Before you begin, decide with your group:

* Name of the new hire ----- Pil So
* Non-technical role at StackFull Software (i.e., recruiter, sales associate, social media associate) ----- Recruiter
* Department they work in (i.e., HR, Sales, Marketing) ---- HR

Step 1

Join the computer to the domain (the domain name is contoso.com). The username/password is administrator/Pa$$w0rd.

Make sure you change the ip address to 172.31.48.240 for the ipv4 address in your driver settings.

Got to control panel and then to Network and Internet.

A screenshot of a computer

Description automatically generated

Network and Sharing Center

A screenshot of a computer

Description automatically generated

Change Adapter Settings

A screenshot of a computer

Description automatically generated

Right click on Ethernet 2 and go to properties

And then go to Internet Protocol Version 4

A screenshot of a computer

Description automatically generated

Double click on the yellow and then go to DNS server address.

A screenshot of a computer

Description automatically generated

Hit Ok on all and then go to the next steps.

Bottom Left type here to search for “this pc” and right click properties and go to rename this pc (advanced) and then go to change.

A screenshot of a computer

Description automatically generated

Then put in the username and password, which is administrator/Pa$$w0rd

A screenshot of a computer

Description automatically generated

You are now welcomed into the domain.

A screenshot of a computer error

Description automatically generated

You can either to 23 things you can either restart it or use CMD: gpupdate /force

In order to accept the policy within Active Directory Or AD for short.

You can also verify when you look at the internet icon to see if your in the domain.

A screenshot of a computer

Description automatically generated

Step 2

Switch to the server. Create a user for the new hire and set a password.

Use the search box or hit the magnifying glass to search for active directory or use the pin to get to active directory.

A computer screen shot of a computer

Description automatically generated

Right click on the contoso.com domain and then go to new and then user.

A screenshot of a computer

Description automatically generated

Then create a password and it’s up to you to decide what password and make sure you check on next login, so the user can set up their own but for this exercise I will uncheck mine.

A screenshot of a computer

Description automatically generated

Verify that it’s in your domain.

A screenshot of a computer

Description automatically generated

Step 3

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

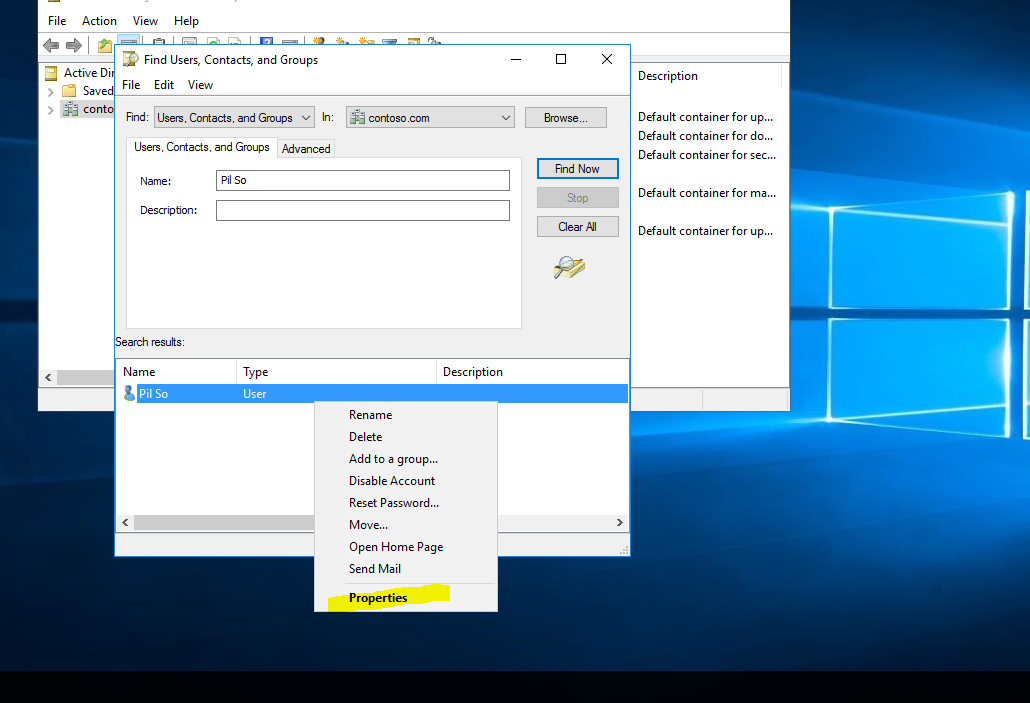
Right click on the domain and go to new and then go to group.

