



Pre-Onboarding Runbook

06.22.2023

Bonnie Bennet

Social Media Associate

Marketing

Owner	Alexander Sanabria
Version	v.1.1
Version Date	23rd June, 2023
In This Book	<ul style="list-style-type: none">● Overview● Goals● Procedures

Overview

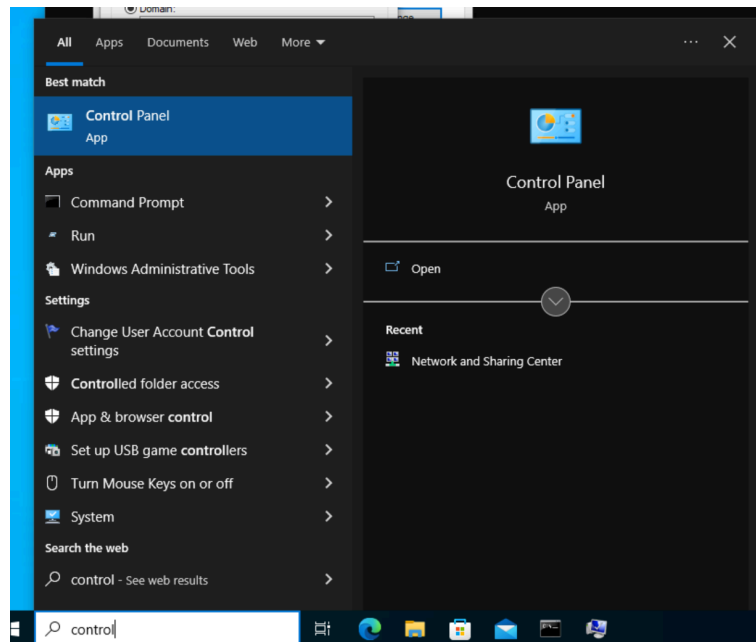
Welcome to the StackFull Software IT team! In this runbook, we will be learning how to use Windows software and technology to navigate day-to-day responsibilities. The basic procedures we will be covering are connecting to the proper domain, adding groups, users, group policies, and navigating the Active Directory via the Command Prompt, GUI and Powershell. (Please note in this runbook, we will be using the username for new hire Bonnie Bennet, and the group name for Marketing, but the variables are changeable for new users.)

Goals

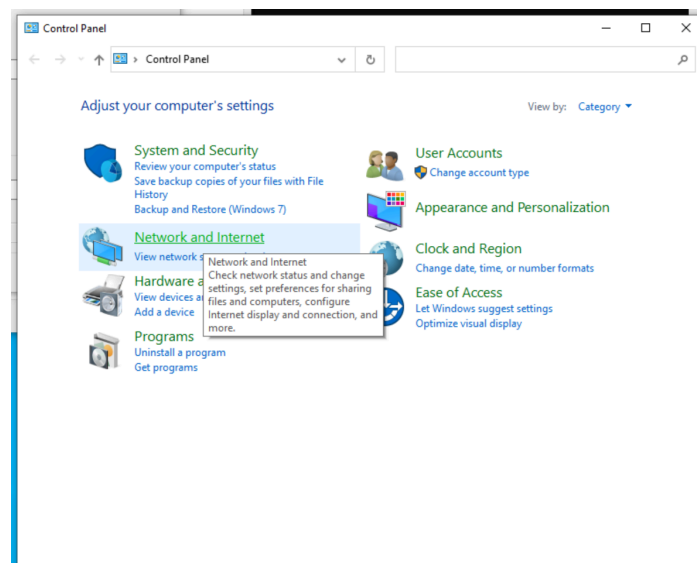
1. Add users, groups, shared folders, and organizational units
2. Edit GPO and apply selected rules to new hires
3. Learn the Event Viewer and navigate through the interface
4. Use Powershell and create scripts to successfully view logs

Process

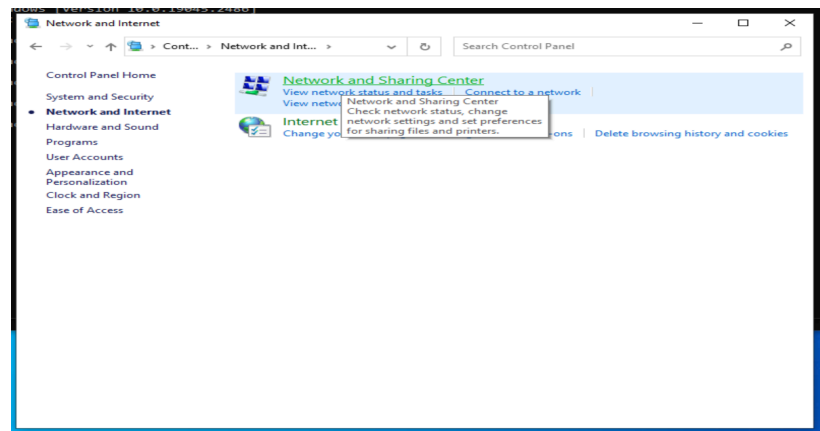
1. For our first task, we will be connecting to the parent domain.
 - a. Click on the Window Bar and type in Control Panel to open



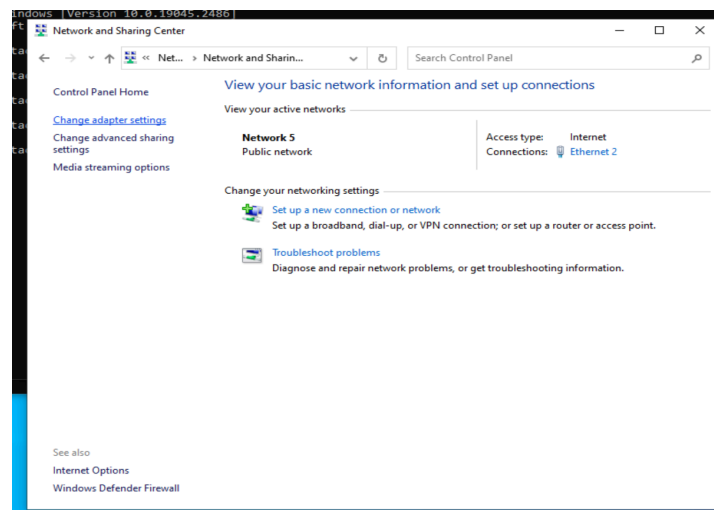
- b. From here, we will open the "Network and Internet" tab in the option menu



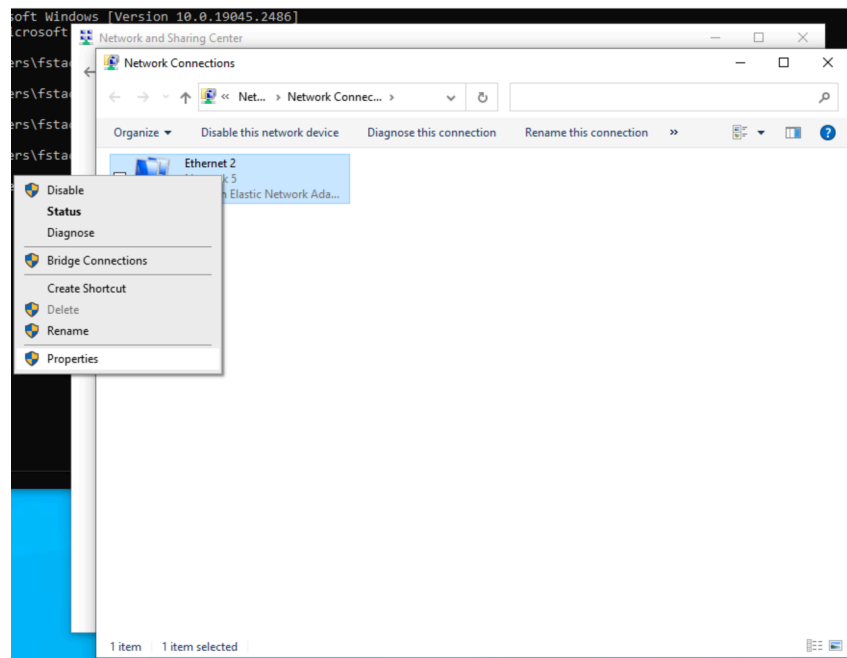
- c. Select "Network and Sharing"



