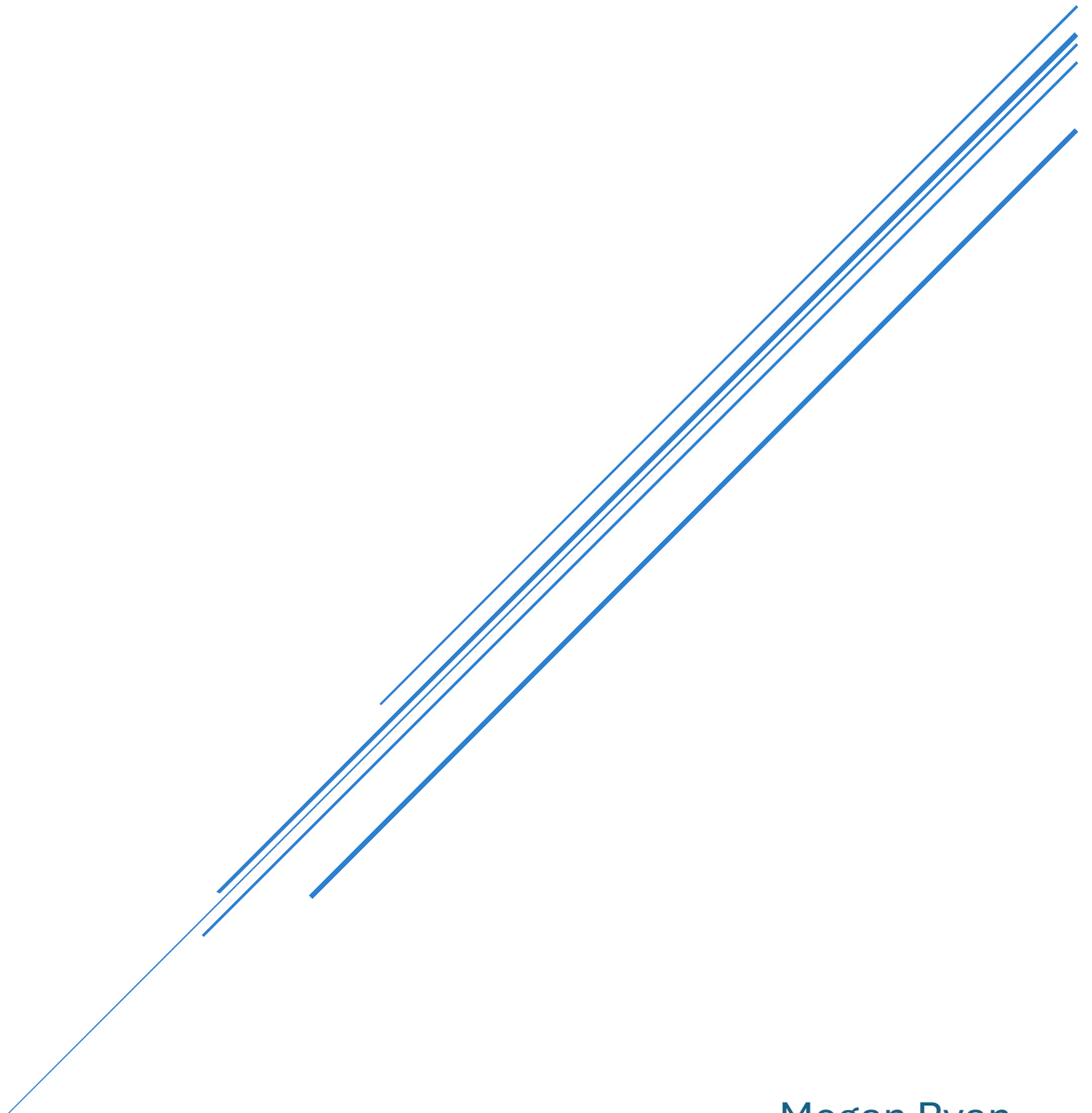


STACKFULL SOTWARE

IT – Pre Onboarding Runbook



Megan Ryan
August 18, 2025

Table of Contents

INTRODUCTION	3
STEP 0 — FIX: POINT CLIENT DNS TO THE DOMAIN CONTROLLER WINDOWS DOMAIN JOIN REQUIRES THE CLIENT TO USE THE DOMAIN CONTROLLER (DC) AS DNS SO IT CAN RESOLVE THE DOMAIN AND LOCATE AD SERVICES.	4
STEP 1 — VERIFY CONNECTIVITY & NAME RESOLUTION	5
STEP 2 — JOIN DESKTOP-1 TO THE DOMAIN.....	5
NOTES & TROUBLESHOOTING	7
STEP 3 — CREATE DEPARTMENT GROUP AND ADD THE NEW HIRE	7
3.0 CREATE THE NEW-HIRE USER (SERVER).....	7
3.1 CREATE THE DEPARTMENT GROUP (SERVER).....	8
3.2 ADD THE NEW HIRE TO HR_DEPARTMENT (SERVER).....	8
3.3 VERIFY MEMBERSHIP ON THE USER OBJECT (SERVER)	9
STEP 4 — CREATE A DEPARTMENT SHARE WITH READ/WRITE (HR)	10
4.1 CREATE THE FOLDER STRUCTURE	10
4.2 SET NTFS (SECURITY) PERMISSIONS.....	10
4.3 PUBLISH THE SMB SHARE (SHARE PERMISSIONS)	11
4.4 CREATE SEED FILE FOR LATER VALIDATION	12
4.5 VERIFY THE SHARE IS PUBLISHED (COMPUTER MANAGEMENT MMC)	13
STEP 5 — CREATE AN OU AND LINK A GPO	13
5.1 CREATE THE OU	13
5.2 MOVE THE USER, GROUP, AND COMPUTER INTO THE OU.....	14
5.3 CREATE AND LINK A GPO TO THE OU	15
STEP 6 — EDIT THE HR_POLICIES GPO AND APPLY RULES.....	16
6.1 CONFIGURE THE LOGON BANNER (STARTUP MESSAGE).....	17
6.2 BLOCK COMMAND PROMPT (WITHOUT BREAKING LOGON SCRIPTS).....	18
6.3 — MAP THE HR SHARE AT USER LOGON (DRIVE MAPS, NO SCRIPTS).....	18
6.4 — REMOVE THE “RUN” COMMAND FROM START.....	19
APPLY & TEST (CLIENT)	20
STEP 7 — FIND THE LAST SUCCESSFUL LOGON FOR YOUR USER (ON THE SERVER)	20

StackFull Software — IT Pre-Onboarding Runbook

7.1 OPEN THE SECURITY LOG.....	21
7.2 FILTER TO SUCCESSFUL LOGONS (EVENT ID 4624)	21
7.3 FIND YOUR SPECIFIC USER (FAST).....	22
7.4 READ THE DETAILS YOU NEED	23
STEP 8.....	23
8.1 OPEN POWERSHELL	23
8.2 WMI.....	24
COMMAND (TYPE EXACTLY): GET-CIMINSTANCE WIN32_PRODUCT SORT-OBJECT INSTALLDATE -DESCENDING SELECT- OBJECT -FIRST 1 NAME,VERSION,VENDOR,INSTALLDATE	24
OUTPUT:	24
STEP 9 — LIST ALL RUNNING SERVICES TO A FILE.....	25
9.1 RUN THE COMMAND.....	25

INTRODUCTION

This runbook defines the **pre-onboarding build** for Windows workstations at StackFull Software. Its purpose is to take a fresh client from “workgroup and unknown” to a **managed, compliant, and ready-for-day-one** state—joined to the **contoso.com** domain, governed by baseline security policy, and provisioned with the resources a new hire needs. The procedures standardize setup, reduce lead time for IT, and cut risk by enforcing least-privilege access and auditable controls from the first login.

The workflow implements four pillars of control:

1. **Identity & Join:** Bind the device to Active Directory, place it in the correct **OU** (**HR_OU**), and ensure the right **user** (**Jordan Smaih / jsmaih**) and **group** (**HR_Department**) relationships exist.
2. **Access & Data:** Publish a departmental share (**HRShare**) with aligned **share + NTFS** permissions (read/write for HR only), and auto-map it at logon.
3. **Policy & Hardening:** Apply a GPO (**HR_Policies**) that shows an interactive **logon banner**, **blocks CMD** for users, **removes Run**, and maps the **H:** drive—delivering consistent posture with minimal manual touch.
4. **Audit & Evidence:** Validate logons in **Event Viewer** (4624), confirm installed software and running services via **PowerShell**, and capture screenshots as evidence.

Scope & Outcomes

After completing this runbook, the target workstation will:

- Be joined to **contoso.com** and located in **HR_OU** with the correct security scope.
- Enforce baseline user restrictions (no CMD, Run removed) and display the standard legal banner.
- Map **H:** to `\\172.31.42.153\HRShare` for HR staff with appropriate write access.
- Produce verifiable artifacts: Security log entries (ID 4624), “latest installed program” output, and `running_services.txt`.

Assumptions & Prerequisites

- **Domain Controller/DNS:** 172.31.42.153 (AD DS + DNS healthy; server uses itself as DNS).
- **Domain:** `contoso.com`; admin credentials available (`Administrator / Pa$$w0rd` for lab).
- **Client:** Windows desktop with IPv4 **Preferred DNS** set to the DC IP.
- You have rights to create **users, groups, OUs, shares, and GPOs** in the lab.