There you will need to put in whatever department the user is in.

A screenshot of a computer

Description automatically generated

And then go to right click on find and then find your user and right click on the name and then go to properties.



Then go to member of tab and then press the add button and then add whatever department he or she is in.

A screenshot of a computer

Description automatically generated

Step 4

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.

There are several ways to do this, but this is how I do it.

Create a folder within the desktop or wherever you like to put the shared folder in.

And then create the documents you want to go back to HR folder and then right click properties.

A screenshot of a computer

Description automatically generated

Go to the sharing tab and then hit share, after which put in a name and then add you can also change permissions when you look at the yellow.

A screenshot of a computer

Description automatically generated

Go back to Desktop 2 and then you can map the network folder into your drive.

Depending on if you know the Network Path.

[\\EC2AMAZ-L3OOUG8\Users\fstack\Desktop\HR](file:///\\EC2AMAZ-L3OOUG8\Users\fstack\Desktop\HR)

A screenshot of a computer

Description automatically generated

Go back to Desktop 2 and then add the network drive into your c drive.

Right click anywhere is a blank space in the devices and drive and go to add a network location.

A screenshot of a computer

Description automatically generated

Hit next and then put the network path on your network drive.

A screenshot of a computer

Description automatically generated

Hit next and you should see it in network location.

A screenshot of a computer

Description automatically generated

Step 5

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.

Go back to server and then right click on the domain. And go to new and then go to organizational unit.

A screenshot of a computer

Description automatically generated

Then create your name and hit ok

A screenshot of a computer

Description automatically generated

Right click on your user and then go to move and move it to the Organizational Unit. Same as follows for the security group.

A screenshot of a computer

Description automatically generated

Step 6

Edit the GPO and apply the following rules:

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

A message should appear whenever the computer starts (do not install unauthorized programs).

Search for Group Policy Management and then click on Default Domain Policy and right click it and then go to edit.

A computer screen with a white box

Description automatically generated

A message should appear whenever the computer starts (do not install unauthorized programs).

In the left pane of the Group Policy Management Editor, navigate to Computer Configuration> Policies > Windows Settings > Security Settings > Local Policies and select Security Options. On the right pane of the console, select the Interactive Logon: Message text for users attempting to logon policy.

After which check define this policy and then write the message you want to put in and then hit apply.

A screenshot of a computer

Description automatically generated

Also which go to interactive logon: Message title for user and double click on that and create a title for this message.

A screenshot of a computer

Description automatically generated

Prevent the user's access to CMD.

In the Group Policy Management Editor by right clicking default domain policy and then go to edit, navigate to User Configuration/Administrative Templates/System. Look for the policy setting “Prevent access to the command prompt” and select Edit.

