1. Introduction

1.1 Identification

Procedure Name

- Technical Group – CIS 216 – Week 8 – File and Share Access Configuration

1.2 KBSUCKS Instructions

Italicization denote items needed to be modified by the student. What is meant by this is that anything that is italicized is required to be filled in with the student's **own words as they document the assignment.** Then you are to *un-italicize* what I have italicized. This includes the Header, Footer, Table of Contents (TOC), the main body, plus anything else. The instructions in 1.2 can be left as is or removed altogether to fit your document.

1.3 Table of Contents

Contents

1.4 Revision Log

Revision	Date	Updated By	Description of Change
1.0	3/5/20	Mitchell Bartch	Document Creation

1.5 Purpose

The purpose of this document is to provide a walkthrough on creating security groups and shared folders on the Windows Server 2016. Assigning permissions will also be discussed.

1.6 Host Information

	Host Architecture
CPU	Intel Core i5-8600K @3.60GHz
Memory Size	16 GB
HD Size	3 TB
NIC	Intel Ethernet Connection 1219-V

1.7 Architectural Information

	Windows Server 2016 (216DC)	Windows 10 Client (216Client)
CPU	Intel Core i5-8600K @3.60GHz	Intel Core i5-8600K @3.60GHz
Memory Size	2 GB	2 GB
HD Size	50 GB	60 GB
NIC	Intel Ethernet Connection 1219-V	Intel Ethernet Connection 1219-V

2. What is the Assignment?

2.1 Summary of the Assignment

The purpose of this assignment is to create a simple to understand and follow document that will detail the steps necessary to create a shared folder between the Windows Server 2016 and the Windows 10 client, create a mapped drive, and discuss shadow copies and NTFS quotas. A user reading this document should be able to recreate the process detailed here.

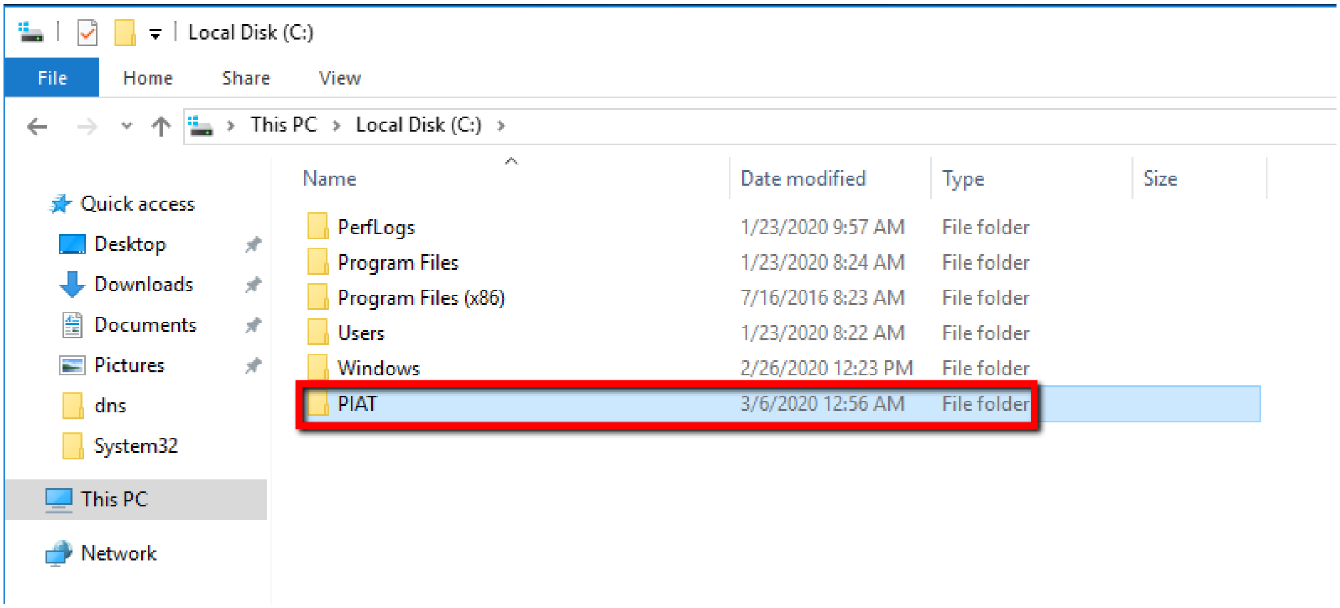
3. Assignment Details

3.1 File and Share Access Configuration

Windows Server 2016 Configuration

We will begin our configuration on the Windows 2016 Server. Start the server and navigate to the C: drive.

In the C: drive create a new folder named "PIAT". This will become our shared drive for the client PC.

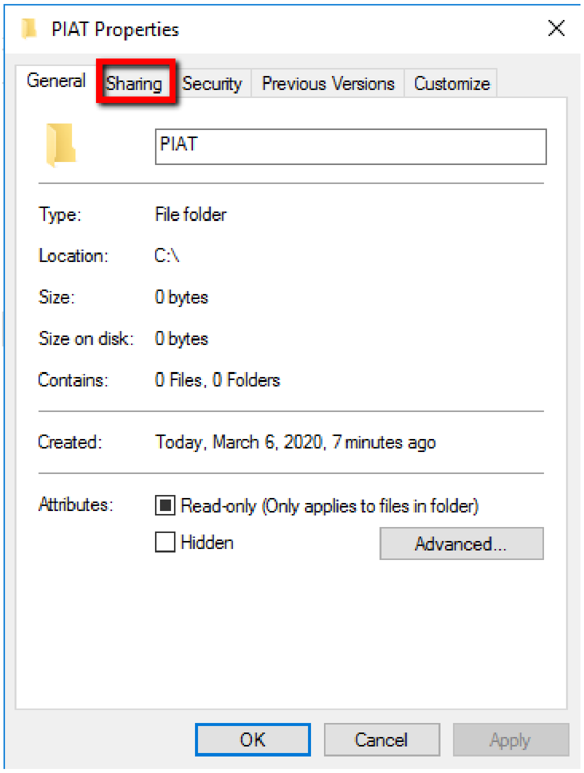


Name	Date modified	Type	Size
PerfLogs	1/23/2020 9:57 AM	File folder	
Program Files	1/23/2020 8:24 AM	File folder	
Program Files (x86)	7/16/2016 8:23 AM	File folder	
Users	1/23/2020 8:22 AM	File folder	
Windows	2/26/2020 12:23 PM	File folder	
PIAT	3/6/2020 12:56 AM	File folder	

Next we will share this folder and modify its share permissions.

On the "PIAT" folder right-click and open Properties.

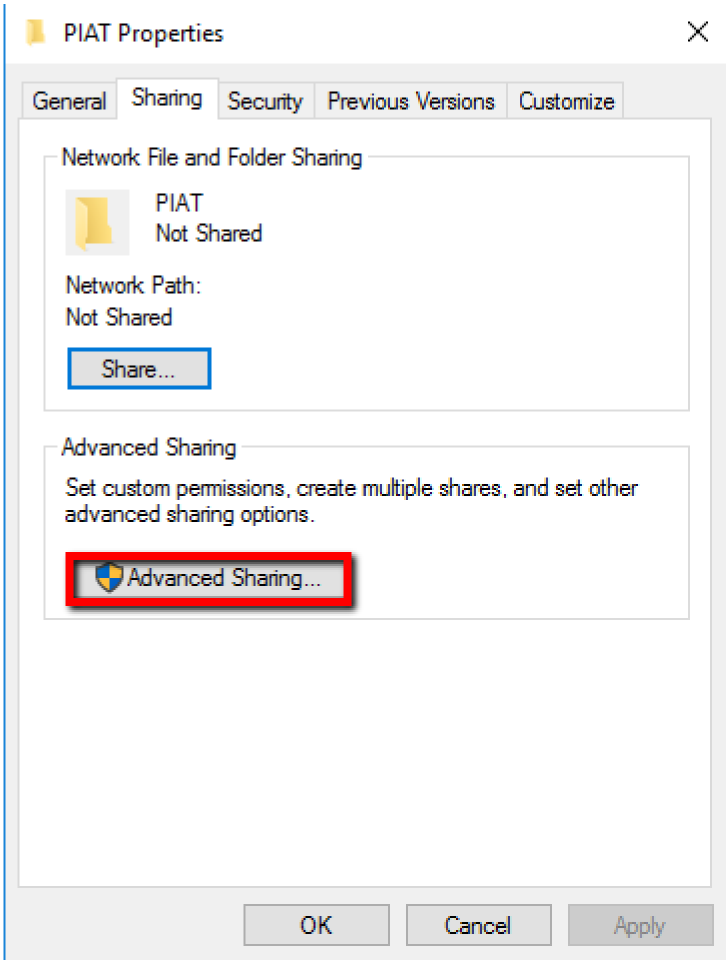
Click the "Sharing" tab.



PIAT

Type: File folder
Location: C:\
Size: 0 bytes
Size on disk: 0 bytes
Contains: 0 Files, 0 Folders
Created: Today, March 6, 2020, 7 minutes ago
Attributes: ■ Read-only (Only applies to files in folder)
□ Hidden

Under the “Sharing” tab click the “Advanced Sharing...” button.



PIAT
Not Shared

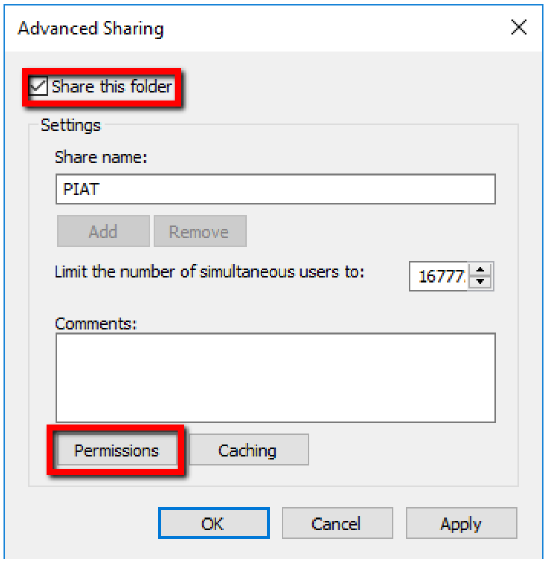
Network Path:
Not Shared

Set custom permissions, create multiple shares, and set other advanced sharing options.

Check the box that says, “Share this folder”.

Leave the share name as “PIAT”.

Click the “Permissions” button.