Evidence & Documentation

Each major step includes a screenshot placeholder. Capture evidence on the client and server as indicated (join confirmations, GPO links, drive map, policy effects, Event Viewer 4624, PowerShell outputs). These artifacts demonstrate control ownership and are suitable for audit or peer review.

ENVIRONMENT SUMMARY

- Domain: contoso.com
- Domain Controller/DNS IP: 172.31.42.153
- Admin credentials used to join domain: administrator / Pa\$\$w0rd
- Client: Desktop-1 (Windows)

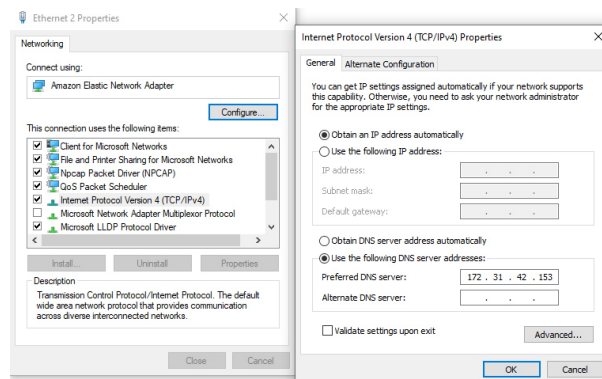
STEP 0 — FIX: POINT CLIENT DNS TO THE DOMAIN CONTROLLER

Windows domain join requires the client to use the Domain Controller (DC) as DNS so it can resolve the domain and locate AD services.

PROCEDURE (DESKTOP-1)

1. Open Control Panel → Network and Sharing Center → Change adapter settings.
2. Right-click the active adapter → Properties → select Internet Protocol Version 4 (TCP/IPv4) → Properties.
3. Select “Use the following DNS server addresses” and set Preferred DNS to 172.31.42.153.
4. Click OK to apply.

Figure 1: Client DNS set to the Domain Controller (172.31.42.153) on Desktop-1.



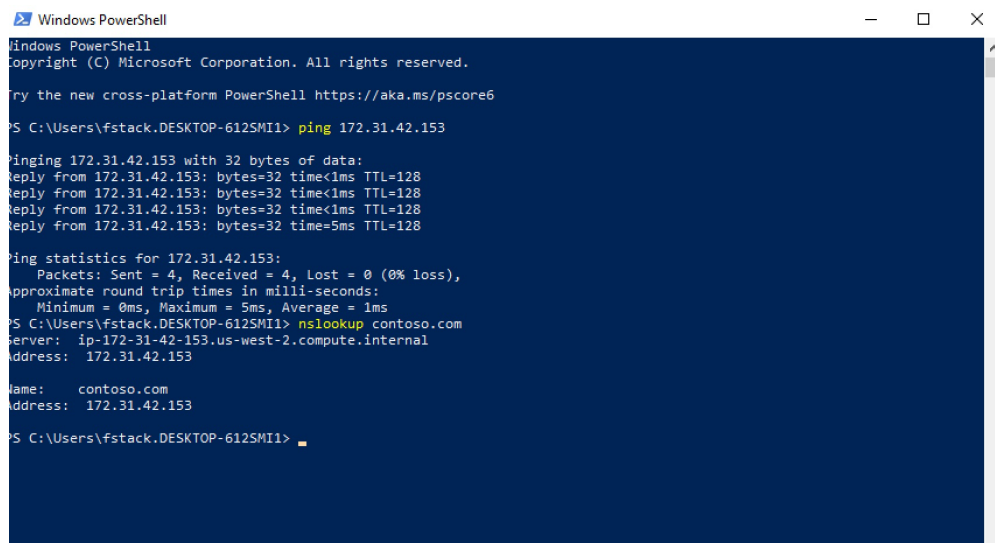
STEP 1 — VERIFY CONNECTIVITY & NAME RESOLUTION

COMMANDS EXECUTED (REFERENCE)

- ping 172.31.42.153
- nslookup contoso.com

EXPECTED RESULTS

- ping replies from 172.31.42.153 (0% loss acceptable).
- nslookup contoso.com resolves to the DC/DNS and shows the DC as the Server.



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\fstack\DESKTOP-612SMI1> ping 172.31.42.153

Pinging 172.31.42.153 with 32 bytes of data:
Reply from 172.31.42.153: bytes=32 time<1ms TTL=128
Reply from 172.31.42.153: bytes=32 time<1ms TTL=128
Reply from 172.31.42.153: bytes=32 time<1ms TTL=128
Reply from 172.31.42.153: bytes=32 time=5ms TTL=128

Ping statistics for 172.31.42.153:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms
PS C:\Users\fstack\DESKTOP-612SMI1> nslookup contoso.com
Server: ip-172-31-42-153.us-west-2.compute.internal
Address: 172.31.42.153

