

Runbook

Setting up machine(s) for new hires.

Introduction:

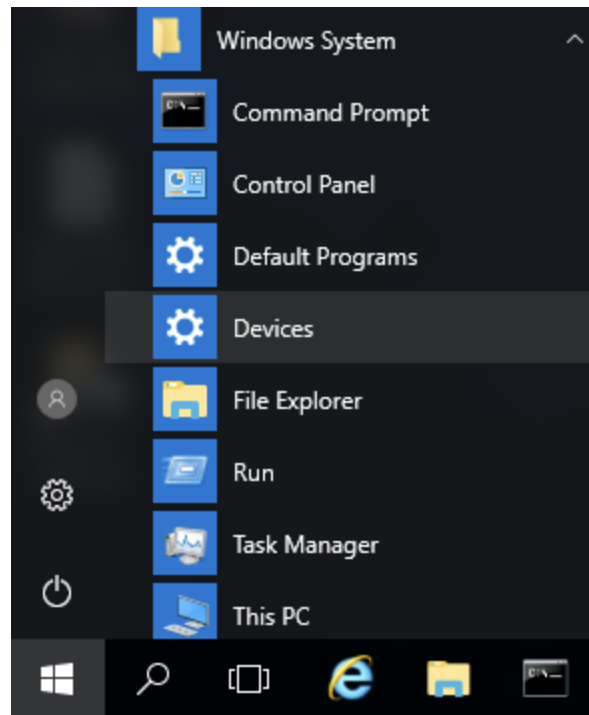
This will provide you a step by step instructions to how to add new users to the active directory, groups, organizational units, and setting up their PC. We will also go through group policies and sharing over the network.

Step 1: Joining the domain.

For step one, we'll need two virtual machines (VMs) opened, our server VM and desktop VM. On our server VM, we need to get the IPv4 address which can be found on the desktop wallpaper labeled "Private IPv4 Address:" (this may be different across different devices).



If this information is not shown or available to you, you can open the command prompt in the start menu under "Windows System"



We will then enter the command `ipconfig /all` and grab the IPv4 address.

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\fstack>ipconfig /all

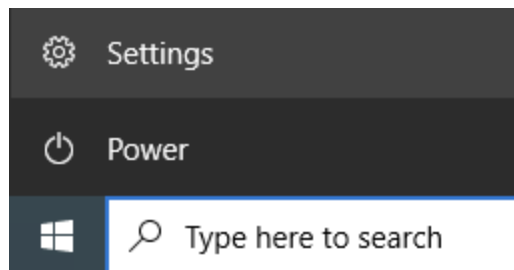
Windows IP Configuration

    Host Name . . . . . : EC2AMAZ-L300UG8
    Primary Dns Suffix . . . . . : contoso.com
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : us-west-2.ec2-utilities.amazonaws.com
                                     us-west-2.compute.internal
                                     contoso.com

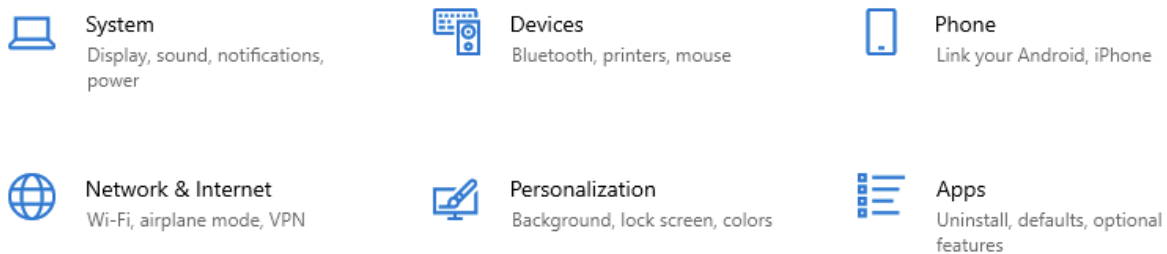
Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . : us-west-2.compute.internal
    Description . . . . . : Amazon Elastic Network Adapter
    Physical Address. . . . . : 0A-B5-55-67-0D-F5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::11dc:70ba:6ec1:9f73%2(Preferred)
    IPv4 Address. . . . . : 172.31.63.29(Preferred)
```

After grabbing that IPv4 address, we'll copy that down and switch on over to our Desktop-2 VM and go to Settings from our start menu.






From the home menu in settings, we're going to go to **Network & Internet**.

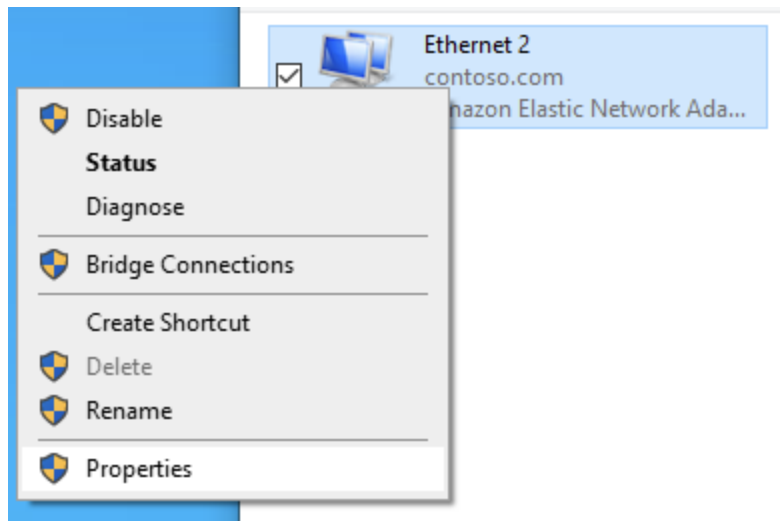


Change adapter options

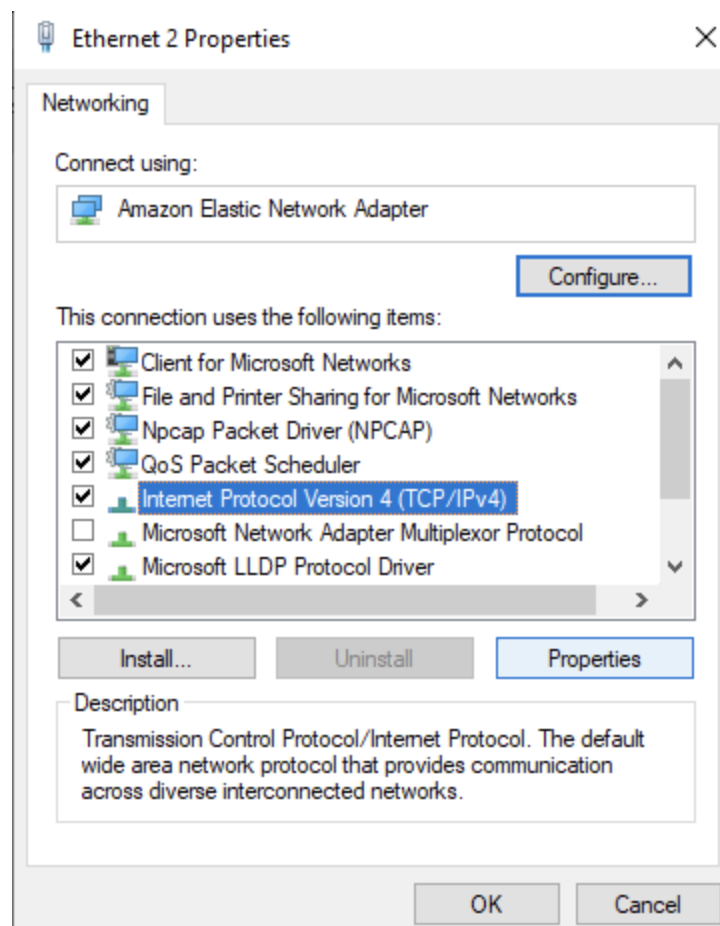
Advanced network settings

-  **Change adapter options**
View network adapters and change connection settings.
-  **Network and Sharing Center**
For the networks you connect to, decide what you want to share.
-  **Network troubleshooter**
Diagnose and fix network problems.

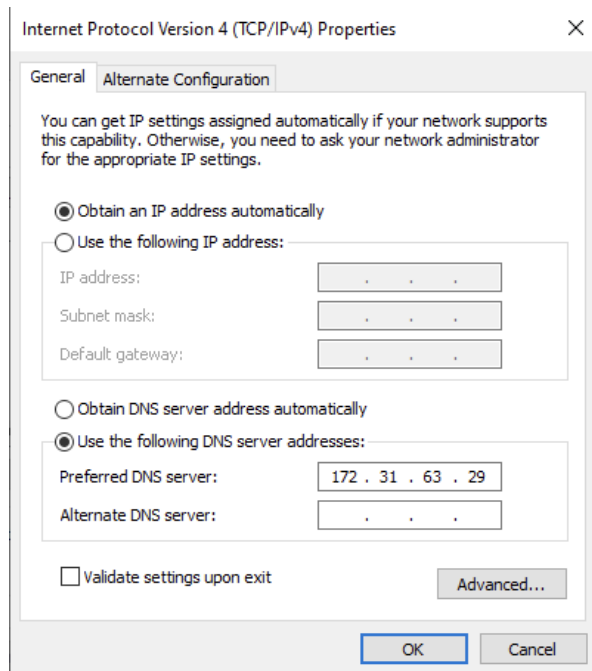
Right click "**Ethernet 2**" and go to properties.



Click on and highlight **"Internet Protocol Version 4 (TCP/IPv4)"** and hit **"Properties"**

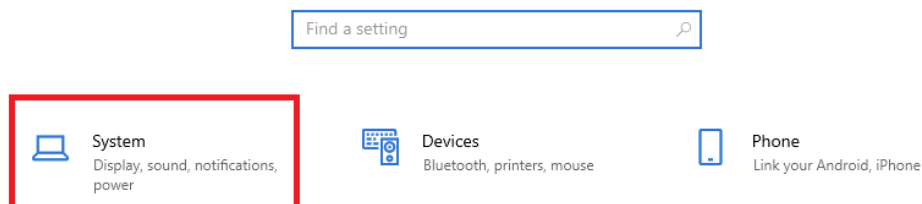


Here, we're going to click **"Use the following DNS server addresses:"** and type in the IPv4 address that we got from our server VM and click OK.

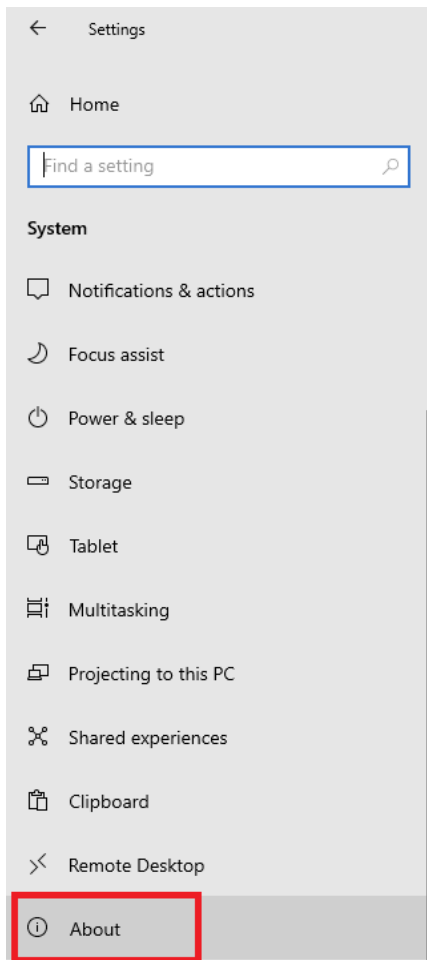