Advanced Sharing

☑ Share this folder

Settings

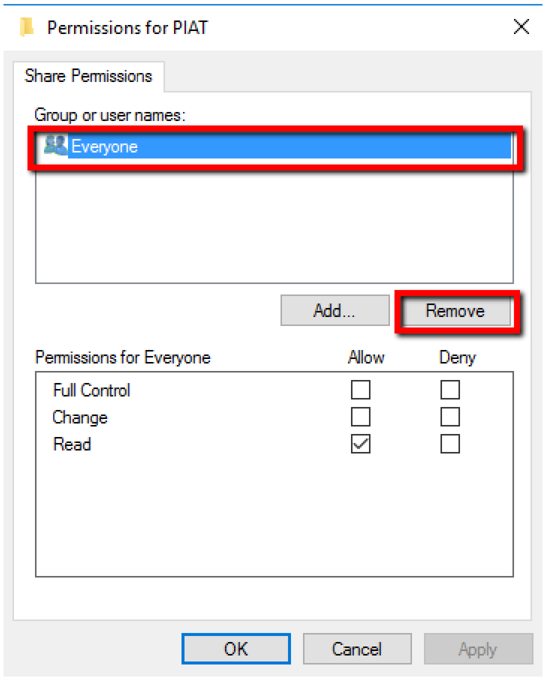
Share name: PIAT

Limit the number of simultaneous users to: 16777

Comments:

On the Permissions window for "PIAT" highlight the group "Everyone" and click the "Remove" button.

We remove the "Everyone" group as it may pose a security risk, next we will add a different group and set some permissions to them.



Permissions for PIAT

Share Permissions

Group or user names:

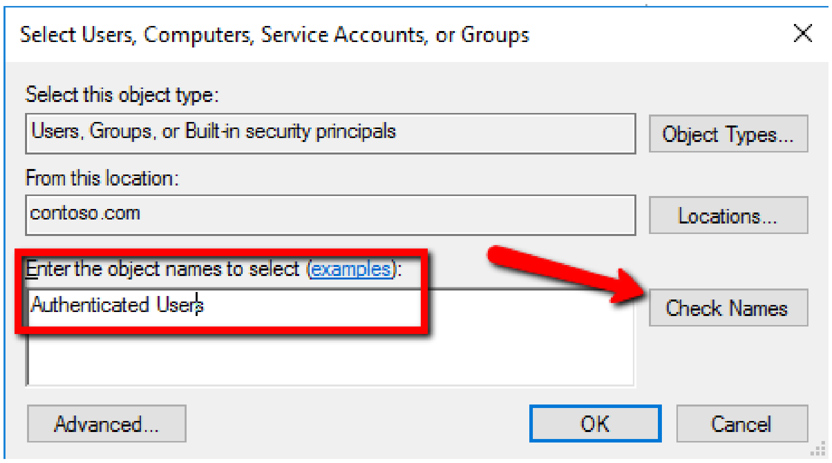
Everyone

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

Click the "Add..." button.

You will be greeted with a new window that will prompt you to enter an object name to add to the share permissions for the "PIAT" folder.

Under "Enter the object names to select" enter "Authenticated Users" and click the "Check Names" button.


Select Users, Computers, Service Accounts, or Groups

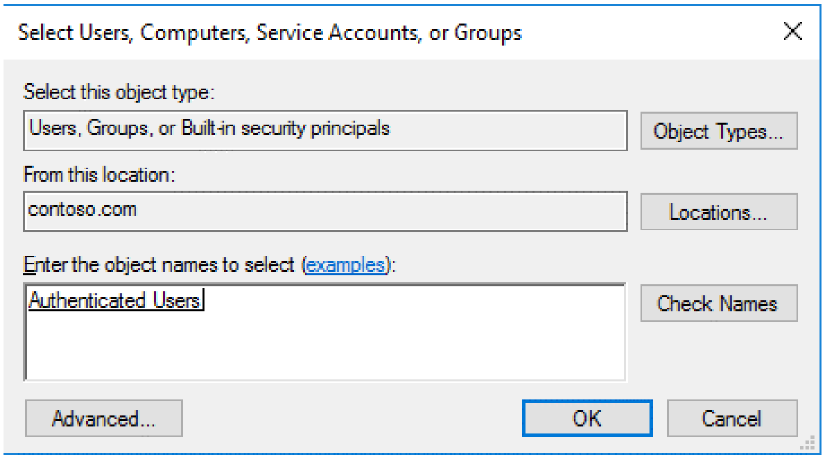
Select this object type: Users, Groups, or Built-in security principals

From this location: contoso.com

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

After a moment it should resolve the entered name and an underline will appear below "Authenticated Users".

An Authenticated User is a user who accesses the system through a logon process.


Select Users, Computers, Service Accounts, or Groups

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

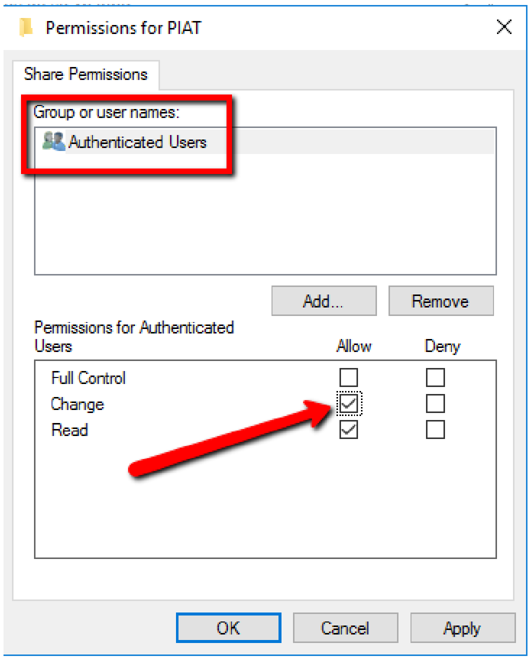
From this location: contoso.com

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

When we pressed the "Check Names" button what happened was the service checked the "contoso.com" domain for the Special Identity group named "Authenticated Users".

Click OK.

Back at the "Permissions for PIAT" window Authenticated users should appear under the "Group or user names:" section. Click the Allow checkbox for Change in the Permissions section below.



Permissions for PIAT

Share Permissions

Group or user names:

Authenticated Users

Permissions for Authenticated Users

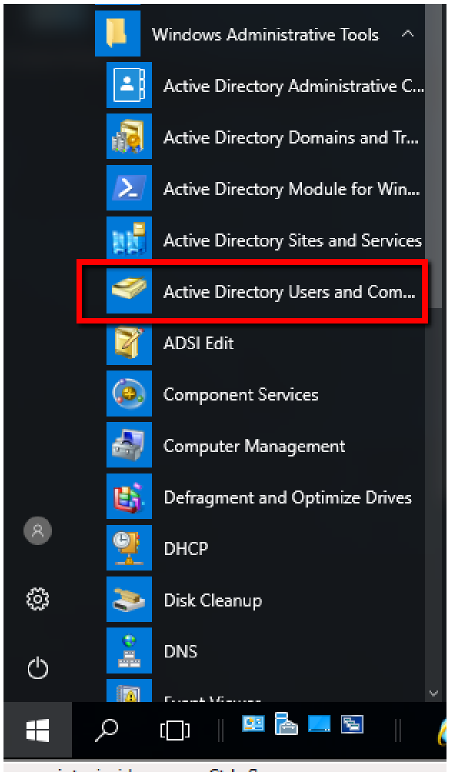
	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

Click Apply.

Click OK.

Next we will use Active Directory to create a security group and a new user account that we will then add to our share folder later.

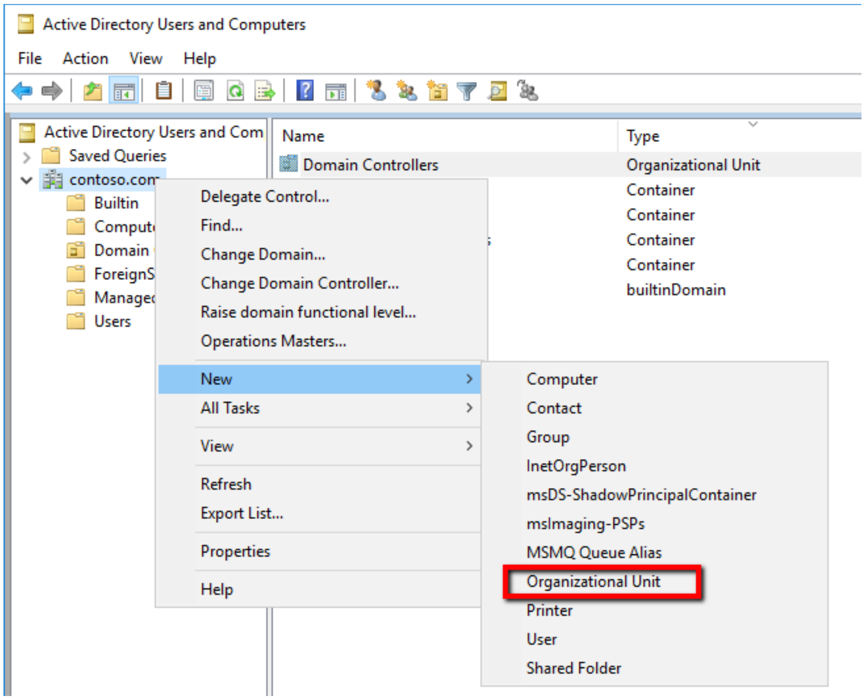
Open Active Directory Users and Computers (ADUC). It can be found under Windows Administrative Tools.


Windows Administrative Tools
Active Directory Administrative C...
Active Directory Domains and Tr...
Active Directory Module for Win...
Active Directory Sites and Services
Active Directory Users and Com...
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS

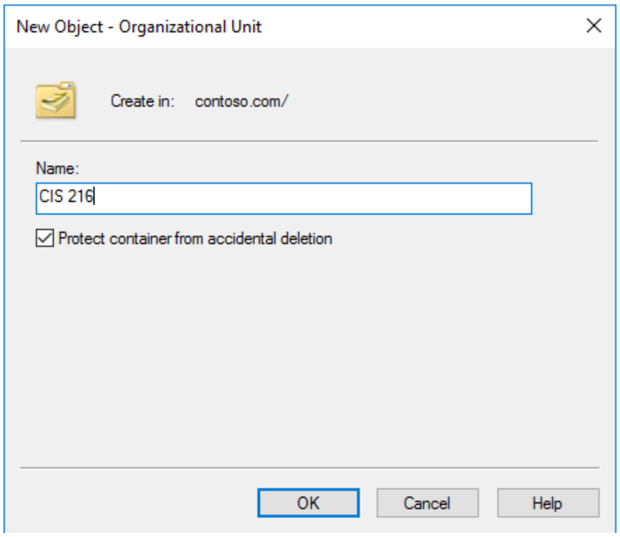
In ADUC expand “contoso.com”.