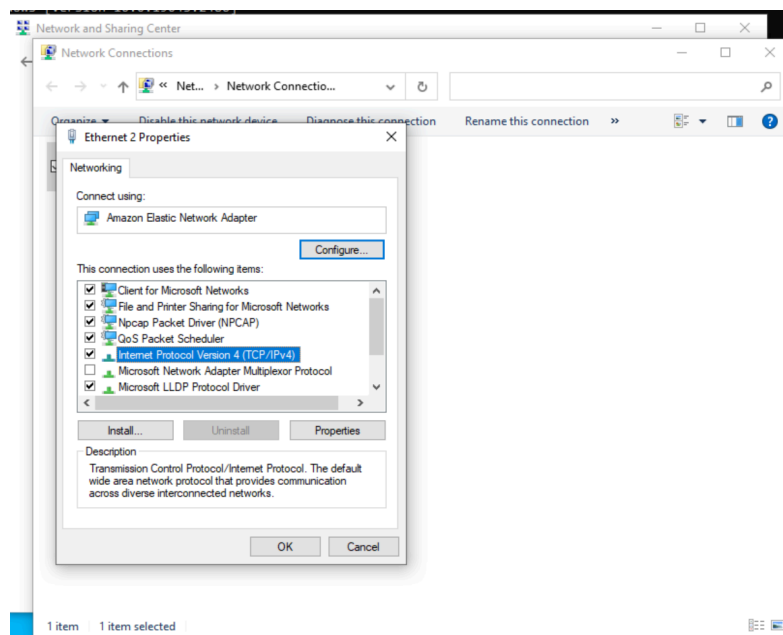
d. Select "Change Adapter Settings"



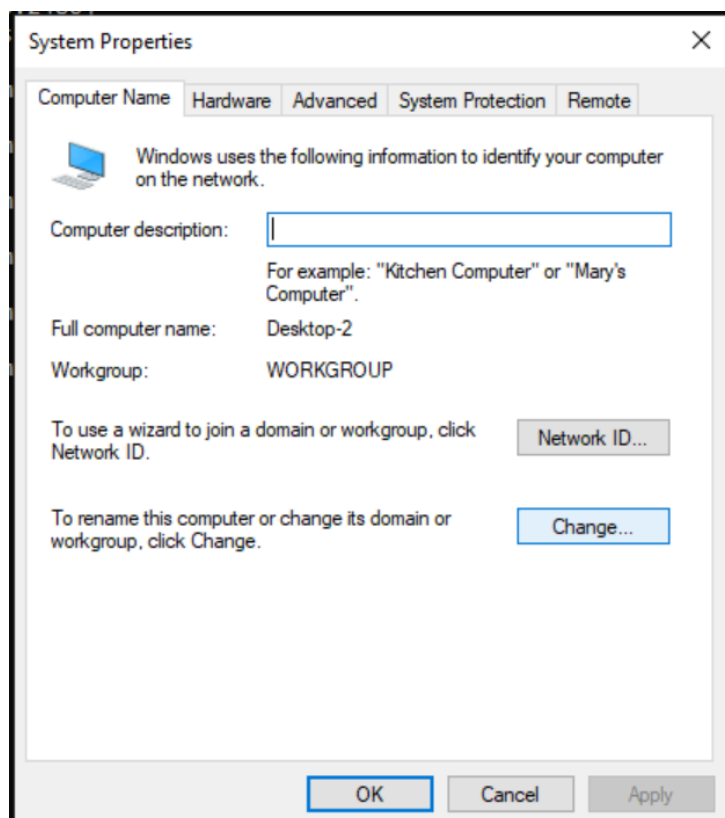
e. RIGHT CLICK on "Ethernet 2" and select Properties



f. In "Properties", click on the IPv4



g. Select "Change"



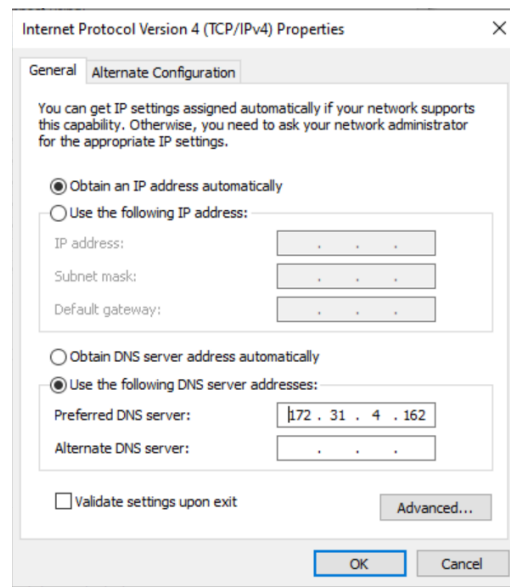
- h. On the server VM (NOT the desktop2 VM), click the details tab and copy the PRIVATE IP address of the server.

The screenshot shows the 'Details' tab of a virtual machine interface. It displays the following information:

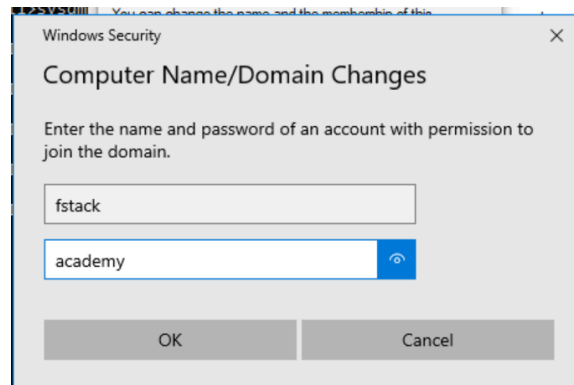
Username:
Status: Ready

Hostname	IP (public)	IP (private)	Port	Access
server	35.87.113.67	172.31.4.162	8443	https://35.87.113.67:8443
desktop-1	34.221.81.2	172.31.8.79	8443	https://34.221.81.2:8443
desktop-2	54.71.198.72	172.31.9.217	8443	https://54.71.198.72:8443

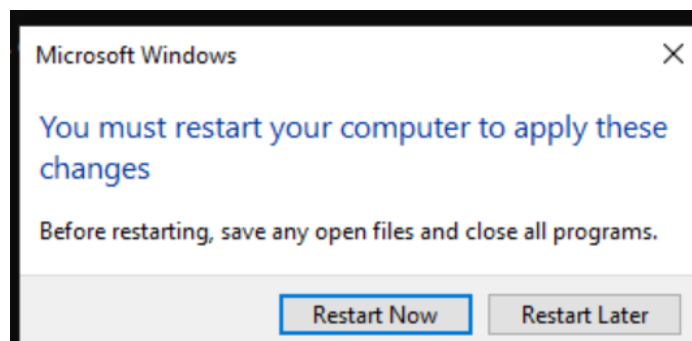
- i. Paste the IP address from the details tab earlier into Desktop2's Preferred DNS server addresses box and click OK



- j. Enter username: fstack and password: academy



- k. Restart Computer and upon restarting Desktop 2 is now on the domain contoso.com



2. Now that our computer is connected to the correct domain, we will familiarize ourselves with adding new users, groups, and sharing files through the appointed department. We will now add a new user.

