Share Permissions and Home Folders

Introduction and/or Background

Tx-Rig is collecting more and more documents and users. It's becoming important to the organization that documents are shared with the proper people.

Texas Rig, Inc.
Fueling The Future.

Objectives

In this project/lab the student will:

- Enable File Sharing
- Create Home Folders
- Configure Shared Network Printing

Equipment/Supplies Needed

- VMWare Workstation Pro
- Windows Server 2019 Virtual Machine

Assessment Criteria

- Take a screenshot of the results of the icacls command (PrtScr#1)
- Take a screenshot of the jgarza.txt document (PrtScr#2)
- Take a screenshot of the results of the icacls command (PrtScr#3)
- Take a screenshot of File Explorer showing the M drive (PrtScr#4)
- Take a screenshot of the results of the **net use** command (PrtScr#5)
- Take a screenshot showing the created home folders (PrtScr#6)
- Take a screenshot of the results of the **net use** command (PrtScr#7)
- Take a screenshot of the results of the net share command (PrtScr#8)
- Take a screenshot of the results of the net share command (PrtScr#9)
- Answer the reflection questions in a text file

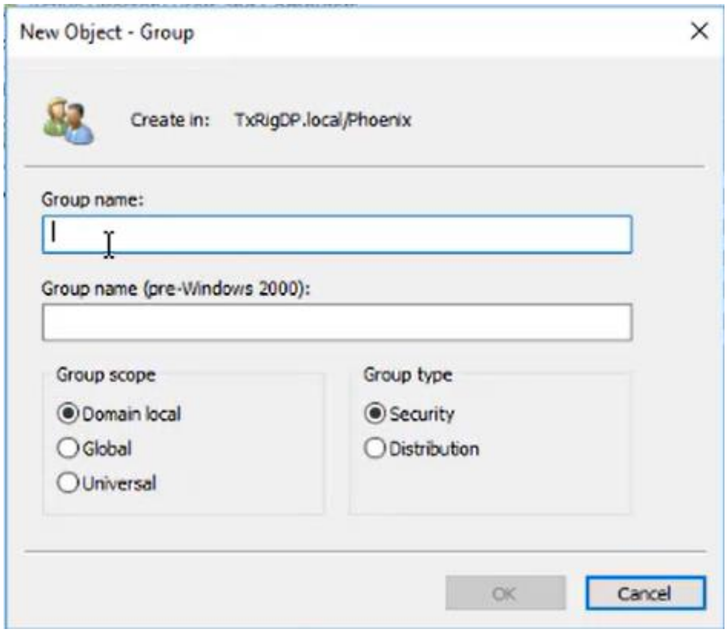
Assignment

Part 1

Exercise 1: Sharing a Folder with the File Sharing Wizard

In this activity, you will use the GUI to configure Share and NTFS permissions on the Windows Server operating system.

1. Log on to your server as ***Administrator.***
2. Open **Active Directory Users and Computers**. Click the **Phoenix** OU. Create a **domain local** group named **TestSharing-DL** to use for permission assignments. Add **jgarza** user account to TestSharing-DL group. Close Active Directory Users and Computers.



New Object - Group

Create in: TxRigDP.local/Phoenix

Group name:

Group name (pre-Windows 2000):

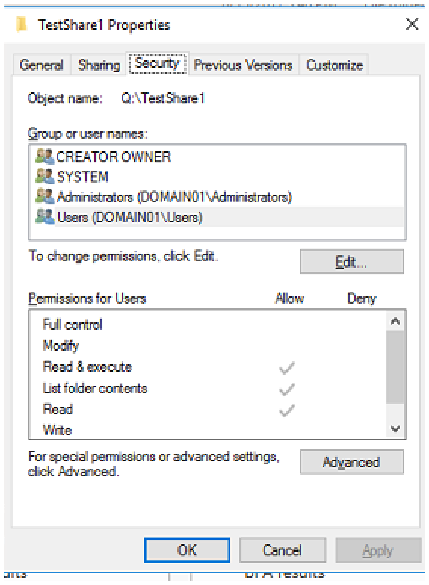
Group scope

● Domain local
○ Global
○ Universal

Group type

● Security
○ Distribution

3. Open **File Explorer**, and click to open the **RAID-5** volume. Create a folder named **TestShare1**.
4. Open the TestShare1 folder's **Properties** dialog box, and click the **Security** tab. Make a note of the permissions assigned on this folder. Close the Properties dialog box.



Object name: Q:\TestShare1

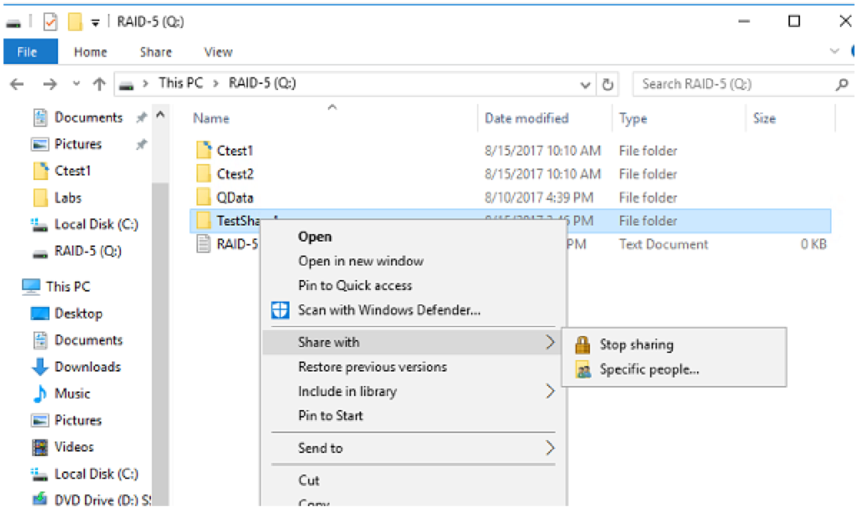
Group or user names:
- CREATOR OWNER
- SYSTEM
- Administrators (DOMAIN01\Administrators)
- Users (DOMAIN01\Users)

To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

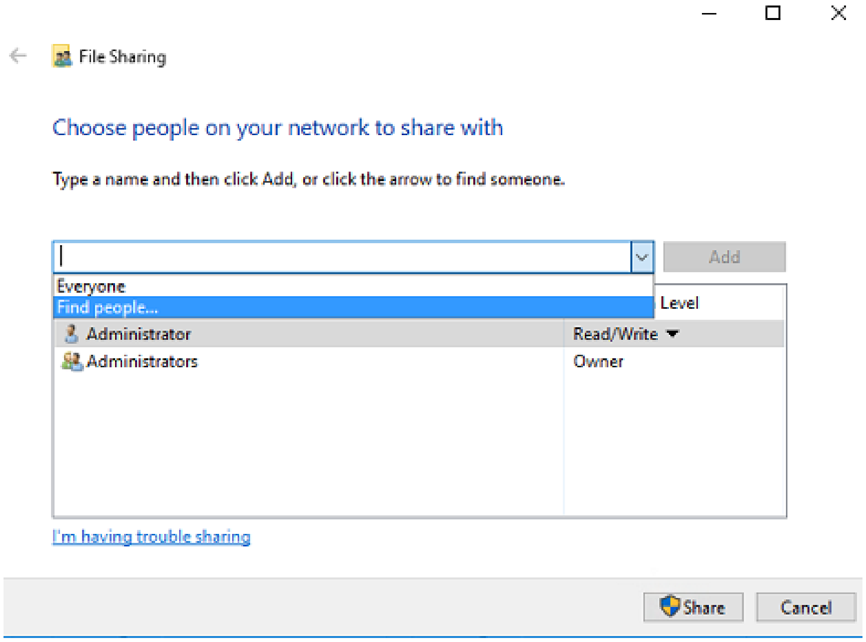
For special permissions or advanced settings, click Advanced.

5. Right-click **TestShare1** in the left pane and click **Give access to** and select **Specific people** to start the File Sharing Wizard.



Name	Date modified	Type	Size
Ctest1	8/15/2017 10:10 AM	File folder	
Ctest2	8/15/2017 10:10 AM	File folder	
QData	8/10/2017 4:39 PM	File folder	
TestSha	PM	File folder	
RAID-5	PM	Text Document	0 KB

6. Click the list arrow next to the **Add** button and click **Find People** in the list.



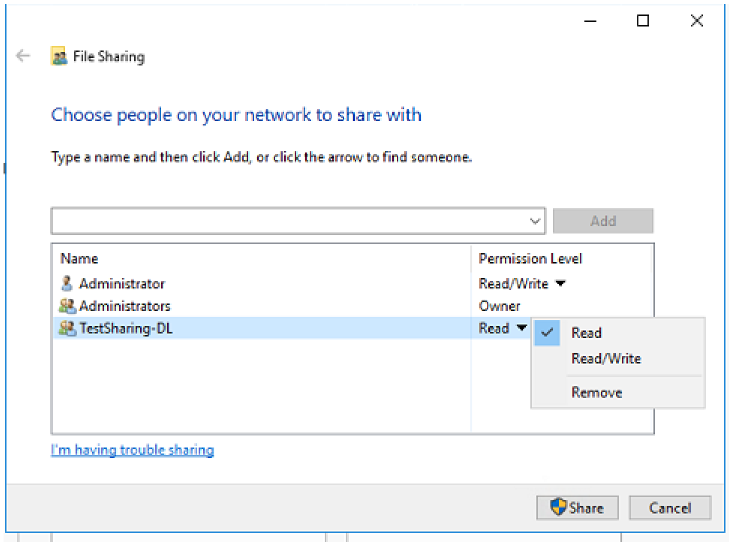
File Sharing

Choose people on your network to share with

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

	Level
Administrator	Read/Write
Administrators	Owner

7. Type **TestSharing-DL**, click **Check Names**, and then click **OK**. In the Permission Level column for the **TestSharing-DL** entry, click the list arrow and click **Read/Write**.