First, we will create a new Organizational Unit (OU) to store our new group and user account.

Right-click “contoso.com” and navigate to New -> Organizational Unit.



Enter the name “CIS 216”.


New Object - Organizational Unit

Create in: contoso.com/

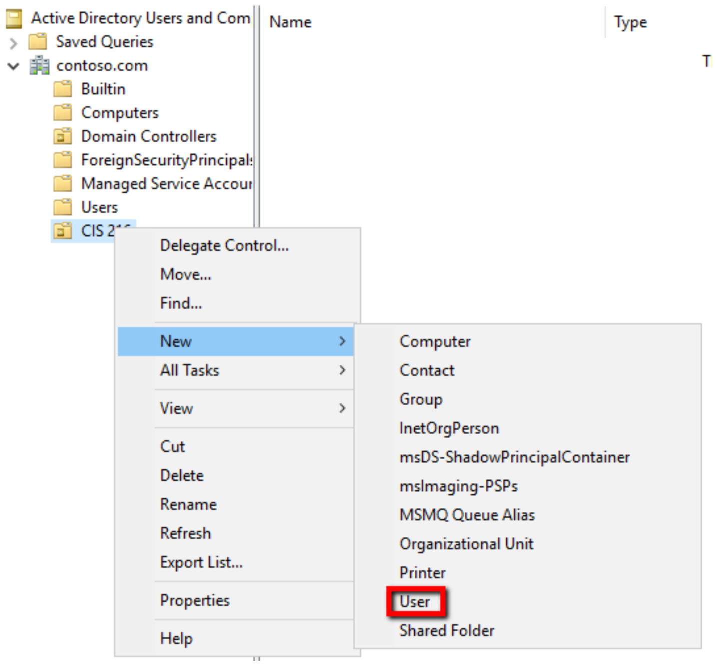
Name:
CIS 216

☑ Protect container from accidental deletion

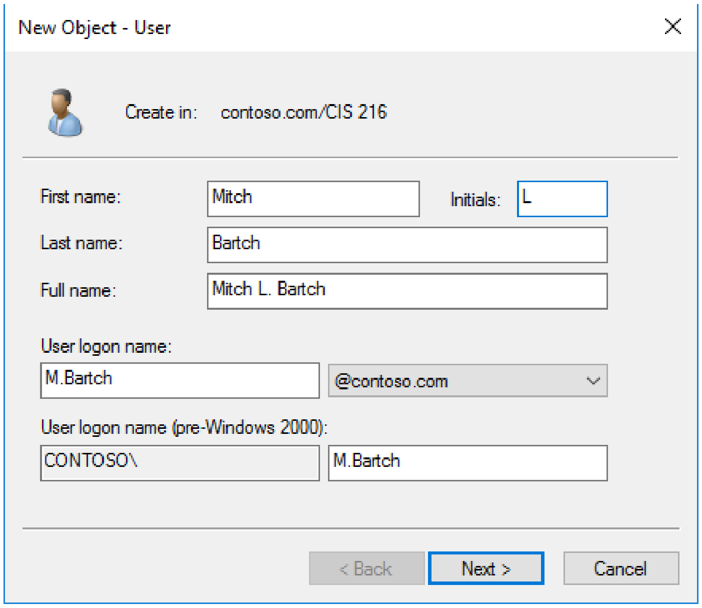
Click OK.

Next we will add a new user account to the CIS 216 OU.

Right-click the new OU and go New -> User.



In the “New Object - User” window we will create a new user account. Enter in the naming information for your user. When you get to the “User logon name:” enter in the name in the following format: First Initial.Last Name as shown in the screenshot below.


New Object - User

Create in: contoso.com/CIS 216

First name: Mitch
Initials: L
Last name: Bartch
Full name: Mitch L. Bartch

User logon name:
M.Bartch @contoso.com

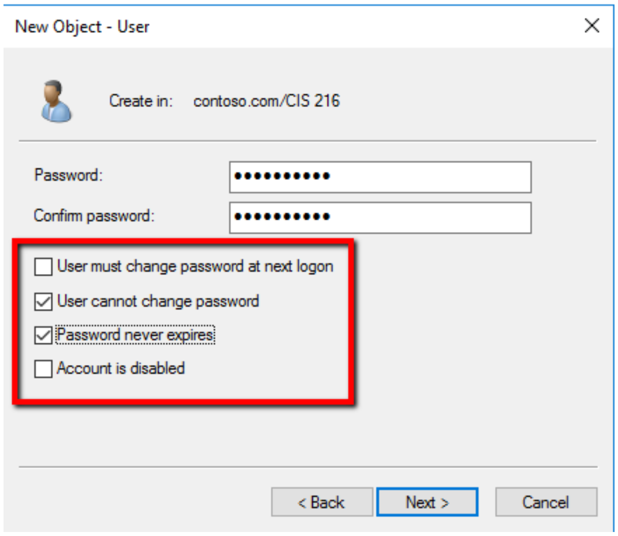
User logon name (pre-Windows 2000):
CONTOSO\ M.Bartch

Take note of the user logon name as we will be logging onto our client later on with this account.

Click Next.

Next enter in a password for the user account. A strong password consisting of at least 8 characters including numbers and special characters is recommended.

Uncheck the box next to “User must change password at next logon” and check the middle two boxes.



New Object - User

Create in: contoso.com/CIS 216

Password: •••••••••••

Confirm password: •••••••••••

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

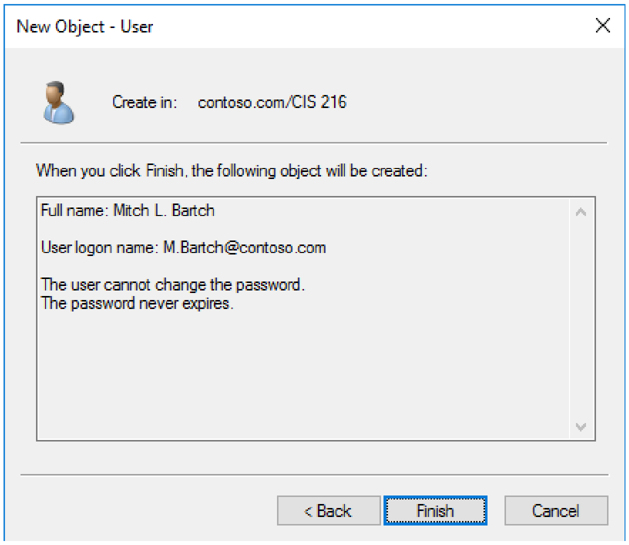
□ Account is disabled

The password for this user account will now never expire and the user will not be able to change it. As a note having a password never expire may not be the best practice in a professional setting as frequent password changes are recommended.

Click Next.

The last page shows a summary of the options you have chosen. Review these to ensure they are correct.

Click Finish.



Create in: contoso.com/CIS 216

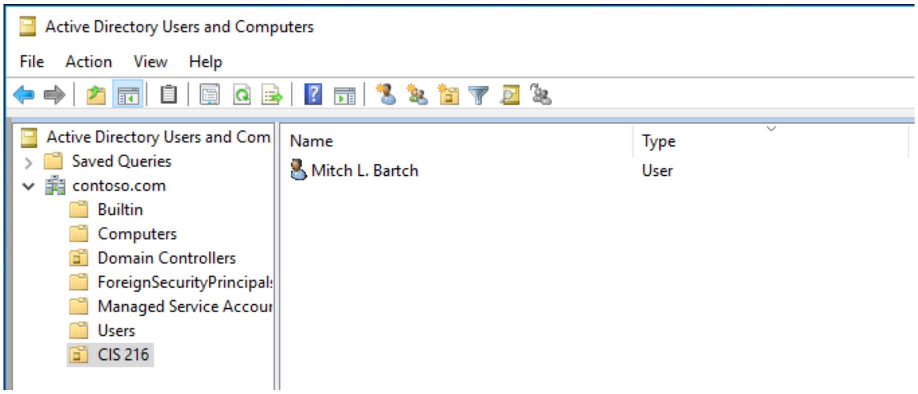
When you click Finish, the following object will be created:

Full name: Mitch L. Bartch

User logon name: M.Bartch@contoso.com

The user cannot change the password.
The password never expires.

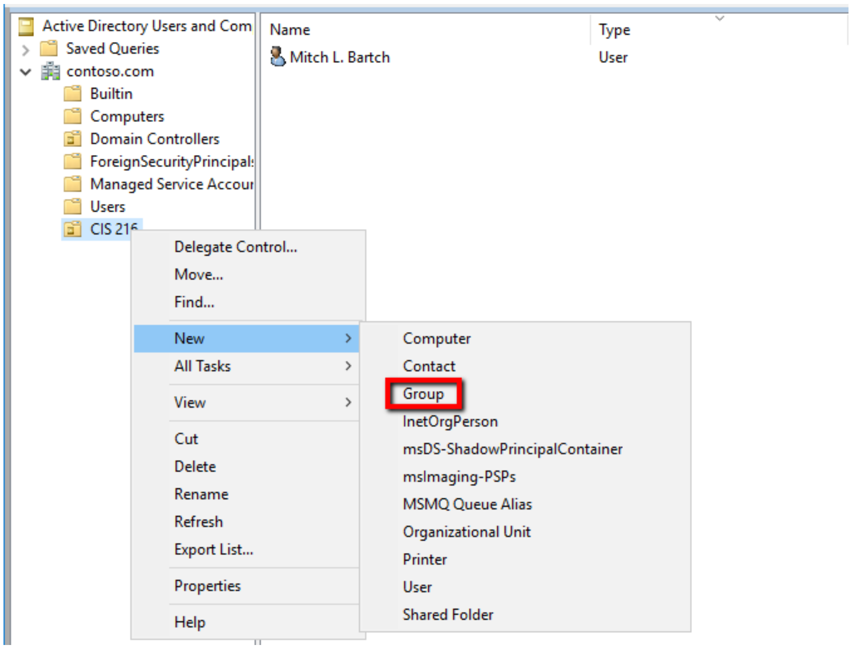
Under the CIS 216 OU our user should have appeared.



Name	Type
Mitch L. Bartch	User

Next we will make a security group in the CIS 216 group.

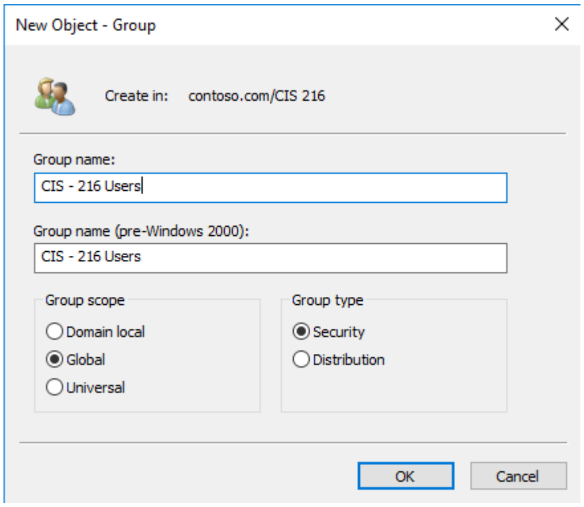
Right-click CIS 216 and go New -> Group.



