ONBOARDING RUNBOOK

Name of new hire: Rufus Belcher
Non-tech role (recruiter, sales, social media, etc): Payroll
Department: HR

Step 1: On Desktop-2
Join a computer to a domain; Parts A & B

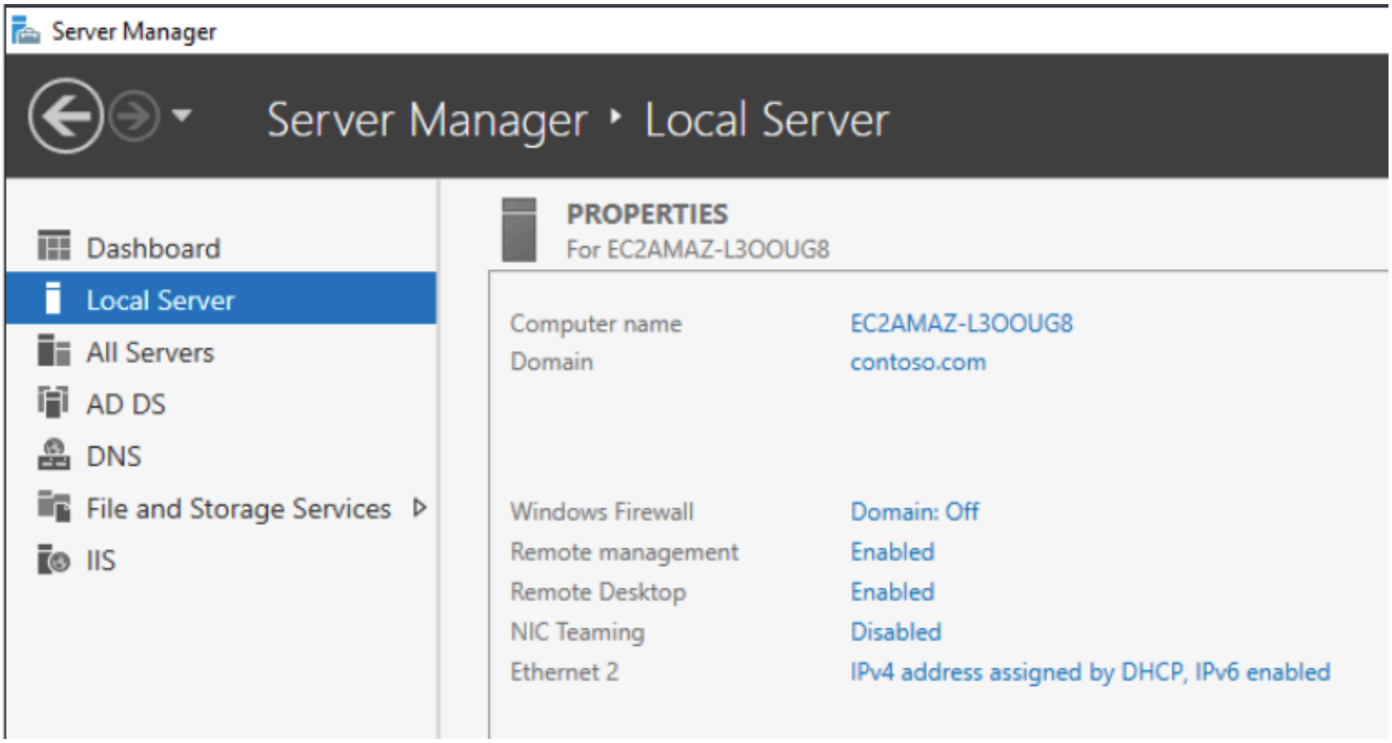
Note: Domain name can be found on the Server through this path - Start Menu; Server Manager app. Once opened, choose Local Server in the left navigation pane, which will list the properties of the server. Domain name is listed under computer name.

A) Open control panel; network and internet, network and sharing center; (left nav pane) change adapter settings; R click on network and select properties; double click "Internet Protocol Version 4 (TCP/IPv4)"; choose radio button "use the following DNS server addresses"; input preferred DNS server IPv4 address; choose okay to continue

B) Open control panel; system and security; system; (Related Settings section) advanced system settings; computer name tab; select change; "member of" domain radio button; enter domain name; enter username and password to confirm; save and close all files, folders, and windows; restart computer to apply changes.

"Un-domain" a computer to a domain
Change/Un-domain system: control panel, system and security, advanced system settings, computer name tab, change button, select Workgroup radio button, type "workgroup", select ok, select ok to confirm pop up message ("After you leave the domain…"), select ok to "Welcome…" message, select ok to restart computer and apply changes, save and close any files or programs, then select "restart now".

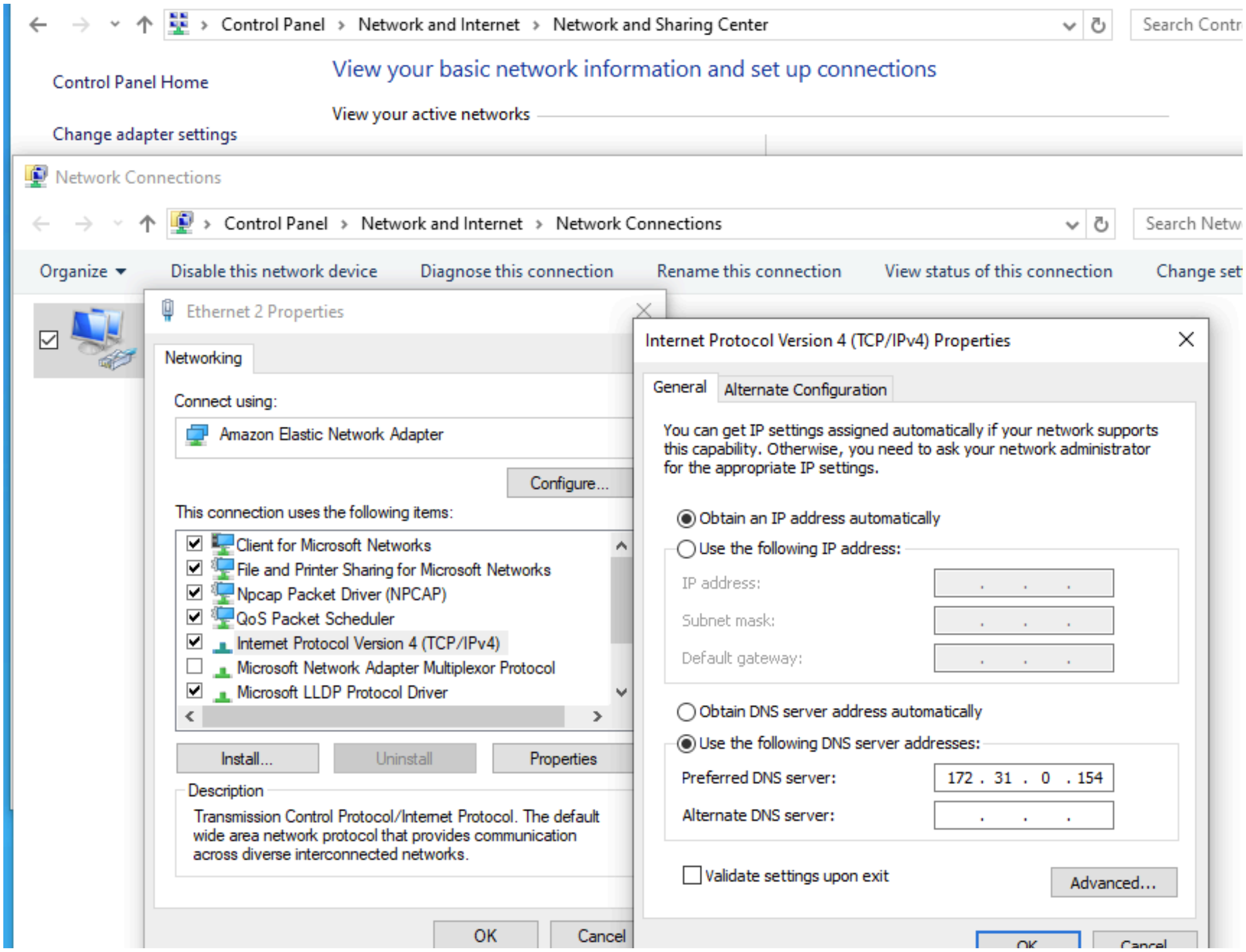
*Domain name image



PROPERTIES
For EC2AMAZ-L3OOUG8

Computer name	EC2AMAZ-L3OOUG8
Domain	contoso.com
Windows Firewall	Domain: Off
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet 2	IPv4 address assigned by DHCP, IPv6 enabled

Step 1 (cont'd)



View your basic network information and set up connections

View your active networks

Connect using:

Amazon Elastic Network Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

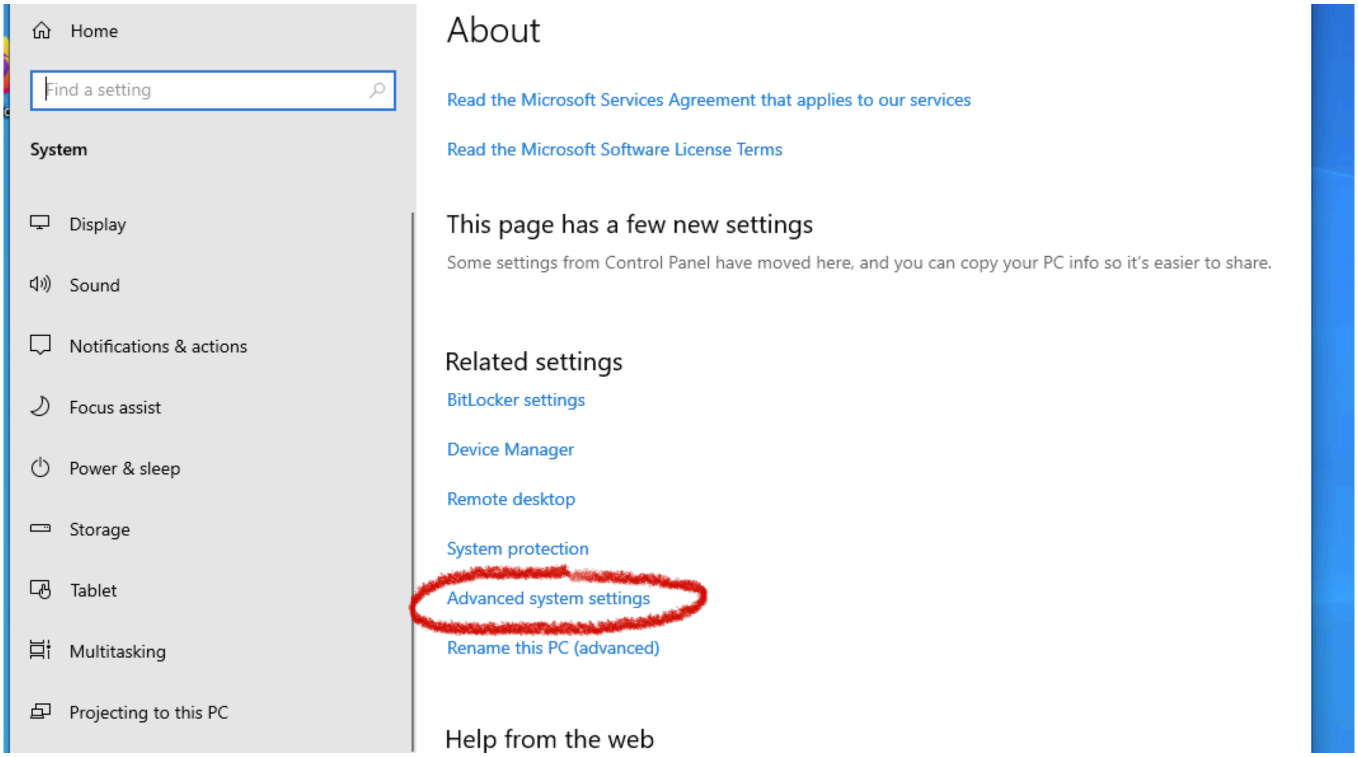
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 31 . 0 . 154

Alternate DNS server: . . .