File Sharing

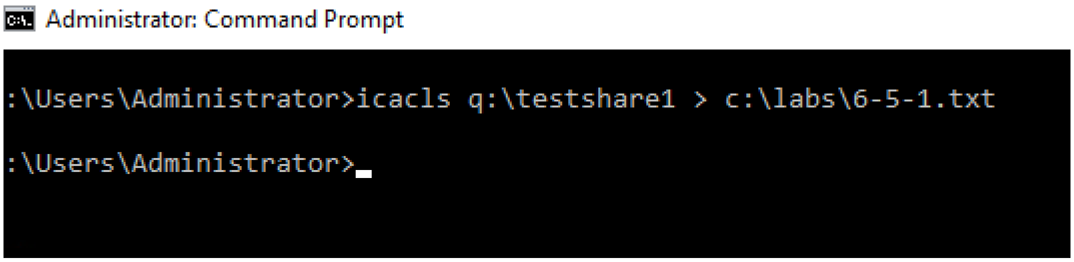
Choose people on your network to share with

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

Name	Permission Level
Administrator	Read/Write
Administrators	Owner
TestSharing-DL	Read

8. Click **Share**. Notice that in the last window of the wizard, you can email links to the shared folder or copy the links to the Clipboard. Click **Done**.
9. Open a command prompt as administrator and type **icacls q:\testshare1**.

10. Take a screenshot of the results of the icacls command (PrtScr#1).

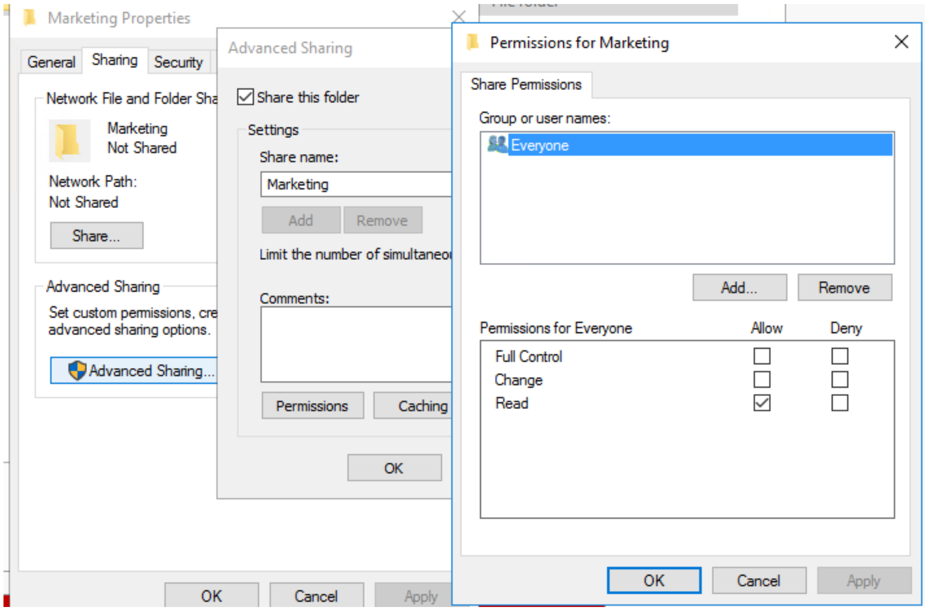


Administrator: Command Prompt

```
:\Users\Administrator>icacls q:\testshare1 > c:\labs\6-5-1.txt

:\Users\Administrator>_
```

Exercise 2: Sharing a Folder with Advanced File Sharing:

1. Log on to your server as ***Administrator***.
2. Open **File Explorer**, and click to open the **RAID-5** volume and create a folder named **Production.**
3. Right-click the **Production** folder and click **Properties.** Click on the **Sharing** tab and click **Advanced Sharing**. Click to select the **Share this folder** check box. Leave the share name as is, and then click the **Permissions** button. By default, the share permission is Allow Read for Everyone.



Marketing Properties

Network File and Folder Sha

Marketing
Not Shared

Network Path:
Not Shared

Advanced Sharing

Set custom permissions, cre
advanced sharing options.

Advanced Sharing

☑ Share this folder

Share name: Marketing

Limit the number of simultaneo

Comments:

Permissions for Marketing

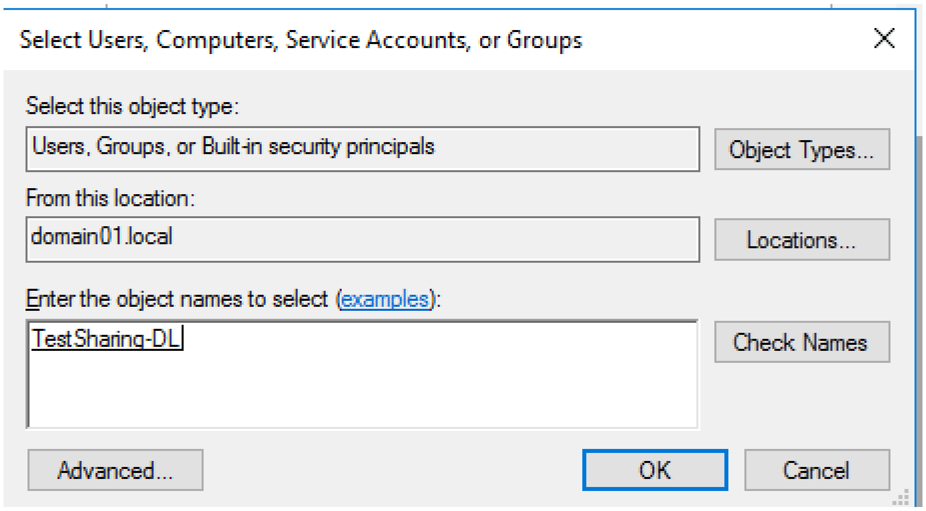
Group or user names:
Everyone

Permissions for Everyone

Permissions for Everyone	Allow	Deny
Full Control	☐	☐
Change	☐	☐
Read	☑	☐

4. Because you don't want the Everyone special identity to have Read permission, click **Remove**. Click **Add**, type **TestSharing-DL**, click **Check Names**, and

then click **OK**.



Select Users, Computers, Service Accounts, or Groups

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

From this location: domain01.local

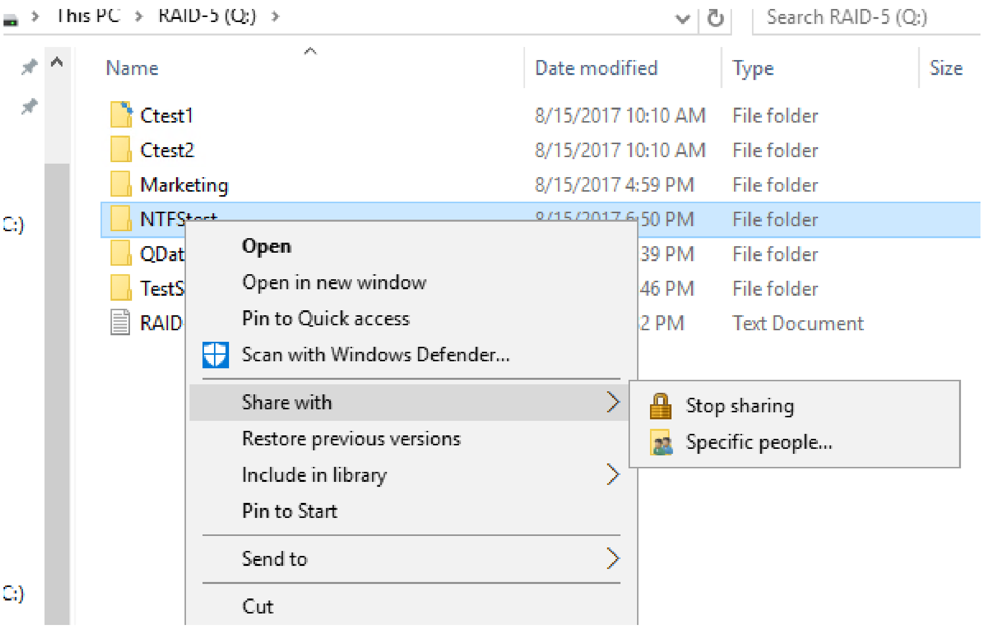
Enter the object names to select (examples): TestSharing-DL

5. You want all users to be able to create files and have full control over files they create, so click the **Full Control** check box in the **Allow** column. Even though users will have Full Control over files they create, NTFS permissions restrict them to Read, Read & execute, and Write on all other files. Click **OK** twice, and then click **Close**.
6. Switch to your **Windows 10** client computer and log on as **jgarza.**
7. Right-click **Start**, select **Run**, type **\\SRV19-XX\Production**, and press **Enter**.
8. Create a file named **jgarza.txt**, make some changes to the file and save it. You should be successful because **jgarza** has Write permissions.
9. Take a screenshot of the jgarza.txt document (PrtScr#2).
10. Sign out of the Windows 10 client computer.