For the group name enter: “CIS - 216 Users”.

Leave the “Group scope” and “Group type” options as they are.

Click OK.


New Object - Group

Create in: contoso.com/CIS 216

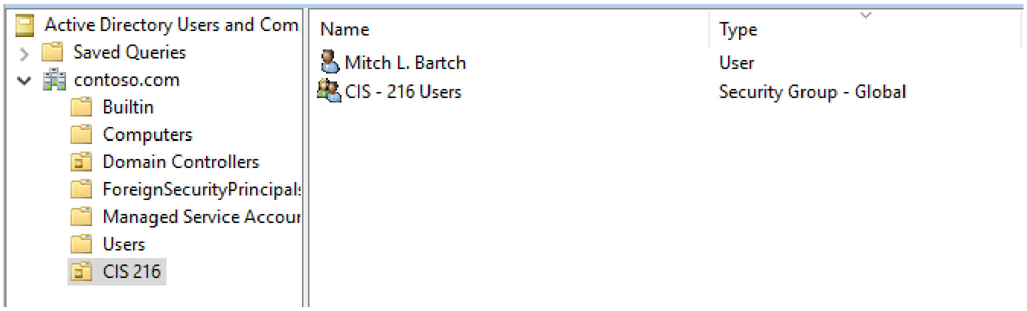
Group name: CIS - 216 Users

Group name (pre-Windows 2000): CIS - 216 Users

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Our security group now also appears in the CIS 216 OU.

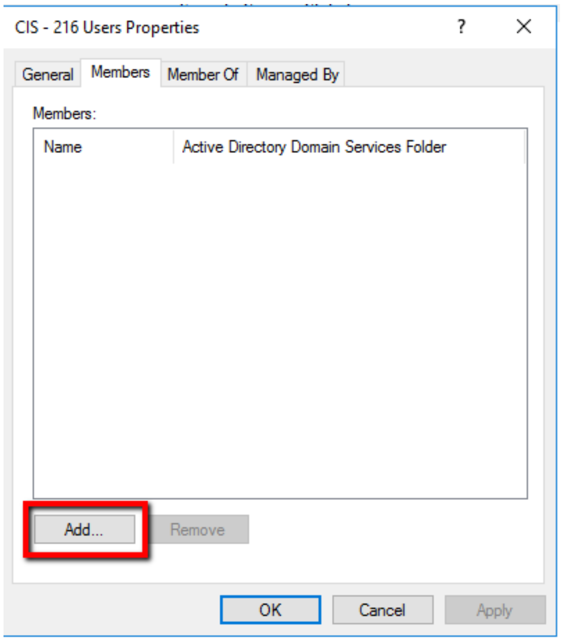


Name	Type
Mitch L. Bartch	User
CIS - 216 Users	Security Group - Global

Next we must add our user account to our security group.

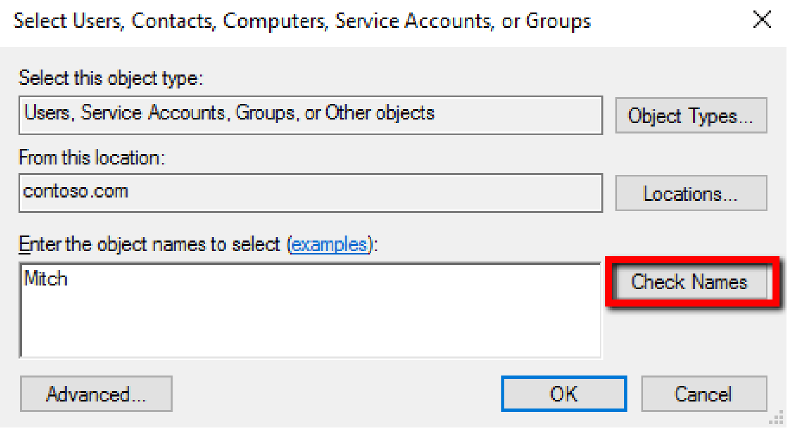
Double-click the CIS 216 group and navigate to the “Members” tab.

Click the “Add...” button to add a user account.



Name	Active Directory Domain Services Folder

Enter in the first name of the user account in the field and click the “Check Names” button.


Select Users, Contacts, Computers, Service Accounts, or Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

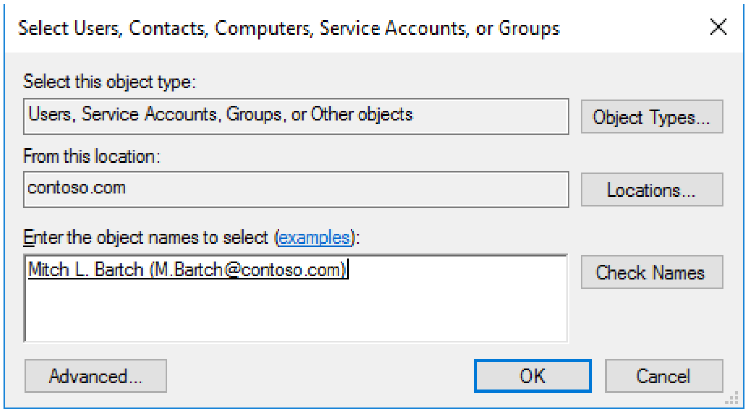
Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
contoso.com

Enter the object names to select (examples):
Mitch

The name should resolve to the full user account name.

Click OK.

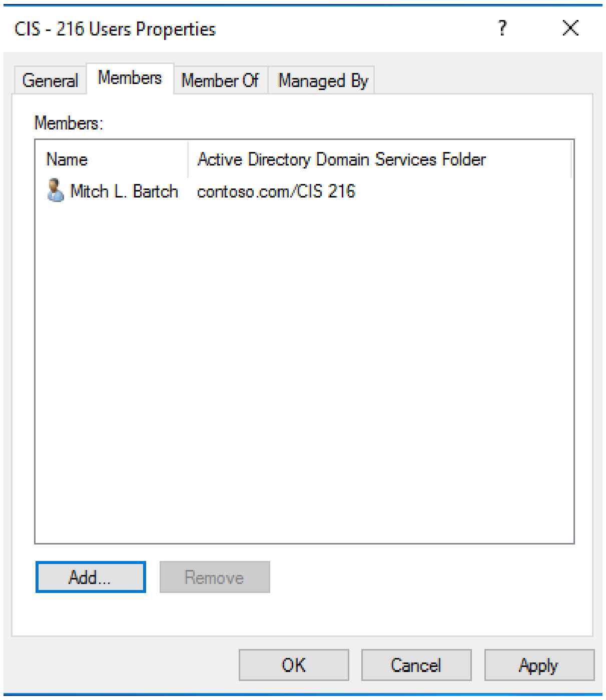

Select Users, Contacts, Computers, Service Accounts, or Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
contoso.com

Enter the object names to select (examples):
Mitch L. Bartch (M.Bartch@contoso.com)

The user account will now appear as a member of the security group.



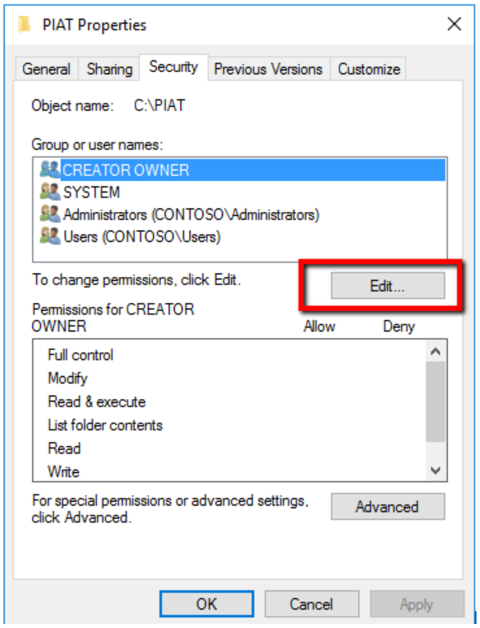
Members:

Name	Active Directory Domain Services Folder
Mitch L. Bartch	contoso.com/CIS 216

Now we will add this group to the NTFS permissions of the “PIAT” folder.

Open the properties window of the “PIAT” folder and navigate to the “Security” tab.

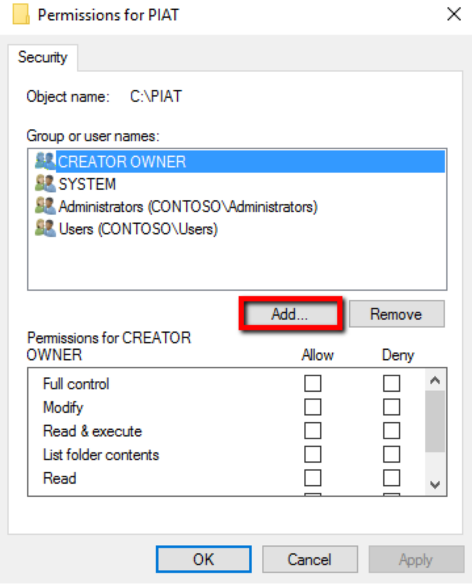
Click the “Edit...” button.



Object name: C:\PIAT

CREATOR OWNER
SYSTEM
Administrators (CONTOSO\Administrators)
Users (CONTOSO\Users)

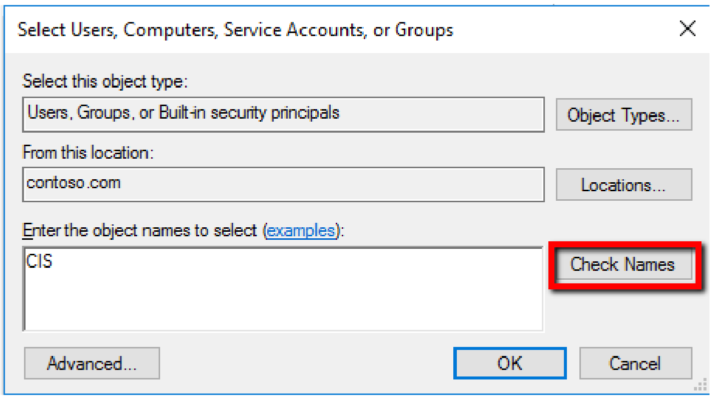
Click the “Add...” button to add our group to the permissions.