```
Hostname: EC2AMAZ-L30OUG8
Instance ID: i-024ddd41783427499
Public IPv4 Address: 52.33.58.232
Private IPv4 Address: 172.31.63.29
Instance Size: r5.large
Availability Zone: us-west-2c
Architecture: AMD64
Total Memory: 16384 MB
Network Performance: Up to 10 Gigabit
```

From here, we can close out of the Network Connections folder and go back to our Settings window and go back to the Home menu and go to **"System"**



On the left side tab, there will be a section called **"About"** we want to head in there.



There will be on the right hand side of the window an option to **"Rename this PC (advanced)"**

About

Your PC is monitored and protected.

[See details in Windows Security](#)

Device specifications

Device name	Desktop-2
Full device name	Desktop-2.contoso.com
Processor	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2.50 GHz
Installed RAM	16.0 GB (15.7 GB usable)
Device ID	BA73C681-C98C-45B2-8091-30DC6A10DCC9
Product ID	00330-80000-00000-AA605
System type	64-bit operating system, x64-based processor
Pen and touch	Pen and touch support with 256 touch points

Copy

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](#)

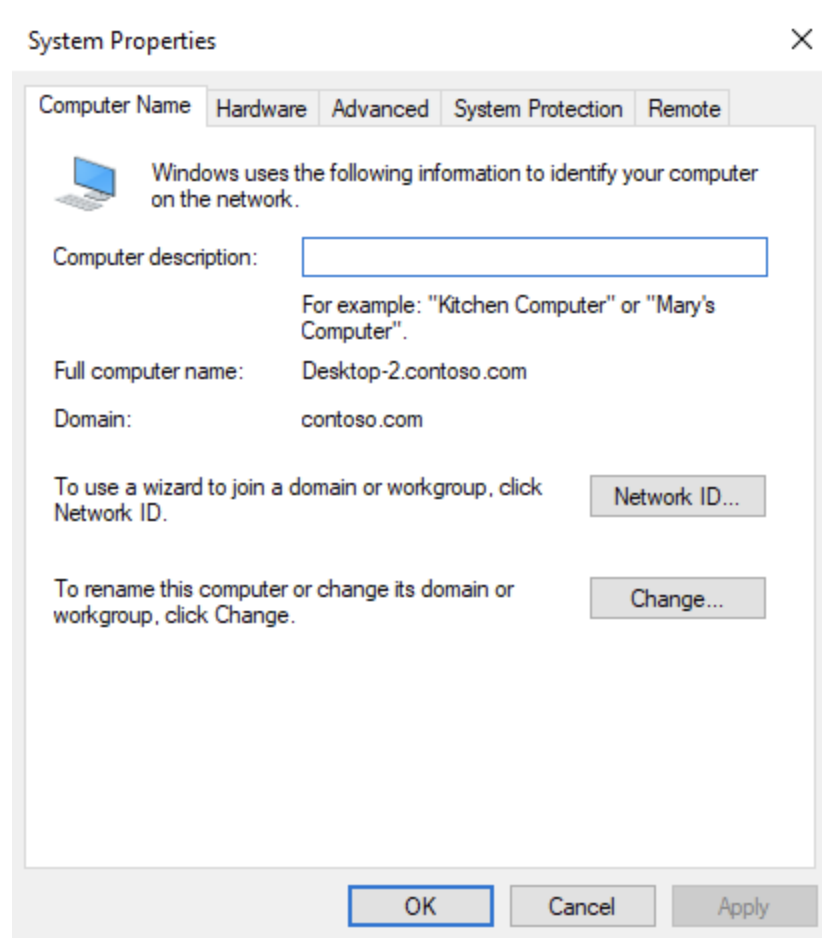
[Remote desktop](#)

[System protection](#)

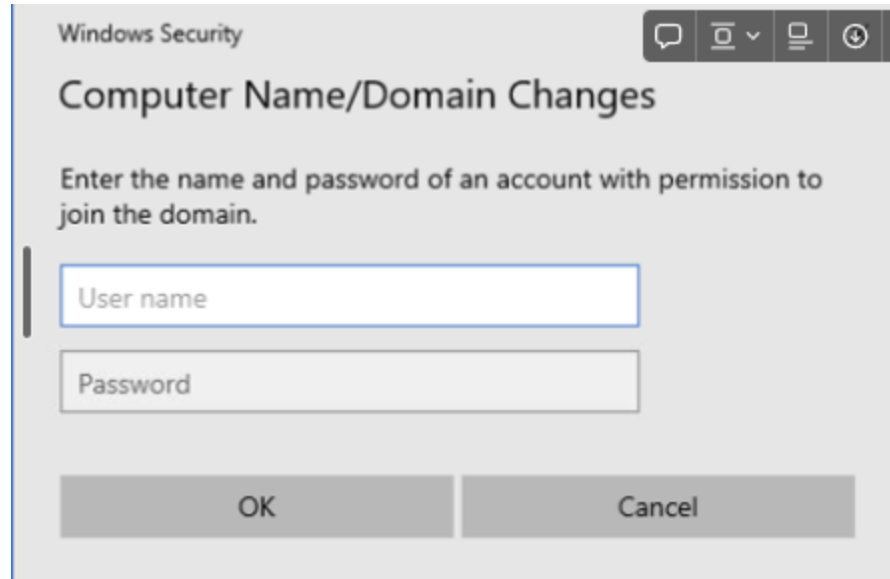
[Advanced system settings](#)

[Rename this PC \(advanced\)](#)

A window will pop up and we want to click **"Change..."**



A new window should pop up and we'll click on the bubble for "**Domain**" and enter contoso.com, click OK and a new window should pop up asking for a username and password.



The information we'll be putting is:

User name: **Administrator**

Password: **Pa\$\$w0rd**

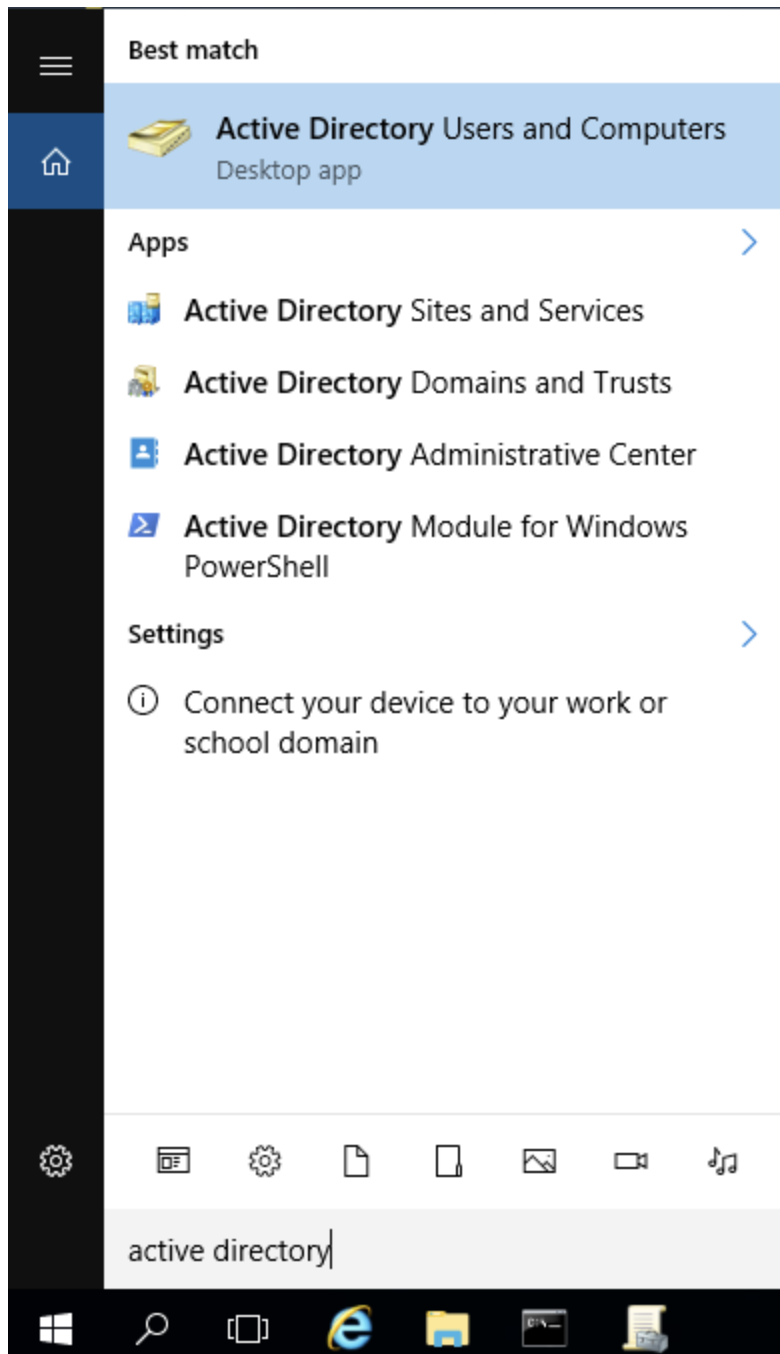
After inputting the correct credentials, you will need to restart the PC to apply the changes to connect to the domain.

This is the end for connecting to Domains.

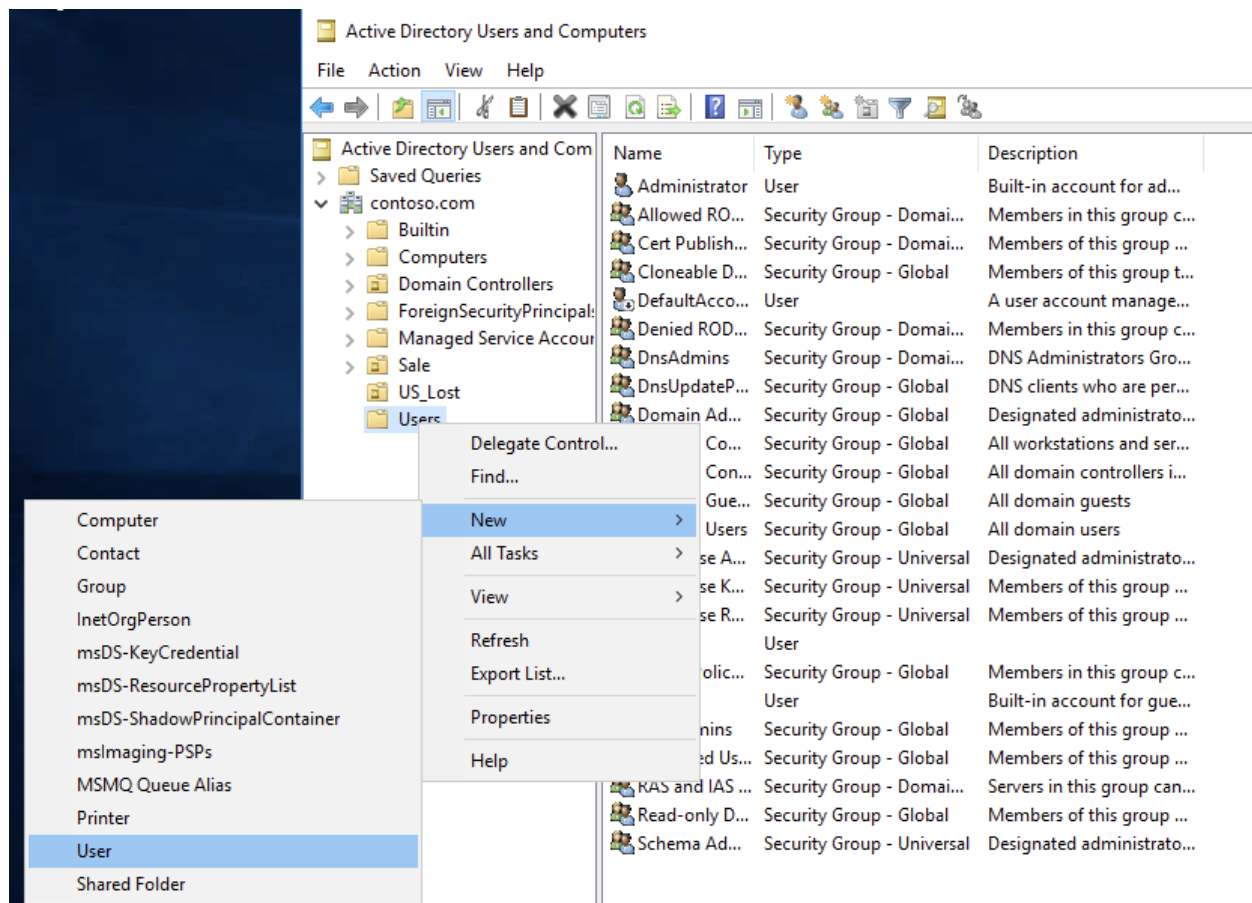
Step 2: Creating a new user

We'll be working on our Server VM for this step.

First off, we'll hit the magnifying glass icon and search for "Active Directory"




When the active directory opens, we'll go ahead and go to **Users** in an open space, we'll right click > **New** > **User**



We will go ahead and fill out information about our new user.

New Object - User ✕

 Create in: contoso.com/Users

First name: Initials:

Last name:


Full name:

User logon name:
 @contoso.com ▼

User logon name (pre-Windows 2000):

For the password settings, we will enter a strong password and have the user change their password to what they want their password to be.