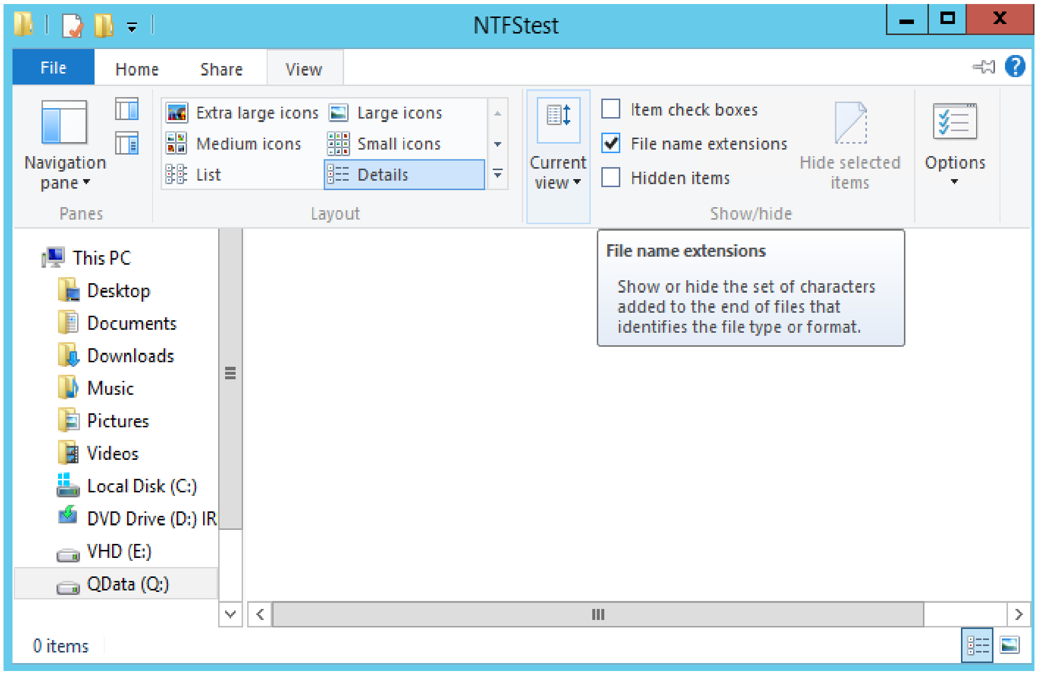
Exercise 3: Working with NTFS Permissions:

1. Log on to your server as ***Administrator.***
2. Open **File Explorer**, navigate to the root of the **RAID-5** volume and create a folder named **NTFStest**.

3. Right-click on the **NTFStest** folder, and click **Share with, Specific people**.



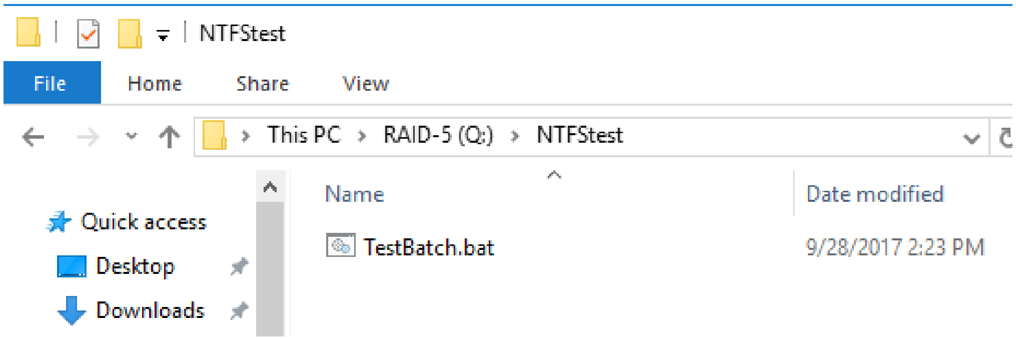
4. Add the **Users** group and give them **Read/Write** permissions and click **Share**, then click **Done**.
5. Open the **NTFStest** folder.
6. First, you want to be able to view file extensions in Windows Explorer so that you can create batch files easily. Click **View** on the toolbar, and then place a check in the box next to **File name extensions**.



File name extensions

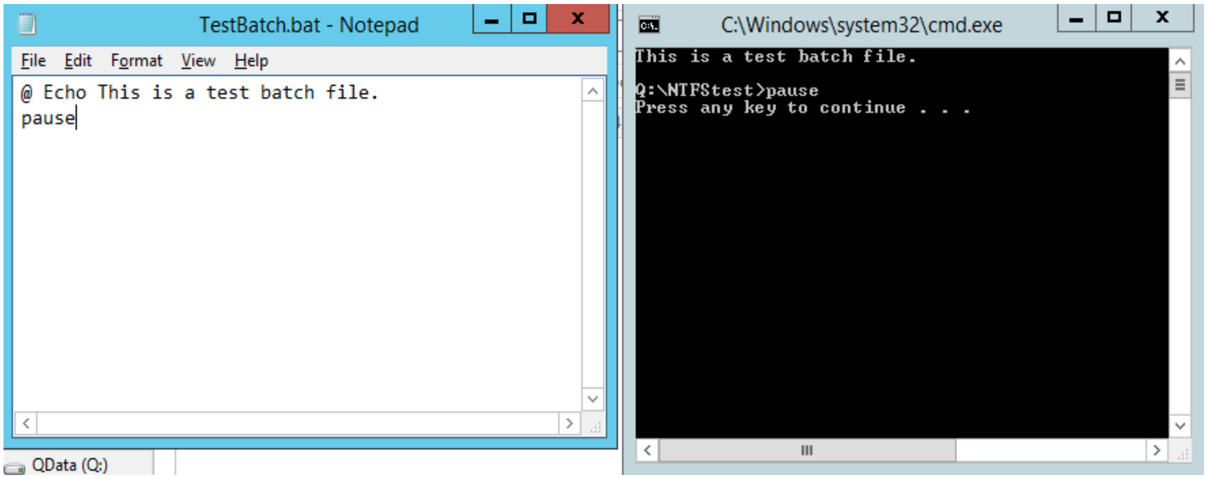
Show or hide the set of characters added to the end of files that identifies the file type or format.

7. Create a text file called **TestBatch.bat** (make sure you remove the .txt file extension from the filename). When asked whether you want to change the file extension, click **Yes**.



TestBatch.bat 9/28/2017 2:23 PM

8. Right-click **TestBatch.bat** and click **Edit**.
9. Type **@ Echo This is a test batch file** and press **Enter**. On the next line, type **Pause**. Save the file, and then exit Notepad. To test your batch file, double-click it. A command prompt window opens, and you should see "**This is a test batch file. Press any key to continue . . .** "

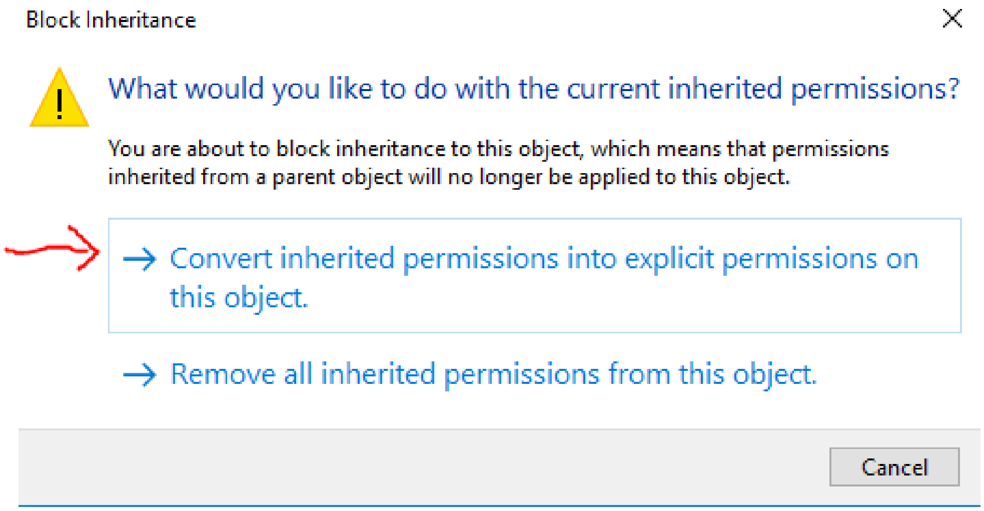


```
@ Echo This is a test batch file.
pause
```

```
This is a test batch file.

Q:\NTFStest>pause
Press any key to continue . . .
```