Object name: C:\PIAT

CREATOR OWNER
SYSTEM
Administrators (CONTOSO\Administrators)
Users (CONTOSO\Users)

In the text field enter “CIS” and click the “Check Names” button.



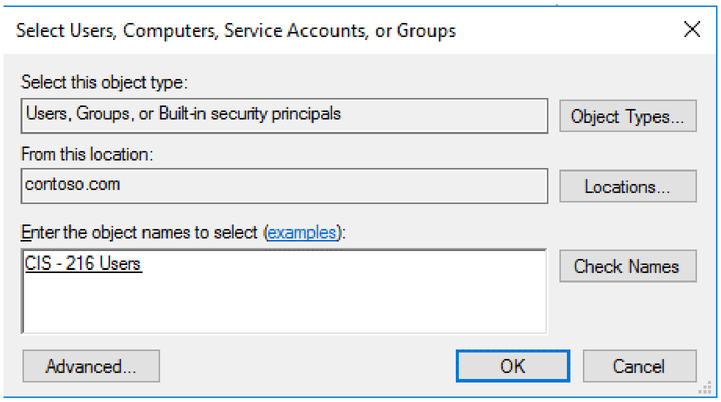
Select this object type: Users, Groups, or Built-in security principals

From this location: contoso.com

Enter the object names to select (examples): CIS

The name should get resolved to our security group.

Click OK.



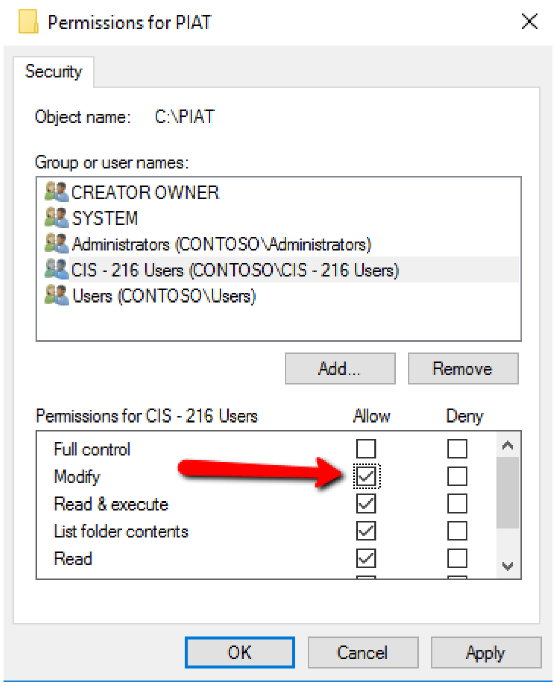
Select this object type: Users, Groups, or Built-in security principals

From this location: contoso.com

Enter the object names to select (examples): CIS - 216 Users

In the permissions window make sure our "CIS - 216 Users" group is highlighted and click the checkmark to allow the Modify permission.

Click OK.



Object name: C:\PIAT

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (CONTOSO\Administrators)
- CIS - 216 Users (CONTOSO\CIS - 216 Users)
- Users (CONTOSO\Users)

Permissions for CIS - 216 Users	Allow	Deny
Full control	☐	☐
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

The “CIS – 216 Users” has now been successfully added to the permissions on the shared folder.

The reason we added the “CIS – 216 Users” group to the permissions for the shared folder is because permissions should always be assigned to security groups as opposed to an individual. If we added individuals to every object they needed permissions to instead of in groups, it would be much more difficult and time consuming to change permissions. Imagine that an individual either leaves the company or their job otherwise changes; you would need to adjust or remove their permissions on each object they had access too. This way we could instead simply remove their account from the respective groups instead of hunting for them on every object they could access.

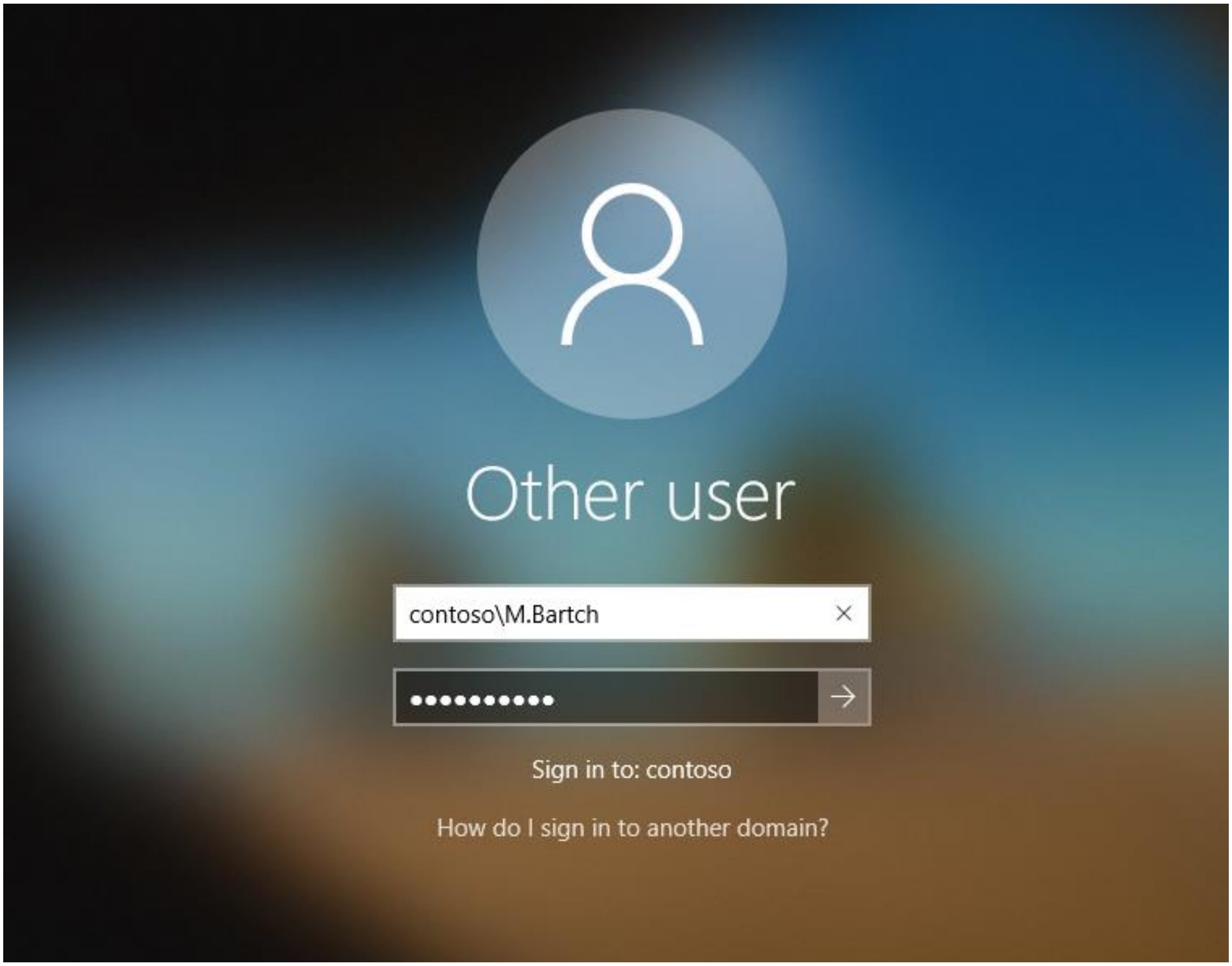
Next we will map a drive for this shared folder on the Windows 10 client computer.

Windows 10 Client Configuration

Launch the Windows 10 (216Client) machine.

Upon reaching the login screen instead of logging on as the Administrator account select the “Other user” option.

Here we will enter in the user account we created in Active Directory and log onto the client as that account. Be sure to preempt the logon name with “contoso\” as you would with the Administrator account as we are not logging in locally.



Other user

contoso\M.Bartch

●●●●●●●●●●●

Sign in to: contoso

How do I sign in to another domain?

After you have signed in, we will map a network drive to the shared folder using Windows PowerShell.

Launch Windows PowerShell.

We will be using the “Z” drive for our network drive.

The command you will be using to perform this action is as follows:

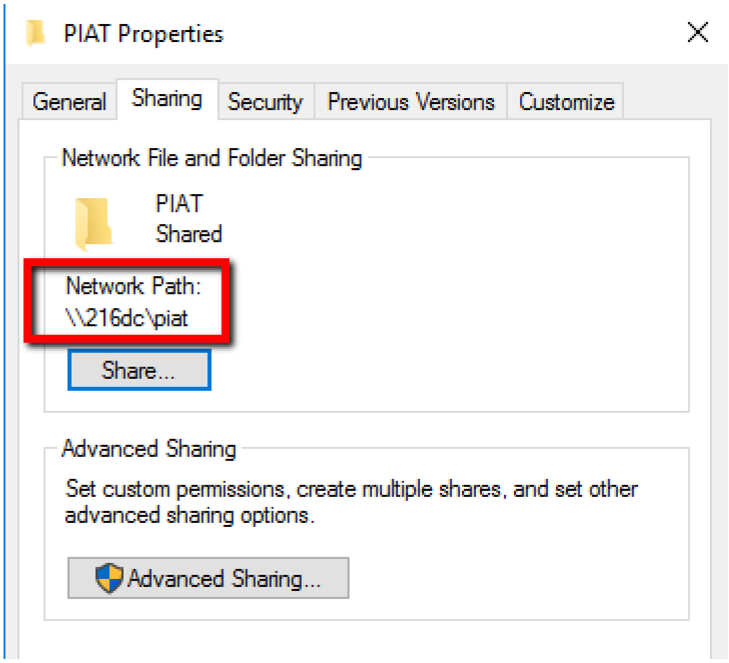
```
net use z: \\216dc\piat /persistent:Yes
```

Let's break down this command a bit so you can understand what it does.

"net use" is a command that is used to connect, remove, and configure shared resources.

"z:" specifies that the "Z" drive will be mapped to our shared folder.

"\\216dc\piat" is the full Universal Naming Convention (UNC) of our shared folder. This specifies where our folder is located on the network. This network path can be found by looking in the "Sharing" tab of the "PIAT" folder.



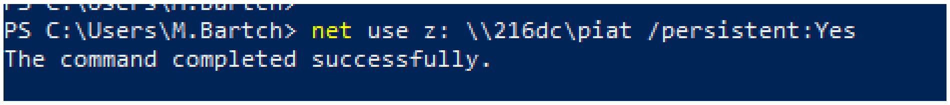
PIAT
Shared

Network Path:
\\216dc\piat

Set custom permissions, create multiple shares, and set other advanced sharing options.