New Object - User ✕

 Create in: contoso.com/Users

Password:

Confirm password:

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

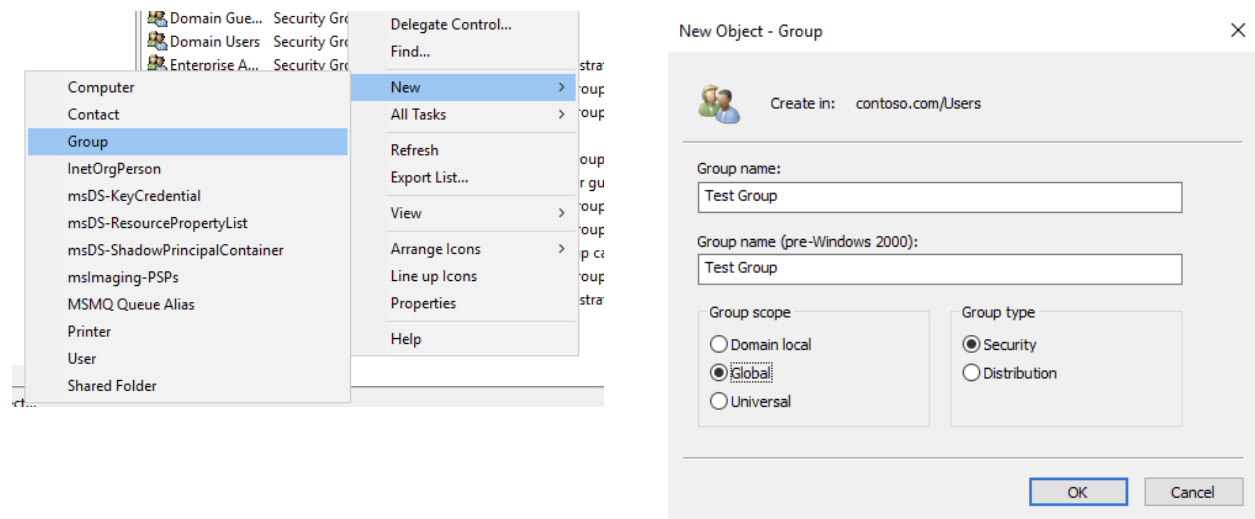
☐ Account is disabled

For good practice we will remember that we will never use the option where users cannot change password, or that their password never expires. If the new hire is not currently working, we will keep their account disabled until their start date.

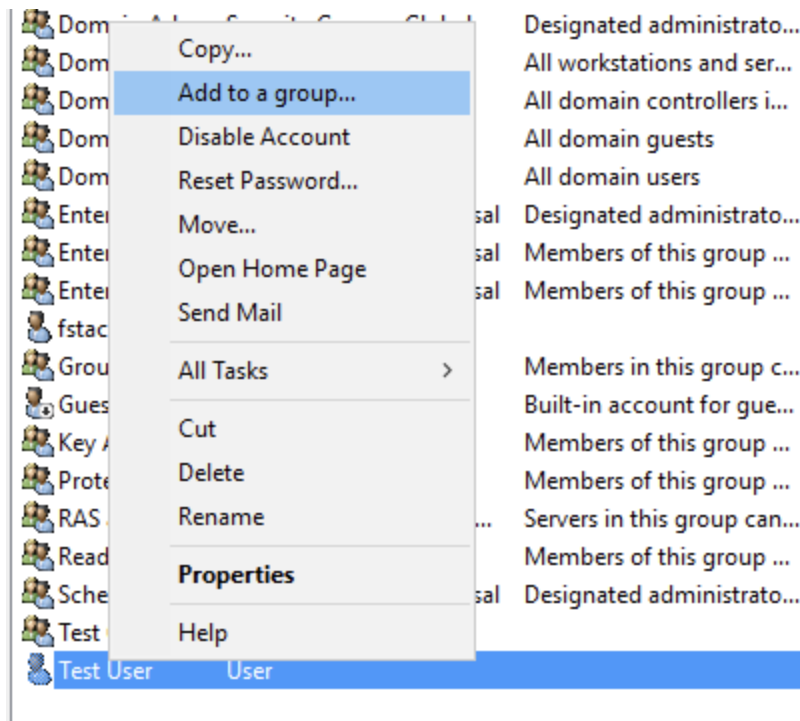
This is the end of creating user accounts.

Step 3: Creating a group and placing users in groups.

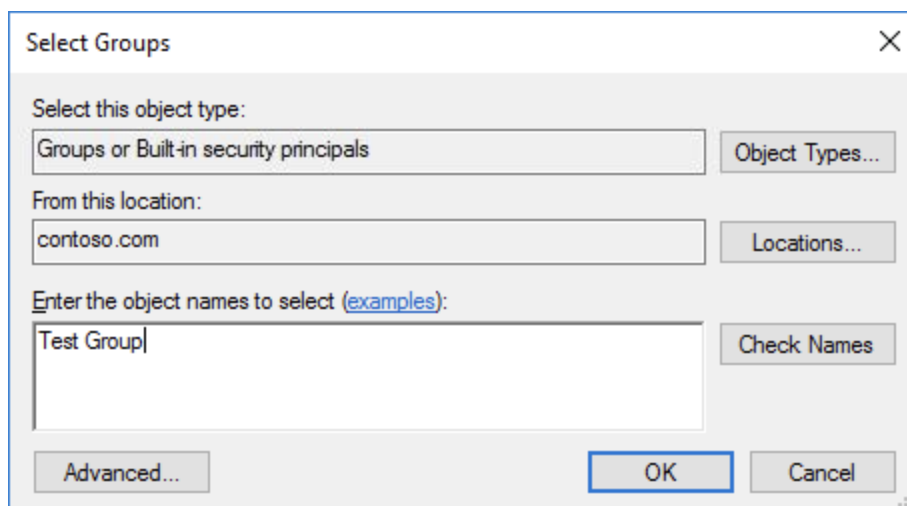
To create a group, we will first head back to our **Active Directory** and in an open space we will again right click > **New** > **Group** and enter your new group name.



To add a user to a group, you may find that user in the Users folder and right click > **Add to a group...**



Once that window pops up, in the bottom box, you may enter the group that you created to assign the user to the group and click OK.



That is the end of adding users to a group.

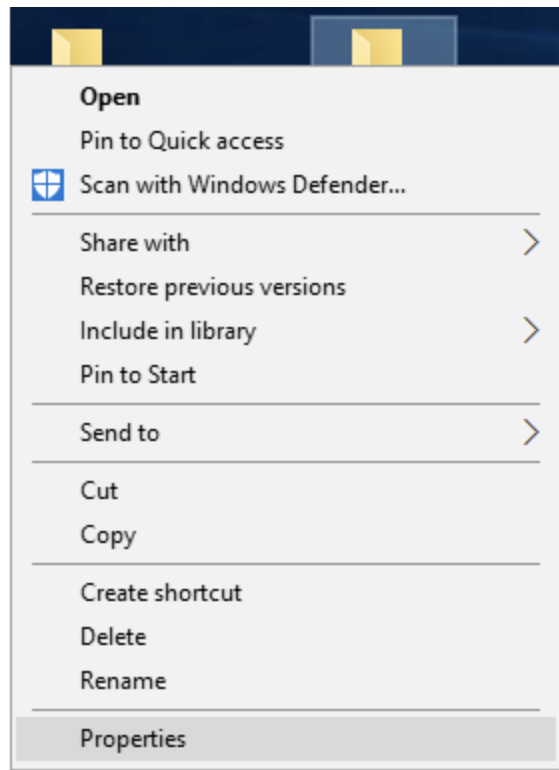
Step 4: Creating a share

To create a share, we will first create a folder and place a random file in this folder, in this case we'll create a text file named "test.txt"

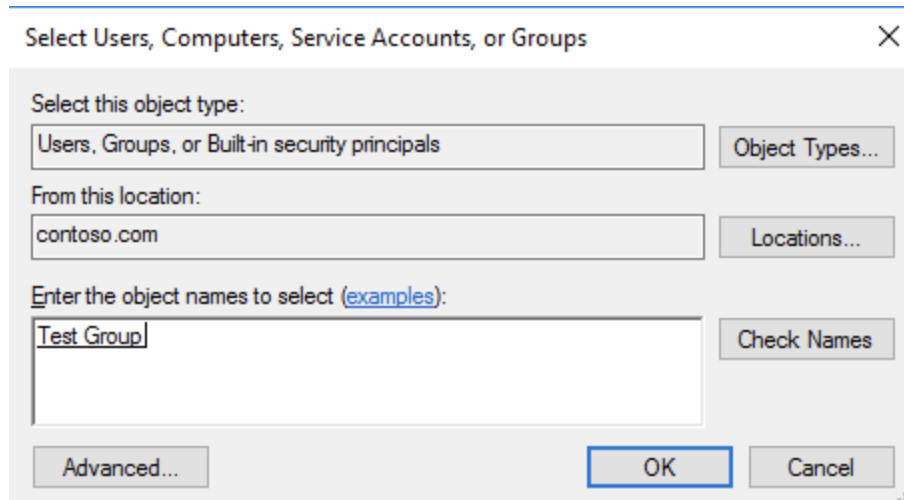
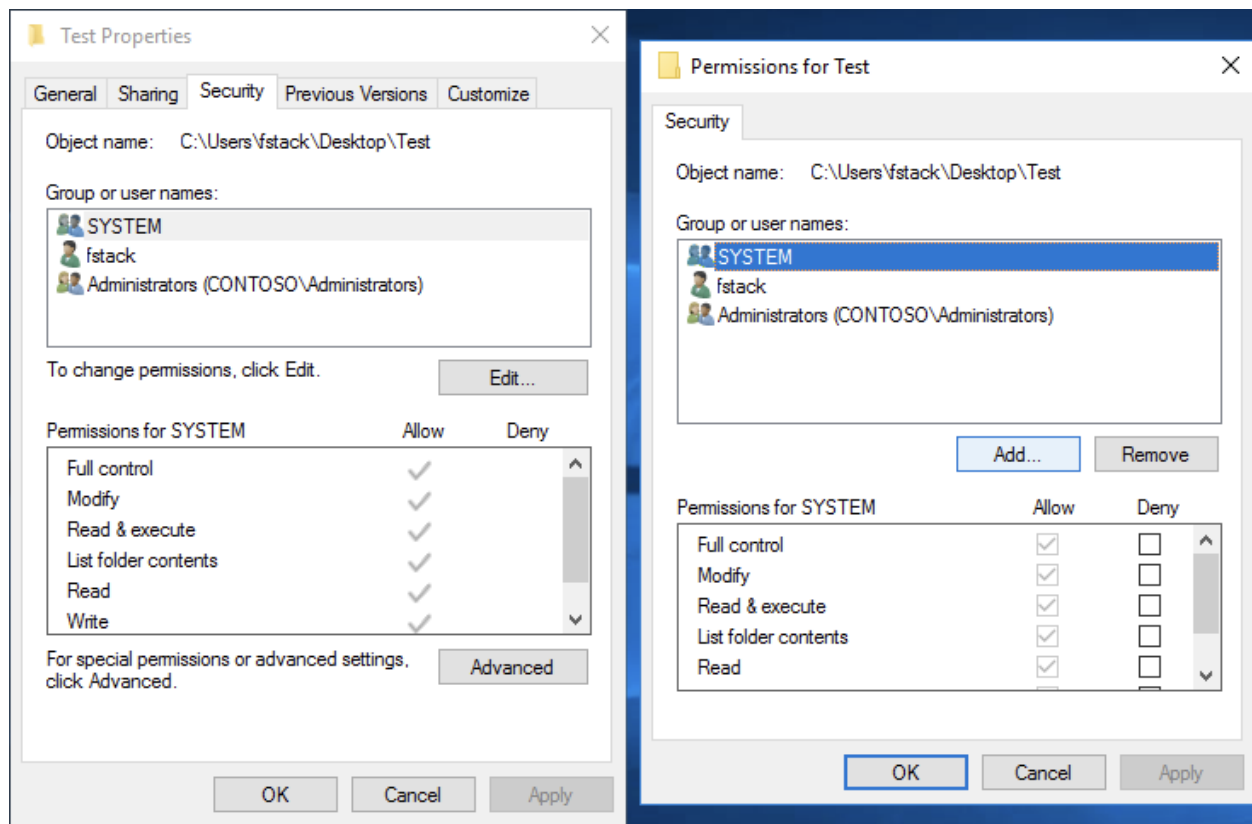
First we'll create the folder on our desktop so right click > **New** > **Folder**

We'll name it after our group. and create a new text document called "test.txt"

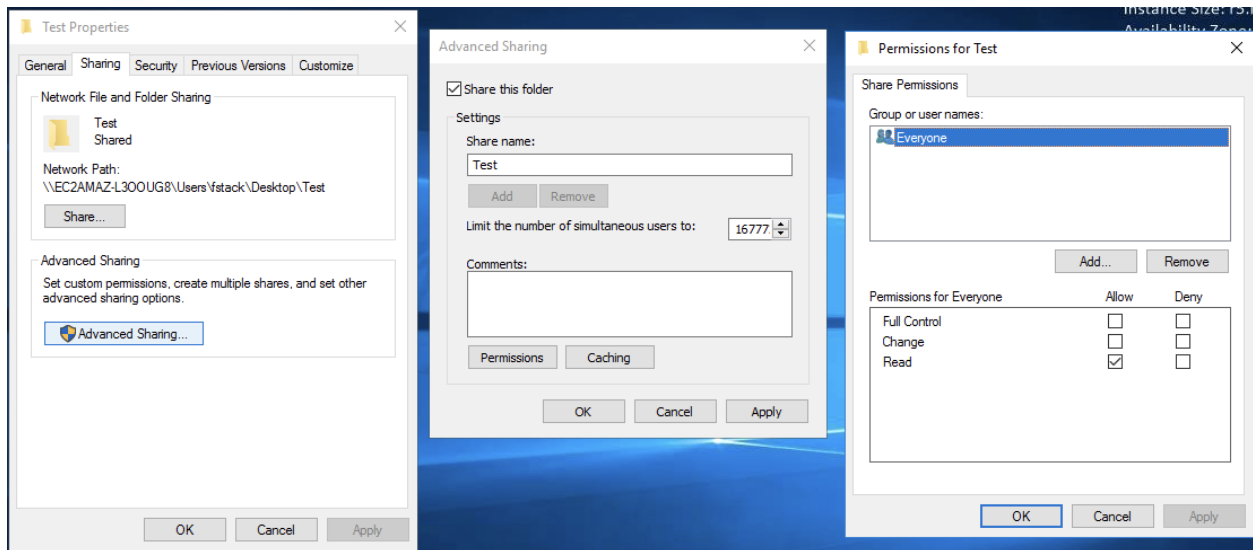
We're going to share this file over the network by right clicking the folder and going to **Properties**



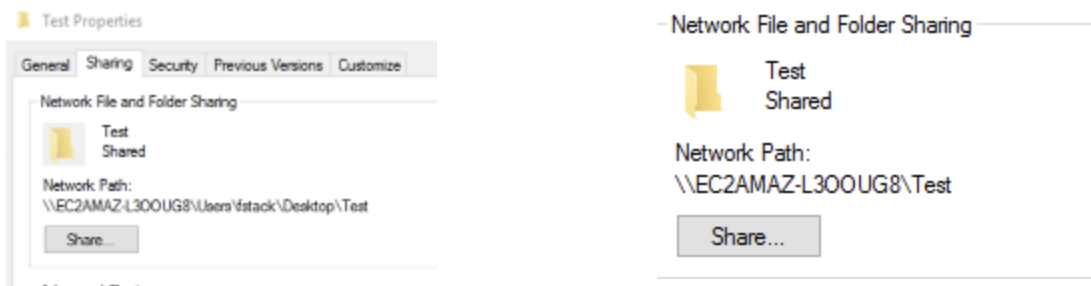
From the new window that popped up, we're going to go into the **Security** tab, edit and add your group to the list and click OK.



Next, we will head over to the **Sharing** tab to the left of **Security**. We will go into **"Advanced Sharing..."** and make sure the box **"Share this folder"** is checked, go into **Permissions**, everyone should have read permissions.



After completing the previous step, the **Network Path** should change.

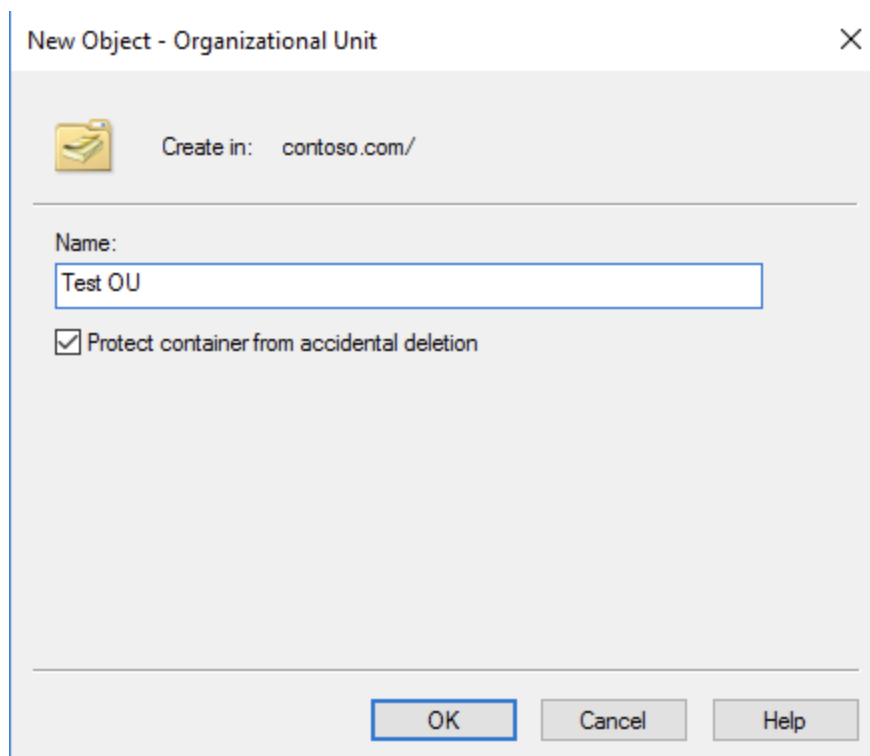
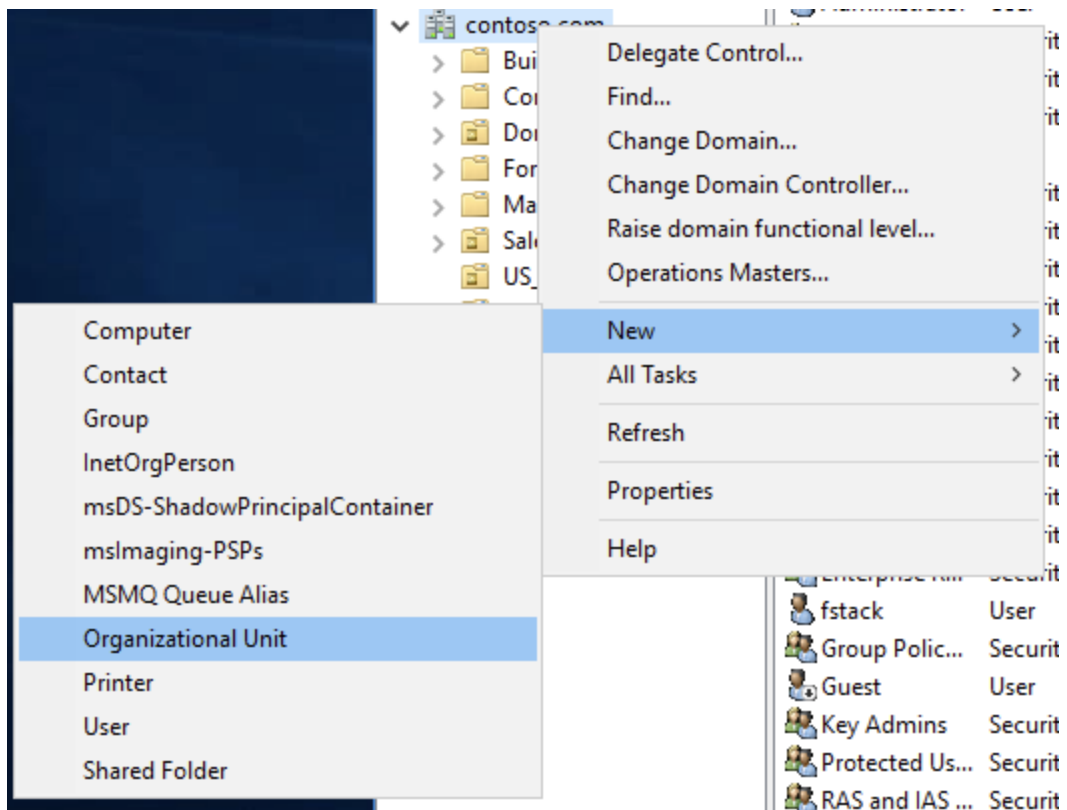


NOTE: Remember the new network path. We will need it for later.

This is the end of sharing over the network.

Step 5: Creating an Organizational Unit and Attaching a Group Policy Object (GPO)