□ Validate settings upon exit



About

Read the Microsoft Services Agreement that applies to our services

Read the Microsoft Software License Terms

This page has a few new settings

Some settings from Control Panel have moved here, and you can copy your PC info so it's easier to share.

Related settings

BitLocker settings

Device Manager

Remote desktop

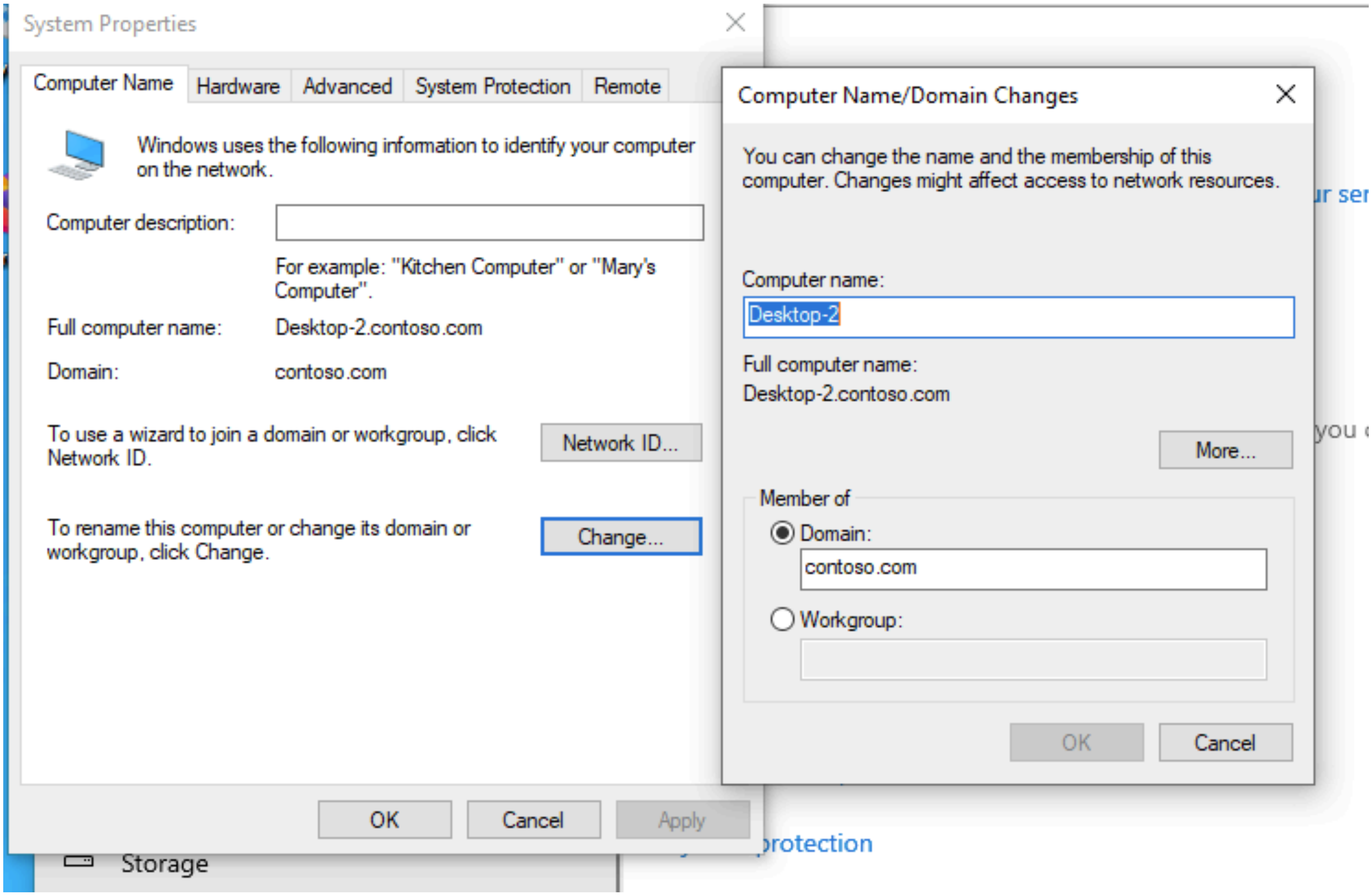
System protection

Advanced system settings

Rename this PC (advanced)

Help from the web

Step 1 (cont’d)



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Desktop-2.contoso.com

Domain: contoso.com

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: Desktop-2

Full computer name: Desktop-2.contoso.com

Member of

● Domain: contoso.com

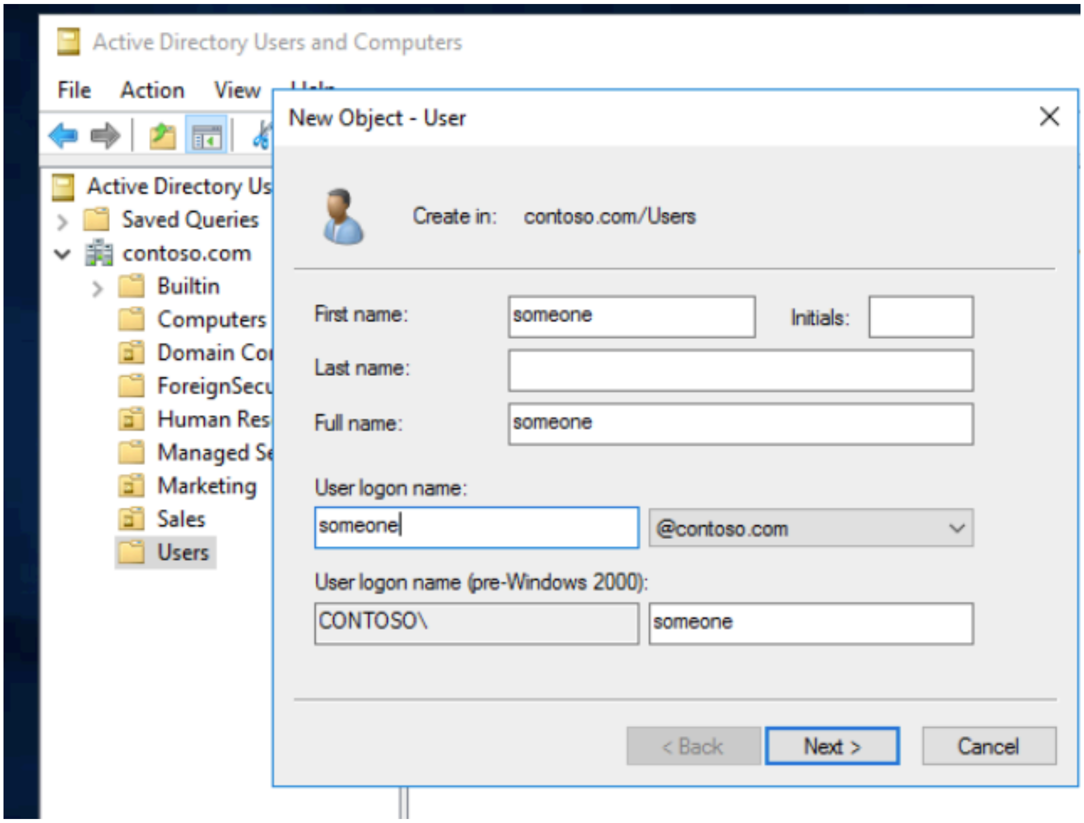
○ Workgroup:

Step 2: On Server and Desktop-2

Create a user for the new hire and set a password

Start Menu; Active Directory Users and Computers (ADUC); R click on Users folder, select New User; use the wizard and fill in the New Object - User form including the username and password; check/uncheck appropriate boxes per SOP; click Finish to complete the process on the server side. On Desktop-2, log in as new user with password to complete the process.

Step 2 (cont'd)



Create in: contoso.com/Users

First name: someone

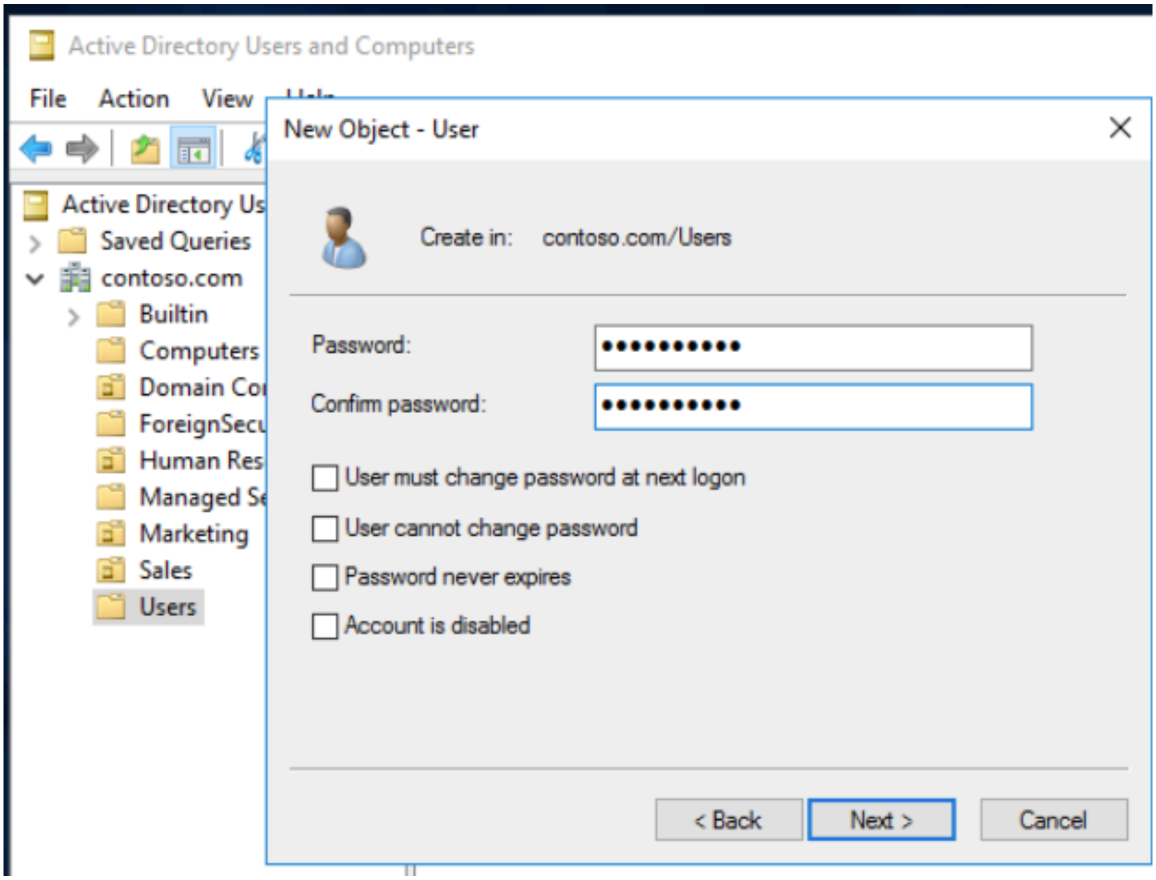
Initials:

Last name:

Full name: someone

User logon name: someone @contoso.com

User logon name (pre-Windows 2000): CONTOSO\ someone



Create in: contoso.com/Users

Password: •••••••••••

Confirm password: •••••••••••

☐ User must change password at next logon

☐ User cannot change password

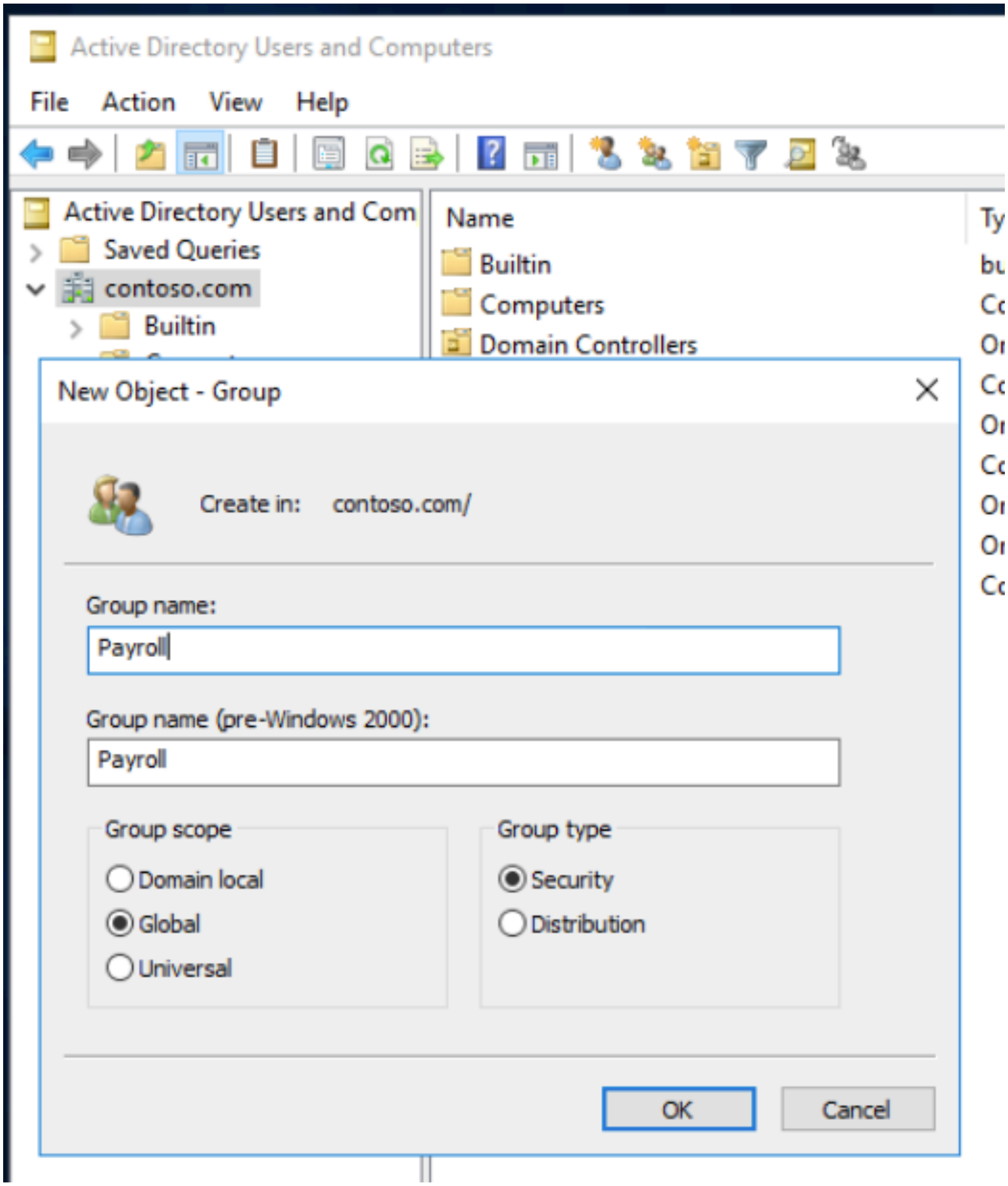
☐ Password never expires

☐ Account is disabled

Step 3: On Server

Create a group with the department name and place the user in that group

Staying in ADUC; R click and choose New Group; fill in group name; choose group scope and type per SOP; click OK



New Object - Group

Create in: contoso.com/

Group name: Payroll

Group name (pre-Windows 2000): Payroll

Group scope
○ Domain local
● Global
○ Universal

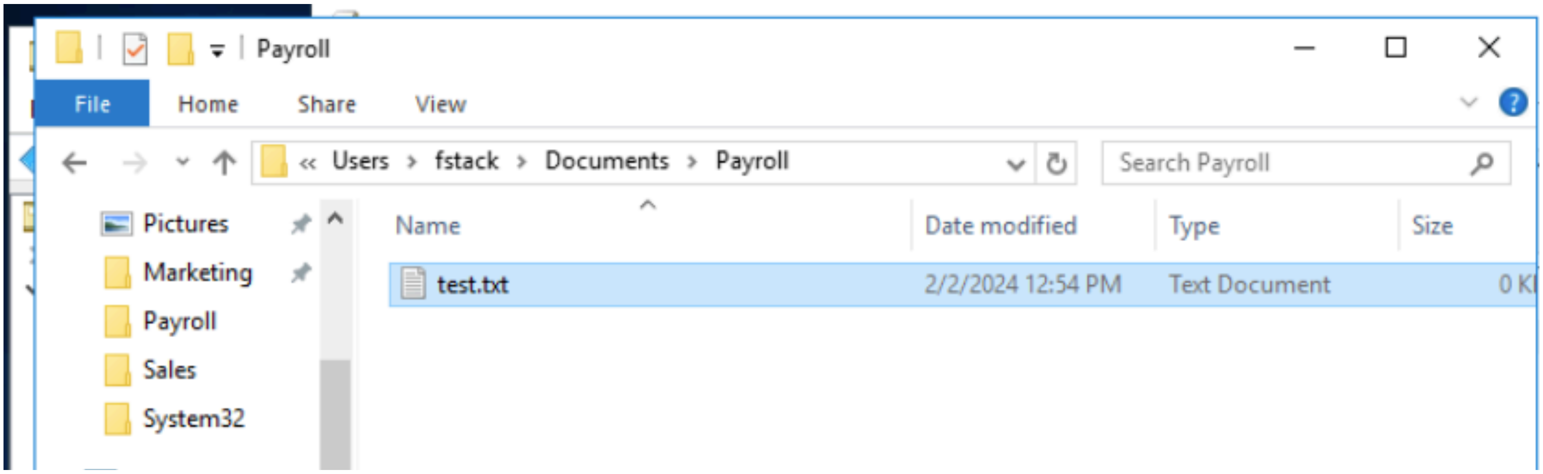
Group type
● Security
○ Distribution

Step 4: On Server

Create a share on the server with the department name and share it only with people who belong to that department (read and write permissions).
In the folder, create a text document called "test.txt".

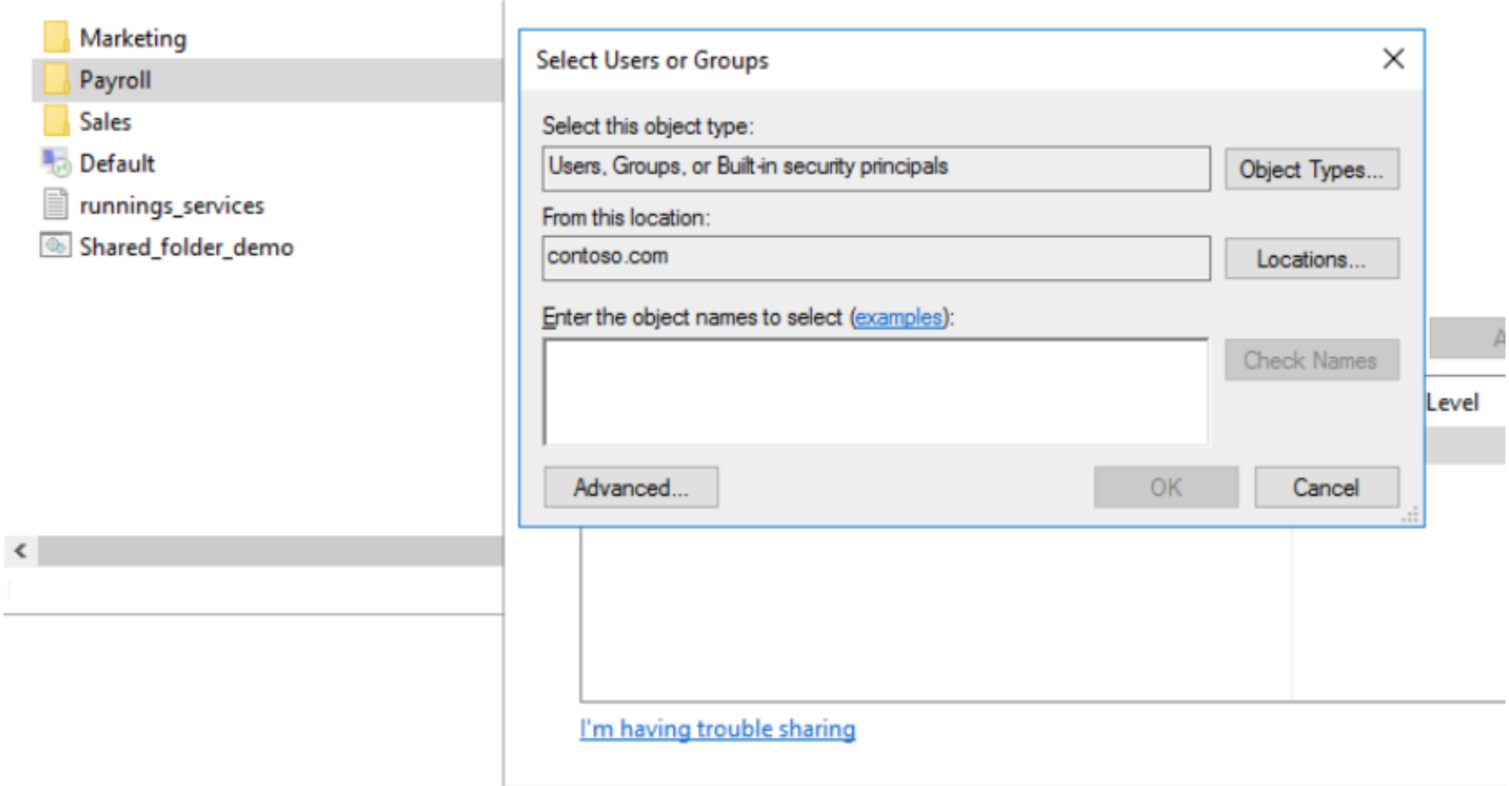
In the taskbar, open the file explorer (folder icon); choose This PC, Documents in the left nav pane; R click on the name and create a new folder labeled Payroll. R click on that folder and create a new text document titled "test.txt" without quotes. File path: C:\Users\fstack\Documents\Payroll\test.txt

R click on the Payroll folder and choose "Share with specific people"; use the drop down bar in the pop up box to find specific users to share the folder. Set the permissions per SOP/Principles of Least Privilege and click Share. You then have the option of emailing the link or copying it into another program.
Payroll (file://EC2AMAZ-L3OOUG8/Users/fstack/Documents/Payroll)