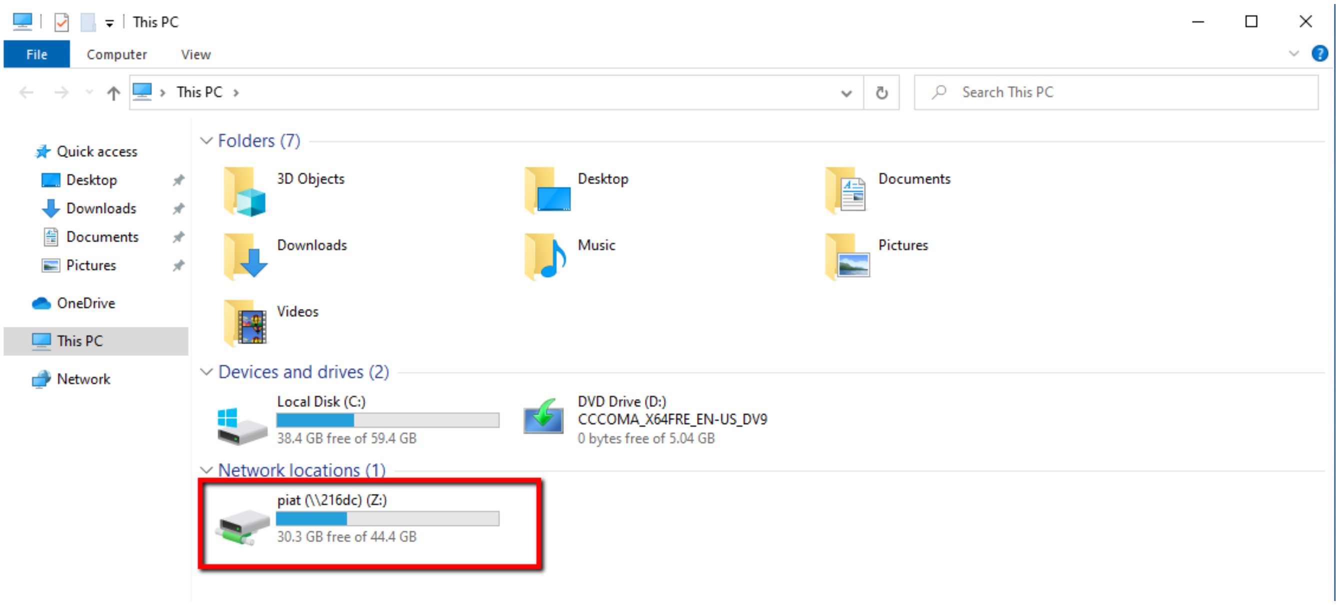
Finally the "/persistent:Yes" option specifies that the mapped drive will remain even when the computer is shut off or restarted. Mapped drives are not persistent by default so if this option is not used once the machine is restarted you would have to add the mapped drive again.

Enter in the "net use z: \\216dc\piat /persistent:Yes" command and hit the "Enter" key.

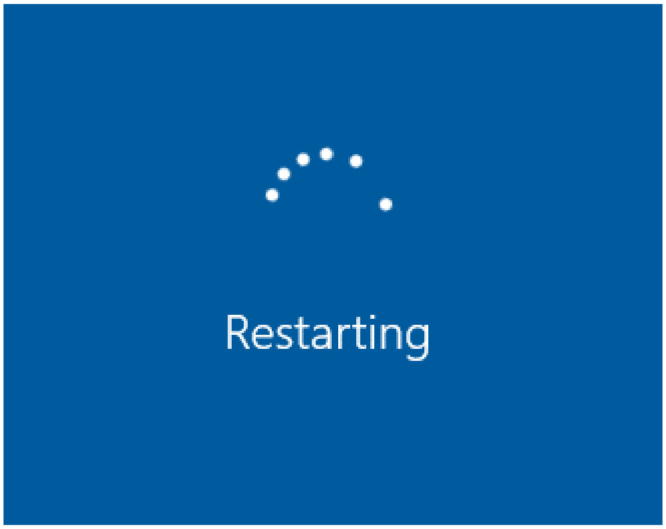


```
PS C:\Users\M.Bartch> net use z: \\216dc\piat /persistent:Yes
The command completed successfully.
```

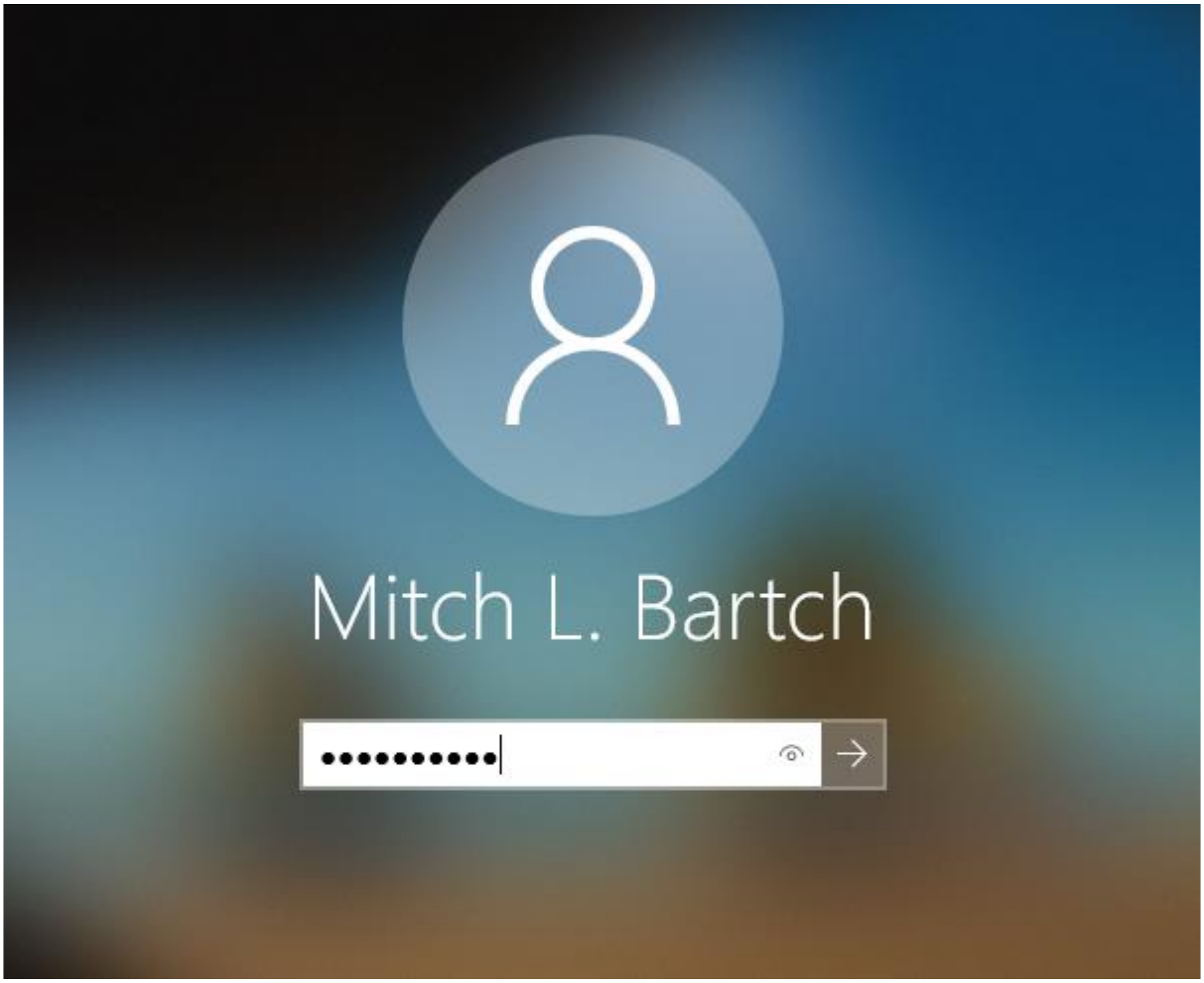
Open "This PC" and you should see the "PIAT" folder mapped to the Z: drive.



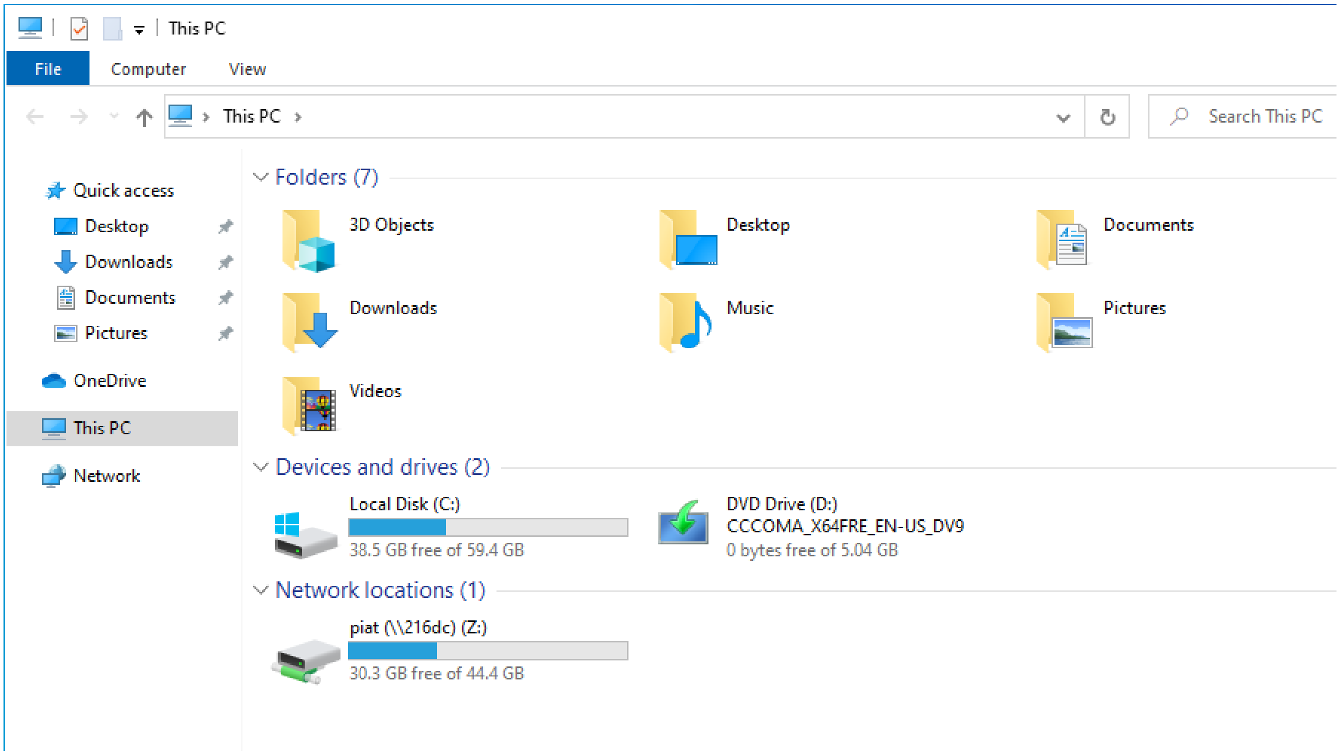
To check that it is persistent restart the client machine.