Name:    contoso.com
Address: 172.31.42.153

PS C:\Users\fstack\DESKTOP-612SMI1>
```

Figure 2: Connectivity and name resolution successful (ping to DC and nslookup contoso.com).

STEP 2 — JOIN DESKTOP-1 TO THE DOMAIN

PROCEDURE (DESKTOP-1)

1. Right-click This PC → Properties → Advanced system settings → Computer Name → Change.
2. Under “Member of,” choose Domain and enter: contoso.com
3. When prompted, provide domain admin credentials:
 - Username: administrator
 - Password: Pa\$\$w0rd
4. Accept the confirmation dialog and restart when prompted.

StackFull Software — IT Pre-Onboarding Runbook

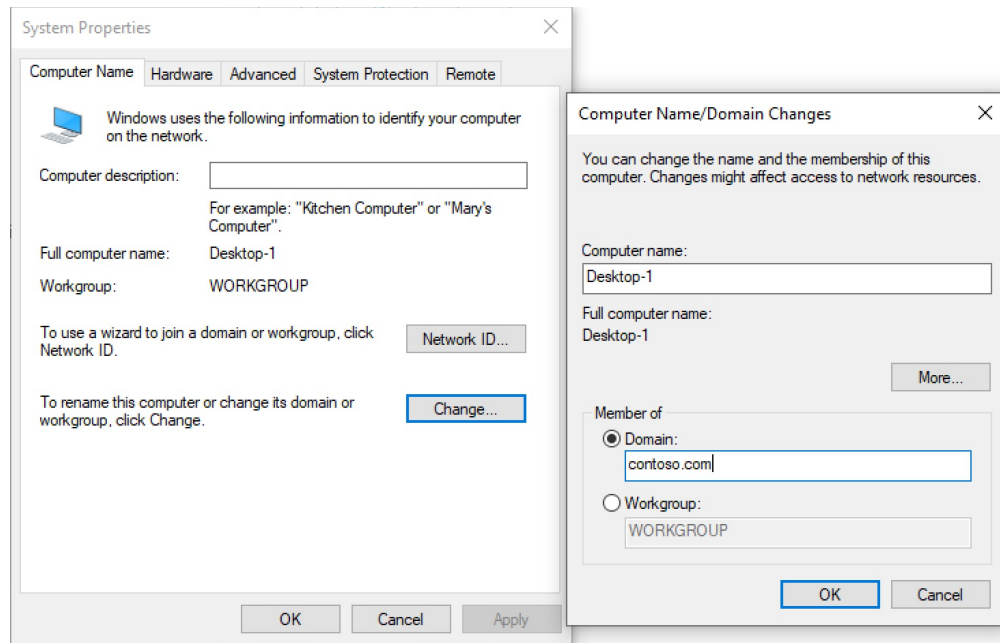


Figure 3: Join dialog showing Desktop-1 joining the domain: contoso.com

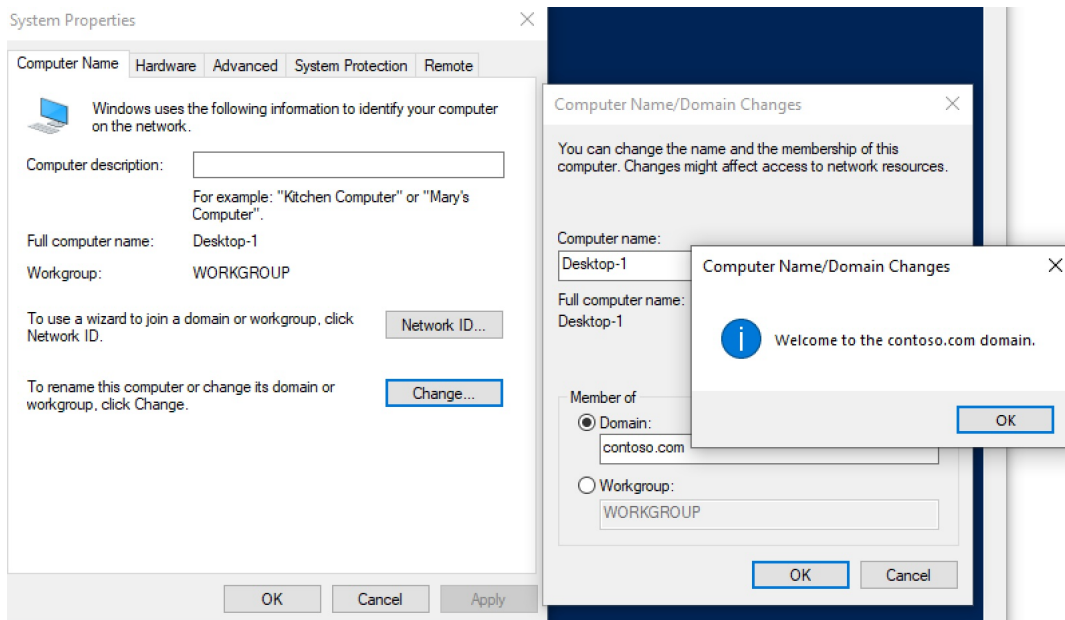


Figure 4: Success dialog — “Welcome to the contoso.com domain.”

NOTES & TROUBLESHOOTING

- If you see “An Active Directory Domain Controller for the domain could not be contacted,” re-check:
 - Client DNS points to the DC (not public DNS).
 - Network connectivity to the DC (same network/segment, no firewall blocking).
 - The DC is running AD DS and DNS services.

STEP 3 — CREATE DEPARTMENT GROUP AND ADD THE NEW HIRE

GOAL

Create a Global Security group for the department and add the new-hire account to it.

3.0 CREATE THE NEW-HIRE USER (SERVER)

1. Server Manager → Tools → Active Directory Users and Computers (ADUC).
2. Expand contoso.com → Users.
3. Right-click Users → New → User.
4. Fill in:
 - First name: Jordan
 - Last name: Smith
 - User logon name (UPN): jsmith@contoso.com
 - (sAMAccountName should be jsmith)
5. Password: Pa\$\$word123 (you may uncheck “User must change password at next logon” for lab).
6. Finish. Verify the account exists in Users.

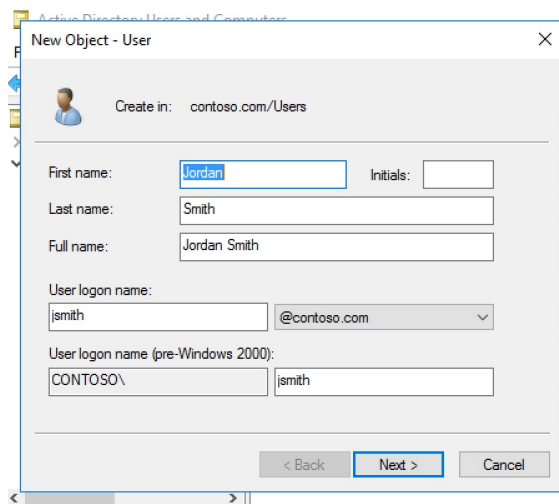


Figure 5: New user wizard — Jordan Smith (jsmith) created in ADUC.

3.1 CREATE THE DEPARTMENT GROUP (SERVER)

1. In contoso.com → Users, right-click → New → Group.
2. Group name: HR_Department
3. Group scope: Global
4. Group type: Security
5. OK.

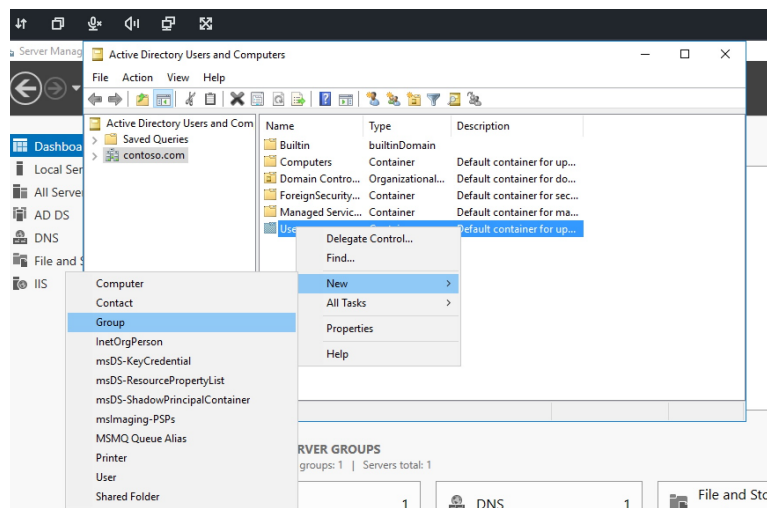


Figure 6: HR_Department Global Security group created under Users

3.2 ADD THE NEW HIRE TO HR_DEPARTMENT (SERVER)

1. HR_Department → Properties → Members → Add...
2. Locations... = contoso.com; Object Types... includes Users.
3. Enter jsmith (or contoso\jsmith) → Check Names → OK.
4. Confirm Jordan Smith (jsmith) appears → Apply → OK.

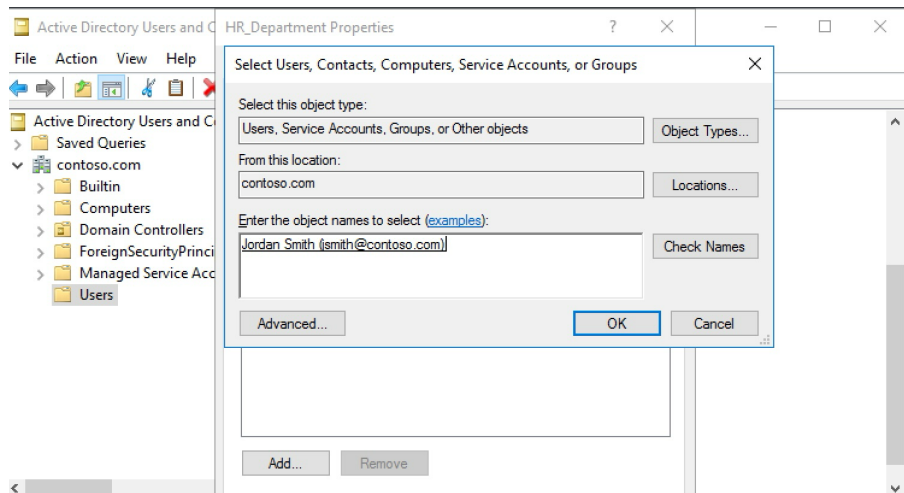