First, we will be opening **Active Directory Users and Computers**, we will then right click our domain which in this case is contoso.com > **New** > **Organizational Unit** and fill out the name for the new OU.



In the new OU, it should be empty. We can add users to this group by going into the **Users** section and dragging users over or right click > move to where you need the selected item to go.

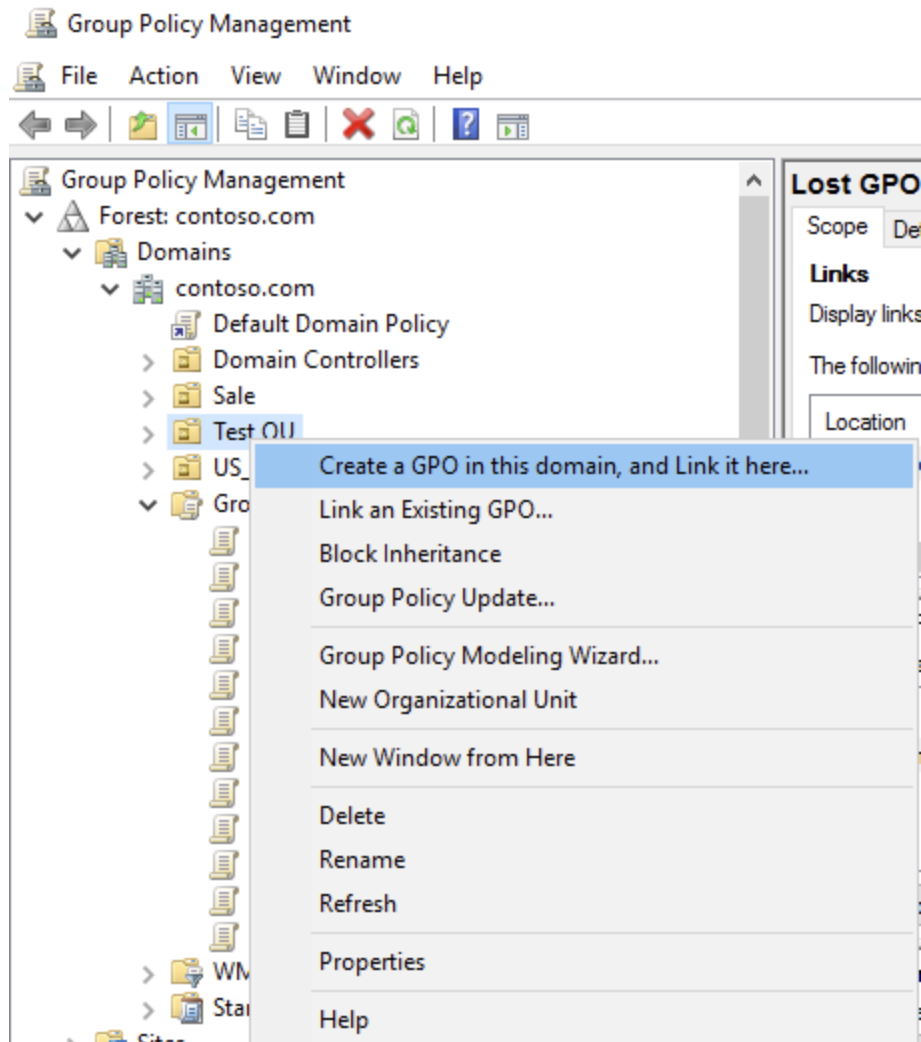
Active Directory Users and Com			Name	Type	Description
> Saved Queries					
▼ contoso.com					
> Built-in					
Computers			DESKTOP-2	Computer	
> Domain Controllers			Lost I. Sauce	User	
> ForeignSecurityPrincipal:			Lost Ones	Security Group - Global	
> Managed Service Account					
> Sale					
US_Lost					
Users					
Test OU					

Note: The current OU is a screenshot from a previous exercise that has the computer listed in the OU.

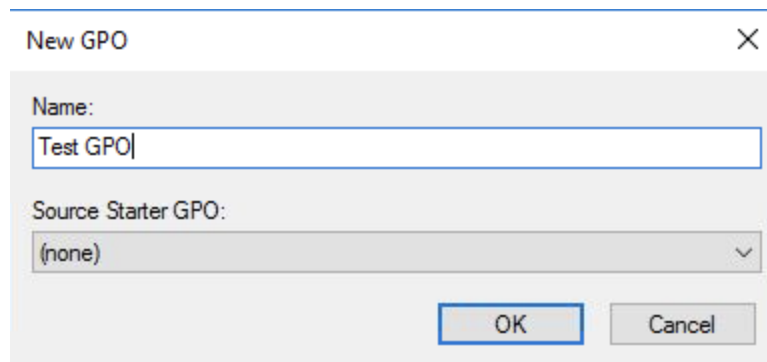
To attach a GPO to this OU, we will have to open **Group Policy Management** by going to the magnifying glass icon and searching for "Group Policy"



We will then find our OU that we just made and right click > **Create a GPO in this domain, and Link it here...**



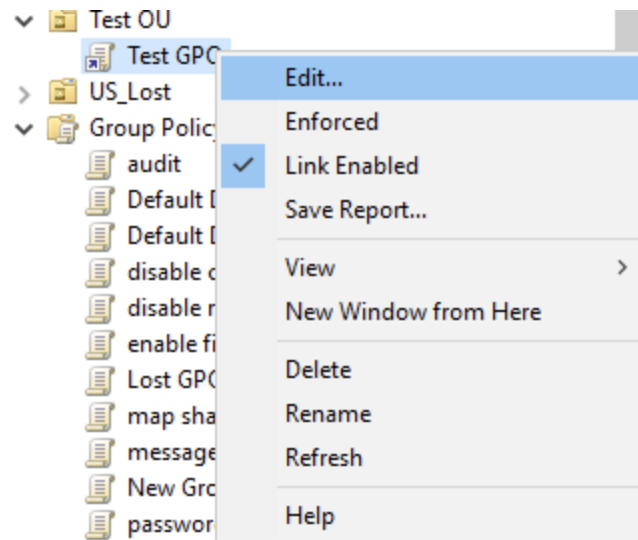
A new window should pop up and we can name it anything that we want it to that makes sense and we know that it'll be the GPO for that OU and click OK.



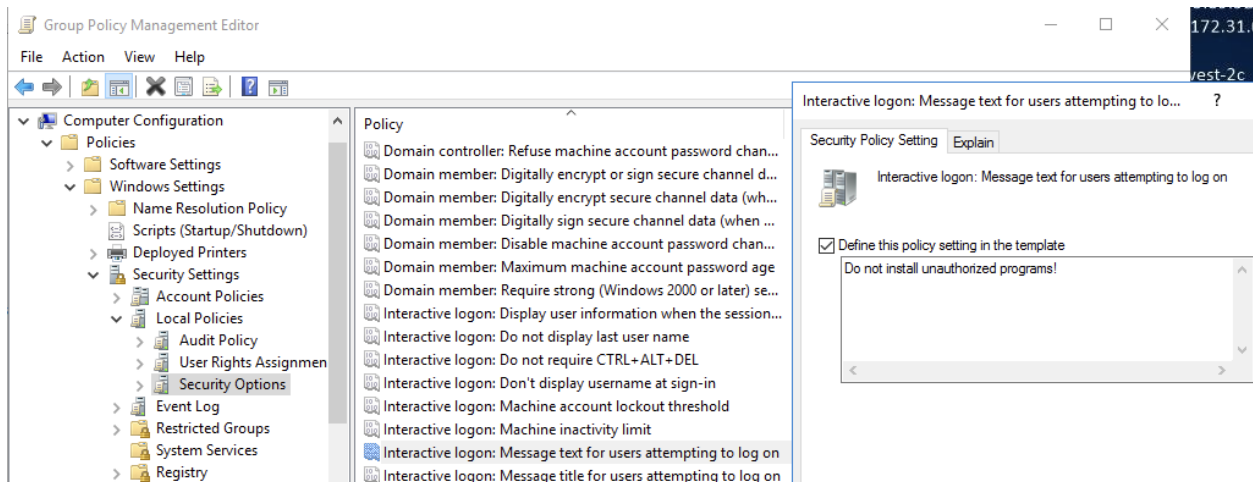
This is the end of creating an OU and attaching a GPO

Step 6: Editing GPO Rules

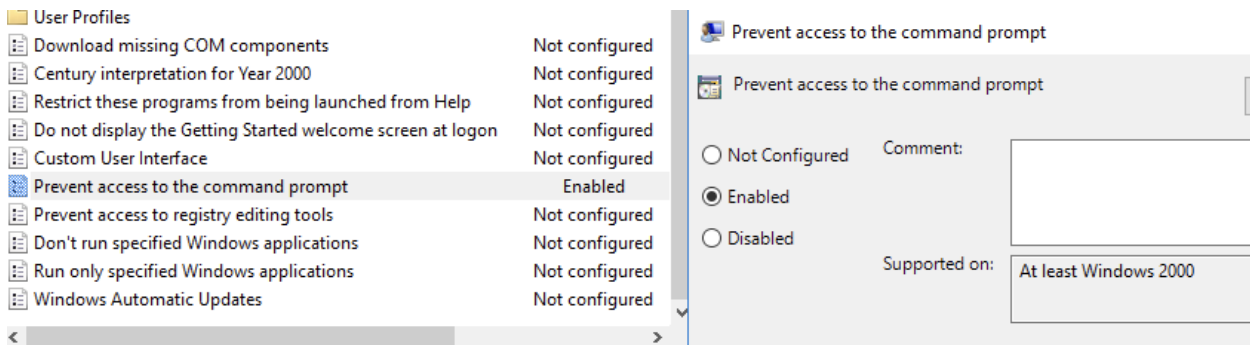
We may now get back to the Group Policy Management, go to our OU and click the drop down menu to see the GPO we just made, right click > **Edit...** to edit our current policies.



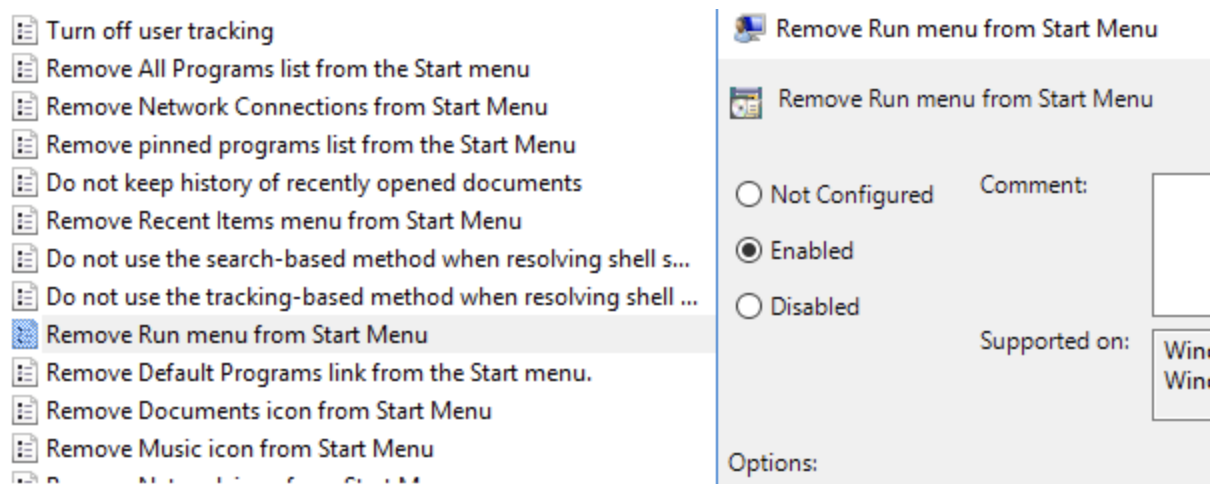
We're going to display a message when the computer boots up not to install unauthorized programs. To get there, under **Computer Configuration > Policies > Windows Settings > Security Settings > Security Options** we will find **"Interactive logon: Message text for users attempting to log on"** we will right click > edit that policy and check the box to define this policy setting in the template and write "Do not install unauthorized programs!" click OK. Repeat this step for the one right below it for **"Interactive logon: Message title for users attempting to log on"**



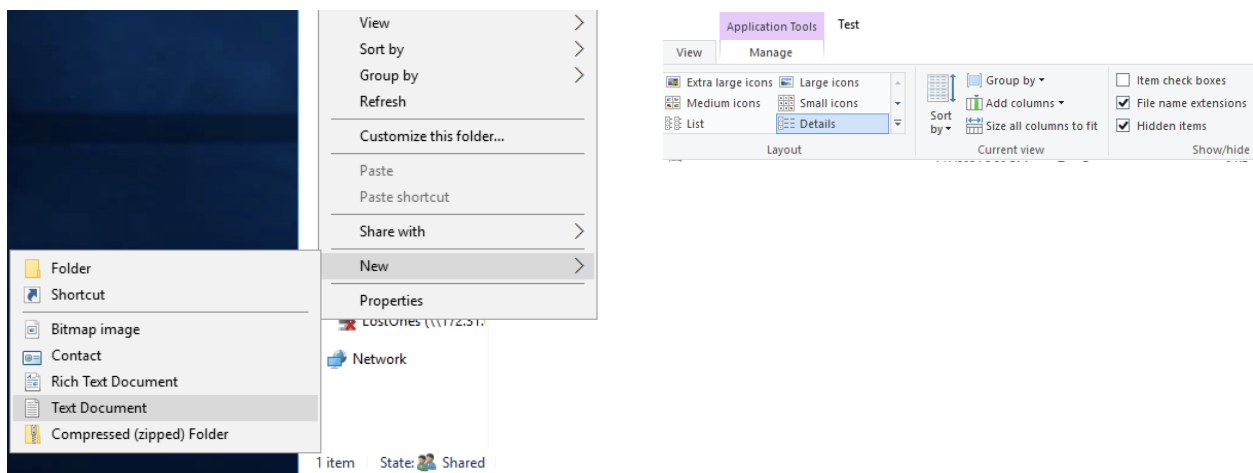