Log back in as the new user account.



Upon returning to “This PC” the mapped drive should still appear.



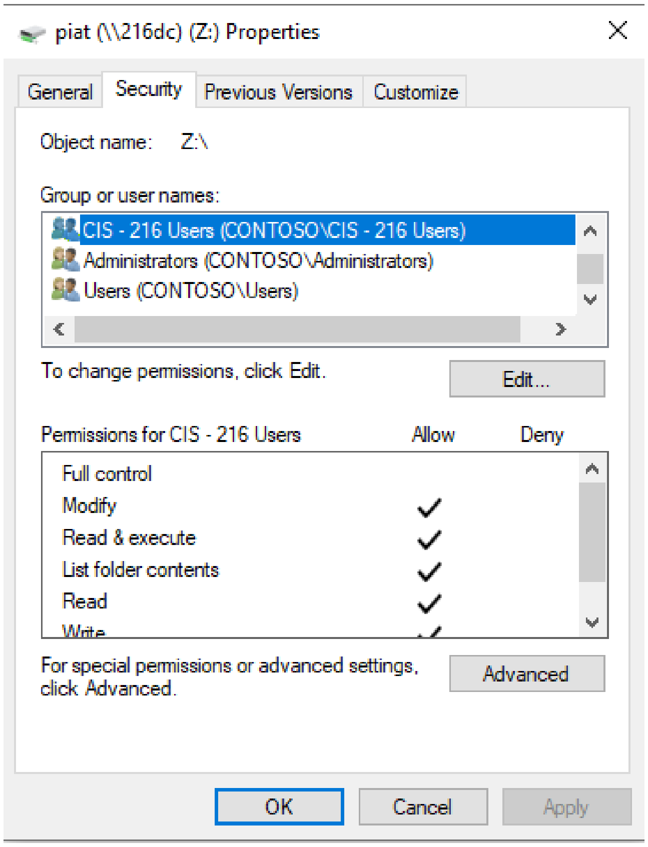
Local Disk (C:)
38.5 GB free of 59.4 GB

DVD Drive (D:) CCCOMA_X64FRE_EN-US_DV9
0 bytes free of 5.04 GB

piat (\\216dc) (Z:)
30.3 GB free of 44.4 GB

All the information on how to map the drive using PowerShell were found at:
https://www.howtogeek.com/118452/how-to-map-network-drives-from-the-command-prompt-in-windows/

If we check the properties of the Z: drive, we can see that the "CIS – 216 Users" security group is there under the "Security" tab.



piat (\\216dc) (Z:) Properties

Object name: Z:\

Group or user names:

- CIS - 216 Users (CONTOSO\CIS - 216 Users)
- Administrators (CONTOSO\Administrators)
- Users (CONTOSO\Users)

To change permissions, click Edit.

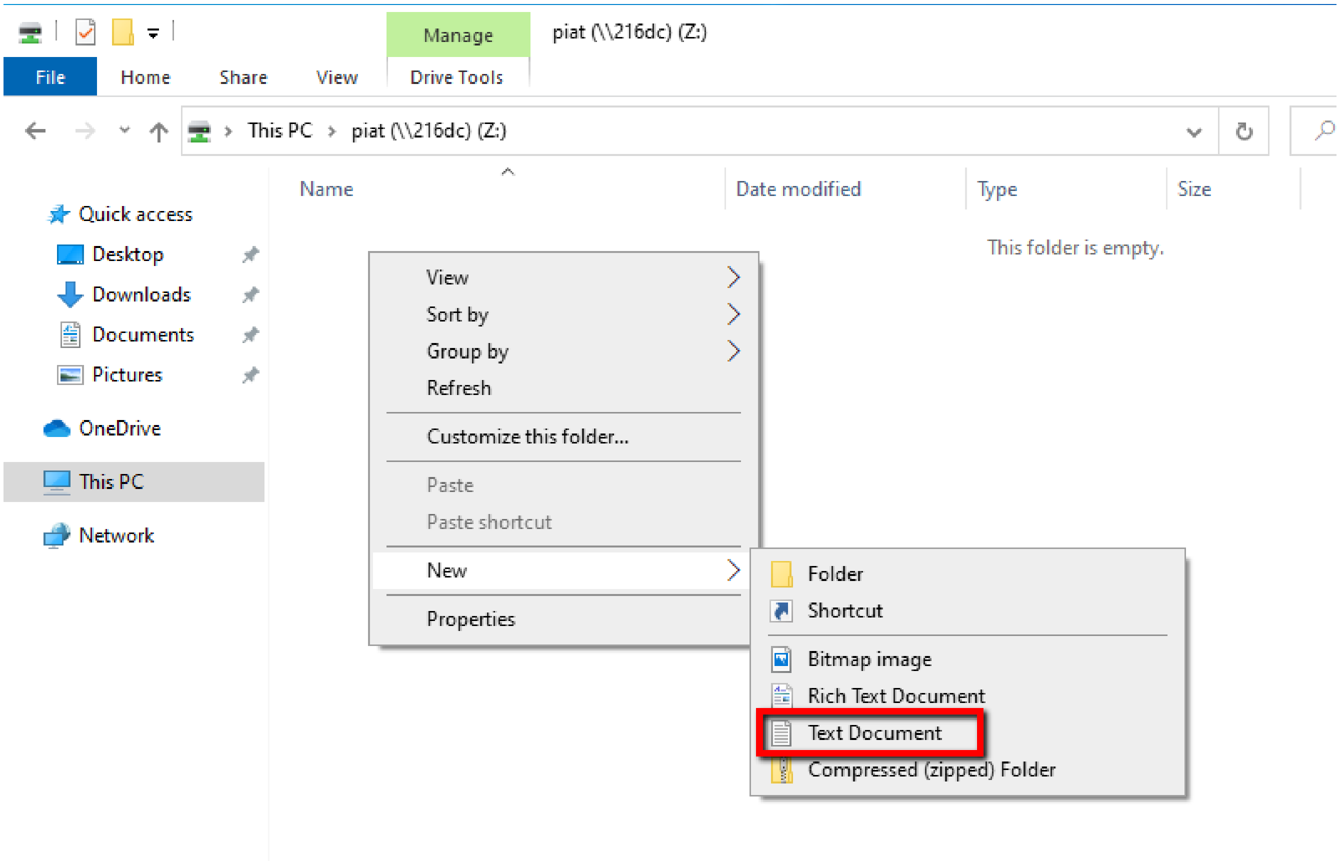
Permissions for CIS - 216 Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

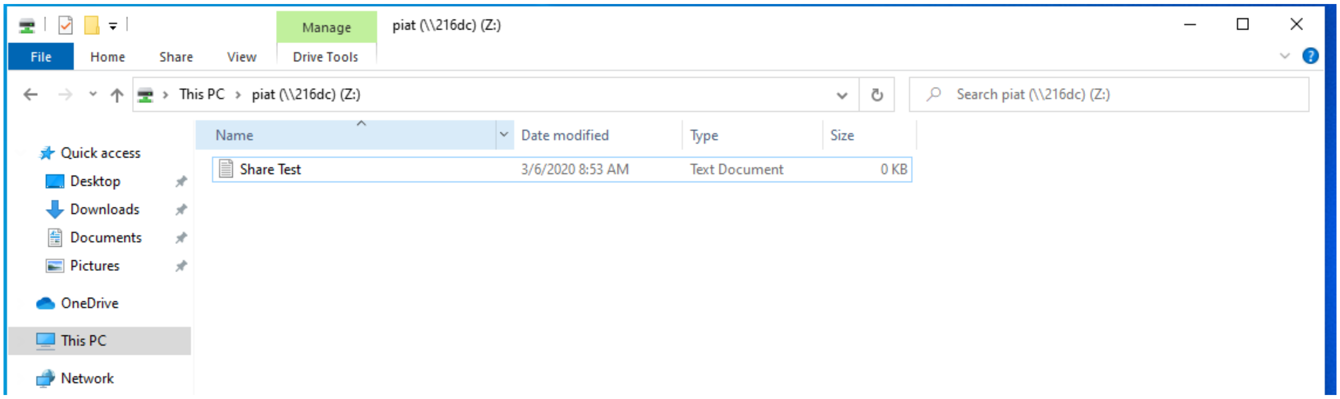
Since we are accessing this share folder over the network with the NTFS permission as Modify and the Share permission as Change, our effective permissions should allow us to read, write, execute, and delete folders and files on the mapped drive. Let's test this by writing a file to the drive.

Open the Z: drive.

Right-click and create a new text document.



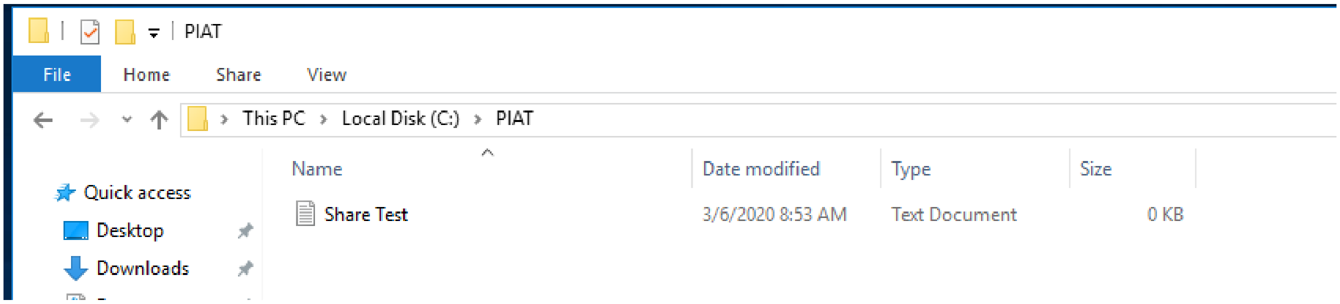
Name the document “Share Test”.



Name	Date modified	Type	Size
Share Test	3/6/2020 8:53 AM	Text Document	0 KB

Let’s see if the document appears on the server.

On 216DC navigate to C: -> PIAT.