10. Press the **spacebar** or **Enter** to close the command prompt window.
11. Right-click the **TestBatch.bat** file and select Properties, click the **Security** tab, and then click **Advanced**. Click **Disable inheritance** to disable inheritance. In the message box that opens, click **Convert inherited**

permissions into explicit permissions on the objet. Click **OK**



Block Inheritance

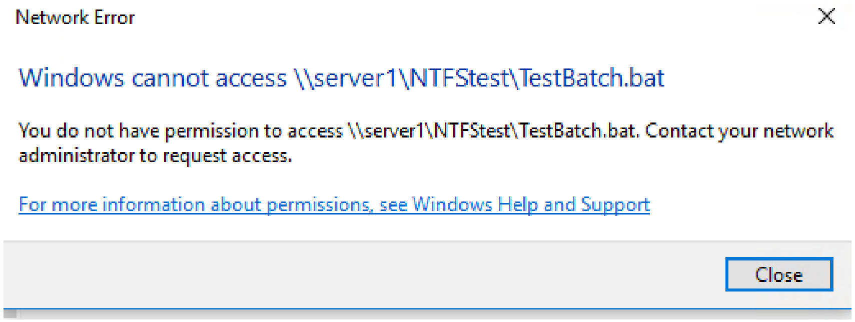
What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

→ Convert inherited permissions into explicit permissions on this object.

→ Remove all inherited permissions from this object.

12. Click **Edit** on the Security tab. Select the Users group. In the Permissions for Users list box, click to clear the **Read & execute** check box in the Allow column and **leave** the **Read** and **Write** checkboxes selected. Click **OK** 3 times.
13. Switch to your **Windows 10** client computer and log on as **jgarza**. Click **Start** and type **\\SRV19-XX\NTFStest**. Double-click the **TestBatch.bat** file. You will receive an error message stating that you do not have permissions to access the file. Click **Close**.



Network Error

Windows cannot access \\server1\NTFStest\TestBatch.bat

You do not have permission to access \\server1\NTFStest\TestBatch.bat. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

14. Close all windows and sign out of the **Windows 10** client computer.
15. Switch back to your **Windows Server**, open a command prompt window and type:

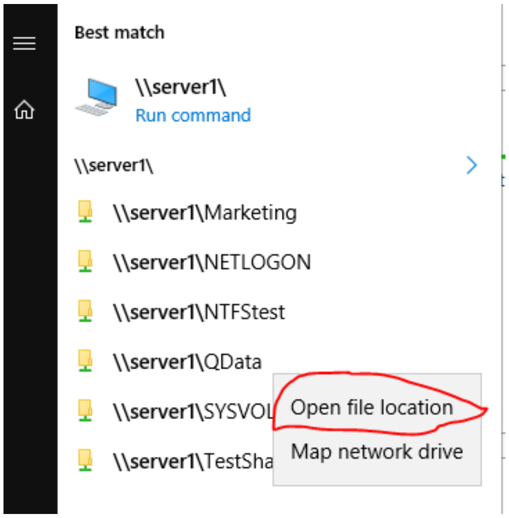
```
icacls q:\ntfstest\testbatch.bat
```

16. Take a screenshot of the results of the icacls command (PrtScr#3).
17. Close all open windows but remain logged on for the next activity.

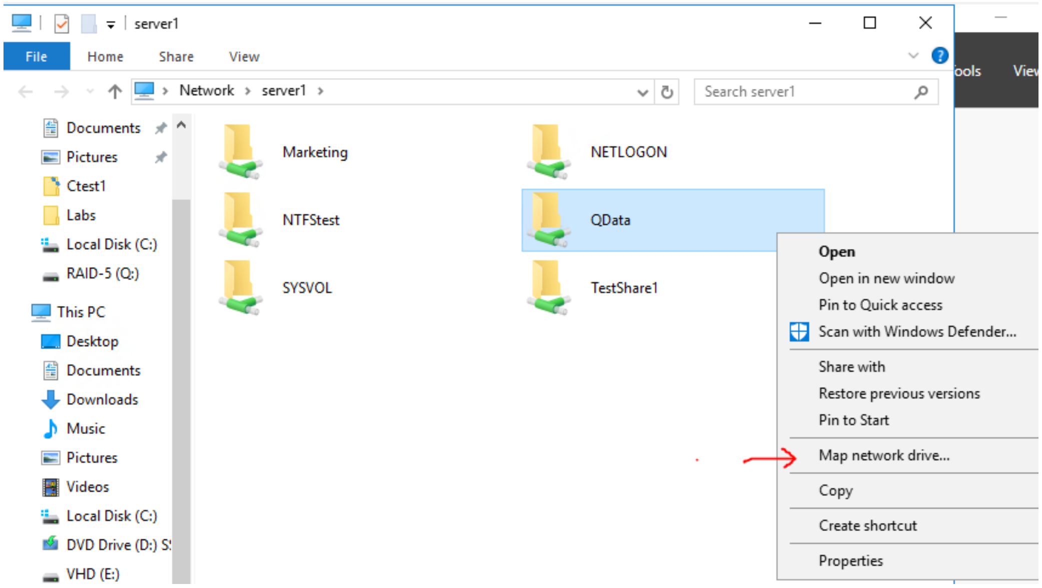
Part 2

In this activity, you will map a network drive on the Windows Server operating system.

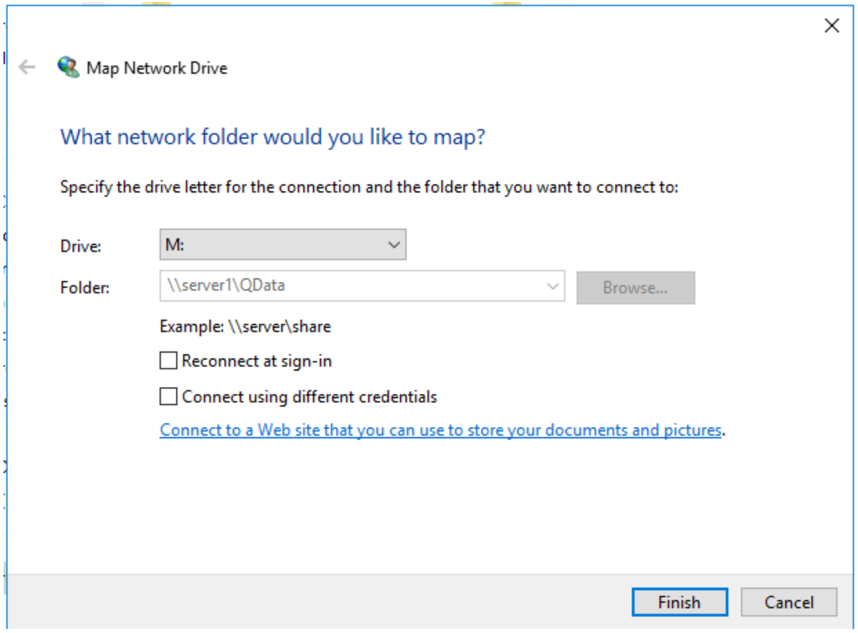
1. Log on to your server as ***Administrator.***
2. Open **File Explorer** and click on **This PC** in the left pane.
3. Double-click the RAID-5 (Q:) volume, right-click in the right pane and select **New Folder.**
4. Name the new folder **QData**.
5. Right-click the **QData** folder you just created and click **Share** and select **Share with specific people**. In the drop down list box, click **Everyone**, and then click the **Add** button.
6. Click the **Everyone** entry in the list box at the bottom. Click the list arrow in the Permission Level column, and then click **Read/Write** in the list. Click the **Share** button, and then click **Done**.
7. Click **Start**, type **\\SRV19-XX**
8. Right-click the **QData** share and click **Open File Location**.