Figure 7: HR_Department — Members tab showing Jordan Smith (jsmith) added.

3.3 VERIFY MEMBERSHIP ON THE USER OBJECT (SERVER)

1. Right-click Jordan Smith → Properties → Member Of.
2. Confirm HR_Department is listed.

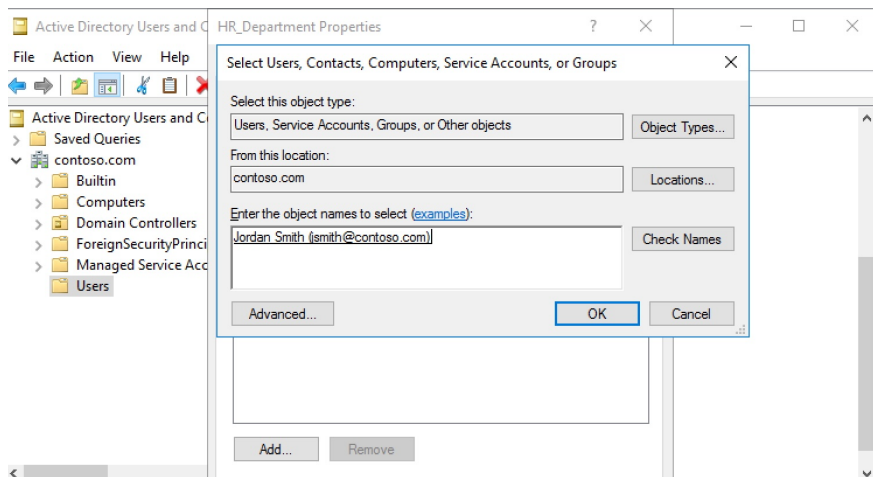


Figure 8: Jordan Smith — Member Of tab includes HR_Department

STEP 4 — CREATE A DEPARTMENT SHARE WITH READ/WRITE (HR)

GOAL

Create a departmental network share for HR that only members of HR_Department can read/write, and add a seed file test.txt.

WHERE

Server (Domain Controller)

4.1 CREATE THE FOLDER STRUCTURE

1. File Explorer → create C:\Shares\HR.

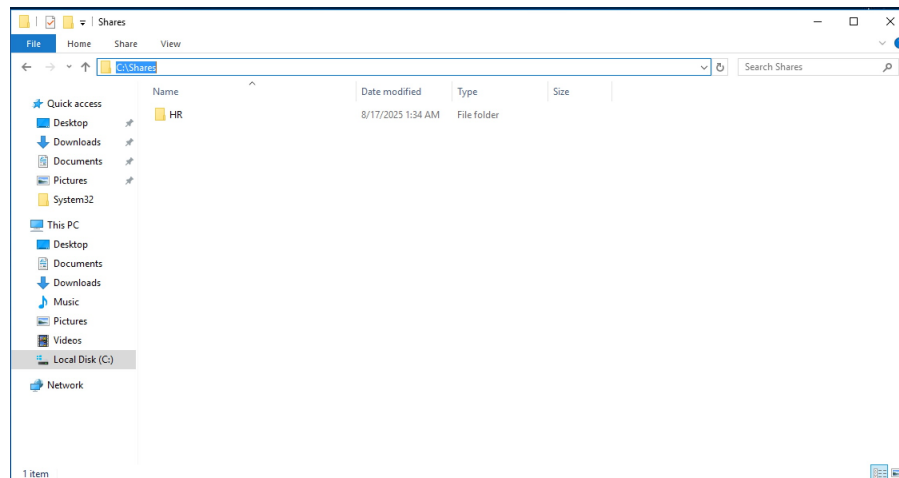


Figure 9: Department folder created at C:\Shares\HR on the server

4.2 SET NTFS (SECURITY) PERMISSIONS

1. Right-click C:\Shares\HR → Properties → Security → Edit.
2. Remove broad principals you don't want (e.g., Users if present).
3. Add CONTOSO\HR_Department with Modify, Read & execute, List folder contents, Read, Write (i.e., Modify).
4. Ensure Administrators and SYSTEM retain Full control. Apply → OK.

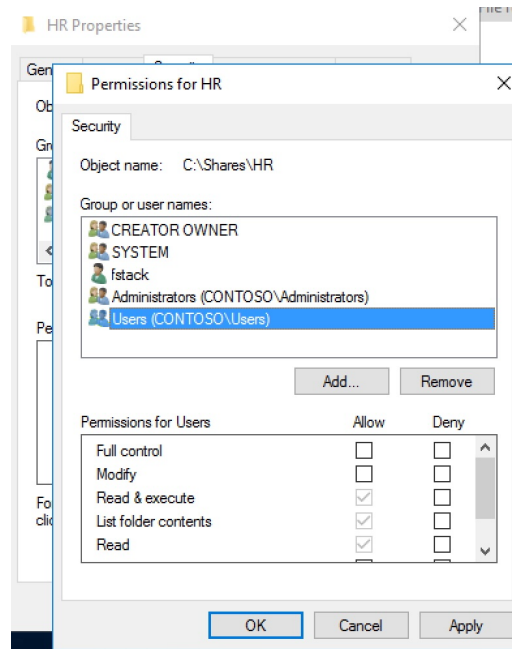


Figure 10: NTFS permissions — HR_Department has Modify; Administrators/SYSTEM have Full control.

4.3 PUBLISH THE SMB SHARE (SHARE PERMISSIONS)

1. C:\Shares\HR → Properties → Sharing → Advanced Sharing.
2. Check “Share this folder”; Share name: HRShare.
3. Permissions: Remove Everyone; Add CONTOSO\HR_Department with Change and Read (no Full Control).
4. OK all dialogs.

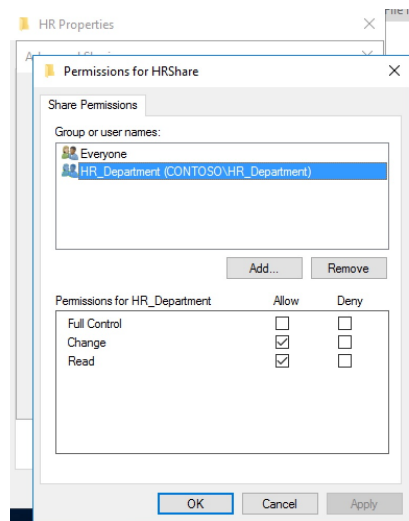


Figure 11: Sharing tab — HRShare created for C:\Shares\HR.

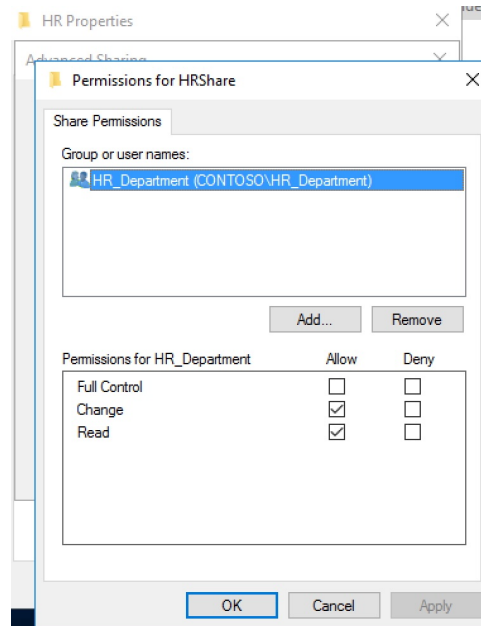


Figure 12: Figure 4.4: Share permissions — only HR_Department with Change + Read (no Everyone).

4.4 CREATE SEED FILE FOR LATER VALIDATION

1. Open C:\Shares\HR.
2. New → Text Document → test.txt.
3. Add a one-liner (e.g., “HR seed file”) and save.

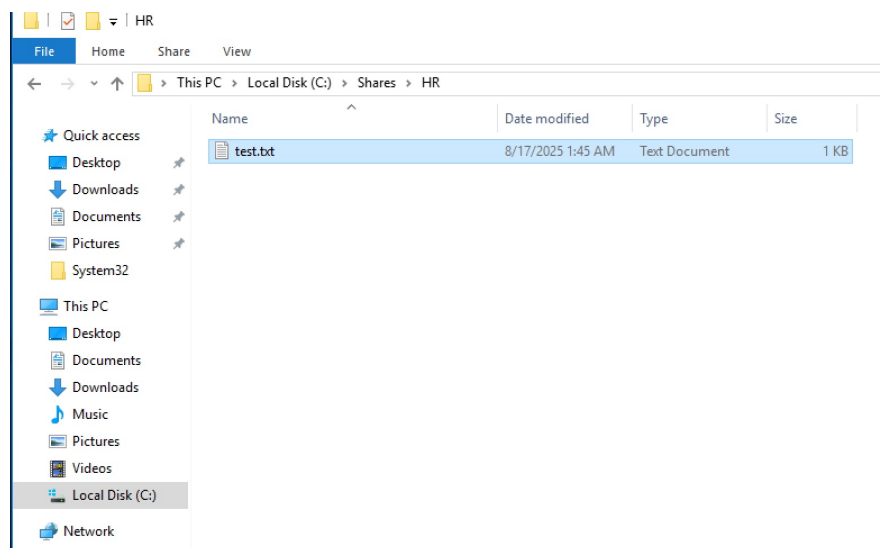


Figure 13: test.txt created inside C:\Shares\HR.

4.5 VERIFY THE SHARE IS PUBLISHED (COMPUTER MANAGEMENT MMC)

1. Server Manager → Tools → Computer Management.
2. System Tools → Shared Folders → Shares.
3. Confirm HRShare → Local Path shows C:\Shares\HR.

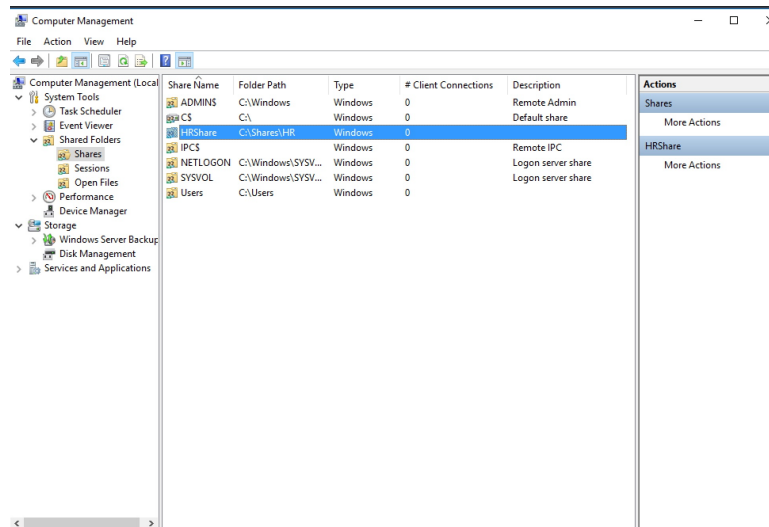


Figure 14: Computer Management — Shared Folders → Shares shows HRShare → C:\Shares\HR.

STEP 5 — CREATE AN OU AND LINK A GPO

Goal

Create an Organizational Unit (OU) for the department, move the user, group, and computer into it, and **link a new GPO** that we'll configure in Step 6.