- a. To check the user names that are already in our network and to make sure the new hire is not already added, we will open the Command Prompt and use the command **net users** and receive the output:

```
C:\Users\fstack>net user

User accounts for \\EC2AMAZ-L300UG8

-----
Administrator          fstack          krbtgt
The command completed successfully.
```

- b. To add the new hire, we are going to use the script: **net user <user name> <password> /add**

```
C:\Windows\system32>net user bbennet password /add
The command completed successfully.
```

*Note: To change the user password from the default password, use syntax **net user <user name> <password>** and create desired password

- c. Verify that the new user has been created by running the net user command again

```
C:\Windows\system32>net users

User accounts for \\EC2AMAZ-L300UG8

-----
Administrator          bbennet         DefaultAccount
fstack                  Guest           krbtgt
localuser2              User1
The command completed successfully.
```

3. It is now time for us to set up a group with the department name so we can put our new hire in the proper group.
- We will be checking for group names in a similar way we checked for user names in the step above. The command we are using is **net localgroup**. This will produce a list of user groups on our computer.

```
C:\Windows\system32>net localgroup

Aliases for \\EC2AMAZ-L300UG8

-----
*Access Control Assistance Operators
*Account Operators
*Administrators
*Allowed RODC Password Replication Group
```

- To create a new local group, we will be using the command **net localgroup <group name> /add**.

```
C:\Windows\system32>net localgroup Marketing /add
The command completed successfully.
```


- c. Confirm the group was successfully added by using the **net localgroup** command again.

```
*IIS_IUSRS
*Incoming Forest Trust Builders
*local_users
*Marketing
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Pre-Windows 2000 Compatible Access
*Print Operators
*RAS and IAS Servers
```

- d. Next, we want to add our new user to this group. To do so, we will be using the command **net localgroup <group name> <user name> /add**

```
C:\Windows\system32>net localgroup Marketing bbennet /add
The command completed successfully.
```

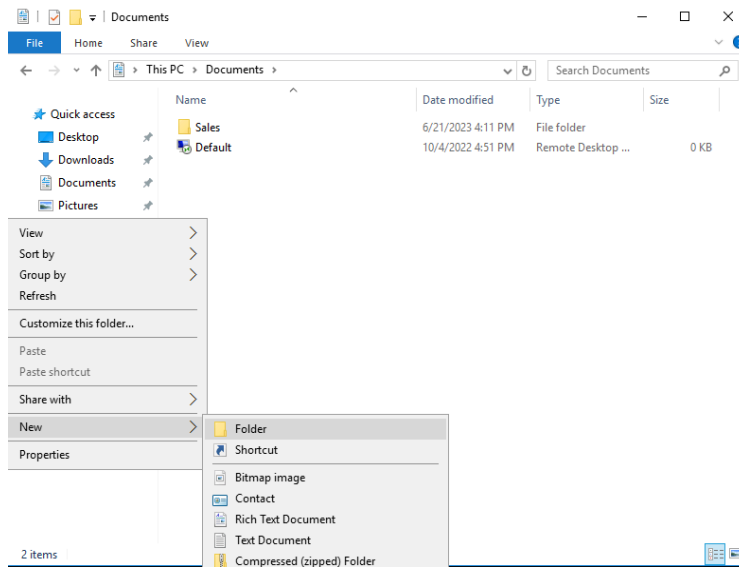
- e. Confirm that the user had been successfully added to the group by running the command **net localgroup <group name>**

```
C:\Windows\system32>net localgroup Marketing
Alias name      Marketing
Comment
Members
-----
bbennet
The command completed successfully.
```

4. Now that our user name and group have been added, we need to create a shared file so only the assigned department can access information in one location. For this task, we will be exiting out of the Command Prompt and entering the system's GUI. To do this, we will be clicking on the "File Explorer" in the Windows Bar at the bottom of our screen.



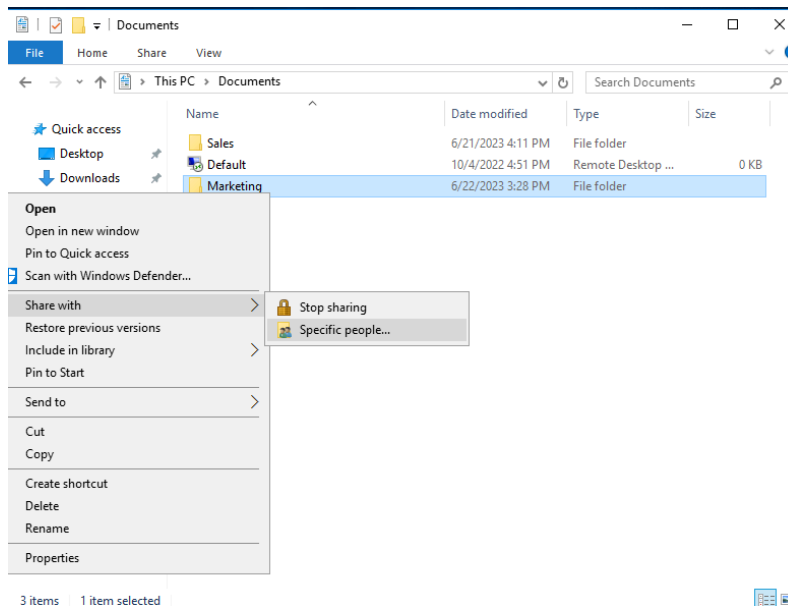
- a. In the GUI, select Documents and RIGHT CLICK, opening the option bar. We can then move down to the New selection and click New Folder. Name this folder. In this example, we will be using "Marketing".



b. Once the folder is created, you should see the new folder.

Name	Date modified	Type	Size
Sales	6/21/2023 4:11 PM	File folder	
Default	10/4/2022 4:51 PM	Remote Desktop ...	0 KB
Marketing	6/22/2023 3:28 PM	File folder	


c. To share it with the correct group, RIGHT CLICK the Marketing folder and select "Share With" and then select "Specific People..."



d. Add members to the group by entering their user name in the Add Bar and hitting Add. In this case, we are adding "bbennet".



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
 fstack	Owner

[I'm having trouble sharing](#)

- e. As this is a shared file, we must make sure that all members of the group have read and write privileges. To do this, we will RIGHT CLICK and select "Read/Write" in the drop down menu. This will assign anyone in the group read/write permissions.

Name	Permission Level
 CONTOSO\bennet	Read
 fstack	Owner



Read ▼
 Read/Write
 Remove

- f. Finally, we want to make this file shareable. If we look at the bottom of the "File Sharing" window, we will see a "share" button. When we click this, we are given the option to email the link or copy and share it with other people.