Next, we will prevent user access to CMD. In the Group Policy Management Editor we will go to **User Configuration > Administrative Templates > System** from here on the right hand side, we will find a couple policies that we can change. We're looking for "**Prevent access to the command prompt**" right click > edit and enable that to take away user access to Command Prompt.



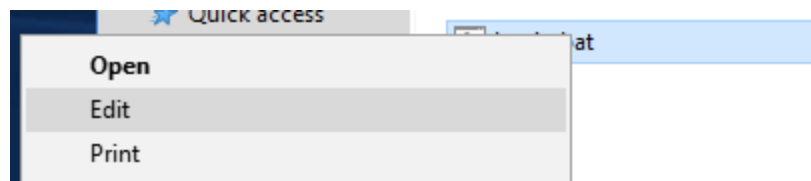
Next we will remove the Run program from users. Here we will go to **User Configuration > Policies > Administrative Templates > Start Menu and Taskbar**. There will be a setting called "**Remove Run menu from Start Menu**" we will edit that and **Enable** that setting to remove access to the Run menu. Click Apply and OK to exit.



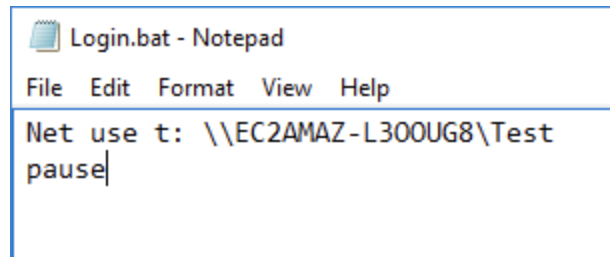
Finally we're going to add a map to the share on the user's account. From here, we're going to go to our folder that we created earlier in this case mine will be "Test" and create a new Text document called "Login.bat" Make sure you have file extensions box checked in the **View** tab



We will now right click **Login.bat** and hit Edit.



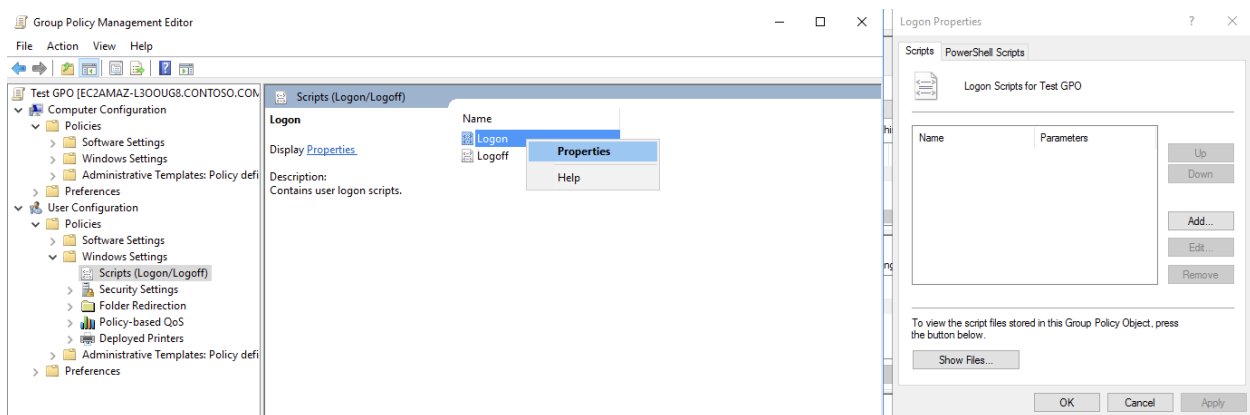
We will now write a script that uses the T drive as a share drive and if the user has permissions for this drive they will automatically have this drive when they log in. \\<hostname/IP>\<File/Folder Name> we want to go ahead and add another line and type pause so when we run this batch file, if anything goes wrong we will be able to see the errors in the command prompt.



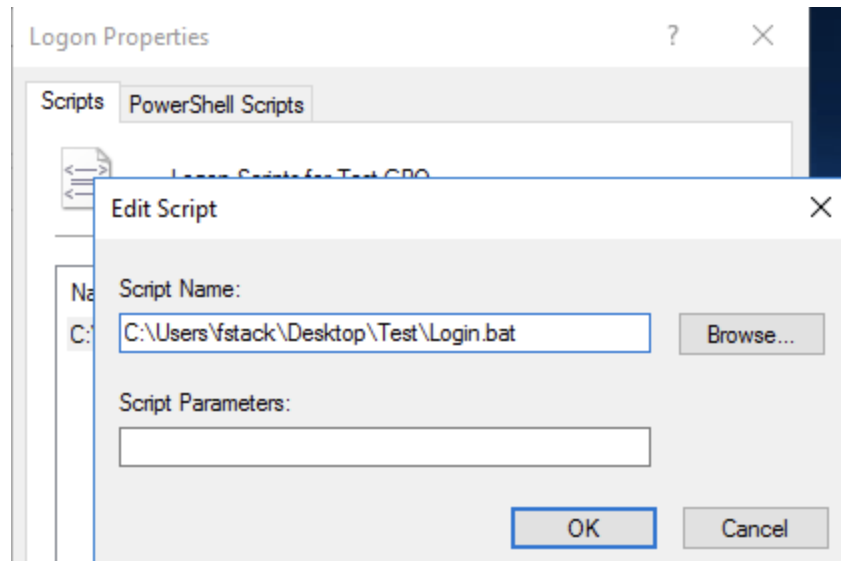
```
Net use t: \\EC2AMAZ-L300UG8\Test
pause
```

From here, there are two different ways where we can input this share to the user.

Method 1: We are going to go to **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)** we will right click on **Logon > Properties**.

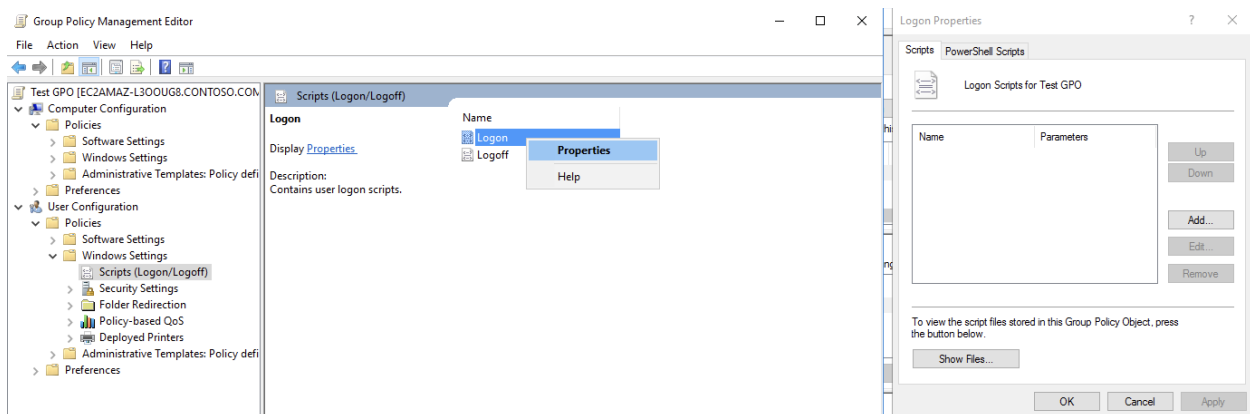


A new window should pop up. We will click on add and another window will pop up, we will put the path to Login.bat so that script will execute when the user logs on to their account if they're in this group.

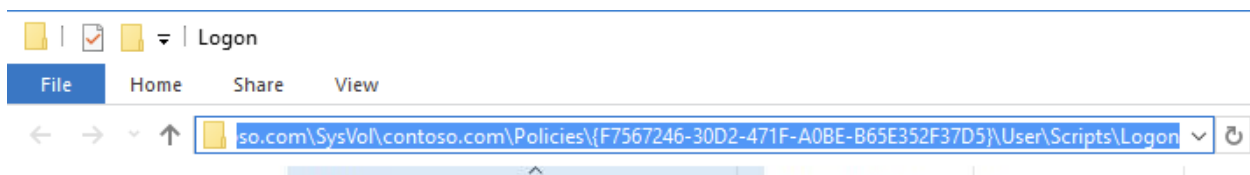


End method 1.

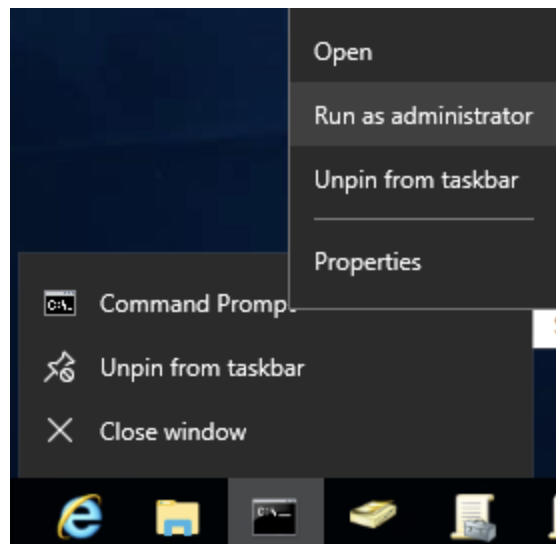
Method 2:



From this menu after you click properties, you may click **Show Files** to be directed into the folder where all files in this folder are executed on login. You may copy this path (Ctrl + C)



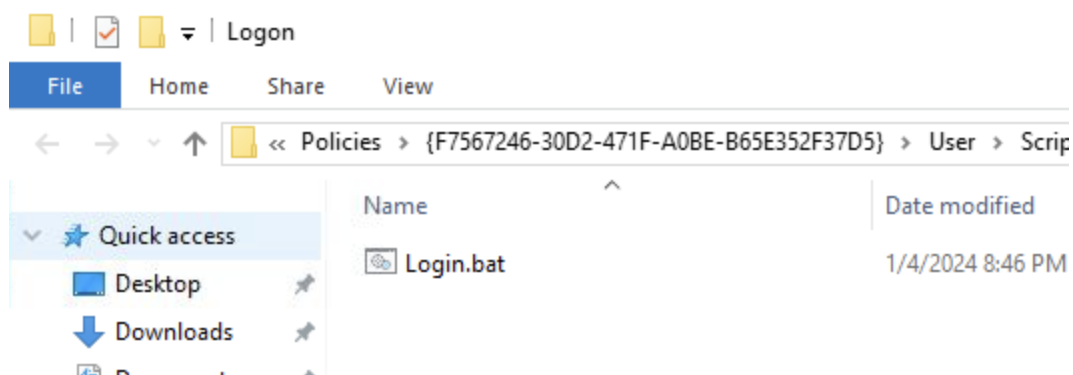
Next you will open command prompt as admin by right clicking the command prompt icon and running the program as admin.



We may now run this command in the admin command prompt.