« Users › fstack › Documents › Payroll

test.txt 2/2/2024 12:54 PM Text Document 0 KB

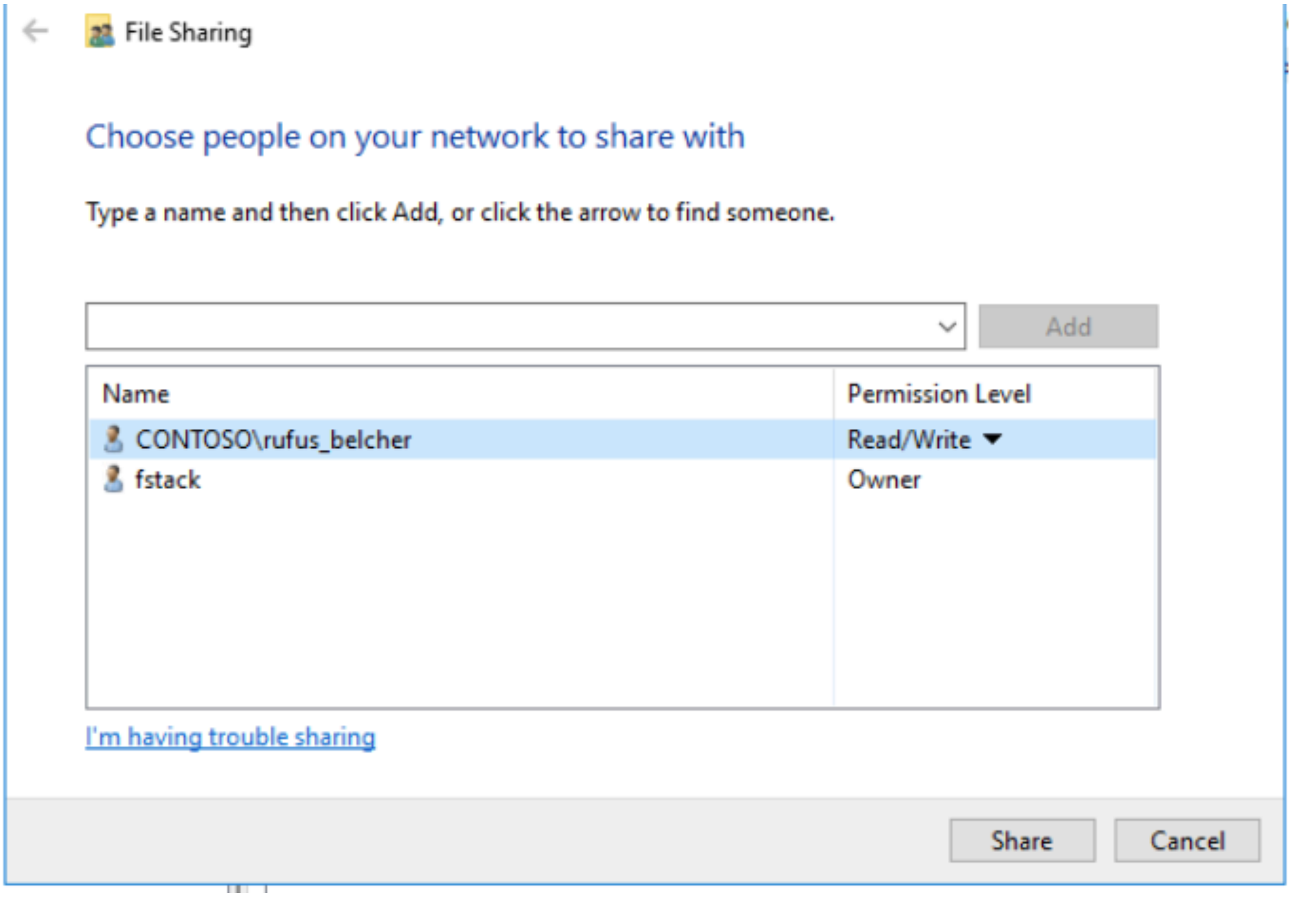


Select this object type:
Users, Groups, or Built-in security principals

From this location:
contoso.com

Enter the object names to select (examples):

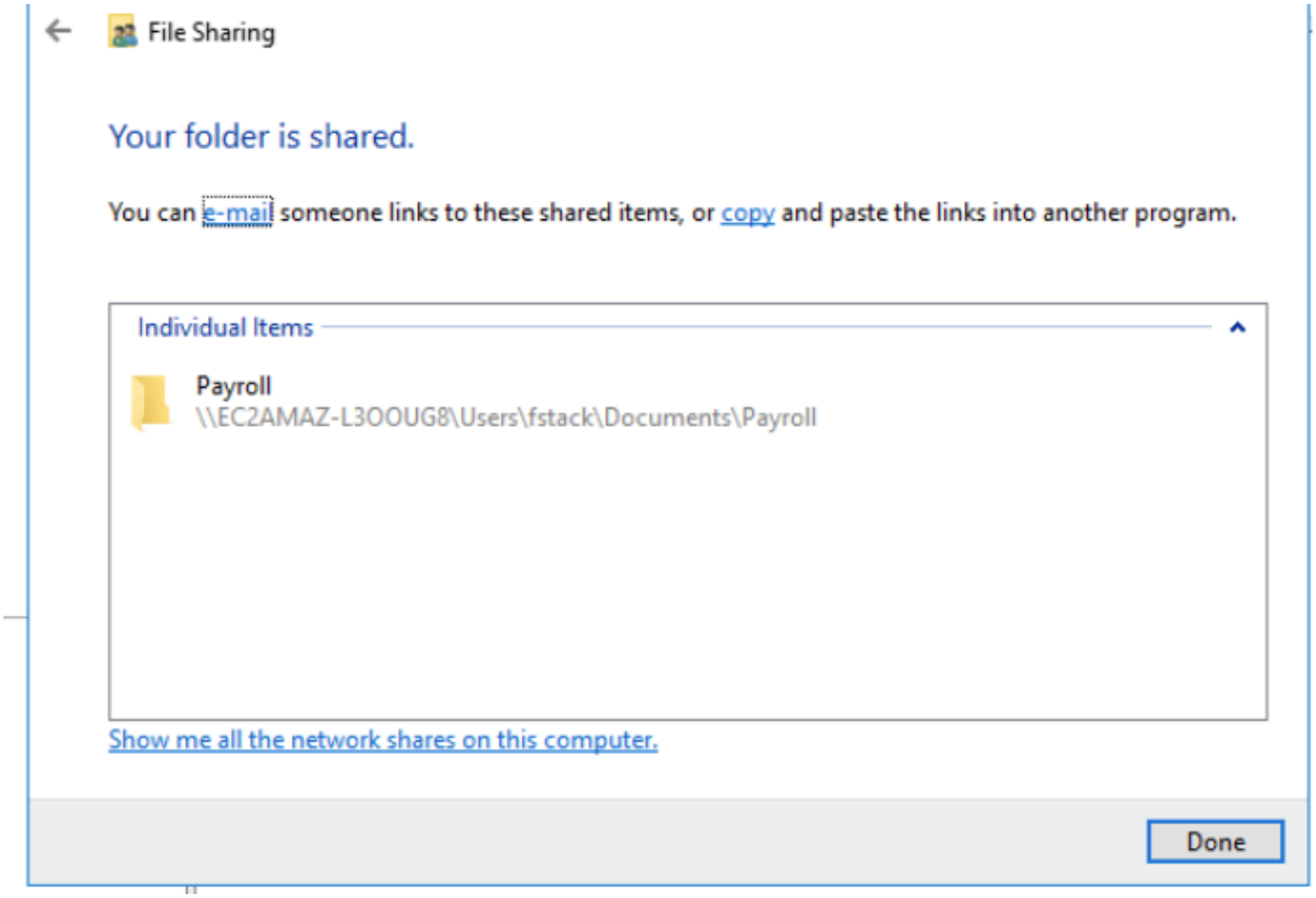
Step 4 (cont'd)



Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
CONTOSO\rufus_belcher	Read/Write ▾
fstack	Owner



Your folder is shared.

You can e-mail someone links to these shared items, or copy and paste the links into another program.

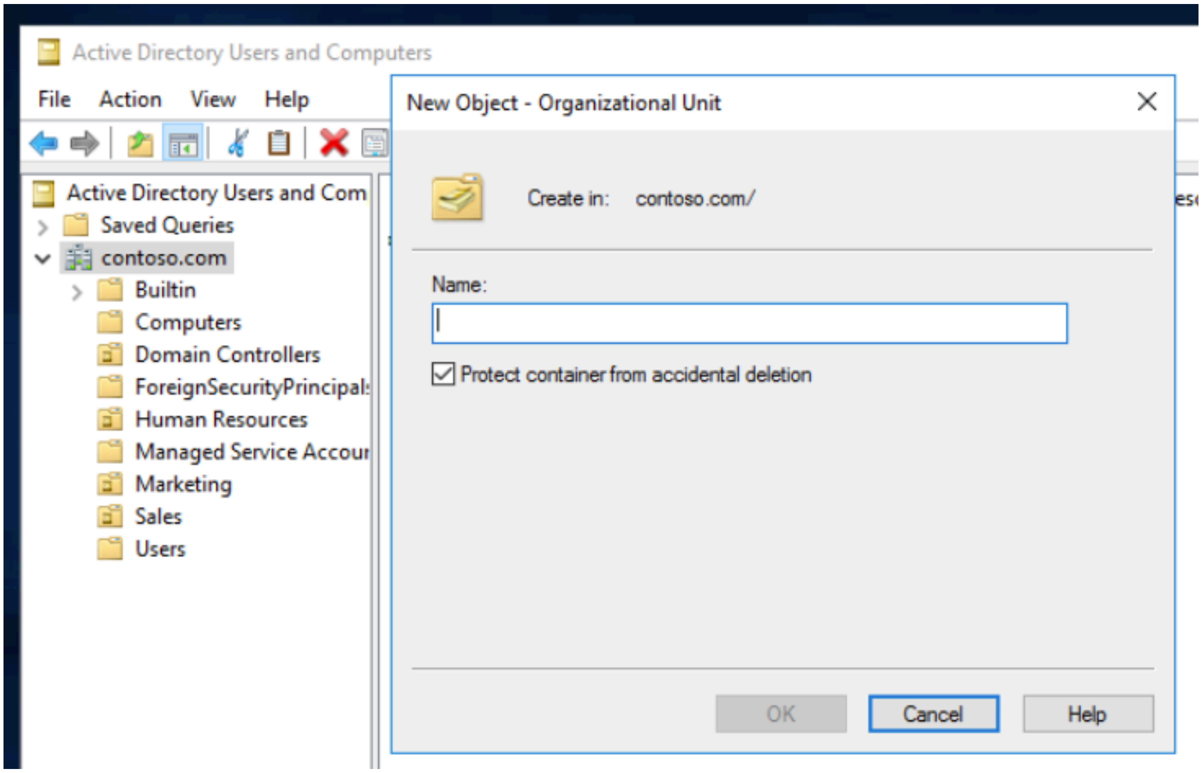
Individual Items

Payroll
\\EC2AMAZ-L3OOUG8\Users\fstack\Documents\Payroll

Step 5: On Server

Create an OU with the department's name and place the user, group, and computer in the OU. Attach a GPO to the OU you created.