←  File Sharing

Choose people on your network to share with

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

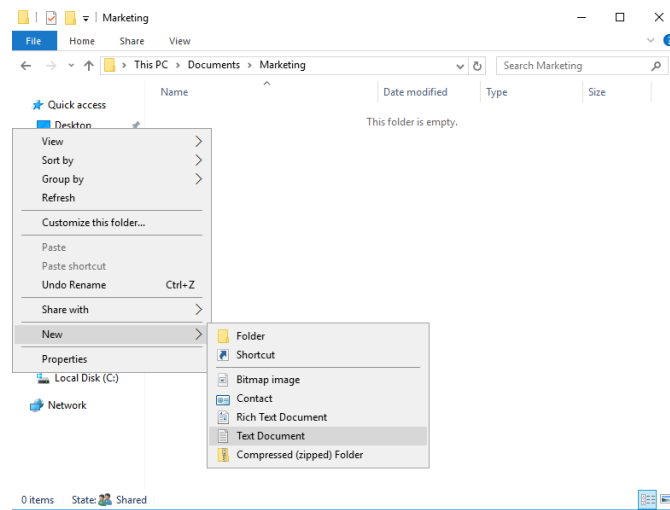
Name	Permission Level
 CONTOSO\bennet	Read/Write ▼
 fstack	Owner

[I'm having trouble sharing](#)

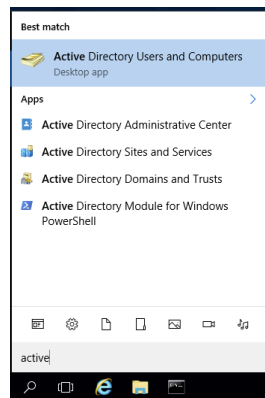
Share
Cancel

- g. To create a new text file in the specific shared folder, simply open the appropriate folder and RIGHT CLICK in the blank space. Move down the drop menu and click "New". Then, in the new pop-up menu, choose "Text"

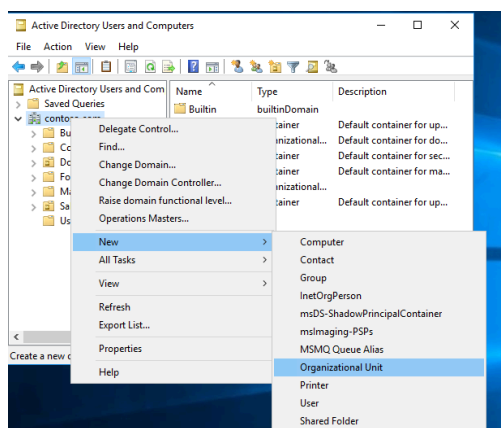
Document” and create. For training purposes, we named this document “test.txt”.



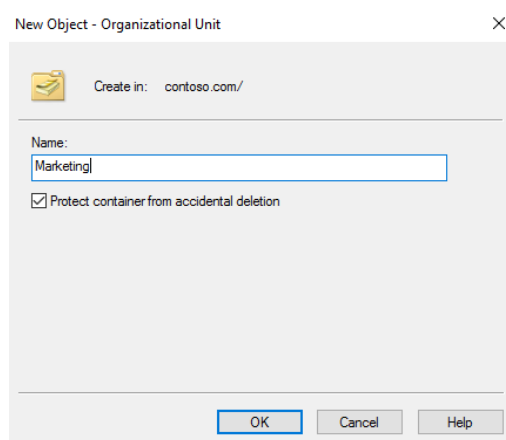
5. Our new user, group, and shared folders are now created, it is time to put them in an organizational unit, also known as an OU. To do this, we will continue to use the GUI. We will also be attaching a Group Policy Object or GPO to the unit.
 - a. Navigate via the search bar in the bottom left of the desktop to “Active Directory Users and Computers”.



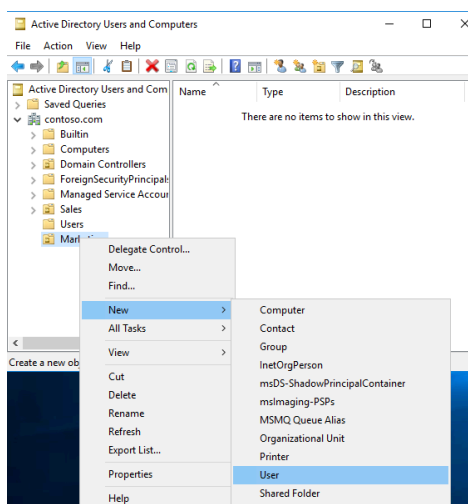
- b. In the new pop-up window, RIGHT CLICK on the contoso.com directory and go to the “New” tab in the drop down menu. From there, click on the “Organizational Unit”.



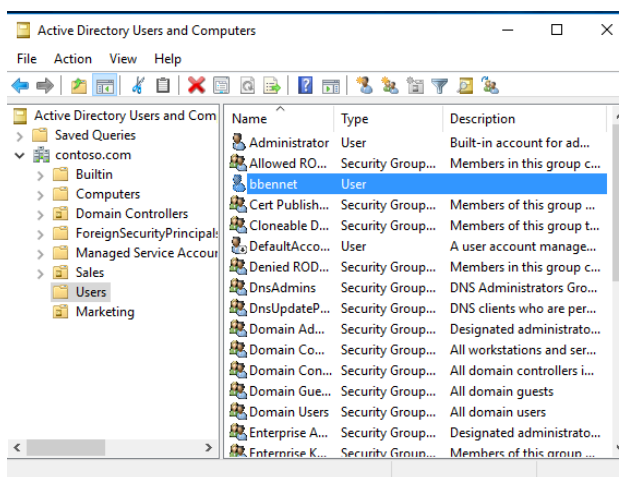
- c. Name the new OU. In this instance, we are naming it "Marketing".



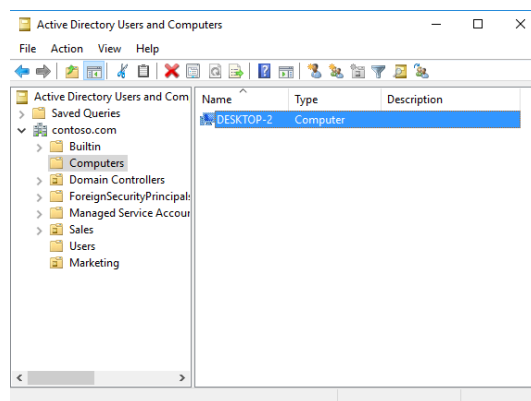
- d. To add a user, RIGHT CLICK on the Marketing OU and move on the drop down menu to "New". Click on "User" from the New menu.



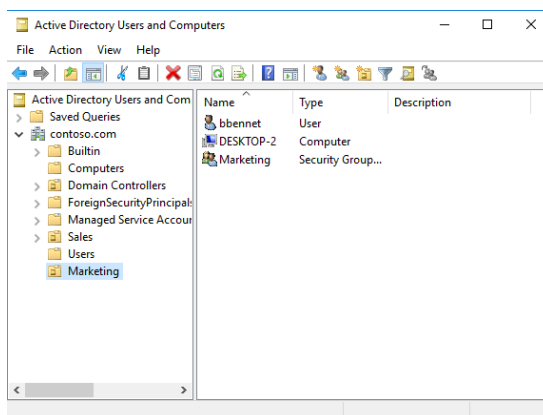
- e. From here, you can add the details of the new user manually, or you can also open the "Users" folder under consoto.com and drag the desired user names and groups into the Marketing OU Folder.



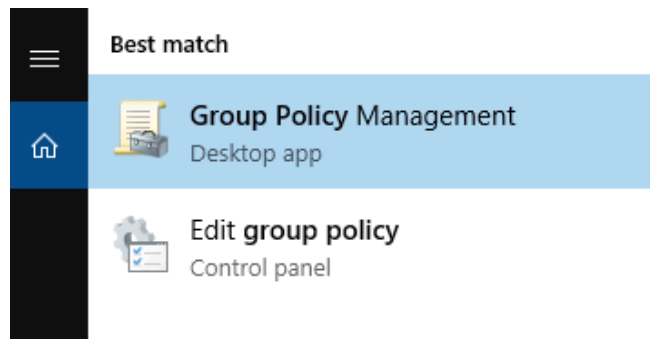
- f. We also want to make sure we add the Computer that the new user is on into the OU. To do this, we simply open the “Computers” folder and drag the correct computer into the OU, like we did the users and groups.