```
C:\Users\fstack\Desktop\Test>copy c:\users\fstack\desktop\test\login.bat \\contoso.com\SysVol\contoso.com\Policies\{F7567246-30D2-471F-A0BE-B65E352F37D5}\User\Scripts\Logon
1 file(s) copied.
```

This will copy Login.bat and place a copy of it in the Logon folder that will execute all files in that folder at logon.



If we manually tried to create this bat file in the folder or copied our previous bat file to this folder, we would have gotten permission denied because our user doesn't have access to do anything in this folder so that's why we ran it through admin command prompt.

End method 2.

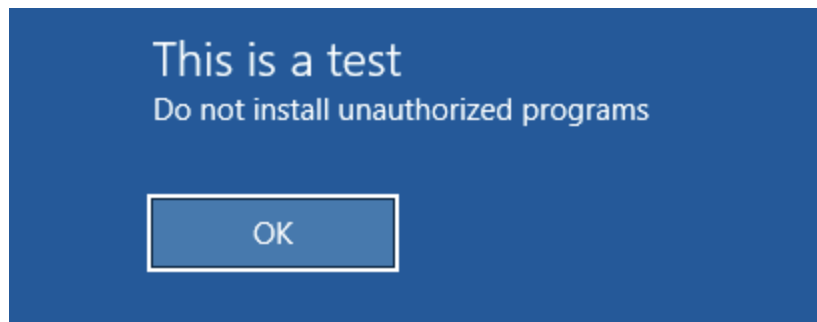
From here we will open our command prompt back up and run the command `gpupdate /force` to update the policies that we just changed. Now when our new user logs in they should have access to our Share drive.