9. Right-click the **QData** folder and select **Map network drive.**



10. Click the Drive list arrow, and click **M:**. By default, the Reconnect at logon box check box is selected, which is what you usually want in this situation. This option means that the M drive always connects to this share when the user logs on. For this lab, click to clear **Reconnect at logon**.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: M:

Folder: \\server1\QData

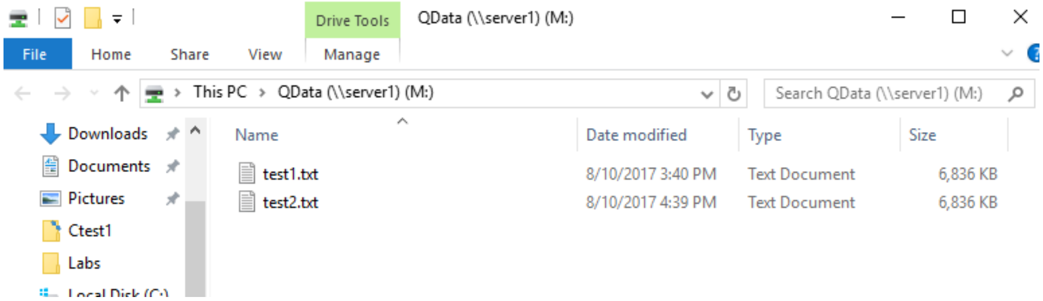
Example: \\server\share

□ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

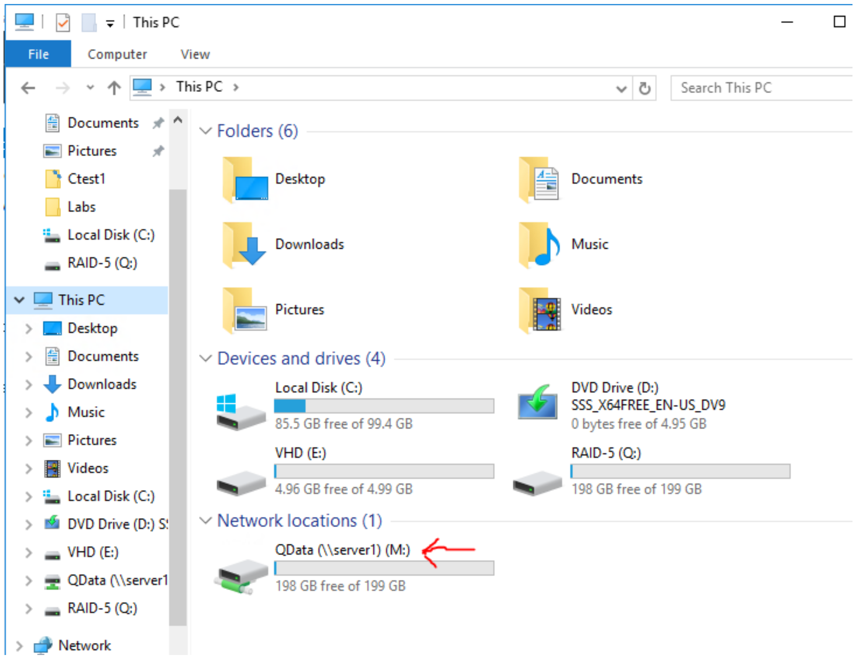
11. Click **Finish**. A File Explorer window opens, showing the contents of the QData share. Close this window.



Name	Date modified	Type	Size
test1.txt	8/10/2017 3:40 PM	Text Document	6,836 KB
test2.txt	8/10/2017 4:39 PM	Text Document	6,836 KB

12. Open **File Explorer** and click on **This PC**. Notice that the M drive is listed along with your local drive letters.

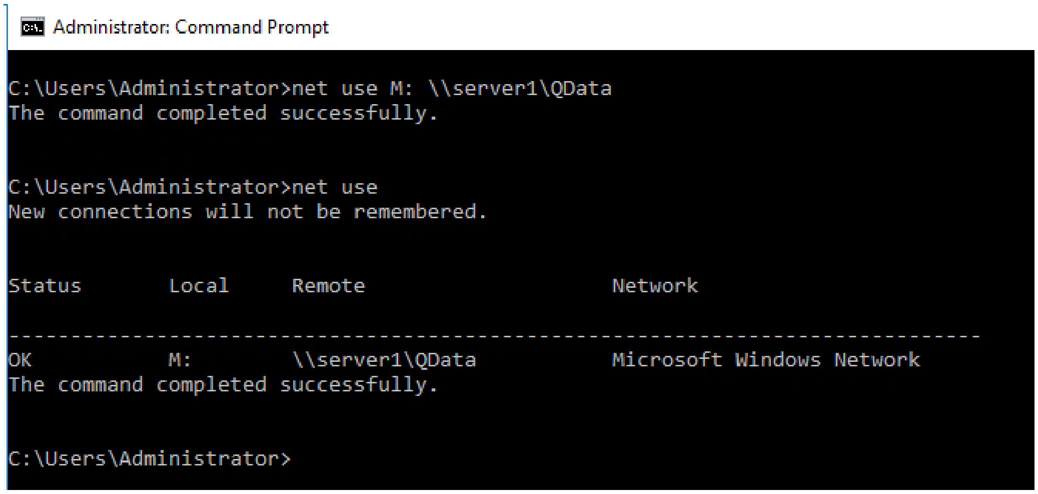
13. Take a screenshot of File Explorer showing the M drive (PrtScr#4).



14. Return to File Explorer and right-click the **M** drive and click **Disconnect**.

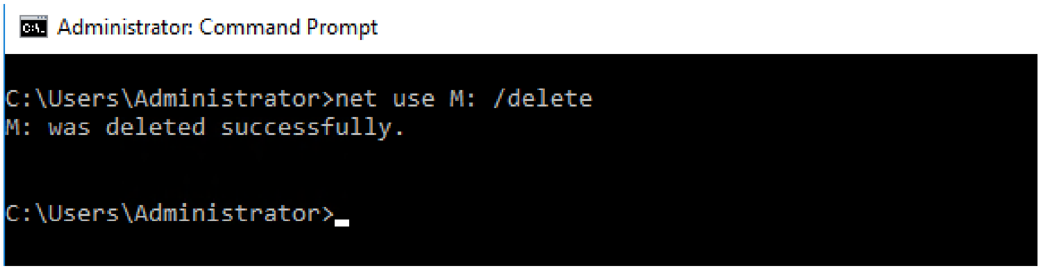
15. Close all open windows. Click **Start**, type **cmd** and press **Enter**.

16. Return to the command prompt, type **net use M: \\SRV19-XX\QData** and press **Enter**. You should get the message "The command completed successfully." Type **net use** and press **Enter**. You see the **M** drive listed and the UNC path to which it connects. Leave the command prompt window open.



```
C:\Users\Administrator>net use M: \\server1\QData
The command completed successfully.


C:\Users\Administrator>net use
New connections will not be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           M:        \\server1\QData           Microsoft Windows Network
The command completed successfully.


C:\Users\Administrator>
```

17. Open **Windows Explorer** and verify that the M drive is indeed there. Go back to the command prompt. Type **net use,** then press **Enter.** Take a screenshot of the results of the **net use** command (PrtScr#5).
18. Type **net use M: /delete** to disconnect the M drive. Network administrators put these types of commands in logon scripts to map drives for users.



```
C:\Users\Administrator>net use M: /delete
M: was deleted successfully.


C:\Users\Administrator>_
```

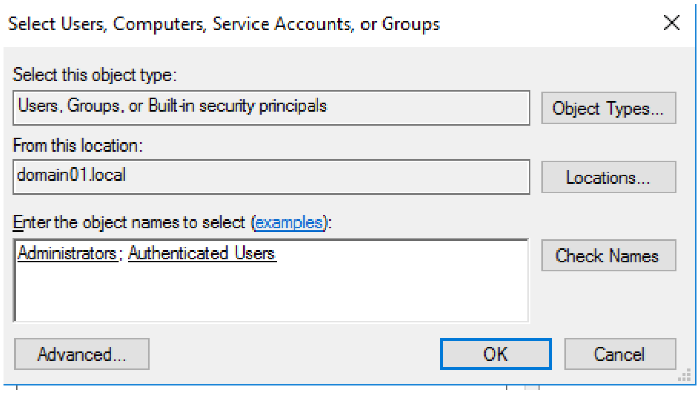
19. Close all open windows but remain logged on for the next activity.

Part 3

In this activity, you will create and map user's home folders on the Windows Server operating system.

1. Log on to your server as ***Administrator***.

2. Create a folder on the **RAID-5** volume named **HomeFolders** (no space) and share it as **HomeFolders** by using **Advanced Sharing.** Click the **Permissions** button, remove the **Everyone** group, and add the **Authenticated Users** group. Also, add the **Administrators** group. Give the Authenticated Users group and Administrators the **Allow Full Control** permission. Click **OK** twice .