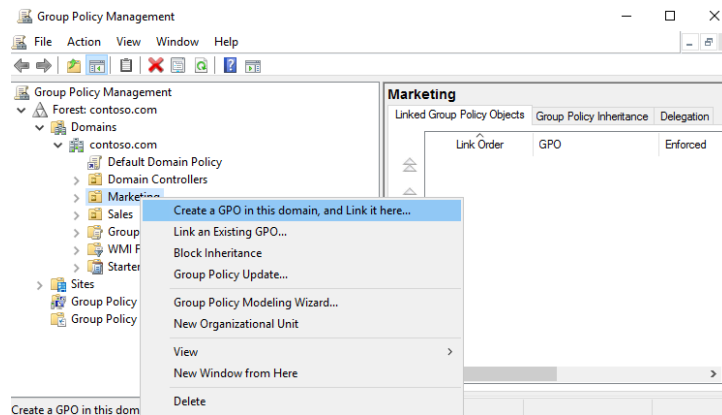
- g. Double check your work by opening the Marketing OU Folder and confirming that the correct users, groups, and computers have been added.



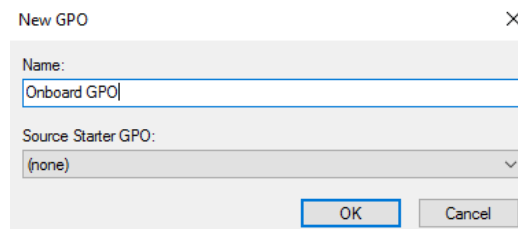
- h. To attach the Group Policy Object, return to the GUI and navigate to Group Policy Management.



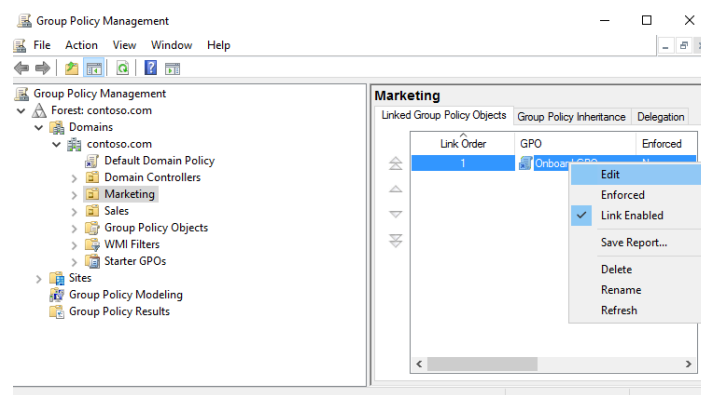
- i. RIGHT CLICK on Marketing OU and click "Create a GPO".



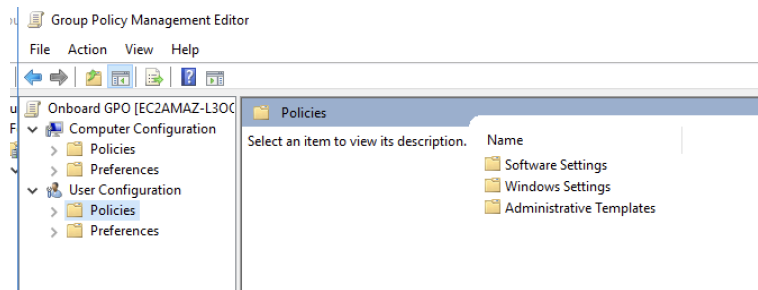
- j. Set a desired name for your GPO. In this instance, we chose the name "Onboarding GPO". Press "OK" and your OU will now have an attached GPO.



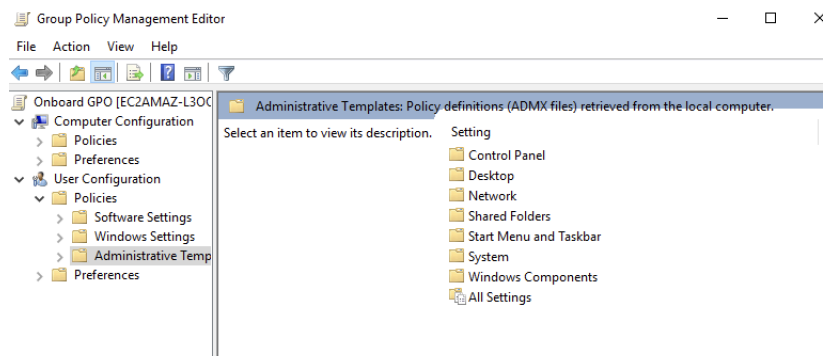
6. Our GPO has been added to the Marketing OU and we need to edit and apply certain rules. We need to add a rule that a message appears when the computer starts, prevent the users access to CMD, add a script to the user's login to map the share folder that was created, and to disable the "Run" command from the Start Menu.
- Right click on the newly created GPO which is located in the OU and then click "Edit" in the drop down menu.



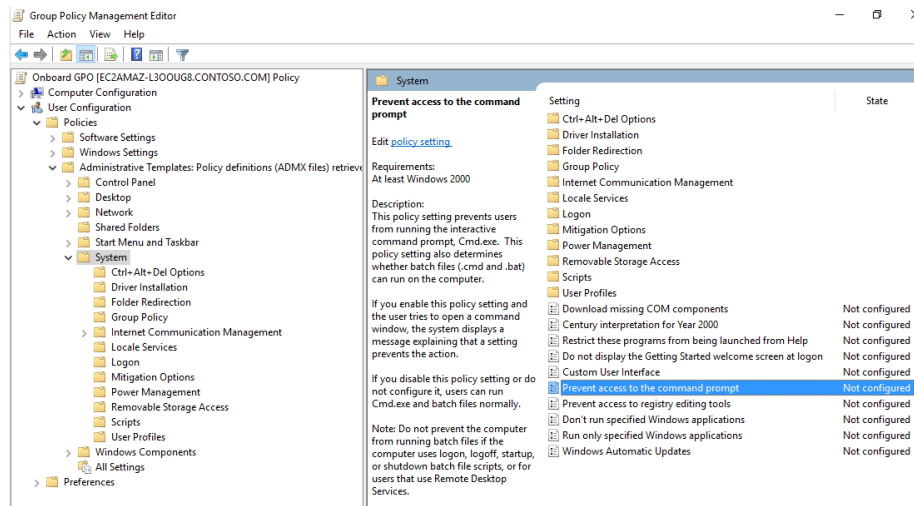
- b. The first thing we want to accomplish is preventing access to CMD. In the GPO edit menu, we will open the drop down menu for “User Configuration”, then “Policies”



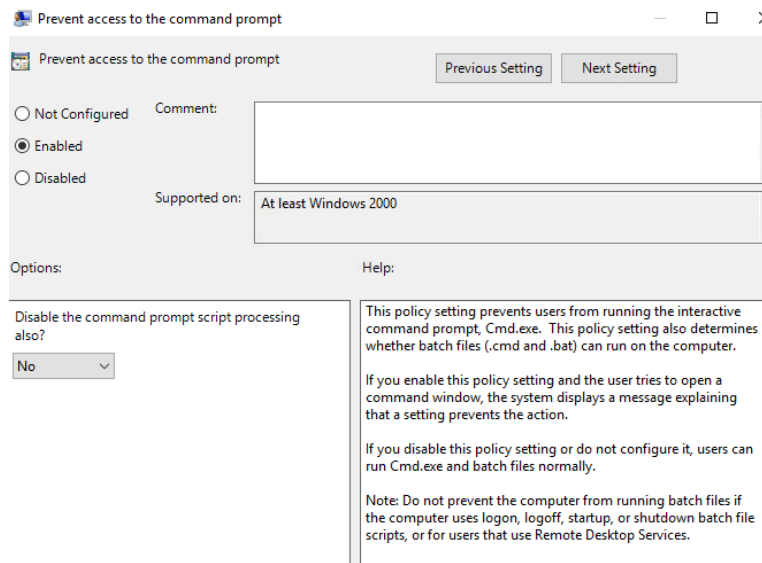
- c. From the “Policies” menu, we will enter the “Administrative Templates”.