```
C:\Users\fstack\Desktop\Test>gpupdate
Updating policy...

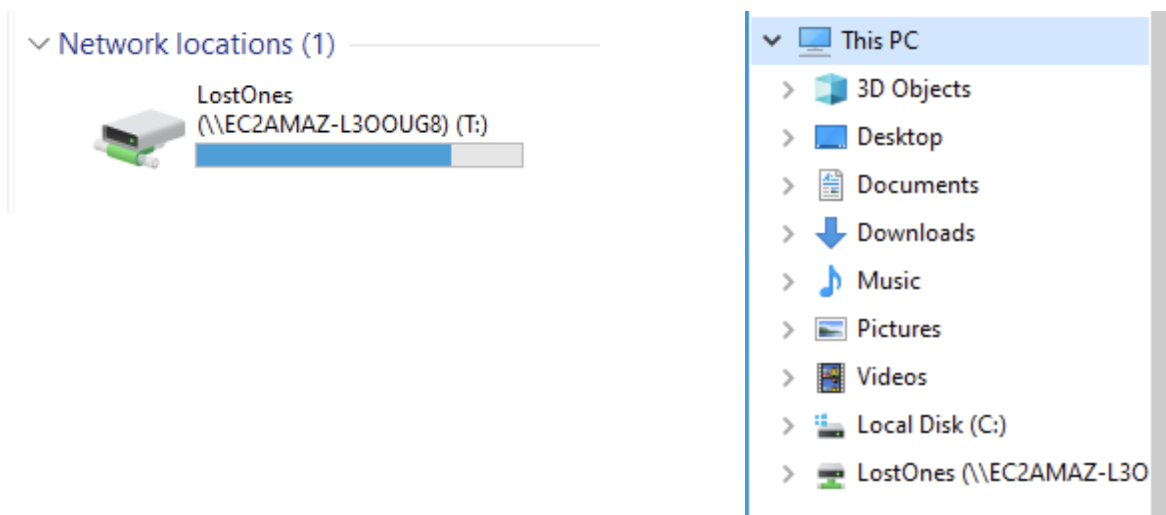
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Note: Some changes you make in Group Policy Management may not apply until restart.