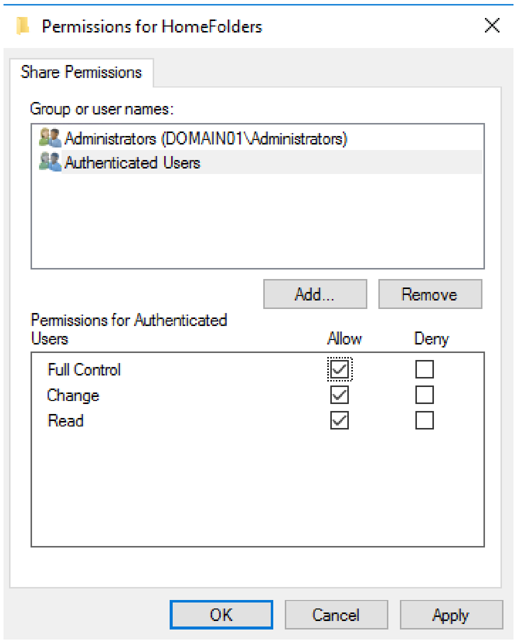


Select Users, Computers, Service Accounts, or Groups

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

From this location:
domain01.local

Enter the object names to select (examples):
Administrators; Authenticated Users



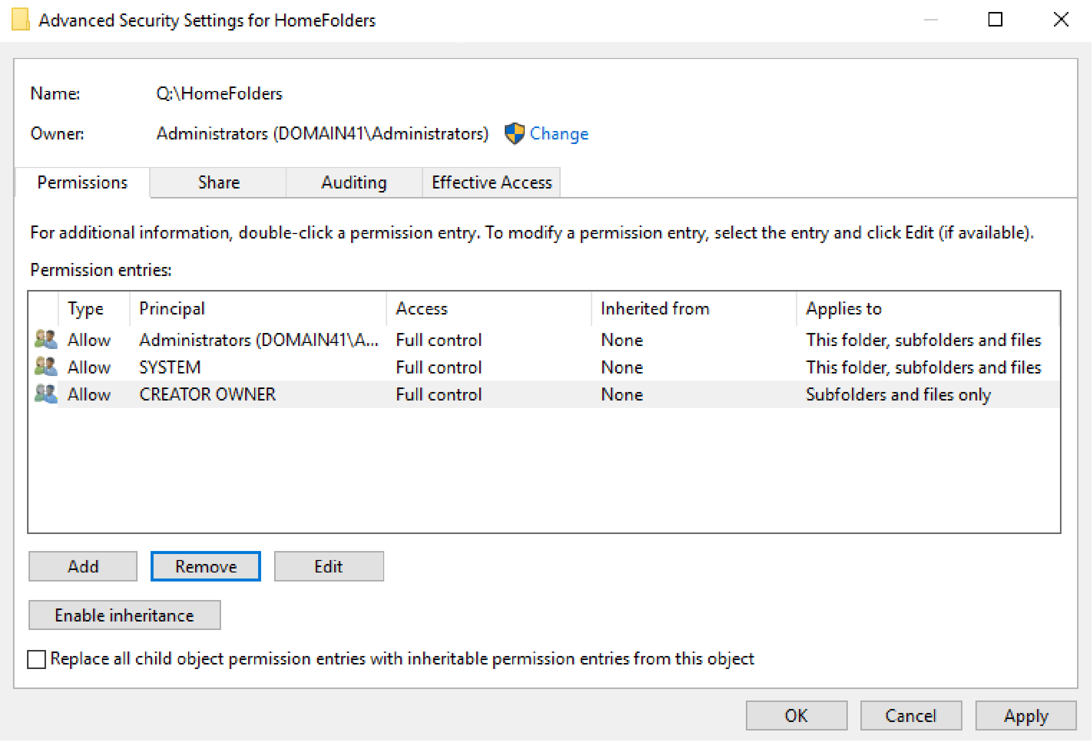
Permissions for HomeFolders

Share Permissions

Group or user names:
Administrators (DOMAIN01\Administrators)
Authenticated Users

Permissions for Authenticated Users	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

3. Click on the Security tab and click Advanced.
4. Click the Disable inheritance button and Convert inherited permissions into explicit permissions
5. Remove both instances of the Users group from the Permissions entries: list


Advanced Security Settings for HomeFolders

Name: Q:\HomeFolders

Owner: Administrators (DOMAIN41\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

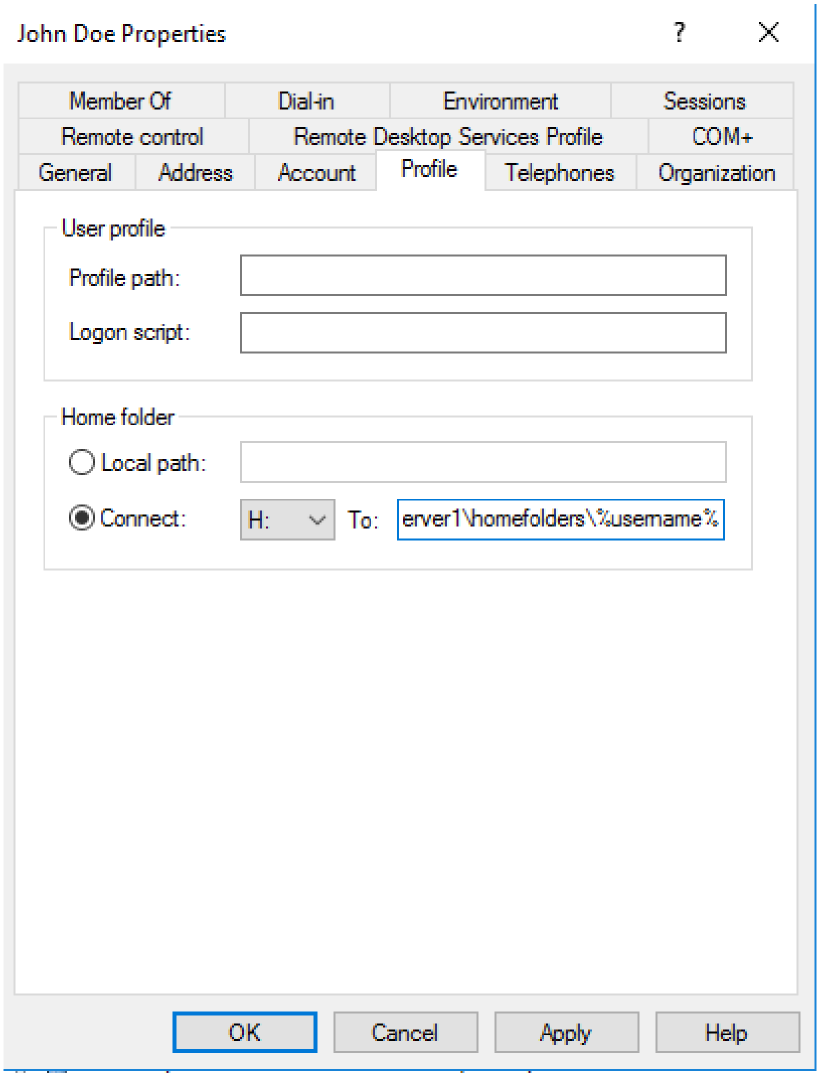
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (DOMAIN41\A...	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

□ Replace all child object permission entries with inheritable permission entries from this object

6. Click OK twice to close the HomeFolders properties sheet.
7. Go to **Active Directory Users and Computers** and create 2 new users in the **Phoenix** OU in your domain: John Smith (**jsmith**) and John Doe (**jdoe**), their password will be **Itnw1354**. Clear the checkbox by **User must change password at next logon.**

8. Right-click on each user's account and select Properties, then select the **Profile** tab, select "**Connect**", choose **H** and type in **\\SRV19-XX\homefolders\%username%.** This will create their home folder. Close Active Directory Users and Computers. **NOTE: %username% is a variable that picks up the actual user's logon name. Also, since you are mapping to a folder that resides on a server, you have to use the server's name, not the domain name.**



John Doe Properties

User profile

Profile path:

Logon script:

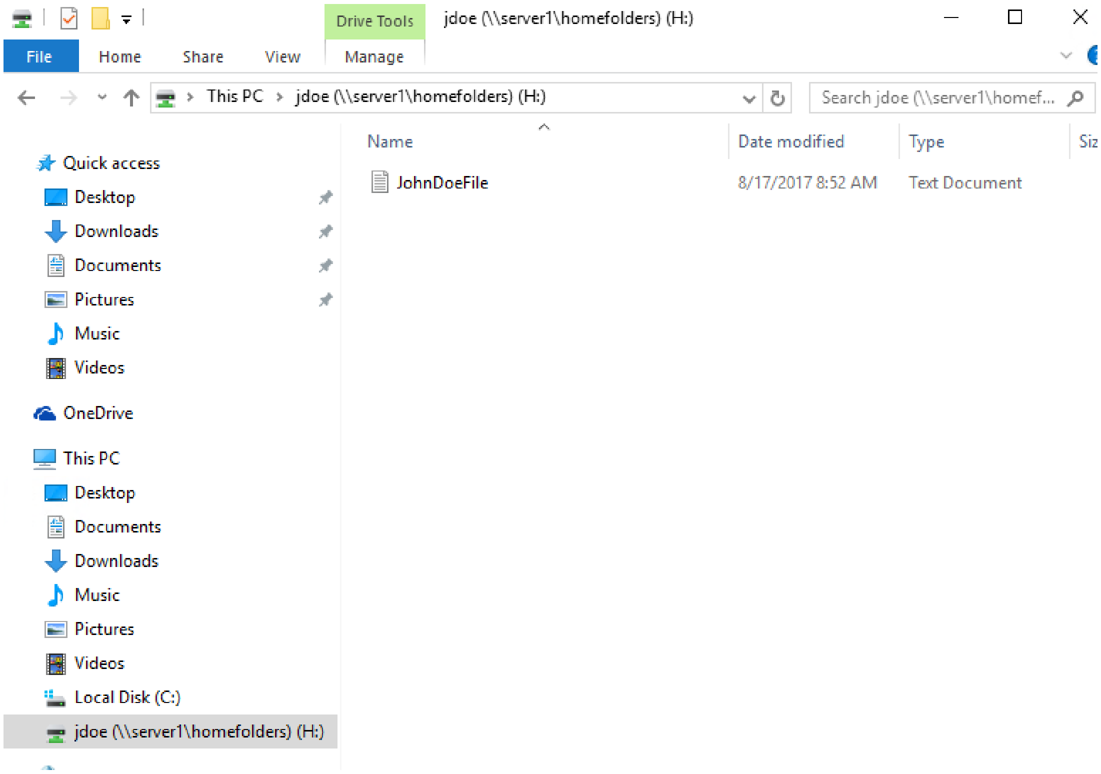
Home folder

○ Local path:

● Connect: H: To: erver1\homefolders\%username%

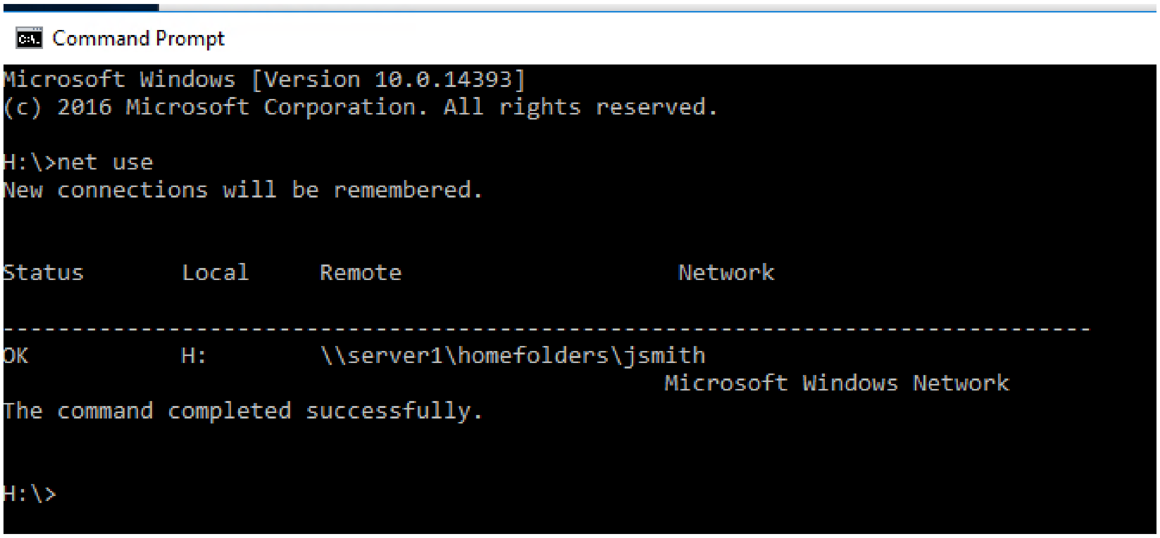
9. Navigate to the RAID-5 volume and double-click the **HomeFolders** folder on the **RAID-5** volume, to verify that each of the user's folders were created.
10. Open a command prompt window and type **dir q:\homefolders** and press **Enter.**
11. Take a screenshot showing the created home folders (PrtScr#6).
12. Switch to your **Windows 10** client computer and log on as each user (jsmith and jdoe) and test the permissions assigned to their home folder by creating a new text document with their first name in the title. They should be able to access only their own folder and files. They should also have a drive

mapped when they open **File Explorer.**



Name	Date modified	Type	Siz
JohnDoeFile	8/17/2017 8:52 AM	Text Document	

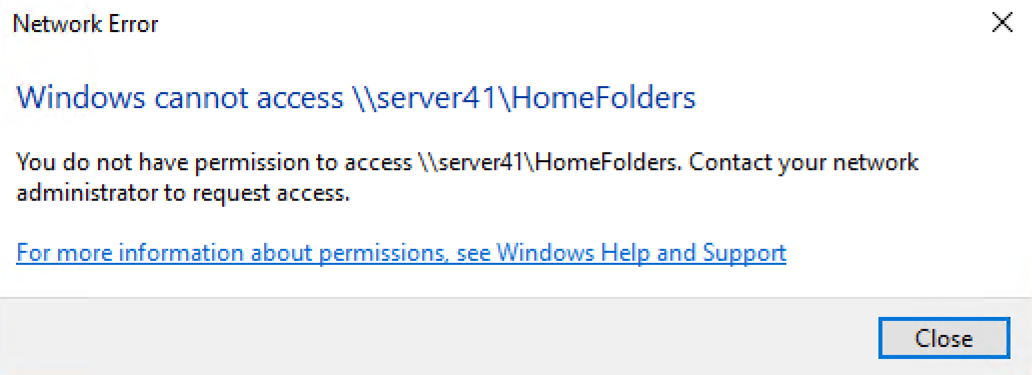
13. While logged on as either John Doe or John Smith, open a command prompt and type **net use** and press **Enter.** You should see the path of their home folder in the results.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

H:\>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           H:        \\server1\homefolders\jsmith
                                                Microsoft Windows Network
The command completed successfully.


H:\>
```

14. At the command prompt type **net use** and press **Enter**.
15. Take a screenshot of the results of the net use command (PrtScr#7).
16. Click Start and type in **\\SRV19-XX**
17. Click on **\\serverxx\HomeFolders** to open the shared folder.

You should receive a Windows cannot access error message. By changing the NTFS permissions to the HomeFolders folder, you ensure that users can only access their own folders on the network.



Network Error

Windows cannot access \\server41\HomeFolders

You do not have permission to access \\server41\HomeFolders. Contact your network administrator to request access.

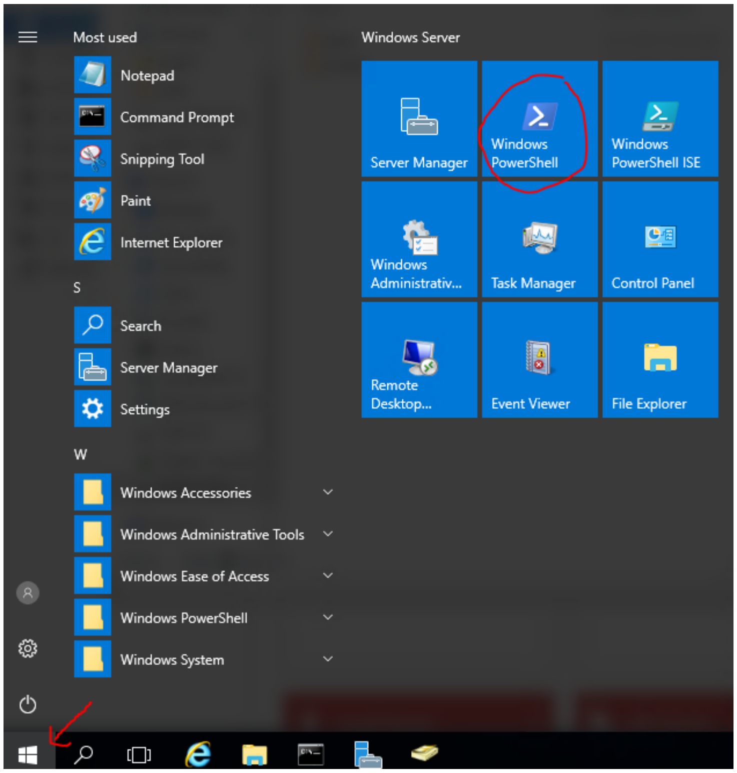
For more information about permissions, see Windows Help and Support

18. Close all windows and log off.

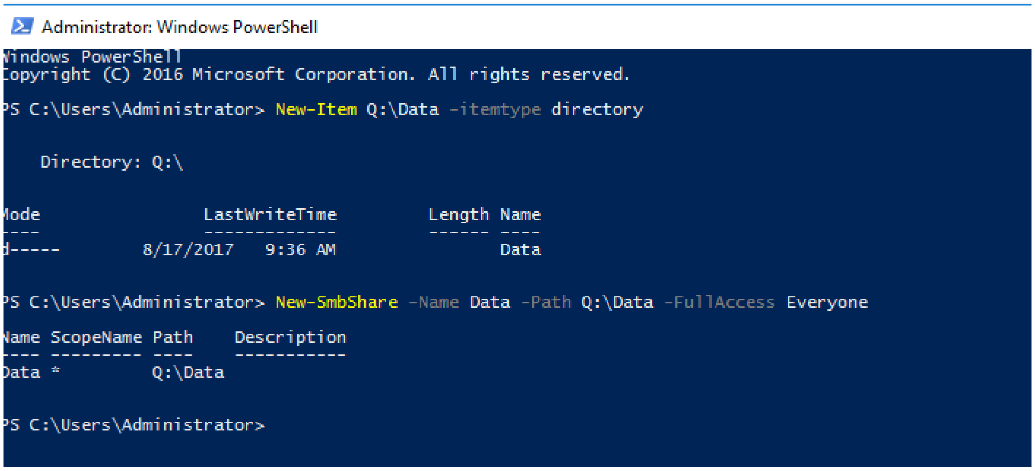
Part 4

In this activity, you will create and share a folder using PowerShell on the Windows Server operating system.

1. Log on to your server as ***Administrator.***
2. Click **Start** and click the **PowerShell** icon on the Start menu.



3. Type **New-Item Q:\Data –itemtype directory** and press **Enter.**
4. Type **New-SmbShare –Name Data –Path Q:\Data –FullAccess Everyone** and press **Enter.**



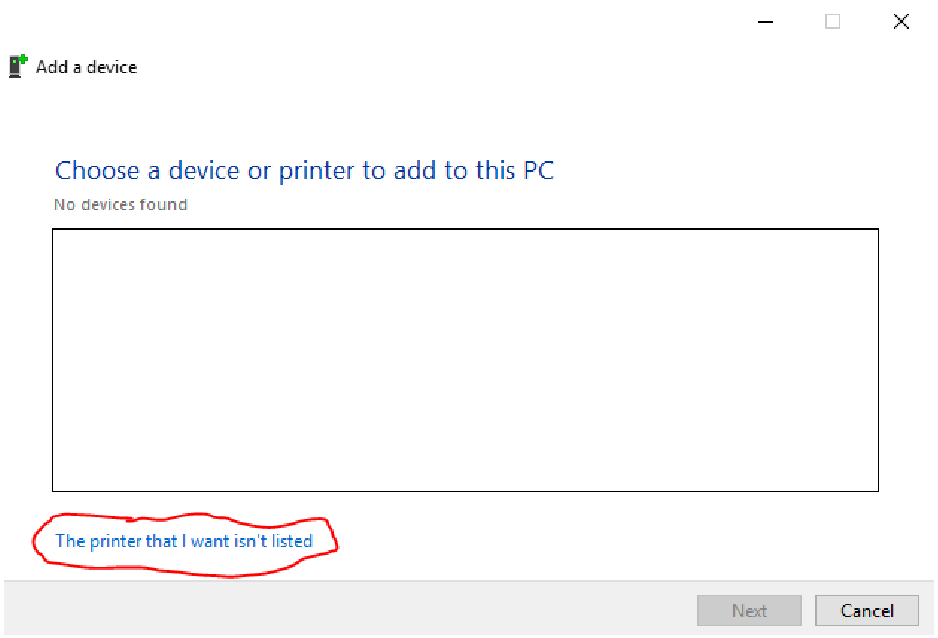
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-Item Q:\Data -itemtype directory


    Directory: Q:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        8/17/2017   9:36 AM                Data


PS C:\Users\Administrator> New-SmbShare -Name Data -Path Q:\Data -FullAccess Everyone

Name ScopeName Path    Description
---- --------- ----    -----------
Data *         Q:\Data


PS C:\Users\Administrator>
```