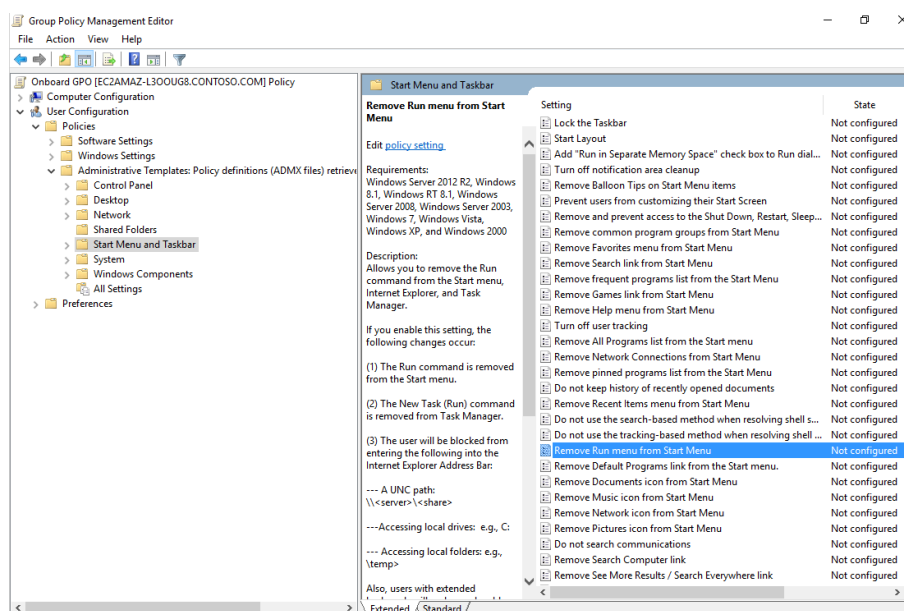
- d. We will then click on “System”. In the System menu we will double left click the “Prevent access to the command prompt” file.



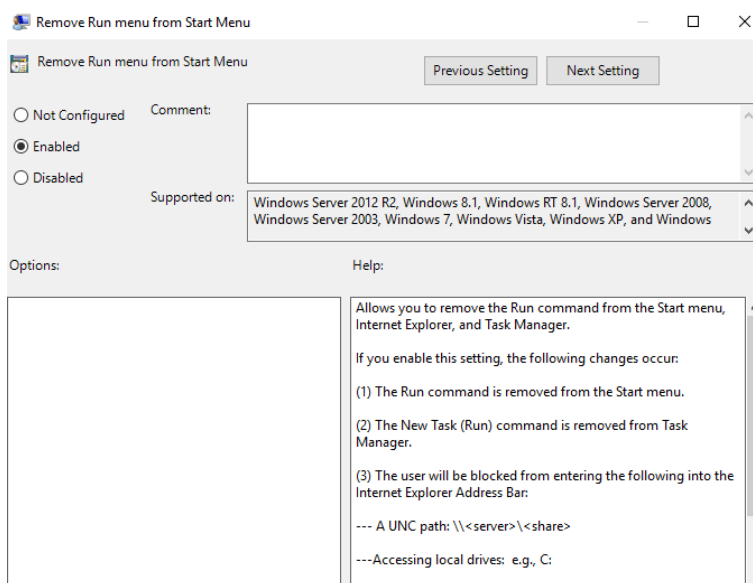
- e. Select Enable and click “OK”. This is to prevent the user from accessing CMD.



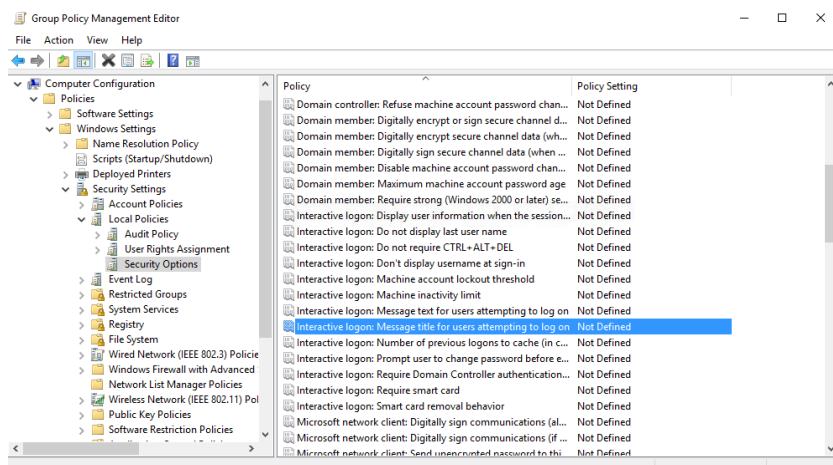
- f. Our next rule we will edit in the GPO is disabling the “Run” command from the Start menu. In the GPO Edit Window, we will stay in the “Administrators Templates” folder under “User Configuration” and switch to the “Start Menu and Taskbar” folder.



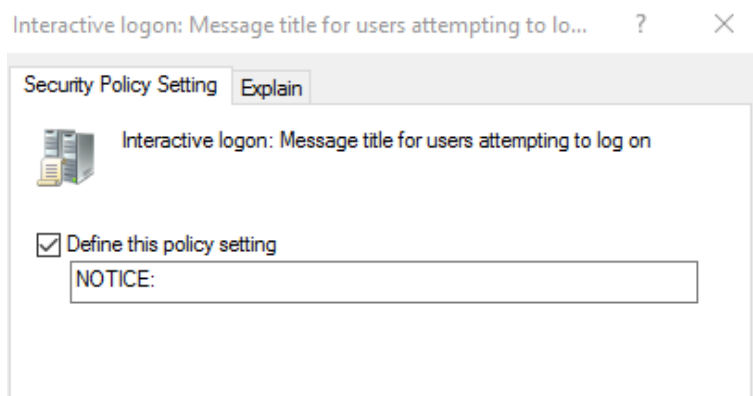
- g. In the folder, locate the file that says "Remove Run menu from Start menu". Select enable and press "OK".



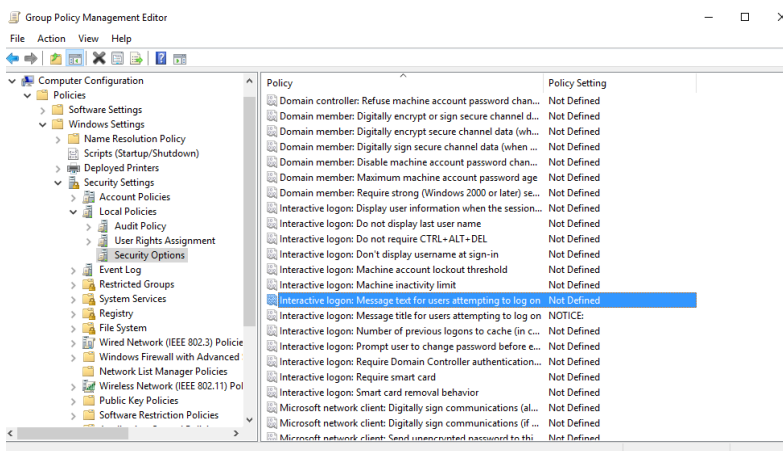
- h. To create an automated message when the computer starts up, we will continue to stay in the Group Policy Management Editor. We will be entering the "Computer Configuration" menu located in the left side window. Similar as to how we navigated the "User Configuration", we will be opening the "Policies" folder, followed by "Window Settings", then "Local Policies". In "Local Policies", we will open "Security settings". Single click "Security Options" and find the policy named "Interactive Logon: Message Title for users". Double click this file.