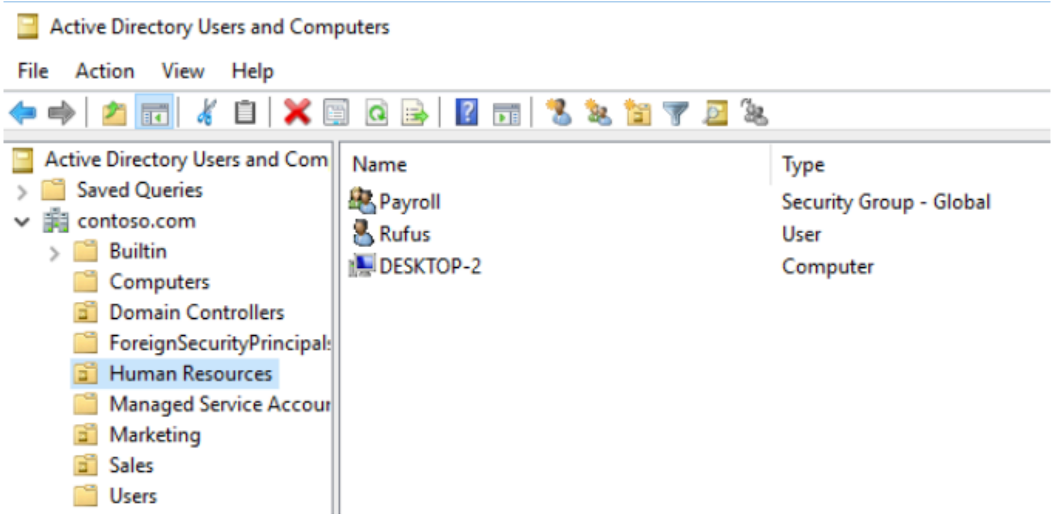
In ADUC; R click on domain name in L nav pane (1st image, shaded gray) and select new organizational unit (OU); fill in the name; check box per SOP (usually left checked); then click OK to accept name.
Drag and drop the user and group (found in Users & Computers folders, L pane) you've already created into this OU (2nd image, highlighted light blue); after each action, when asked "are you sure?", choose yes.
Attach GPO to OU: (3rd image reference) open start menu or search for group policy management app; expand domain name (3 towers icon) to find relevant OU; R click on OU folder and select Create a GPO in this domain, and Link it here…; name it and choose OK to save. The new GPO will appear in the next window and be available for configuring/editing.



Create in: contoso.com/

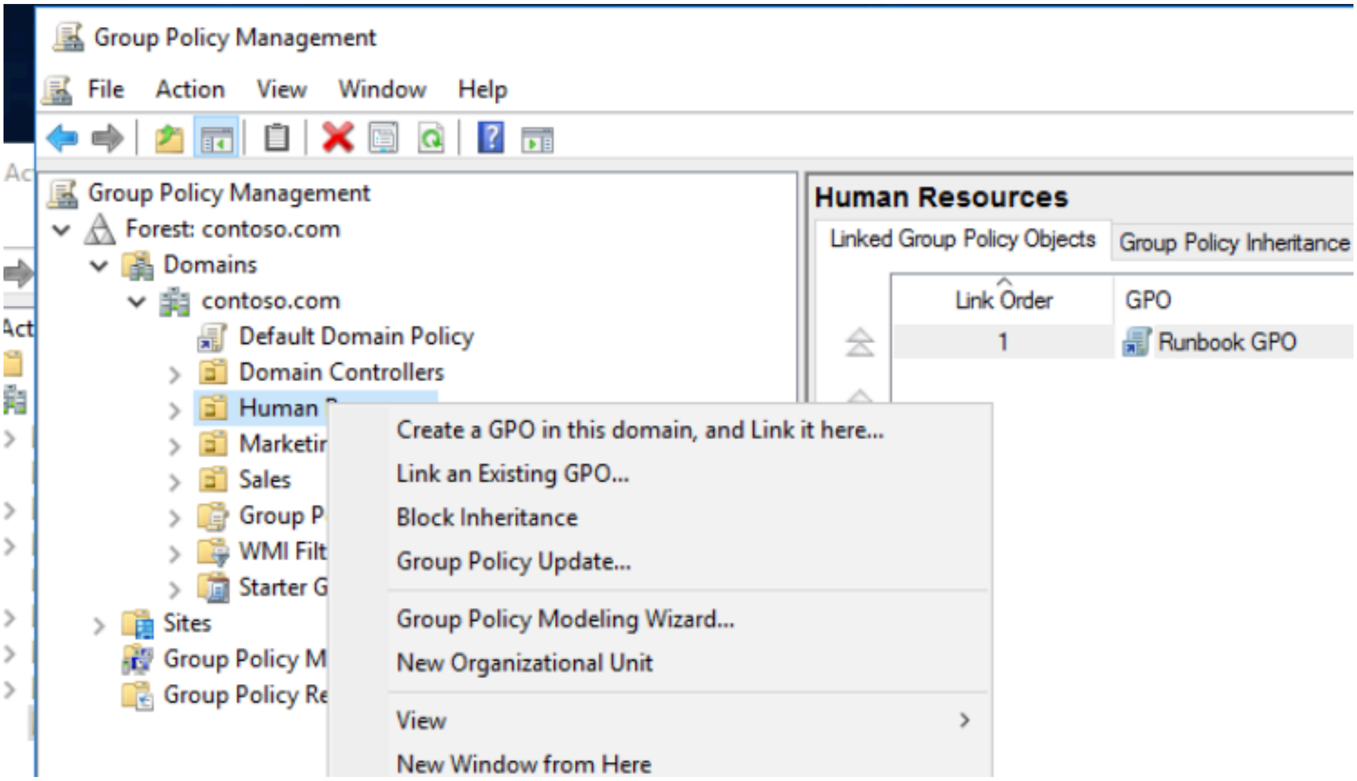
Name:

☑ Protect container from accidental deletion



Name	Type
Payroll	Security Group - Global
Rufus	User
DESKTOP-2	Computer

Step 5 (cont'd)



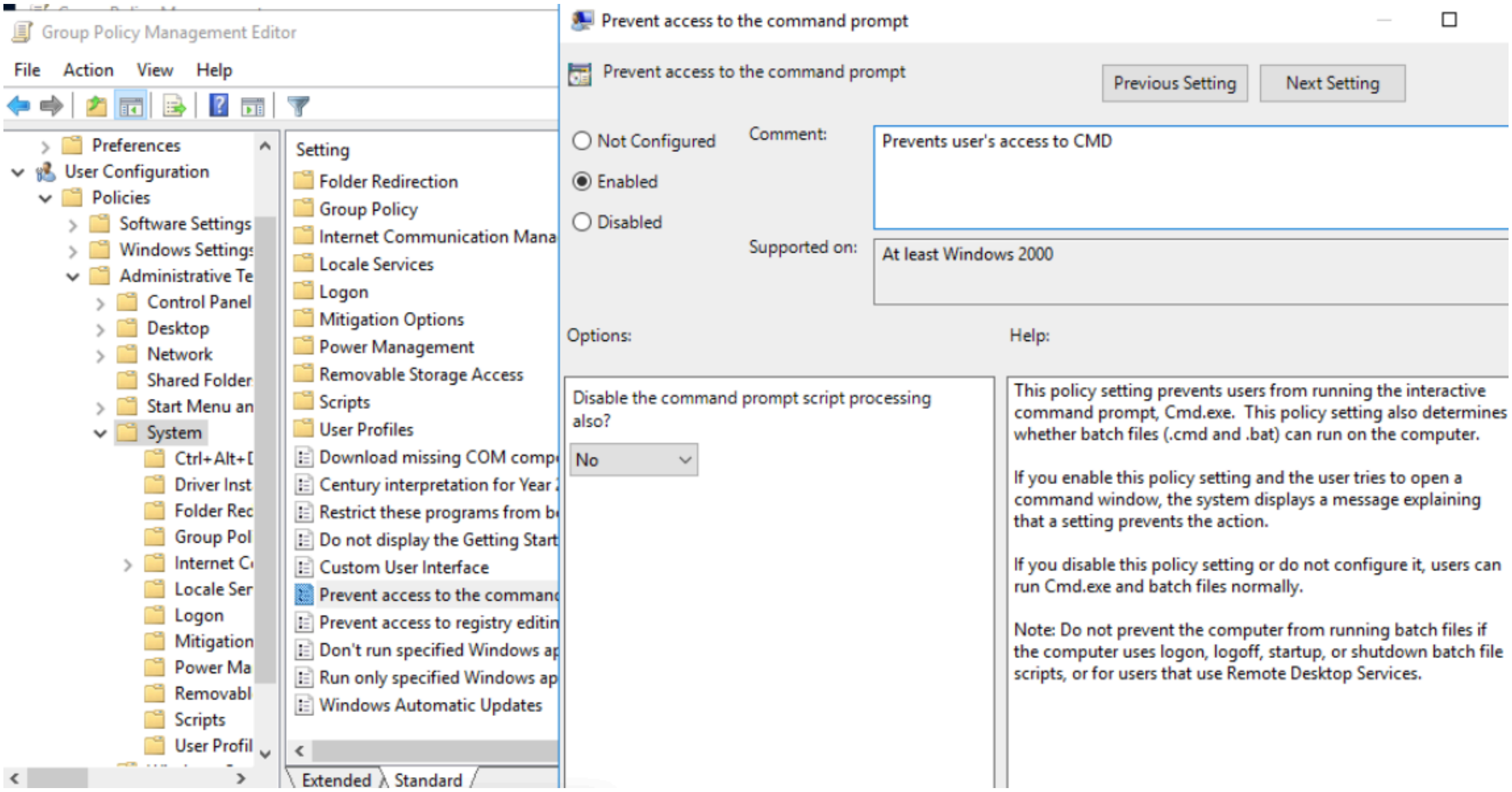
Step 6: On Server

Edit the GPO and apply the following rules:

A. Prevent the user's access to CMD.
B. Add script to the user's login to map the share you created.
C. A message should appear whenever the computer starts (do not install unauthorized programs).
D. Disable the run command from the start menu.

R click on the name of the newly created & linked GPO and select Edit. A new window pops up.

Step 6A: use the left nav pane to follow the path; User config; Policies; Admin templates; System; “Prevent access to the command prompt”. Enable the script, add any admin comments, leave Options: question set to “No”, then choose Apply to save and/or OK to close the pop up box.



Prevent access to the command prompt

○ Not Configured
● Enabled
○ Disabled

Comment: Prevents user's access to CMD

Supported on: At least Windows 2000

Options:

Disable the command prompt script processing also? No

Help:

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.