We can see that before anyone logs in when the computer boots up this message will now be displayed.



We also see that our user has access to our Share drive when he goes and opens the file explorer.

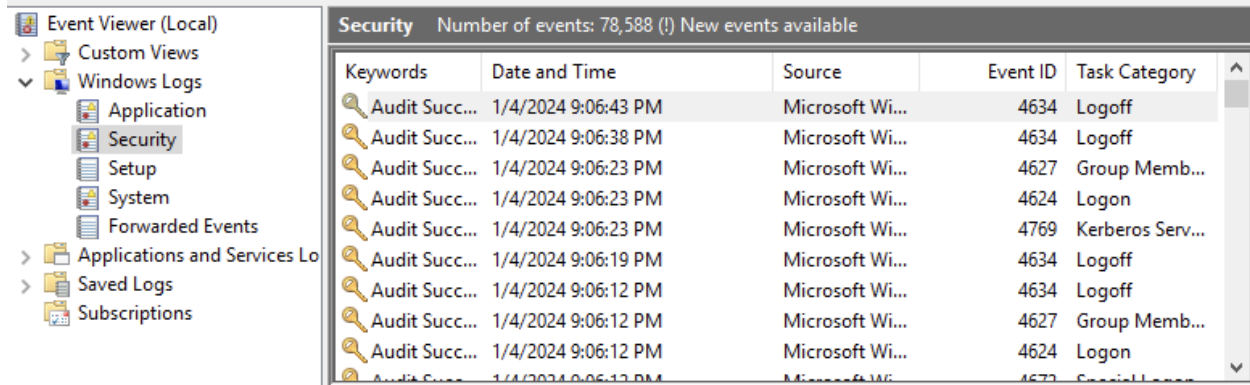


Step 7: Event Viewer

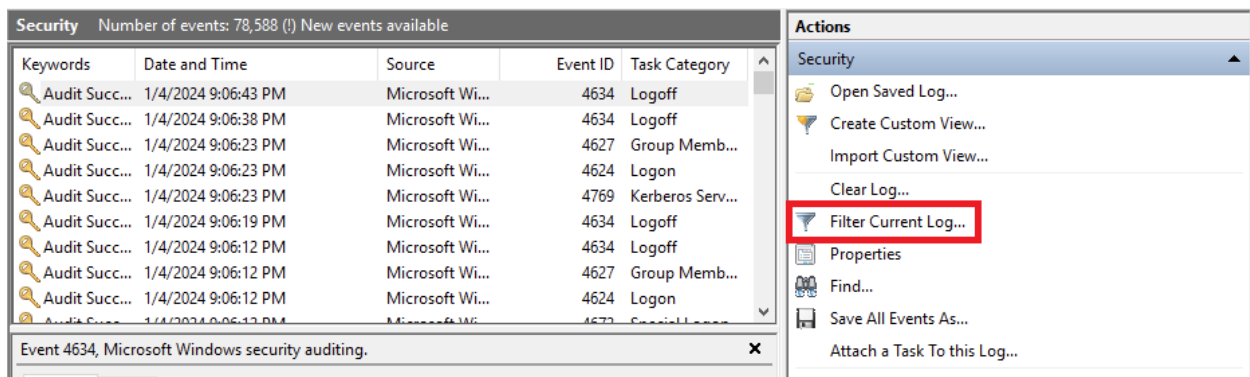
To access the event viewer, go to the magnifying glass and search for "Event Viewer"



From here we want to see the last successful login from our user so on the left hand side of the viewer, we want to go into **Windows Logs > Security**.



Next on the right hand side, there will be **Filter Current Log**



Where it says "<All Event IDs>" we're going to replace that with the Event ID "4624". This will look for all successful logons and we can sort by date and time if we need to.

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4624

Task category:

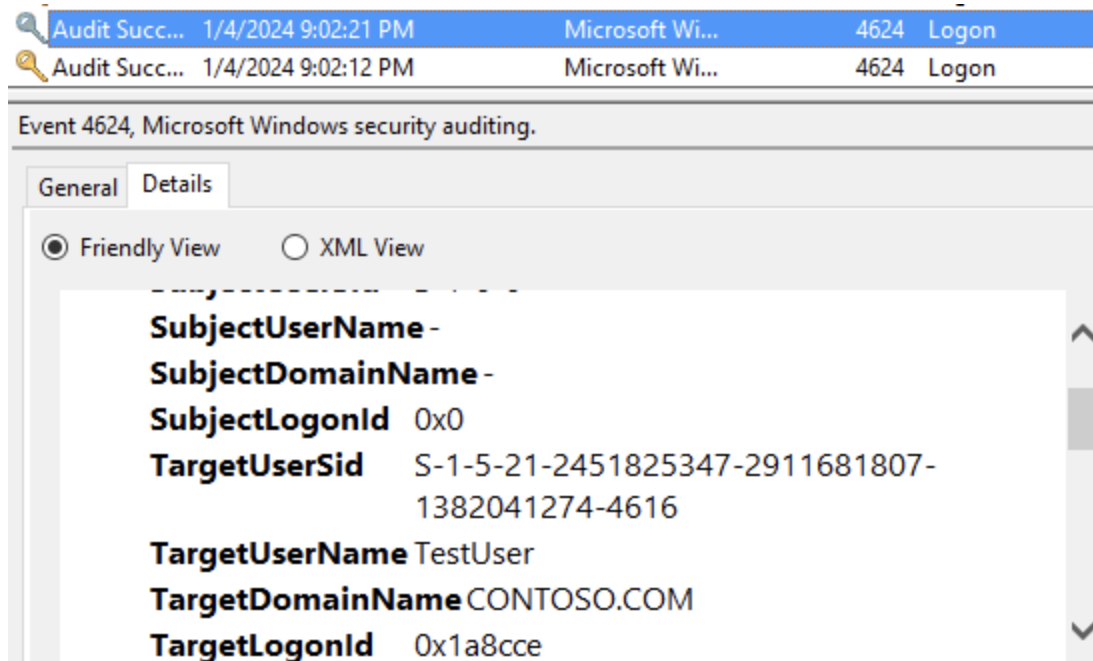
Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

After some browsing, we can see that here is when our user last logged on successfully.

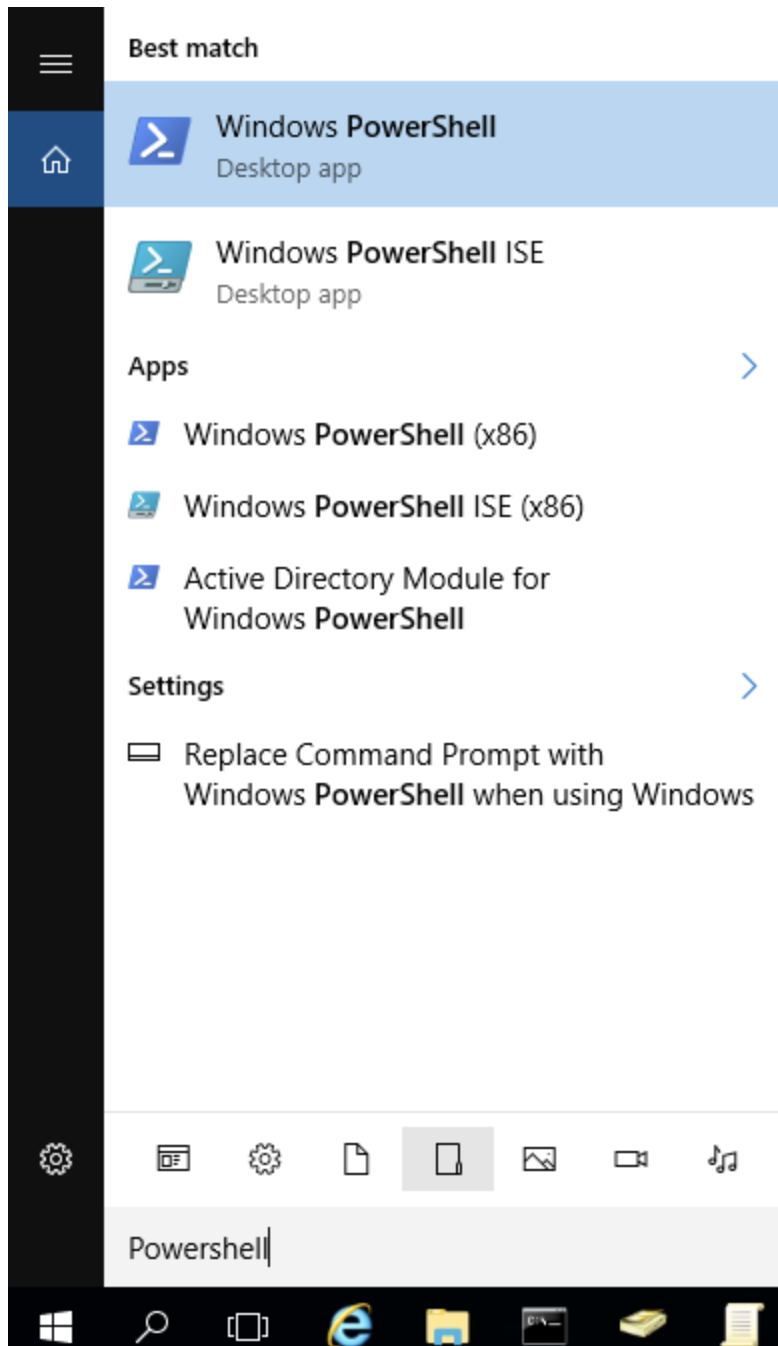


If we wanted to we can right click and save that event so we can pull up the details later.

End of Step 7.

Step 8: Using PowerShell to check latest program installed.

To check the latest program installed, we're going to open Windows PowerShell through the start menu under Windows PowerShell or search by using the magnifying glass and searching for "PowerShell"



After running the command `Get-WmiObject -Class Win32_Product | Sort-Object InstallDate -Descending | Select-Object Name, InstallDate` we should have results that look like this and we can see Amazon SSM Agent was the latest program installed.


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

PS C:\Users\fstack> Get-WmiObject -Class Win32_Product | Sort-Object InstallDate -Descending | Select-Object Name, InstallDate

Name                                     InstallDate
----
Amazon SSM Agent                        20230212
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332 20221010
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332 20221010
NICE DCV Virtual Display                20220915
NICE Desktop Cloud Visualization Server (64 bit) 20220915
aws-cfn-bootstrap                      20220810
AWS Tools for Windows                  20220810
AWS PV Drivers                         20220511
```

End of Step 8.

Step 9: PowerShell script that lists all running services to file.

First off we're going to go to **Windows PowerShell ISE**, this can be found again by searching or going to the start menu and going to Windows PowerShell folder. Here we can create scripts and test them.

Here I wrote a script:

```
write-host "Getting a list of all your running services and putting them in a text file on your desktop."
Get-Service | Where-Object { $_.Status -eq 'Running' } | Select-Object DisplayName, ServiceName, Status | Out-File -FilePath "C:\Users\fstack\desktop\running_services.txt"
```

The script was 2 lines, the first line telling the user running the script that it is getting a list of all their running services and putting it in a text file on their desktop. The second line gets all their running services and creates a file called "running_services.txt" Every time this is ran, it will not append, it will overwrite the pre-existing information.

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

ServiceScript.ps1 X
1 write-host "Getting a list of all your running services and putting them in a text file on your desktop."
2 Get-Service | Where-Object { $_.Status -eq 'Running' } | Select-Object DisplayName, ServiceName, Status | Out-File -FilePath "C:\Users\fstack\desktop\running_services.txt"

Get-Service : The term 'Get-Service' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At C:\Users\fstack\Desktop\ServiceScript.ps1:2 char:30
+ Get-Service | Where-Object { $_.Status -eq 'Running' } | Select-Object ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Get-Service:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\fstack> C:\Users\fstack\Desktop\ServiceScript.ps1
Getting a list of all your running services and putting them in a text file on your desktop.

PS C:\Users\fstack> C:\Users\fstack\Desktop\ServiceScript.ps1
Getting a list of all your running services and putting them in a text file on your desktop.

PS C:\Users\fstack> C:\Users\fstack\Desktop\ServiceScript.ps1
Getting a list of all your running services and putting them in a text file on your desktop.

PS C:\Users\fstack>
```

End Step 9.

Conclusion

These were all the steps I taken to join a domain, create a new user with a password, create a group and OU, adding users to the group and OU creating share drives, creating and editing group policies and some basic PowerShell. Please let me know if there's anything you need more information on.