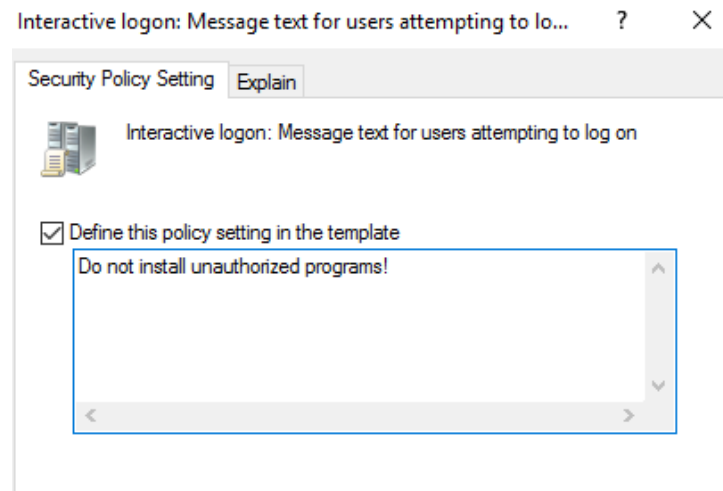
- i. Select Define this policy and type in the header of your message box, we use in this instance "Notice:" then press "OK".



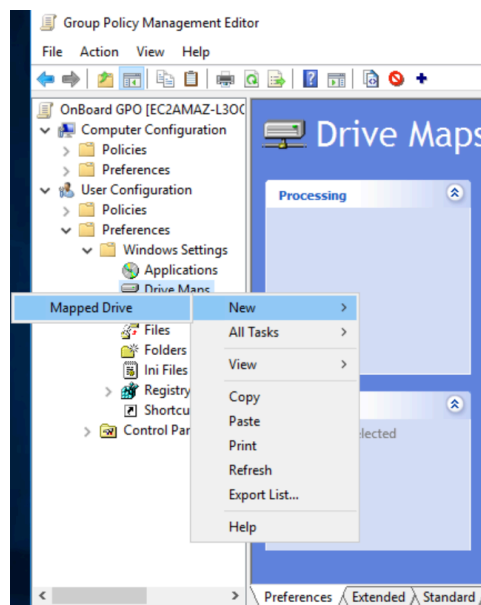
- j. Next double click the policy named "Interactive logon: Message text for users attempting to log on"



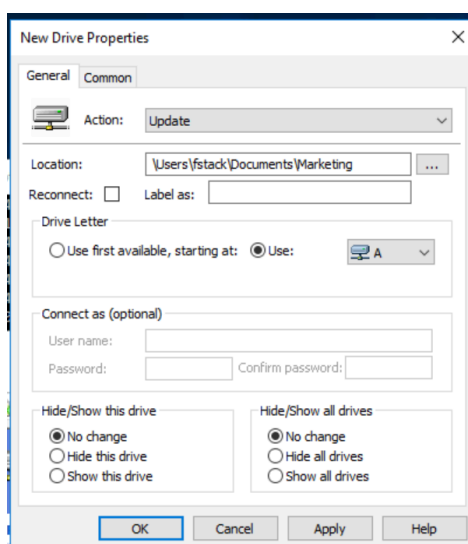
- k. Select the define this policy box and type in your message that you want to appear. Then click "OK".



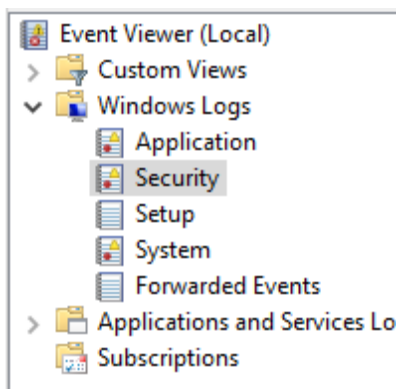
- l. The final rule we will be editing into the GPO will be to add a script to the user's login to map the share you created. To begin, we will stay in the Group Policy Management Editor window. Return to the "User Configuration" folder and go to "Preferences". Open the "Windows Settings" folder and open the Drive Maps. RIGHT CLICK on the "Drive Maps" file and select "Mapped Drive" under the "New" drop down menu.



- m. Paste the absolute path of the shared folder in the Location box; select "Use" and choose drive "A" and select OK. For this instance, the absolute path is `\\Users\fstack\Documents\Marketing`.



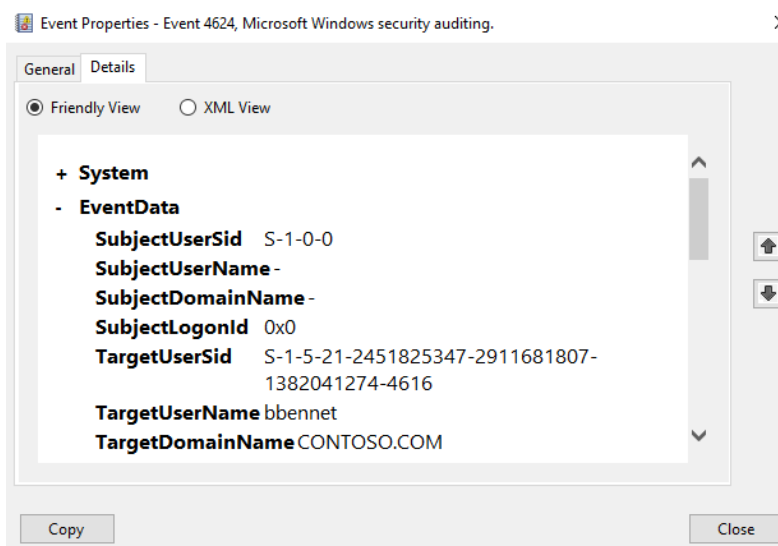
7. Our GPO and OU are now set up, so it is time to check the Event Viewer on the Server Machine to view any successful login attempts from the user. For this, we will be looking for bbnnet login information. **Note: We will be logged in on the domain administrator account.**
 - a. Open the Event Viewer in the GUI and select the drop down menu for "Windows Logs" and then select "Security".



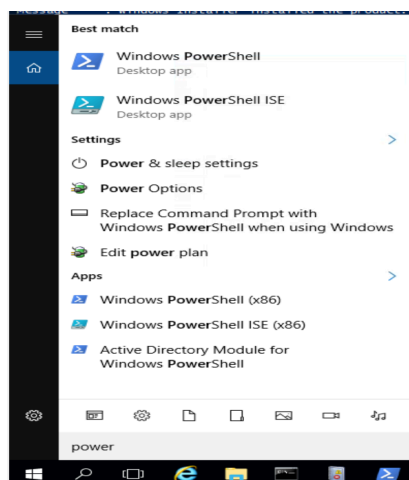
- b. We can filter for specific items by clicking the Task Category column or the Date and Time column. This will sort the available events and make navigation easier. Using this method we can find the most recent Logon Task Category entry. Double click it.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	6/22/2023 5:48:23 PM	Microsoft Win...	4634	Logoff
Audit Success	6/22/2023 5:48:23 PM	Microsoft Win...	4627	Group Membe...
Audit Success	6/22/2023 5:48:23 PM	Microsoft Win...	4624	Logon
Audit Success	6/22/2023 5:48:23 PM	Microsoft Win...	4627	Group Membe...
Audit Success	6/22/2023 5:48:23 PM	Microsoft Win...	4624	Logon
Audit Success	6/22/2023 5:48:23 PM	Microsoft Win...	4627	Group Membe...

- c. Click the details tab and scroll down to find information related to this entry. If you look at "TargetUserName" we can see which user logged on at this time for this entry. In this example it is bbennet.