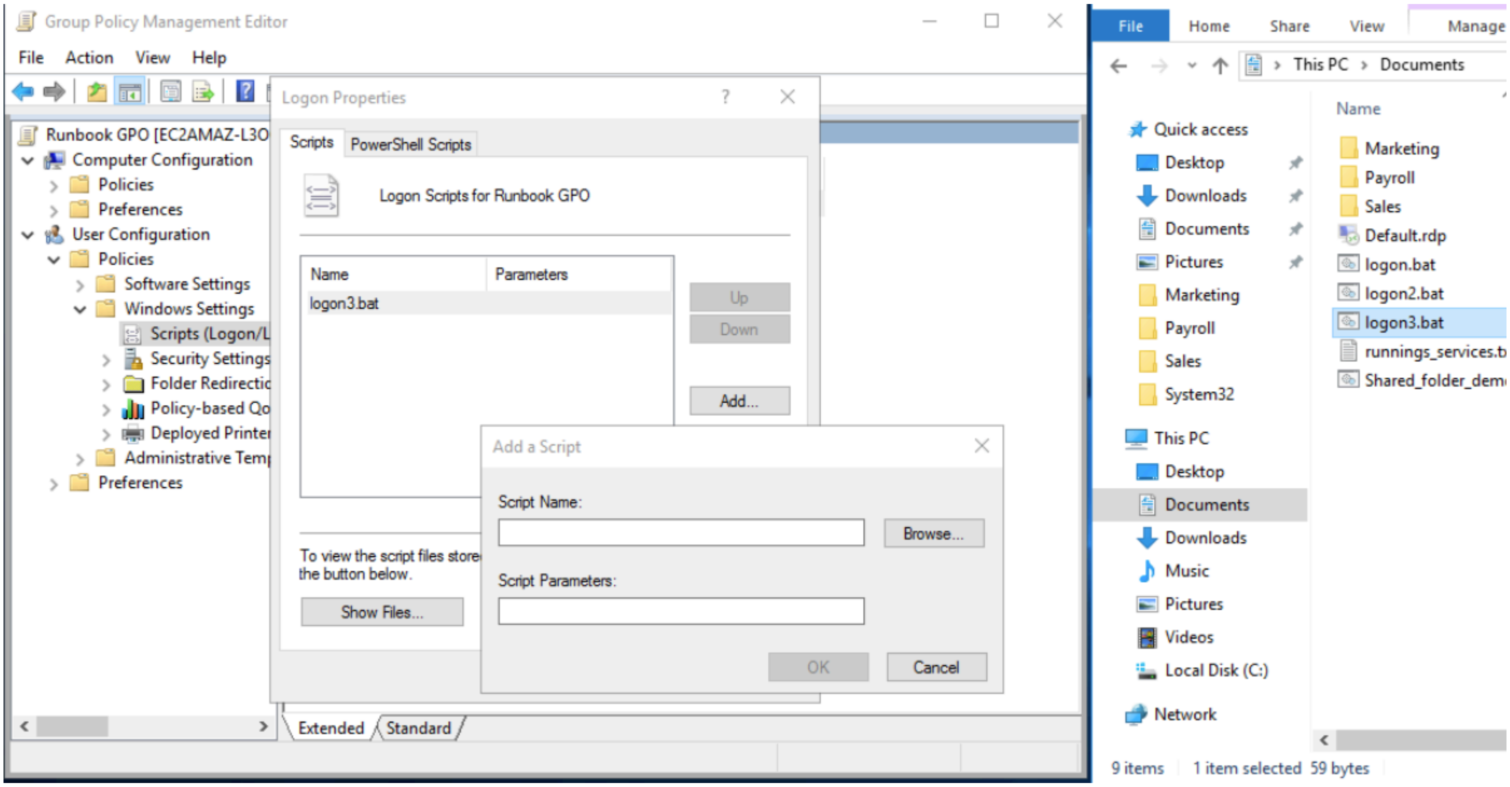
If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

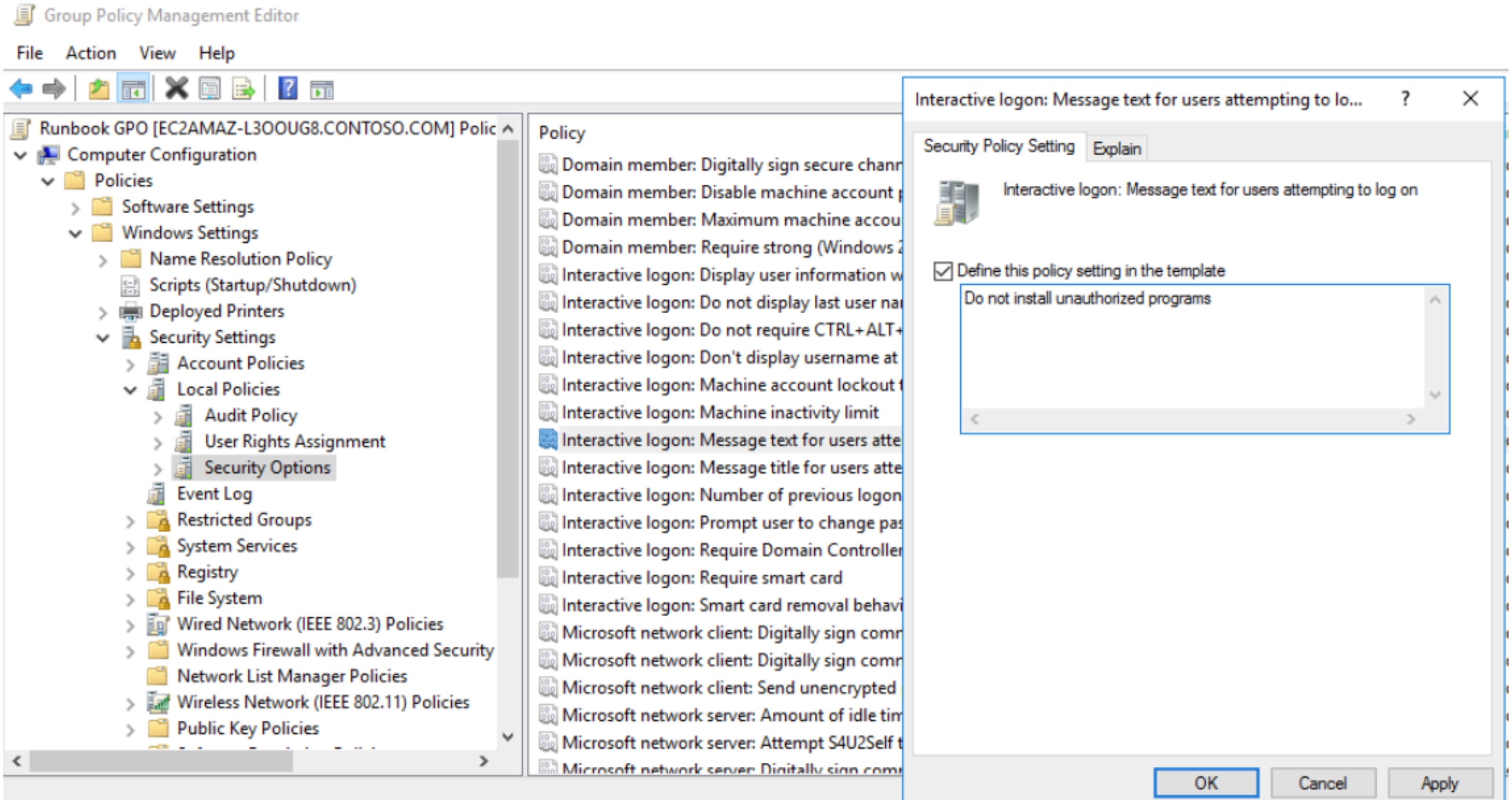
Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

Step 6B: add .bat script to user logon to map the share you created

Create logon script in notepad “net use y: \\EC2AMAZ-L3OOUG8\Users\fstack\Documents\Payroll” and save as .bat file. Navigate to logon properties in GPO using the image below. Choose Add, then Browse. In the File Explorer window Right click on script file “logon3.bat” and Paste into Script Name in Add a Script window. The script file will populate in the previous window (Add a script). Choose Apply to save and OK to close the window. Sign into Desktop-2 as rufus_belcher to confirm changes.
*optional: sign in as an admin on Desktop-2 and run “gpupdate /force”



Step
6C: Use left pane to follow path; Computer config; Policies; Window Settings; Security Settings; Local Policies; “Interactive logon: Message text….”; edit message to “Do not install unauthorized programs.”; choose Apply to save then OK to close window.


Group Policy Management Editor
File
Action
View
Help
Runbook GPO [EC2AMAZ-L3OOUG8.CONTOSO.COM] Polic
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Policy
Domain member: Digitally sign secure chann
Domain member: Disable machine account
Domain member: Maximum machine accou
Domain member: Require strong (Windows
Interactive logon: Display user information w
Interactive logon: Do not display last user na
Interactive logon: Do not require CTRL+ALT+
Interactive logon: Don't display username at
Interactive logon: Machine account lockout
Interactive logon: Machine inactivity limit
Interactive logon: Message text for users atte
Interactive logon: Message title for users atte
Interactive logon: Number of previous logon
Interactive logon: Prompt user to change pa
Interactive logon: Require Domain Controlle
Interactive logon: Require smart card
Interactive logon: Smart card removal behavi
Microsoft network client: Digitally sign comr
Microsoft network client: Digitally sign comr
Microsoft network client: Send unencrypted
Microsoft network server: Amount of idle tim
Microsoft network server: Attempt S4U2Self
Microsoft network server: Digitally sign comr
Security Policy Setting
Explain
OK
Cancel
Apply

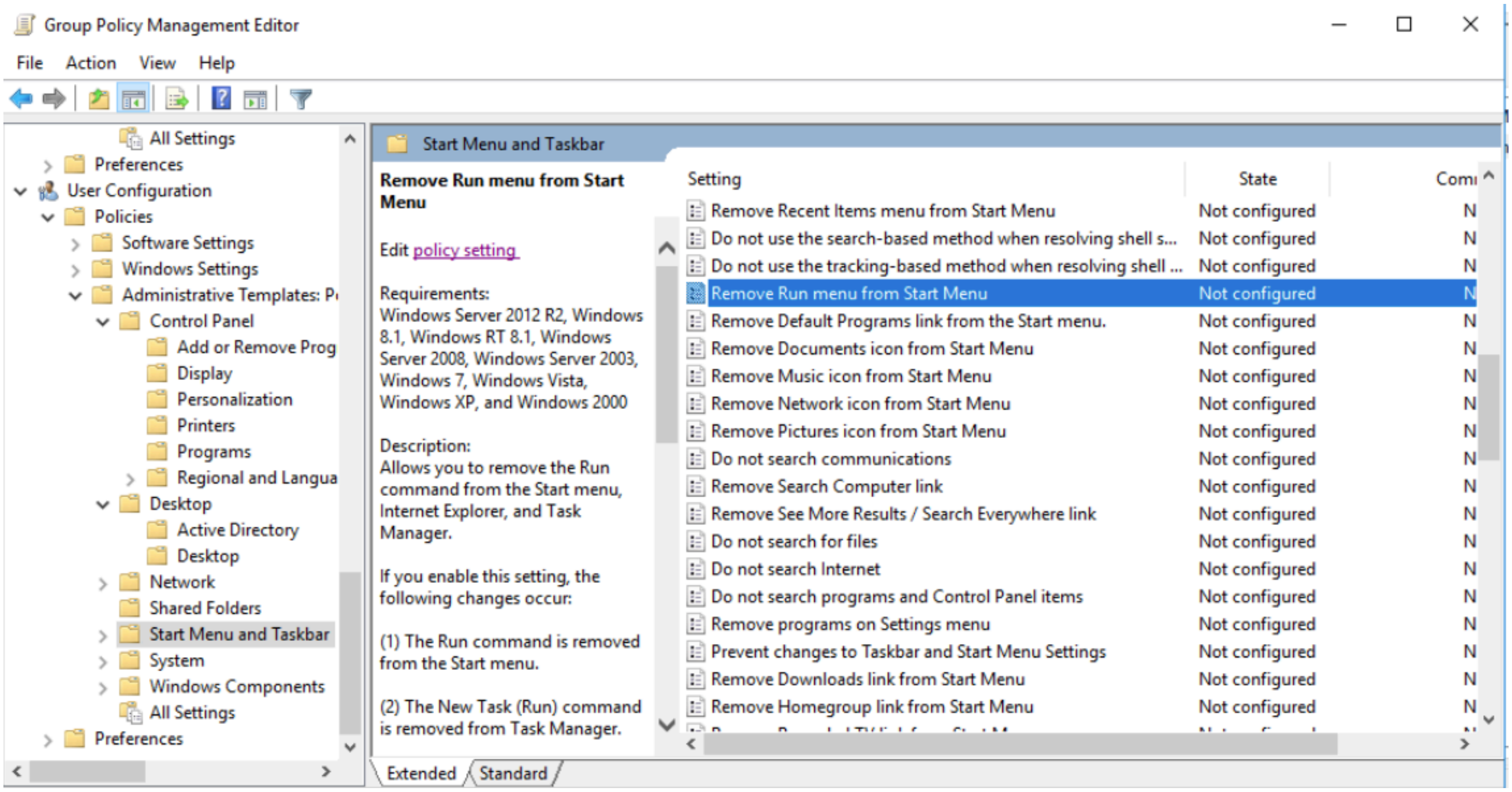
Interactive logon: Message text for users attempting to lo...