Where

Server (Domain Controller)

5.1 Create the OU

1. Open **Active Directory Users and Computers (ADUC)**
 - Server Manager → **Tools** → **Active Directory Users and Computers**
2. In the left pane, **right-click the domain contoso.com** → **New** → **Organizational Unit**.
3. **Name:** HR_OU
4. Leave **"Protect container from accidental deletion"** checked (recommended).
5. Click **OK**.

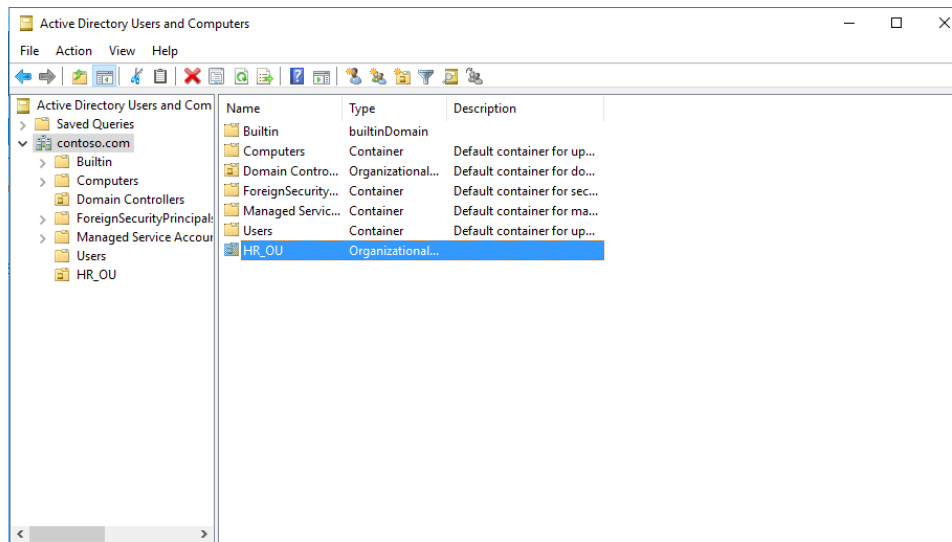


Figure 15: HR_OU created under the contoso.com domain in ADUC.

5.2 Move the User, Group, and Computer into the OU

We previously created:

- **User:** Jordan Smith (jsmith) — currently under **Users**
- **Group:** HR_Department — currently under **Users**
- **Computer:** DESKTOP-1 — typically under **Computers**

Move via ADUC (drag-and-drop):

1. In ADUC, expand **contoso.com** and select the source containers:
 - **Users** (for jsmith and HR_Department)
 - **Computers** (for DESKTOP-1)
2. **Drag** each object into **HR_OU**.
3. If you see an error like **"Access is denied"**, right-click the object → **Properties** → **Object** tab → uncheck **"Protect object from accidental deletion,"** then move again.

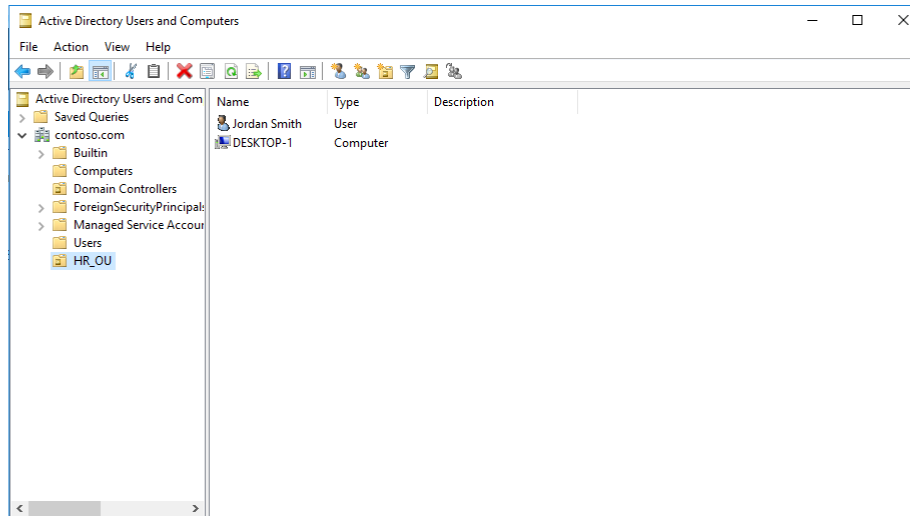


Figure 16: HR_OU containing the user (jsmith), group (HR_Department), and computer (DESKTOP-1).

5.3 Create and Link a GPO to the OU

We'll only **create and link** the GPO here. We'll **edit** the GPO policies in **Step 6**.

Open Group Policy Management (GPMC):

- Server Manager → **Tools** → **Group Policy Management** (or run gpmc.msc)

Create & Link:

1. In the left pane of GPMC, expand **Forest: contoso.com** → **Domains** → **contoso.com**.
2. **Right-click HR_OU** → **"Create a GPO in this domain, and Link it here..."**
3. **Name:** HR_Policies → **OK**
4. Confirm HR_Policies now appears **linked** under HR_OU.

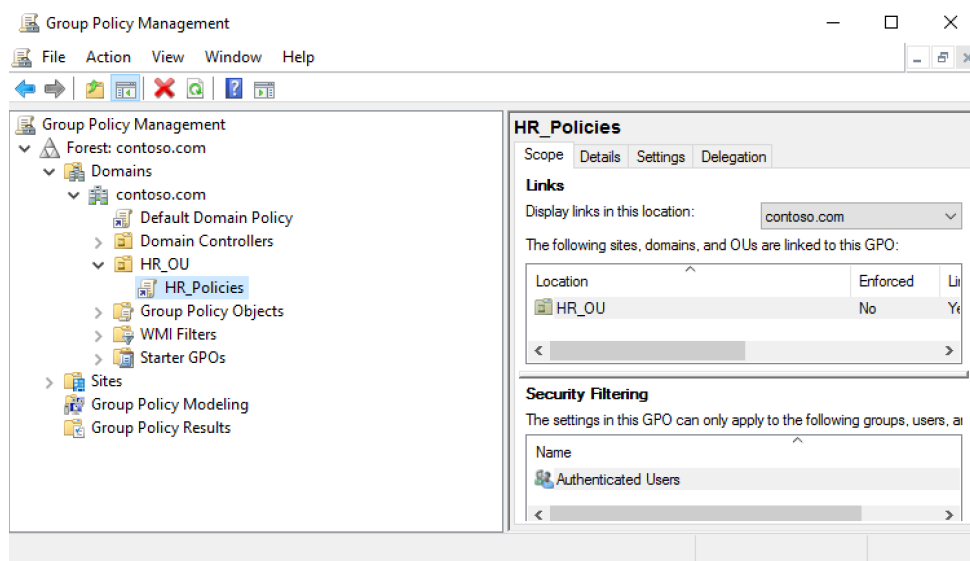


Figure 17: GPMC showing HR_Policies linked to HR_OU.

STEP 6 — EDIT THE HR_Policies GPO AND APPLY RULES

Goal

Configure the GPO linked to HR_OU to:

1. Show a startup/logon message (“Do not install unauthorized programs.”)
2. Block Command Prompt (CMD) for users
3. Map the HR share at user logon
4. Remove the **Run** command from Start

Where

Server (Domain Controller) — **Group Policy Management** (gpmc.msc)

Scope Reminder

- HR_Policies must be **linked to HR_OU**
- **User (jsmith)** and **computer (DESKTOP-1)** should be **inside HR_OU** (done in Step 5)

6.1 Configure the Logon Banner (Startup Message)