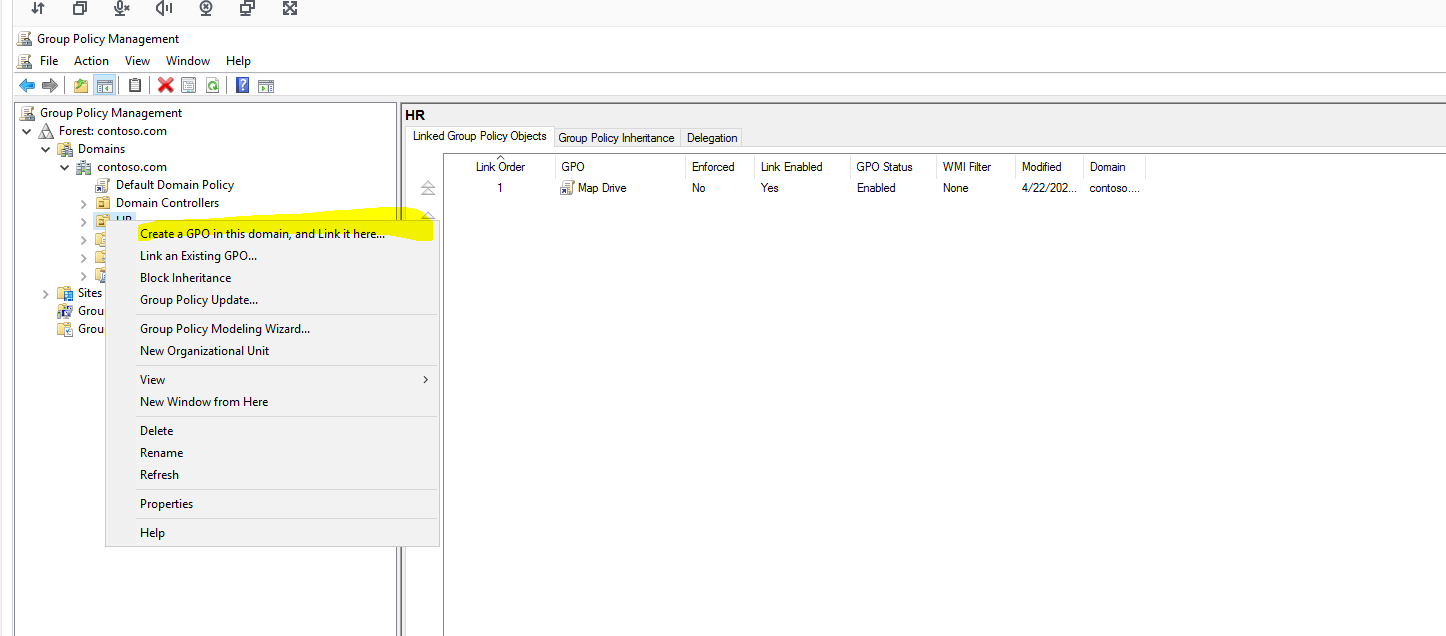
After which you Enabled it and hit apply and Ok.

A screenshot of a computer

Description automatically generated

Add script to the user's login to map the share you created.

Go to group policy management and then go to HR and right click to get to create a GPO in this domain.



Name the GPO to however you want it to be.

A screenshot of a computer

Description automatically generated

And then hit ok. After which right click the map drive and go to edit.

A screenshot of a computer

Description automatically generated

After which you go to User configuration --- preferences --- windows settings –then to drive map.

A screenshot of a computer

Description automatically generated

Double click on Drive Maps and then right click new and the map drive. Put the path you want in the location and make sure you label it as and put a map letter on it as well. And use create as the action.

A screenshot of a computer

Description automatically generated

Disable the run command from the start menu.

First you need to create another GPO within HR and make the policy Disable Run Command. After which you need to right click Disable Run Command and go to edit.

A screenshot of a computer

Description automatically generated

Open Group Policy Editor and navigate to User Configuration > Administrative Templates > Start Menu and Taskbar. Double-click on Remove Run menu from Start Menu. Then go to hit Enabled and hit ok.

A screenshot of a computer

Description automatically generated

Once everything is done go to CMD right click make sure you’re using administrative credentials after which. “gpupdate /force” to make sure that desktop2 can catch the policies.

A computer screen shot of a computer screen

Description automatically generated

Step 7

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).

administrator/Pa$$w0rd.

Sign out and then use the administrator account in red, and then go search using the magnifying glass event viewer.

After which Windows Logs---- Security----

A screenshot of a computer

Description automatically generated

Check the logs make sure your in Logon in Task Category

NullSID security ID – time stamp: 4/22/2024 time: 8:46.

Step 8

Use PowerShell to check what the latest program installed on the computer was.

Press the Windows Key + X and select Windows PowerShell (Admin).

Type in “wmic qfe list”.

This will tell you all the updates and programs installed on the computer was.

A blue screen with white text

Description automatically generated

Step 9

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

Go to PowerShell and make sure you’re an administrator.

After which copy the code and run it, it should execute a text file in your c drive.

A screenshot of a computer

Description automatically generated

Get-Service | where {$\_.Status -eq "Running"} | Out-File "C:\running\_services.txt"

A screenshot of a computer

Description automatically generated