Interactive logon: Message text for users attempting to log on

☑ Define this policy setting in the template

Do not install unauthorized programs

Step 6D: Use the left nav pane to follow the path; User config; Policies; Admin templates; Start Menu and Taskbar; “Remove Run menu from Start Menu”. Enable the script, add any admin comments, then choose Apply to save and/or OK to close the pop up box.



Start Menu and Taskbar

Remove Run menu from Start Menu

Edit policy setting

Requirements:
Windows Server 2012 R2, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, Windows XP, and Windows 2000

Description:
Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager.

If you enable this setting, the following changes occur:

(1) The Run command is removed from the Start menu.

(2) The New Task (Run) command is removed from Task Manager.

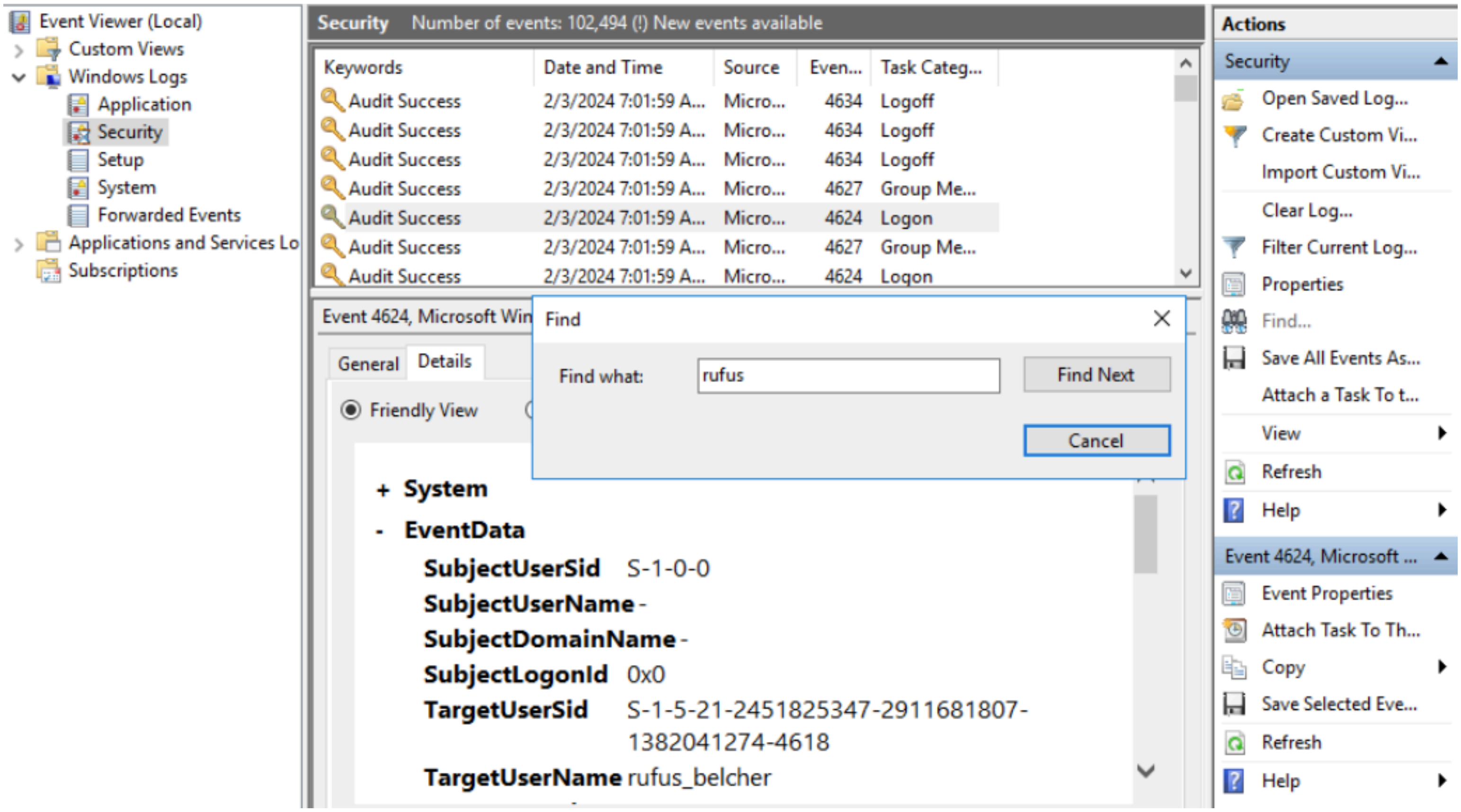
Setting	State	Comi
Remove Recent Items menu from Start Menu	Not configured	N
Do not use the search-based method when resolving shell s...	Not configured	N
Do not use the tracking-based method when resolving shell ...	Not configured	N
Remove Run menu from Start Menu	Not configured	N
Remove Default Programs link from the Start menu.	Not configured	N
Remove Documents icon from Start Menu	Not configured	N
Remove Music icon from Start Menu	Not configured	N
Remove Network icon from Start Menu	Not configured	N
Remove Pictures icon from Start Menu	Not configured	N
Do not search communications	Not configured	N
Remove Search Computer link	Not configured	N
Remove See More Results / Search Everywhere link	Not configured	N
Do not search for files	Not configured	N
Do not search Internet	Not configured	N
Do not search programs and Control Panel items	Not configured	N
Remove programs on Settings menu	Not configured	N
Prevent changes to Taskbar and Start Menu Settings	Not configured	N
Remove Downloads link from Start Menu	Not configured	N
Remove Homegroup link from Start Menu	Not configured	N

Step 7: On Server:

Check the Event Viewer on the server machine and write down the last successful login from your user. (Note: You must log in with the domain administrator account).

Run cmd as admin; type in the command “net user Administrator /active:yes” without quotes. After retrieving the required information, retype the command, replacing yes with no.

Type “event viewer” in taskbar searchbox OR start menu; windows admin tools; event viewer. Use the left pane to navigate to Windows Logs; Security. Use the right pane, find option to search for the user name. Choose find next until the middle pane “Security” shows a row wih Audit Success, Event ID 4624, and Task Category Logon. Annotate the Date and Time (see image).



Security Number of events: 102,494 (!) New events available

Keywords	Date and Time	Source	Even...	Task Categ...
Audit Success	2/3/2024 7:01:59 A...	Micro...	4634	Logoff
Audit Success	2/3/2024 7:01:59 A...	Micro...	4634	Logoff
Audit Success	2/3/2024 7:01:59 A...	Micro...	4634	Logoff
Audit Success	2/3/2024 7:01:59 A...	Micro...	4627	Group Me...
Audit Success	2/3/2024 7:01:59 A...	Micro...	4624	Logon
Audit Success	2/3/2024 7:01:59 A...	Micro...	4627	Group Me...
Audit Success	2/3/2024 7:01:59 A...	Micro...	4624	Logon

Event 4624, Microsoft Win

Find what: rufus

+ System

- EventData

SubjectUserSid S-1-0-0

SubjectUserName -

SubjectDomainName -

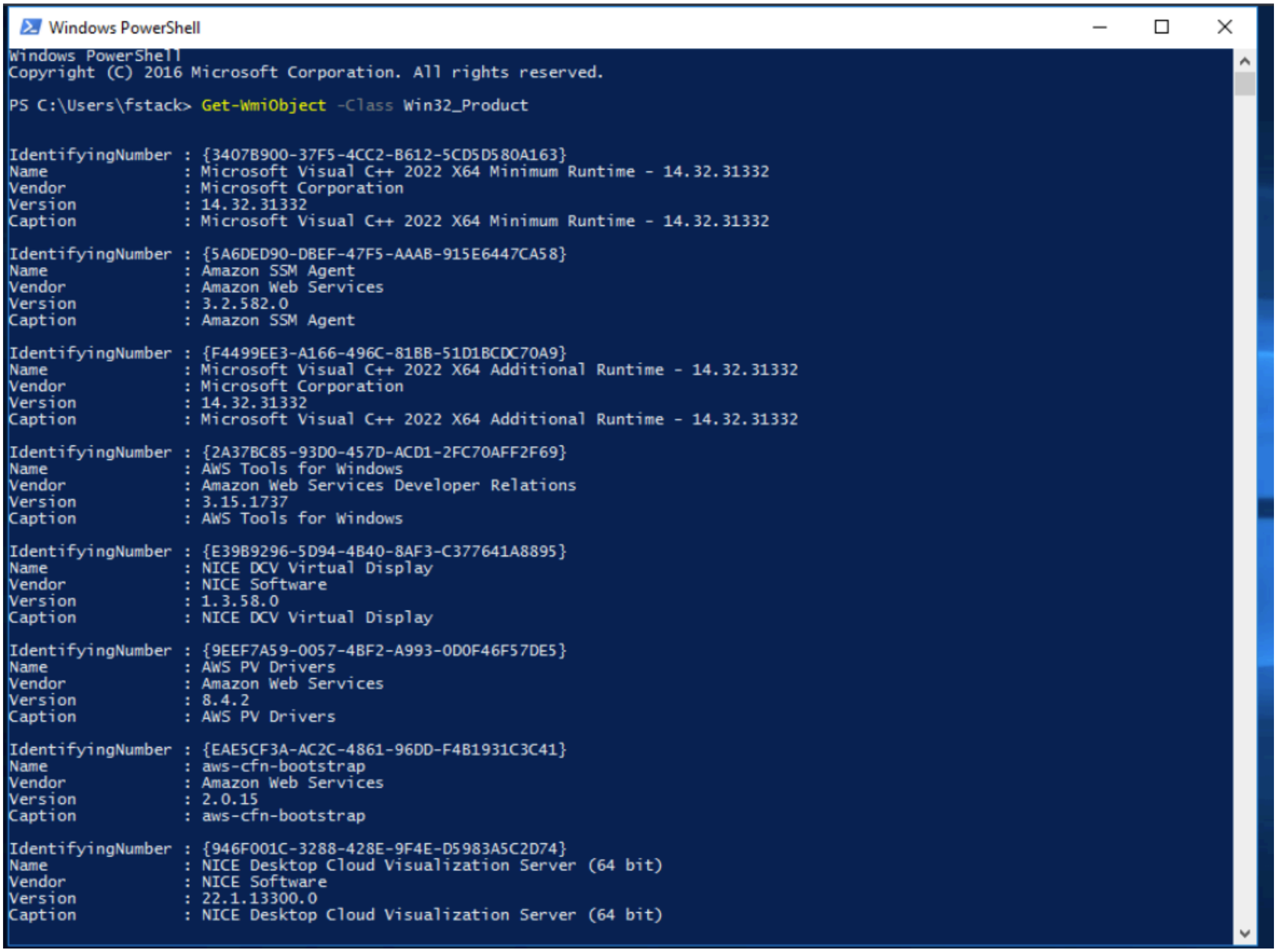
SubjectLogonId 0x0

TargetUserSid S-1-5-21-2451825347-2911681807-1382041274-4618

TargetUserName rufus_belcher

Step 8: On Desktop-2:
Check the latest program installed on the computer

Open PowerShell app: Windows icon to open Start menu; scroll to find folder labeled Windows PowerShell; OR type powershell in taskbar search box.
Type the following command, ensuring proper spelling, punctuation, spacing, and w/out quotes:
“Get-WmiObject -Class Win32_Product”; enter to run