Path

Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options

Settings

- **Interactive logon: Message title for users attempting to log on** → **Enabled**
 - **Title:** Notice
- **Interactive logon: Message text for users attempting to log on** → **Enabled**
 - **Text:** Do not install unauthorized programs.

Actions

1. Right-click **HR_Policies** → **Edit**
2. Navigate to the path above
3. Set **Title** and **Message text** as specified → **OK**

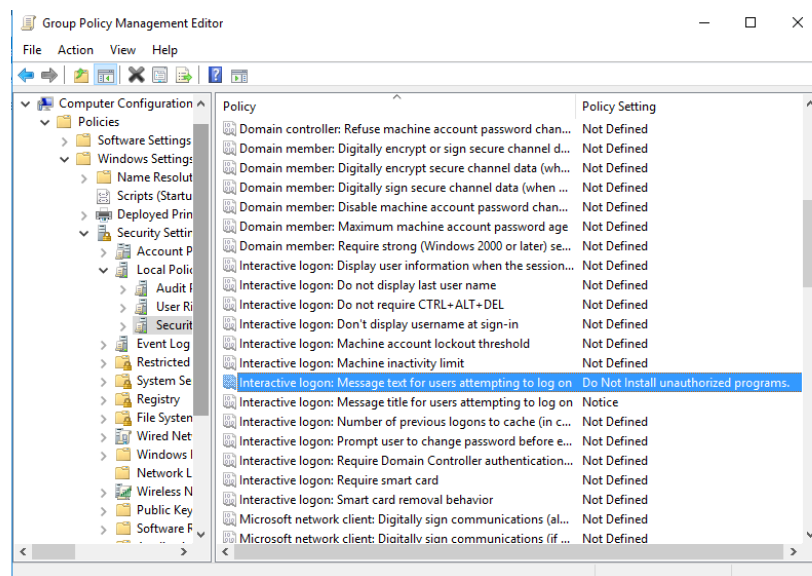


Figure 18: Security Options with Interactive logon title and text configured.

6.2 Block Command Prompt (without breaking logon scripts)

Path

User Configuration → Policies → Administrative Templates → System

Policy

- **Prevent access to the command prompt → Enabled**
 - **Disable the command prompt script processing also? = No**
(Keeps CMD blocked for users, but still allows any batch scripts that Group Policy might run.)

Actions

1. In the same GPO Editor, navigate to the path above
2. Open **Prevent access to the command prompt** → set **Enabled**
3. Set **“Disable the command prompt script processing also?” = No** → OK

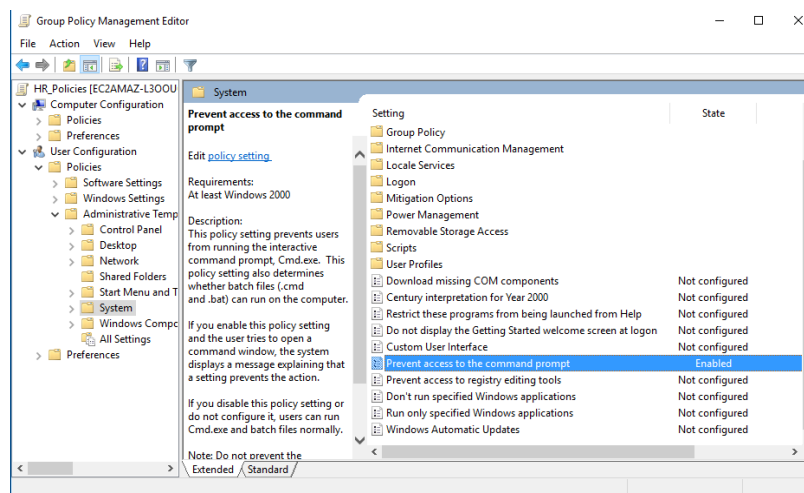


Figure 19: **Prevent access to the command prompt** = Enabled; script processing = No.

6.3 — Map the HR share at user logon (Drive Maps, no scripts)

Where: Server → **Group Policy Management** → HR_OU → **HR_Policies** → **Edit**

1. In the editor: **User Configuration** → **Preferences** → **Windows Settings** → **Drive Maps**
2. Right-pane: **Right-click** → **New** → **Mapped Drive**
3. Fill out:
 - **Action:** Create

- **Location:** \\172.31.42.153\HRShare (use your server IP or name)
 - **Drive Letter:** H:
 - **Reconnect:** ☒ (checked)
 - **Label (optional):** HR Share
4. **Common tab:** leave defaults (you can tick **Run in logged-on user's context** if you like) → **OK**.

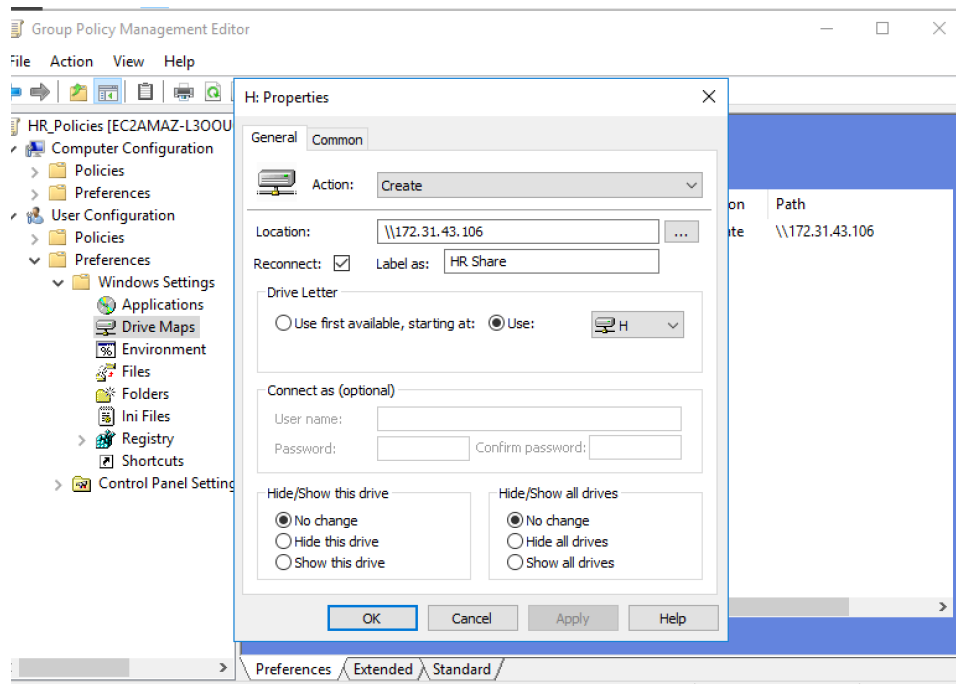


Figure 20: Drive Maps item showing H: → \\172.31.42.153\HRShare.

6.4 — Remove the “Run” command from Start

Where: Same GPO editor

1. **User Configuration → Policies → Administrative Templates → Start Menu and Taskbar**
2. Open **Remove Run menu from Start Menu** → set to **Enabled** → **OK**.

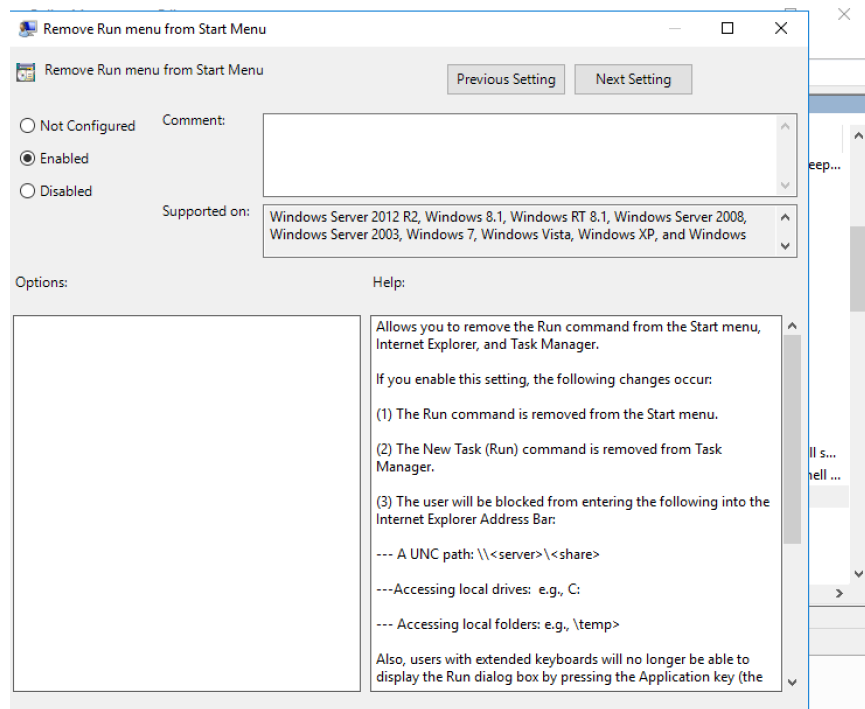


Figure 21: Policy window showing Enabled.

Apply & test (client)

On DESKTOP-2:

1. **Reboot** (or sign out/in) and log in as **CONTOSO\jsmaih**.
2. Open **File Explorer** → confirm **H:** appears and opens the HR share.
