administrative Templates → System → Prevent access to the command prompt → Enabled.



- **Logon script:** User Config → Windows Settings → Scripts (Logon) → add **map-drive.bat**:
`net use S: \\SRV-FILE01\Sales /persistent:yes`



- **Remove Run menu:** User Config → Administrative Templates → Start Menu and Taskbar → Remove Run menu from Start Menu → Enabled.



Step 7 – Verify Successful Logon

1. On the server, open **Event Viewer** → **Windows Logs** → **Security**.
2. Filter for **Event ID 4624** and the new hire's username.
3. Confirm logon type and timestamp.

Step 8 – Check Latest Installed Program

1. On the workstation, open **PowerShell**.
2. Run:
`Get-WmiObject Win32_Product | Sort-Object InstallDate -Descending | Select-Object -First 1`
3. Review the output for the most recent installation.

```
PS C:\Windows\system32> Get-WmiObject -Class Win32_Product

IdentifyingNumber : {3407B900-37F5-4CC2-B612-5CD5D580A163}
Name              : Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332
Vendor           : Microsoft Corporation
Version          : 14.32.31332
Caption          : Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332

IdentifyingNumber : {5A6DED90-DBEF-47F5-AAAB-915E6447CA58}
Name              : Amazon SSM Agent
Vendor           : Amazon Web Services
Version          : 3.2.582.0
Caption          : Amazon SSM Agent

IdentifyingNumber : {F4499EE3-A166-496C-81BB-51D1BCDC70A9}
Name              : Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332
Vendor           : Microsoft Corporation
Version          : 14.32.31332
Caption          : Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332

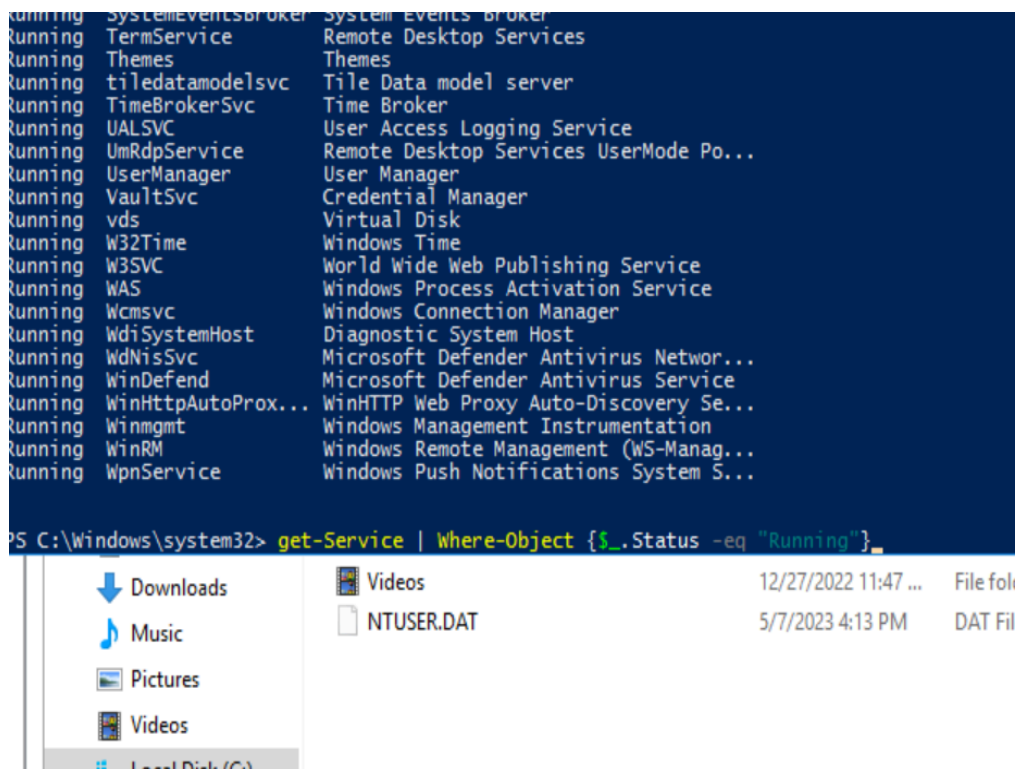
IdentifyingNumber : {2A37BC85-93D0-457D-ACD1-2FC70AFF2F69}
Name              : AWS Tools for Windows
Vendor           : Amazon Web Services Developer Relations
Version          : 3.15.1737
Caption          : AWS Tools for Windows

IdentifyingNumber : {E39B9296-5D94-4B40-8AF3-C377641A8895}
Name              : NICE DCV Virtual Display
Vendor           : NICE Software
```

Log Name:

Step 9 – Export Running Services

1. On the workstation, open **PowerShell**.
2. Run:
`Get-Service | Where-Object {$_.Status -eq 'Running'} | Out-File C:\Temp\running_services.txt`
3. Check `C:\Temp\running_services.txt` for the list of running services.



The image shows a PowerShell terminal window with a list of running services and their full names. Below the terminal, a File Explorer window is open, showing the 'Local Disk (C:)' with folders like Downloads, Music, Pictures, and Videos, and files like Videos and NTUSER.DAT.

Running	Service Name	Full Name
Running	SystemEventsBroker	System Events Broker
Running	TermService	Remote Desktop Services
Running	Themes	Themes
Running	tiledatamodelsvc	Tile Data model server
Running	TimeBrokerSvc	Time Broker
Running	UALSvc	User Access Logging Service
Running	UmRdpService	Remote Desktop Services UserMode Po...
Running	UserManager	User Manager
Running	VaultSvc	Credential Manager
Running	vds	Virtual Disk
Running	W32Time	Windows Time
Running	W3SVC	World Wide Web Publishing Service
Running	WAS	Windows Process Activation Service
Running	Wcmsvc	Windows Connection Manager
Running	WdiSystemHost	Diagnostic System Host
Running	WdNisSvc	Microsoft Defender Antivirus Networ...
Running	WinDefend	Microsoft Defender Antivirus Service
Running	WinHttpAutoProx...	WinHTTP Web Proxy Auto-Discovery Se...
Running	Winmgmt	Windows Management Instrumentation
Running	WinRM	Windows Remote Management (WS-Manag...
Running	WpnService	Windows Push Notifications System S...

PS C:\Windows\system32> get-Service | Where-Object {\$_.Status -eq "Running"} | Out-File C:\Temp\running_services.txt

File Explorer (C:):

- Downloads
- Music
- Pictures
- Videos
- Videos (12/27/2022 11:47 ...)
- NTUSER.DAT (5/7/2023 4:13 PM)