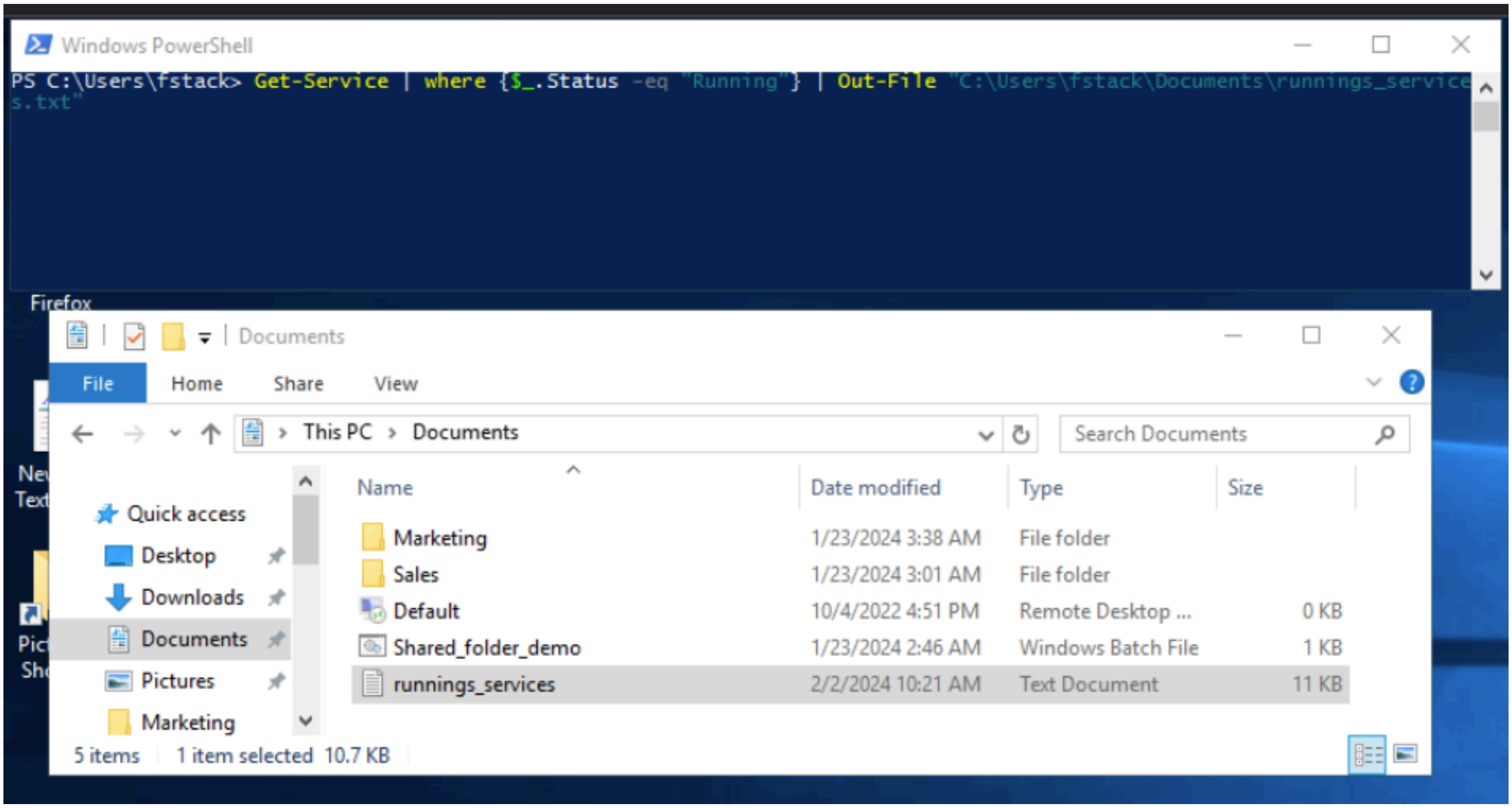


```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\fstack> 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
Version           : 1.3.58.0
Caption           : NICE DCV Virtual Display

IdentifyingNumber : {9EEF7A59-0057-4BF2-A993-0D0F46F57DE5}
Name              : AWS PV Drivers
Vendor            : Amazon Web Services
Version           : 8.4.2
Caption           : AWS PV Drivers

IdentifyingNumber : {EAE5CF3A-AC2C-4861-96DD-F4B1931C3C41}
Name              : aws-cfn-bootstrap
Vendor            : Amazon Web Services
Version           : 2.0.15
Caption           : aws-cfn-bootstrap

IdentifyingNumber : {946F001C-3288-428E-9F4E-D5983A5C2D74}
Name              : NICE Desktop Cloud Visualization Server (64 bit)
Vendor            : NICE Software
Version           : 22.1.13300.0
Caption           : NICE Desktop Cloud Visualization Server (64 bit)
```

Step 9: On Desktop-2:

Write a PowerShell script that gives a list of all running services and puts it in a file named running_services.txt

Open PowerShell and type the following script:
Get-Service | where {$_.Status -eq “Running”} | Out-File “C:\Windows\Documents\running_services.txt”

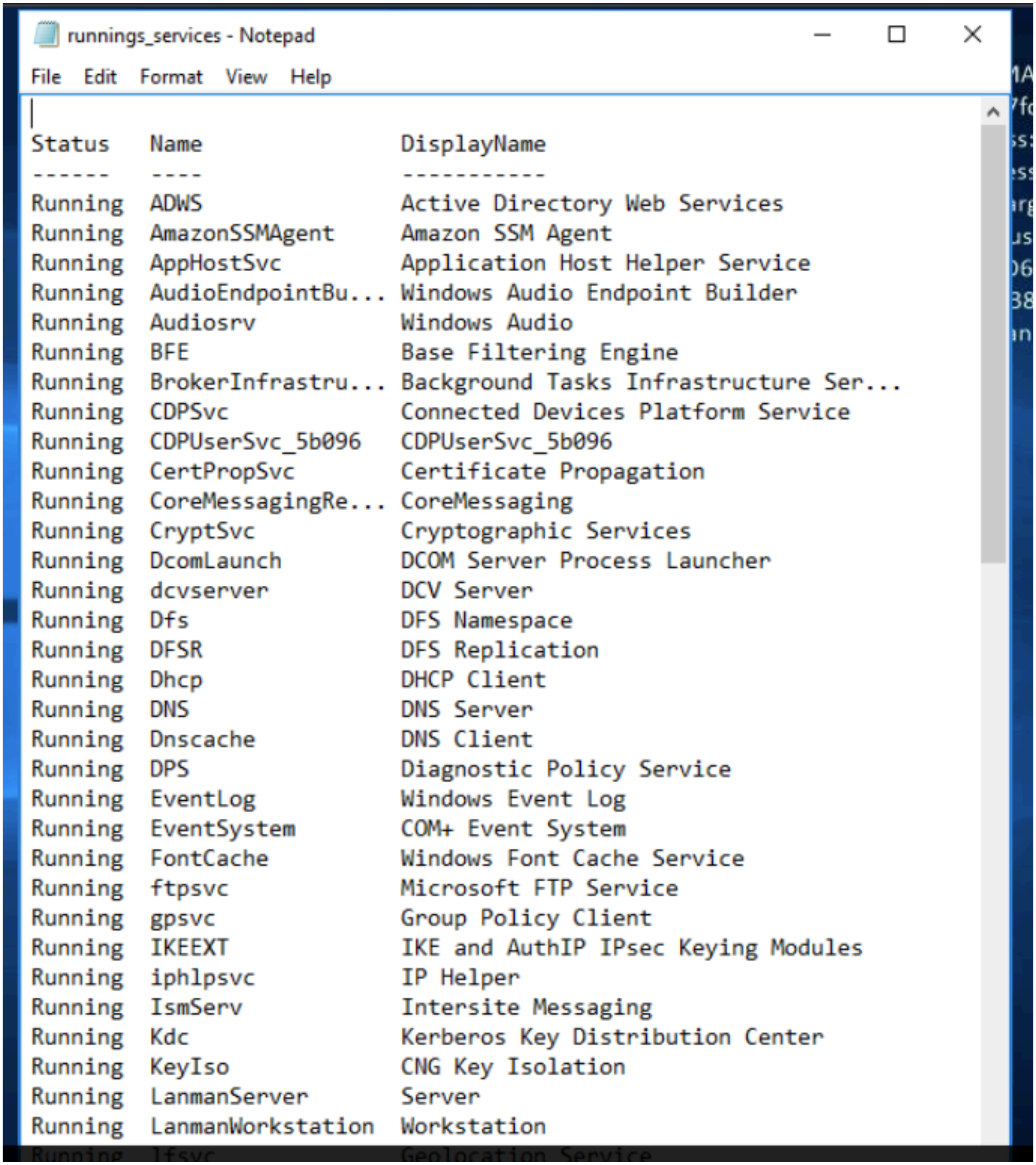


```
PS C:\Users\fstack> Get-Service | where {$_.Status -eq "Running"} | Out-File "C:\Users\fstack\Documents\runnings_service
s.txt"
```

Name	Date modified	Type	Size
Marketing	1/23/2024 3:38 AM	File folder	
Sales	1/23/2024 3:01 AM	File folder	
Default	10/4/2022 4:51 PM	Remote Desktop ...	0 KB
Shared_folder_demo	1/23/2024 2:46 AM	Windows Batch File	1 KB
runnings_services	2/2/2024 10:21 AM	Text Document	11 KB

5 items 1 item selected 10.7 KB

Step 9 (cont'd):



```
Status   Name               DisplayName
------   ----               -----------
Running  ADWS               Active Directory Web Services
Running  AmazonSSMAgent     Amazon SSM Agent
Running  AppHostSvc         Application Host Helper Service
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Running  BFE                Base Filtering Engine
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Running  CDPSvc             Connected Devices Platform Service
Running  CDPUserSvc_5b096   CDPUserSvc_5b096
Running  CertPropSvc        Certificate Propagation
Running  CoreMessagingRe... CoreMessaging
Running  CryptSvc           Cryptographic Services
Running  DcomLaunch         DCOM Server Process Launcher
Running  dcvserver          DCV Server
Running  Dfs                DFS Namespace
Running  DFSR               DFS Replication
Running  Dhcp               DHCP Client
Running  DNS                DNS Server
Running  Dnscache           DNS Client
Running  DPS                Diagnostic Policy Service
Running  EventLog           Windows Event Log
Running  EventSystem        COM+ Event System
Running  FontCache          Windows Font Cache Service
Running  ftpsvc             Microsoft FTP Service
Running  gpsvc              Group Policy Client
Running  IKEEXT             IKE and AuthIP IPsec Keying Modules
Running  iphlpsvc           IP Helper
Running  IsmServ            Intersite Messaging
Running  Kdc                Kerberos Key Distribution Center
Running  KeyIso             CNG Key Isolation
Running  LanmanServer       Server
Running  LanmanWorkstation  Workstation
Running  lfsvc              Geolocation Service
```