3. Open **Start** → confirm **Run** is gone (Win+R may also be blocked, depending on build).

Screenshots to grab (client):

- Explorer with **H:** mapped to \\172.31.42.153\HRShare
- Start menu with **Run** missing

STEP 7 — FIND THE LAST SUCCESSFUL LOGON FOR YOUR USER (ON THE SERVER)

Goal

On the **Domain Controller**, find the **latest successful logon** event for your user (e.g., jsmaih) and record the details.

Sign in as

CONTOSO\Administrator (domain admin)

7.1 Open the Security log

1. On the server: **Start** → type “**Event Viewer**” → open.
2. In the left pane, expand **Windows Logs** → **Security**.

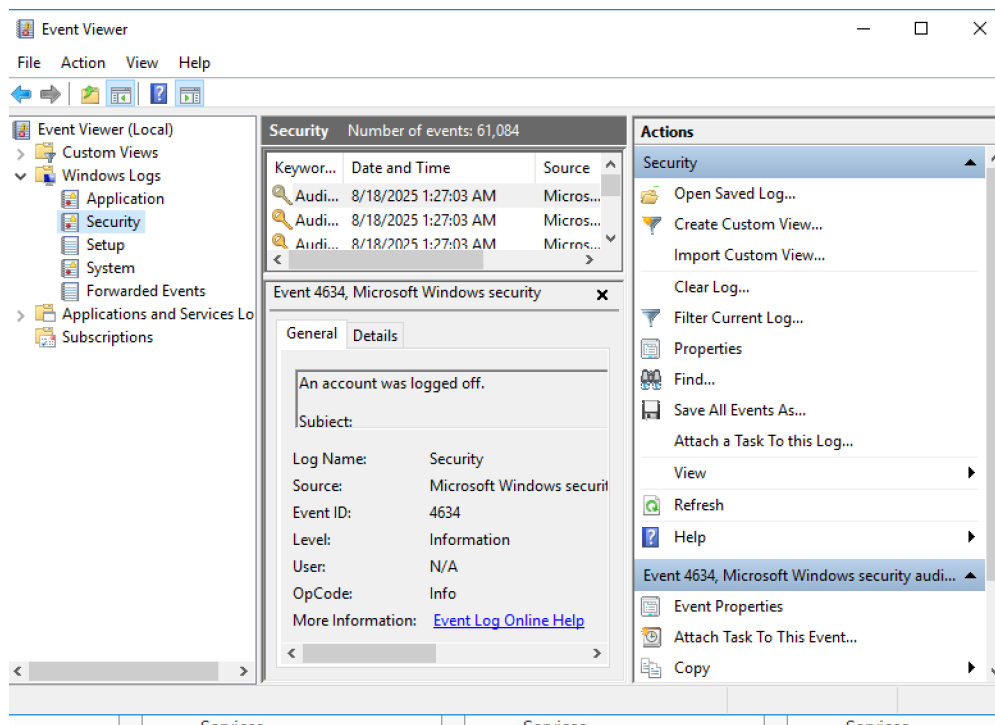


Figure 22: Event Viewer → Windows Logs → Security.

7.2 Filter to successful logons (Event ID 4624)

1. In **Security**, click **Filter Current Log...** (right pane **Actions**).
2. In **Event IDs**, type: **4624**
3. Click **OK**.

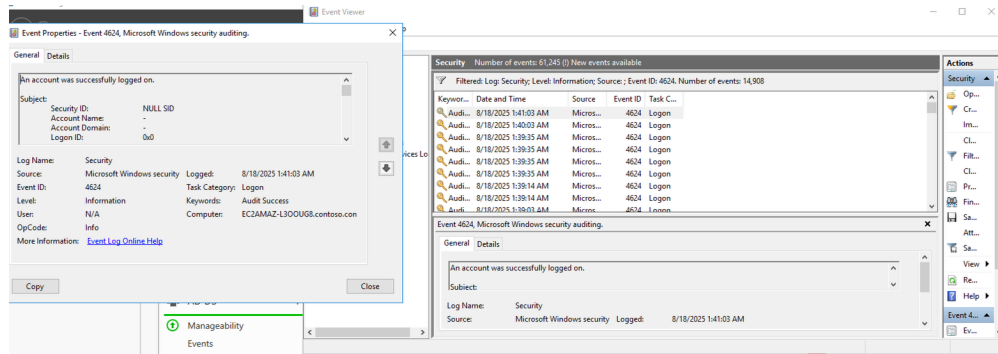


Figure 23: Filter Current Log → Event IDs = 4624.

7.3 Find your specific user (fast)

1. With the filtered list visible, press **Ctrl+F** (or click **Find...** in **Actions**).
2. In **Find what**, type your username: **jsmiah** → **Find Next**.
 - This jumps to the next 4624 (success logon) that contains **jsmiah**.

Tip: If it lands on an older one, click once in the middle pane and press **Shift+F10** → **Sort by** → **Date and Time** (or click the **Date and Time** column header) to get newest at top, then use **Find** again.

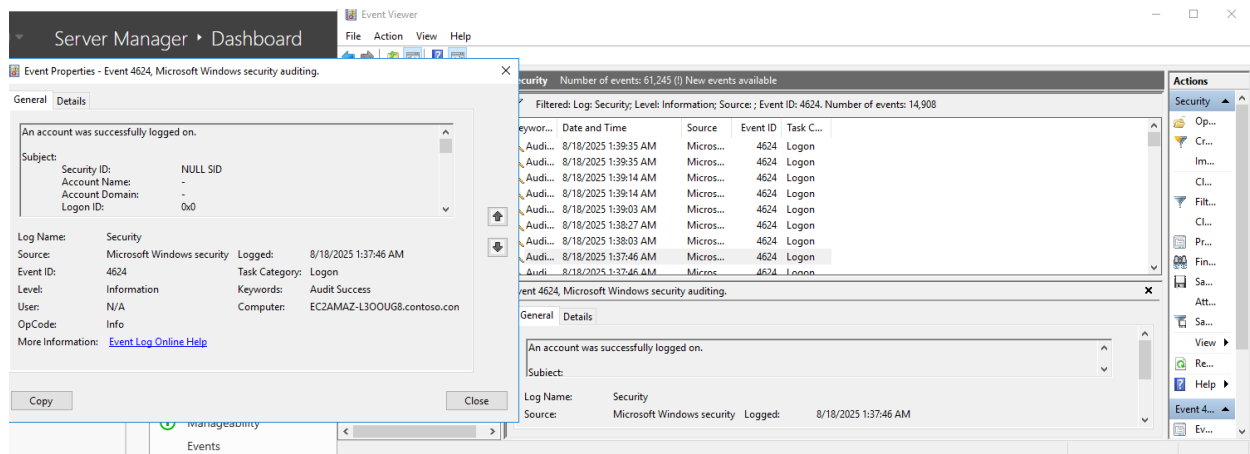


Figure 24: Find dialog searching for jsmith.

7.4 Read the details you need

1. Double-click the matching **4624** event for **jsmaih**.
2. In the **General** tab, scroll to **New Logon** and **Network Information** sections.
3. **Write down these fields** (for your report):
 - **Time** (top of the dialog)
 - **New Logon → Account Name:** jsmaih
 - **New Logon → Account Domain:** CONTOSO
 - **Logon Type:** (e.g., **2** = console, **3** = network, **10** = RDP)
 - **Network Information → Workstation Name** (if present)
 - **Network Information → Source Network Address** (client IP, if present)

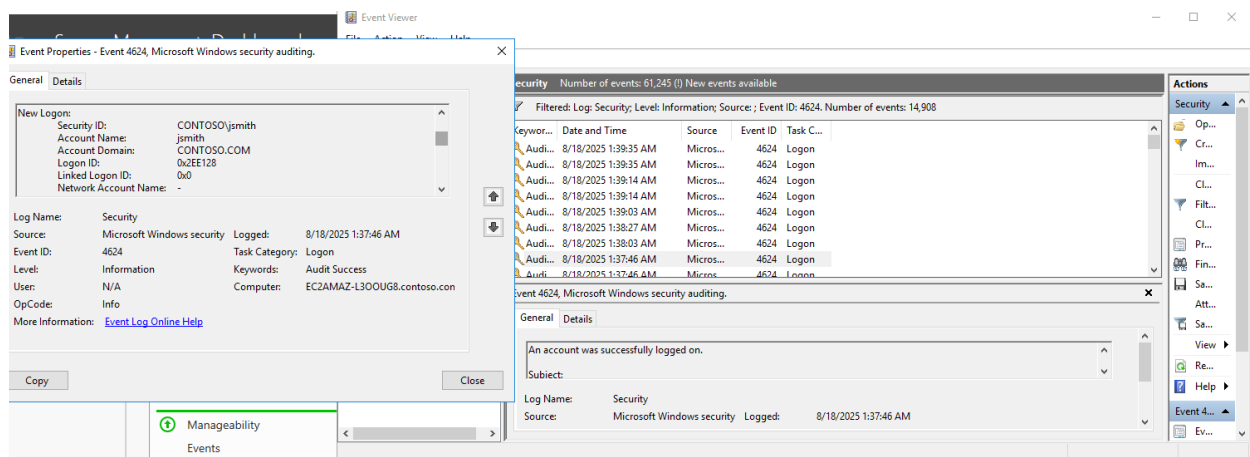


Figure 25: Event 4624 details — New Logon and Network Information.

STEP 8

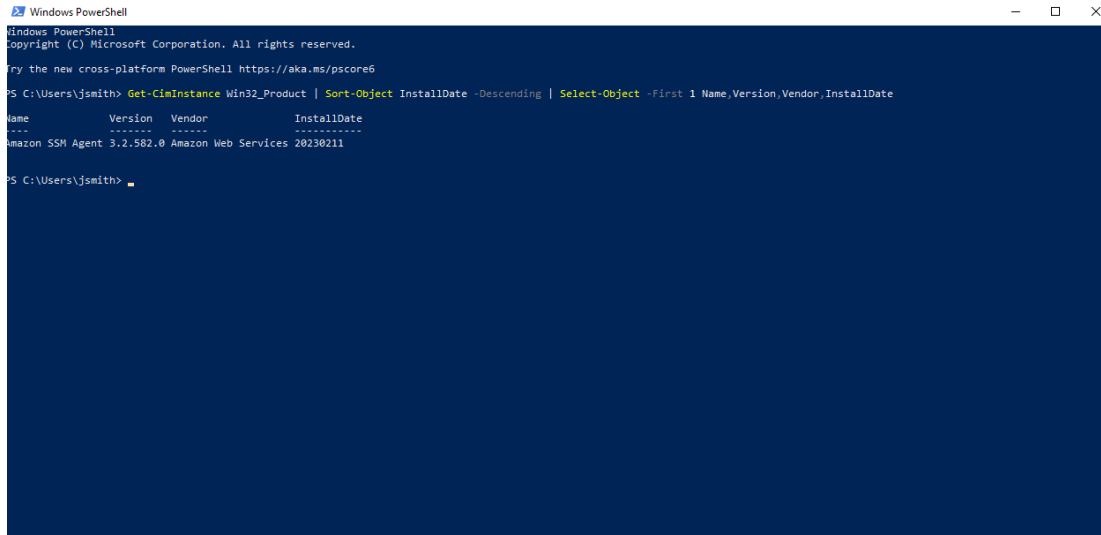
8.1 Open PowerShell

1. Click **Start**, type **PowerShell**, right-click **Windows PowerShell** → **Run as administrator**.
2. Confirm the blue console opens.

8.2 WMI

Command (type exactly):