8. As we are now familiar with the Command Prompt, GPO and Event Viewer, we will now use the PowerShell to check what the latest program installed on the computer was. To begin this process, we open the Powershell as an administrator by right clicking it after searching for it on the start bar.



- a. Enter this the script `Get-WinEvent -ProviderName msiinstaller | where id -eq 1033 | select timecreated,message | FL *`. We will quickly break down this script line to make it understandable.
- `Get-WinEvent` is the command to output events from the event log.
 - `-ProviderName msiinstaller` msiinstaller is the name of the provider we are searching for.

- iii. The pipeline operator connects the **Get** command to the **where** command. In the second part of this script, we are looking for the ID that is equal to 1033 (1033 is the product language code for English).
- iv. The pipeline is used once again to connect a third command in the script. The **select** command shifts the script from locating a specific ID to a time message as we can see in the **timecreated,message** string.
- v. Finally, we pipeline the commands into a final command line. **FL** is abbreviated from Format-List. The ***** is a wildcard. This means that the output will include anything else in the script after the specific command strings.

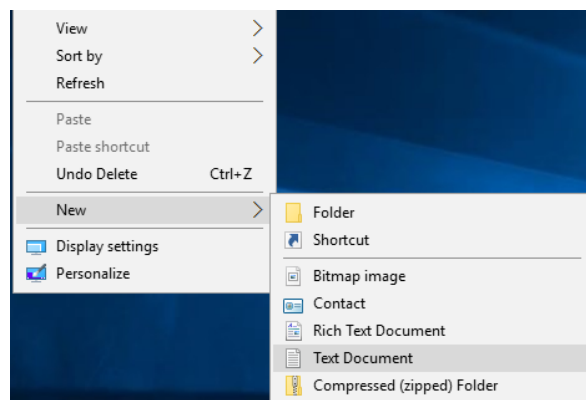
```

Select Administrator: Windows PowerShell
PublisherId      : cwsnlh2xyewy
PackageUserInformation : {S-1-5-21-2451825347-2911681807-1382041274-500 [CONTOSO\Administrator]: Installed, S-1-5-21-2451825347-2911681807-1382041274-1008 [CONTOSO\Fstack]: Installed}
IsResourcePackage  : False
IsBundle           : False
IsDevelopmentMode   : False

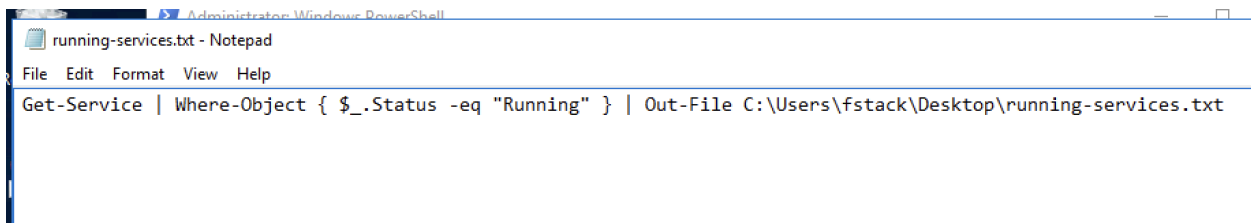
PS C:\Windows\system32>
PS C:\Windows\system32> Get-WinEvent -ProviderName msiinstaller | where id -eq 1033 | select timecreated,message | FL
TimeCreated      : 2/12/2023 12:59:48 AM
Message          : Windows Installer installed the product. Product Name: Amazon SSM Agent. Product Version: 3.2.582.0. Product Language: 1033. Manufacturer: Amazon Web Services. Installation success or error status: 0.
TimeCreated      : 10/10/2022 3:55:45 PM
Message          : Windows Installer installed the product. Product Name: Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332. Product Version: 14.32.31332. Product Language: 1033. Manufacturer: Microsoft Corporation. Installation success or error status: 0.
TimeCreated      : 10/10/2022 3:55:45 PM
Message          : Windows Installer installed the product. Product Name: Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332. Product Version: 14.32.31332. Product Language: 1033. Manufacturer: Microsoft Corporation. Installation success or error status: 0.
TimeCreated      : 9/15/2022 3:39:47 PM
Message          : Windows Installer installed the product. Product Name: Amazon SSM Agent. Product Version: 3.1.1767.0. Product Language: 1033. Manufacturer: Amazon Web Services. Installation success or error status: 0.
TimeCreated      : 9/15/2022 4:15:11 AM
Message          : Windows Installer installed the product. Product Name: NICE Desktop Cloud Visualization Server (64 bit). Product Version: 22.1.13300.0. Product Language: 1033. Manufacturer: NICE Software. Installation success or error status: 0.
TimeCreated      : 9/15/2022 4:14:20 AM
Message          : Windows Installer installed the product. Product Name: NICE DCV Virtual Display. Product Version: 1.3.58.0. Product Language: 1033. Manufacturer: NICE Software. Installation success or error status: 0.
PS C:\Windows\system32>

```

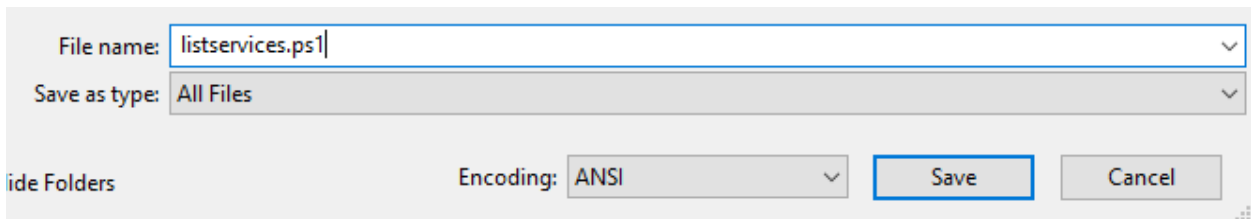
- b. Obtain the list from the script and choose the first installed program as the answer.
9. Now that we know how a script for Windows PowerShell looks, we will write one that gives a list of all running services and puts it in a file named "running-services.txt".
- a. To create a blank text document, RIGHT CLICK on the desktop and select "New". In the drop down menu, select "Text Document". Rename it "running-services.txt".



- b. Enter the script you wish to run. In this instance, we are using `Get-Service | Where-Object { $_.Status -eq "Running" } | Out-File C:\Users\fstack\Documents\running-services.txt`
- `Get-Service` is the command we will use to get a list of services.
 - `Where-Object` is the next command that will select objects based on values.
 - `{ $_ }` Is a placeholder so we can search for an event status that is equal to "Running".
 - The pipeline will then create a new output file from the absolute path. In this case, it is `C:\Users\fstack\Documents\running-services.txt`



- c. When we save the file, we will use Save As and name it "listservices.ps1". Using the ".ps1" extension is what we use to save PowerShell text scripts.



- d. When we run PowerShell, we must go to the location of the text file. We will use the above absolute path for that. Then we change into the directory, input `.\running-services.txt` to receive output. The Notepad text document we created will appear on the desktop.
- e. A new file is also created named PAUSE on the desktop. If we open this file, we see a list of services that are running.

PAUSE - Notepad

File Edit Format View Help

Status	Name	DisplayName
Running	ADWS	Active Directory Web Services
Running	AmazonSSMAgent	Amazon SSM Agent
Running	AppHostSvc	Application Host Helper Service
Running	AppInfo	Application Information
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_5b621	CDPUserSvc_5b621
Running	CertPropSvc	Certificate Propagation
Running	CoreMessagingRe...	CoreMessaging
Running	CryptSvc	Cryptographic Services
Running	DcomLaunch	DCOM Server Process Launcher
Running	dcdserver	DCV Server
Running	Dfs	DFS Namespace
Running	DFSRepl	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