5. Type **net share** and press **Enter.**
6. Take a screenshot of the results of the net share command (PrtScr#8).
7. Close all open windows but remain logged on for the next activity.

Part 5

In this activity, you will use the Control Panel to install a printer on the Windows Server operating system.

1. Log on to your server as ***Administrator.***
2. Right-click **Start**, select **Run**, type **Control Panel,** click OK. Select D**evices and printers** under **Hardware**.
3. Click **Add a printer**.
4. In the next window, click **The printer that I want wasn't listed**.



Add a device

Choose a device or printer to add to this PC

No devices found

The printer that I want isn't listed

5. On the next screen, select **Add a local printer with manual settings** and click **Next.**
6. Use an existing port (LPT1) and click **Next.**
7. For the manufacturer, select **MS Publisher Color Printer**, for the printer, and click **Next.**
8. (If that printer can't be found, any other printer will do.)
9. Change the printer name to **Sales Color Printer** and click **Next**.
10. Uncheck **Set as Default Printer**. (This printer does not exist, so do not try to print a test page.)
11. In the Printer Sharing window, click the **Do Not share this printer** option button.
12. Click **Next,** then **Finish** on the next screen.
13. Remain logged on and leave the Control Panel open for the next activity.

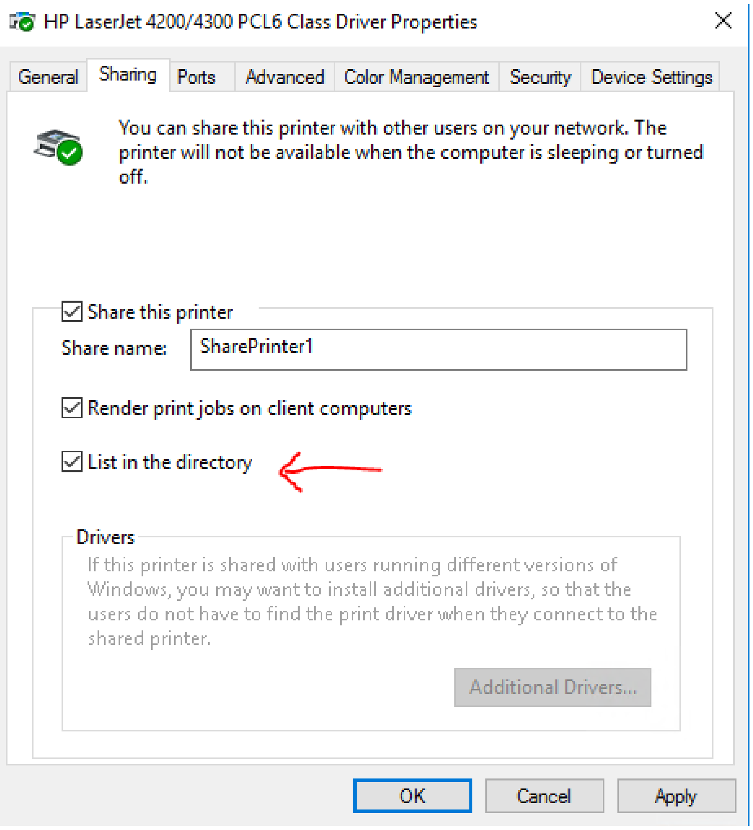
Part 6

In this activity, you will use the Control Panel to share a printer on the Windows Server operating system.

1. Log on to your server as ***Administrator.***
2. Right-click **Start**, select **Run**, type **Control Panel,** click **Devices and printers** under **Hardware**.

3. Right-click the printer you installed earlier and click **Printer Properties**. Click the **Sharing** tab. Click to select the **Share this** printer check box. Share the printer as **SharePrinter1.**

4. Click to select the **List in the directory** check box, and then click **OK**. Your printer is then published to Active Directory so that users can find it.



You can share this printer with other users on your network. The printer will not be available when the computer is sleeping or turned off.

☑ Share this printer

Share name: SharePrinter1

☑ Render print jobs on client computers

☑ List in the directory

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

5. Right-click the printer again and click **Printer Properties**. Click the **Ports** tab. You can add a port or change a port's configuration, such as changing the IP address of a TCP/IP port. If you have two or more identical printers, you can click the Enable printer pooling option and select additional ports for this printer.
6. Click the **Security** tab. Printers don't have share permissions; they have permissions only in the Security tab, and they work similarly to NTFS permissions. Click the ACEs in the Group or user names list box, and review the permissions for each one. Click **OK**, and close any open windows.
7. Open a command prompt and type **net share** and press **Enter.**

8. Take a screenshot of the results of the net share command (PrtScr#9). Close all open windows and sign out.

Reflection

1. What is the benefit of using Home Folders?
2. Why would you want to map a network drive?

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Take a screenshot of the results of the icacls command (PrtScr#1) (10 points)	
	Criteria #2:Take a screenshot of the jgarza.txt document (PrtScr#2) (10 points)	
	Criteria #3: Take a screenshot of the results of the icacls command (PrtScr#3) (10 points)	
	Criteria #4: Take a screenshot of File Explorer showing the M drive (PrtScr#4) (10 points)	
	Criteria #5: Take a screenshot of the results of the **net use** command (PrtScr#5) (10 points)	
	Criteria #6:Take a screenshot showing the created home folders (PrtScr#6) (10 points)	
	Criteria #7:Take a screenshot of the results of the **net use** command (PrtScr#7) (10 points)	
	Criteria #8:Take a screenshot of the results of the net share command (PrtScr#8) (10 points)	

	Criteria #9:Take a screenshot of the results of the net share command (PrtScr#9) (10 points)	
	Criteria #10: Answer the reflection questions in a text file (10 points)	