```
Get-CimInstance Win32_Product | Sort-Object InstallDate -Descending | Select-Object -First 1 Name,Version,Vendor,InstallDate
```



The screenshot shows a Windows PowerShell window with the following text:

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\jsmith> Get-CimInstance Win32_Product | Sort-Object InstallDate -Descending | Select-Object -First 1 Name,Version,Vendor,InstallDate

Name                Version  Vendor              InstallDate
-----
Amazon SSM Agent 3.2.582.0 Amazon Web Services 20230211

PS C:\Users\jsmith> _
```

Figure 26: PowerShell of Last Installed Package

Output:

```
PS C:\Users\jsmith> Get-CimInstance Win32_Product | Sort-Object InstallDate -Descending |
Select-Object -First 1 Name,Version,Vendor,InstallDate
```

Name	Version	Vendor	InstallDate
Amazon SSM Agent	3.2.582.0	Amazon Web Services	20230211

STEP 9 — List All Running Services to a File

Goal

Generate a list of all **running** Windows services and save it to `running_services.txt` on the signed-in user's Desktop.

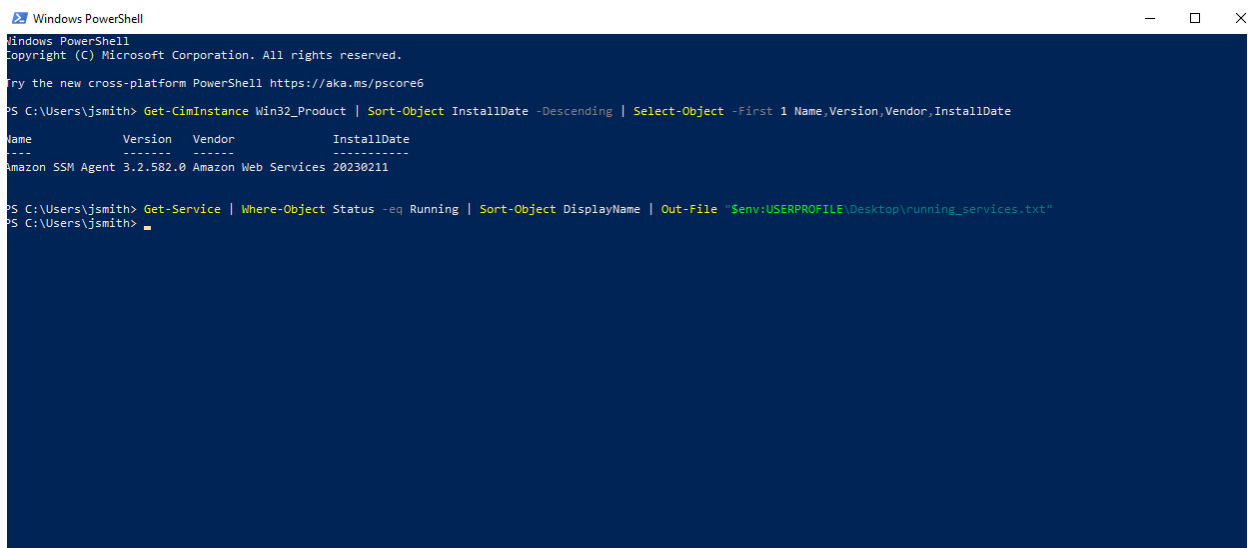
Where

Client workstation (e.g., **DESKTOP-2**) → **Windows PowerShell**

9.1 Run the command

1. Open **Start** → **Windows PowerShell** (normal window is fine).
2. Type the following **single line** and press **Enter**:

```
Get-Service | Where-Object Status -eq Running | Sort-Object DisplayName | Out-File  
"$env:USERPROFILE\Desktop\running_services.txt"
```



The screenshot shows a Windows PowerShell window with the following content:

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

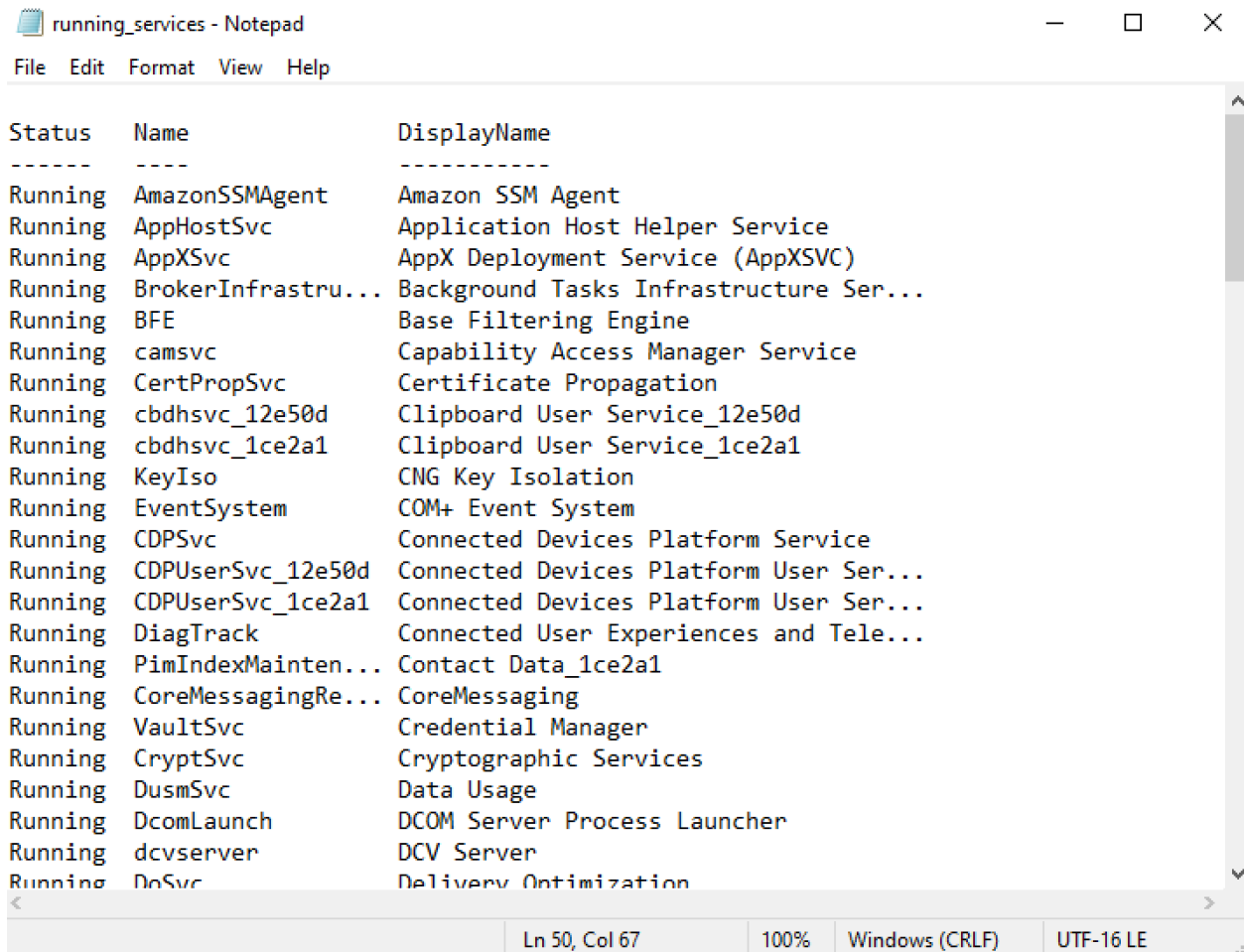
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\jsmith> Get-CimInstance Win32_Product | Sort-Object InstallDate -Descending | Select-Object -First 1 Name,Version, Vendor, InstallDate

Name          Version  Vendor          InstallDate
----          -
Amazon SSH Agent 3.2.502.0 Amazon Web Services 20230211

PS C:\Users\jsmith> Get-Service | Where-Object Status -eq Running | Sort-Object DisplayName | Out-File "$env:USERPROFILE\Desktop\running_services.txt"
PS C:\Users\jsmith>
```

Figure 27: PowerShell Script to List All Running Processes



```

running_services - Notepad
File Edit Format View Help

Status      Name                DisplayName
-----
Running     AmazonSSMAgent      Amazon SSM Agent
Running     AppHostSvc           Application Host Helper Service
Running     AppXSvc              AppX Deployment Service (AppXSVC)
Running     BrokerInfrastru...   Background Tasks Infrastructure Ser...
Running     BFE                  Base Filtering Engine
Running     camsvc               Capability Access Manager Service
Running     CertPropSvc          Certificate Propagation
Running     cbdhsvc_12e50d       Clipboard User Service_12e50d
Running     cbdhsvc_1ce2a1       Clipboard User Service_1ce2a1
Running     KeyIso               CNG Key Isolation
Running     EventSystem          COM+ Event System
Running     CDPSvc               Connected Devices Platform Service
Running     CDPUserSvc_12e50d    Connected Devices Platform User Ser...
Running     CDPUserSvc_1ce2a1    Connected Devices Platform User Ser...
Running     DiagTrack            Connected User Experiences and Tele...
Running     PimIndexMainten...   Contact Data_1ce2a1
Running     CoreMessagingRe...   CoreMessaging
Running     VaultSvc             Credential Manager
Running     CryptSvc             Cryptographic Services
Running     DusmSvc              Data Usage
Running     DcomLaunch           DCOM Server Process Launcher
Running     dcvserver            DCV Server
Running     DnSvc                Delivery Optimization

```

Ln 50, Col 67 100% Windows (CRLF) UTF-16 LE

Figure 28: running_services.txt