Name	Date modified	Type	Size
Share Test	3/6/2020 8:53 AM	Text Document	0 KB

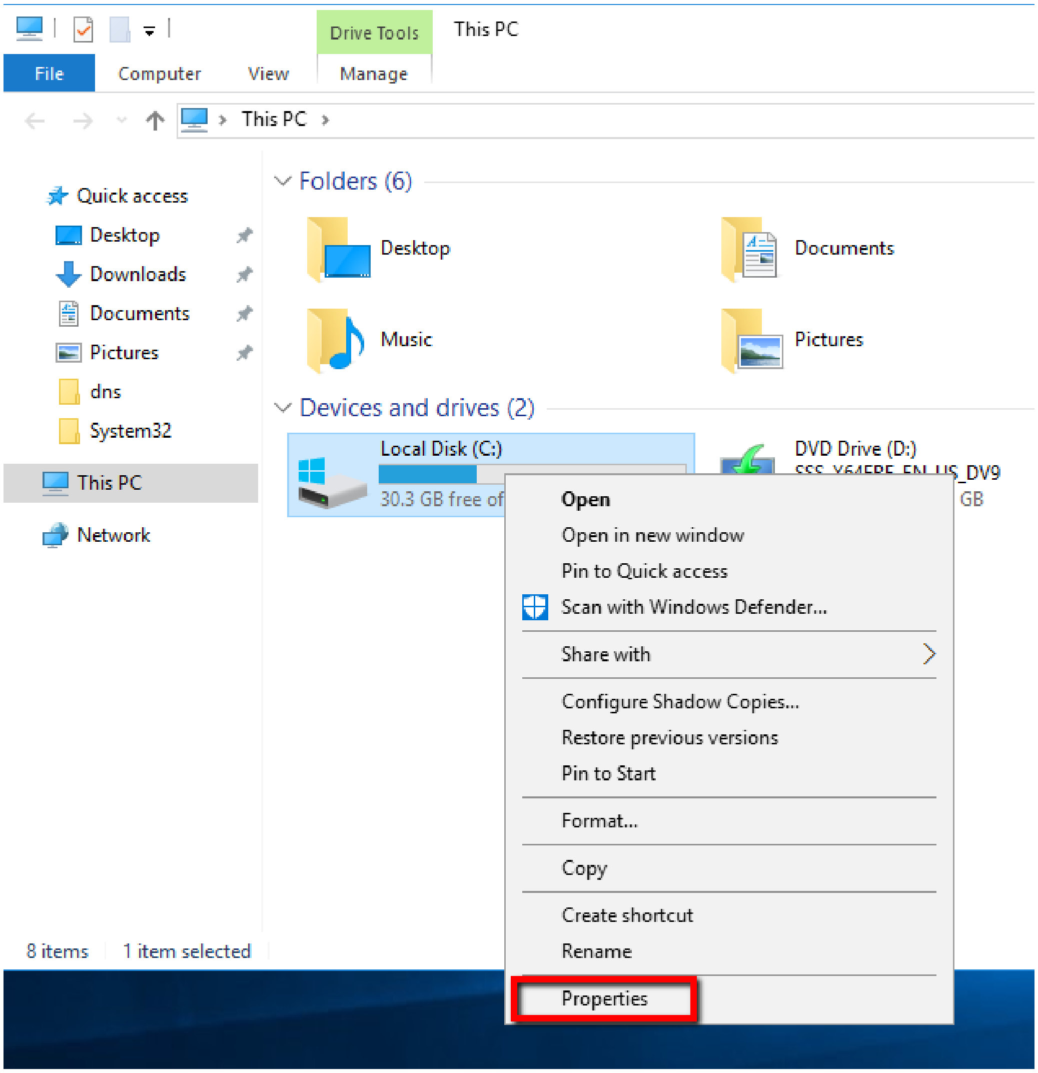
The share is successful.

Shadow Copies and Quota

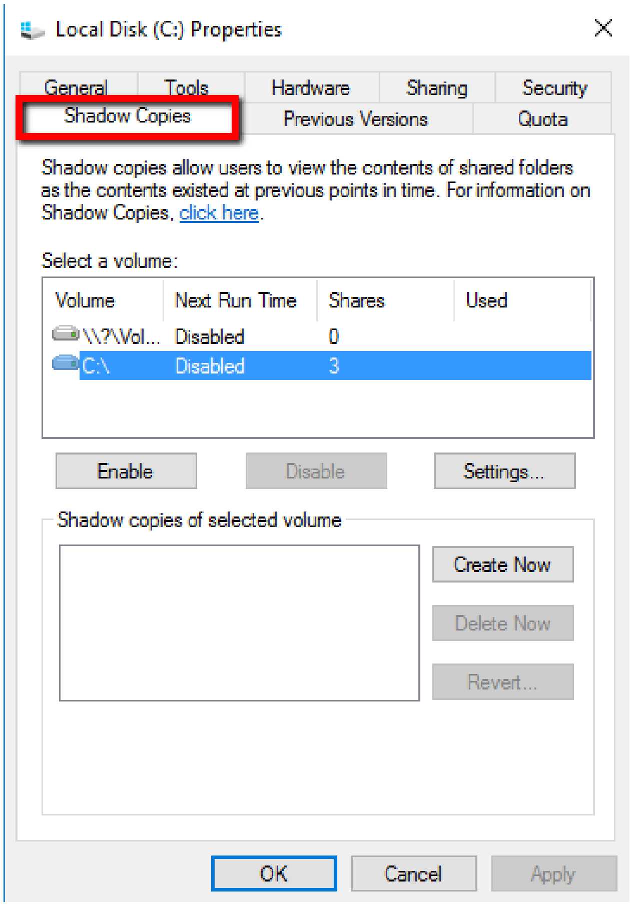
Next we will return to the 216DC server and create a shadow copy of the C: drive.

A shadow copy is a snapshot of a computer volume. This functions as a backup of sorts as you can access previous versions of a file on the volume shadow copies is enabled on. These snapshots can be taken even when the volume is in use.

Go to “This PC” and right-click the C: drive. Click “Properties”.



Navigate to the “Shadow Copies” tab.



Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.

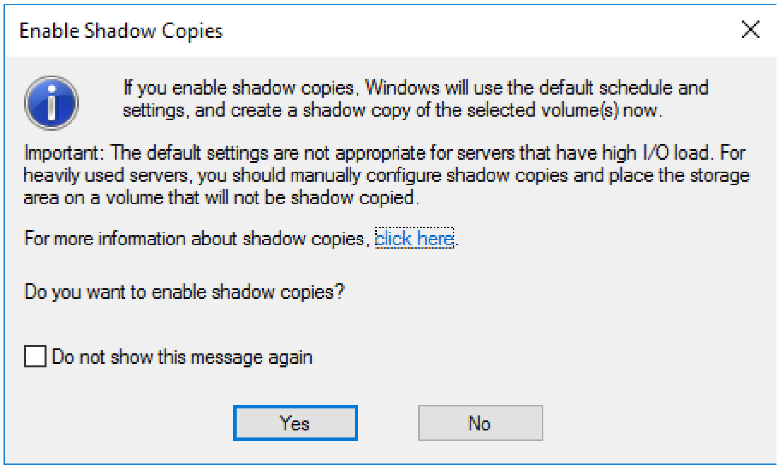
Select a volume:

Volume	Next Run Time	Shares	Used
\\?\Vol...	Disabled	0	
C:\	Disabled	3	

Click the “Enable” button to enable creation of shadow copies of the C: drive.

A window will appear saying that a shadow copy of the drive will be created now and that it will use the default schedule and settings.

Click Yes.



Enable Shadow Copies

If you enable shadow copies, Windows will use the default schedule and settings, and create a shadow copy of the selected volume(s) now.

Important: The default settings are not appropriate for servers that have high I/O load. For heavily used servers, you should manually configure shadow copies and place the storage area on a volume that will not be shadow copied.

For more information about shadow copies, click here.

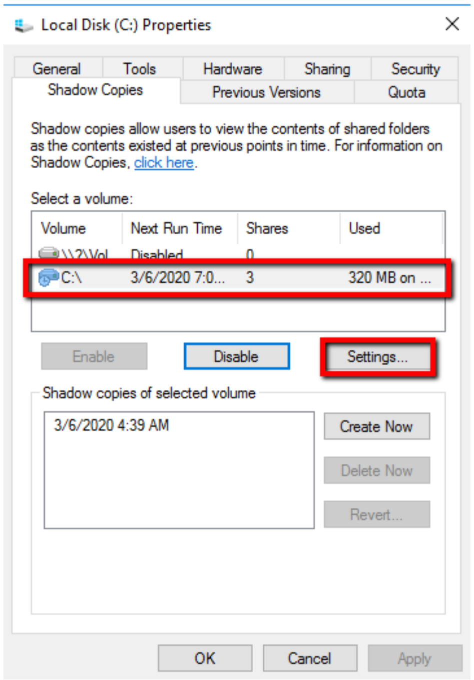
Do you want to enable shadow copies?

□ Do not show this message again

The C: drive will now have a shadow copy of it made.

Back at the “Shadow Copies” tab you can see when the next shadow copy run will be performed.

Click the “Settings...” button.



Local Disk (C:) Properties

Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.

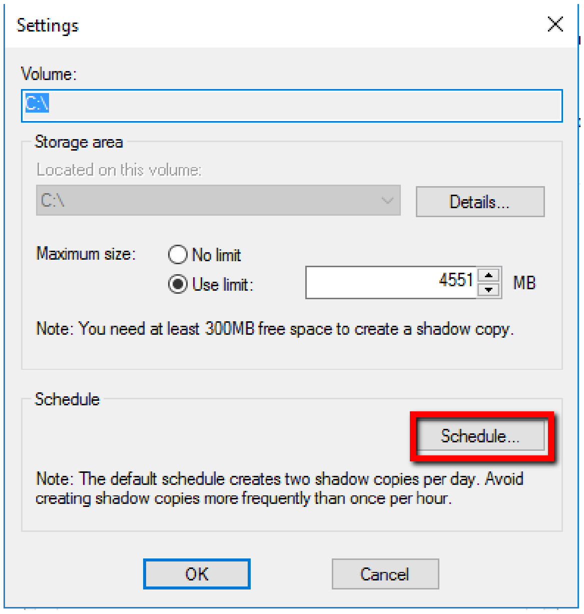
Select a volume:

Volume	Next Run Time	Shares	Used
\\?\Vol...	Disabled	0	
C:\	3/6/2020 7:0...	3	320 MB on ...

Shadow copies of selected volume

3/6/2020 4:39 AM

Click the “Schedule...” button to see how often shadow copies will be made.



Settings

Volume: C:\

Storage area

Located on this volume: C:\ Details...

Maximum size: ○ No limit
● Use limit: 4551 MB

Note: You need at least 300MB free space to create a shadow copy.

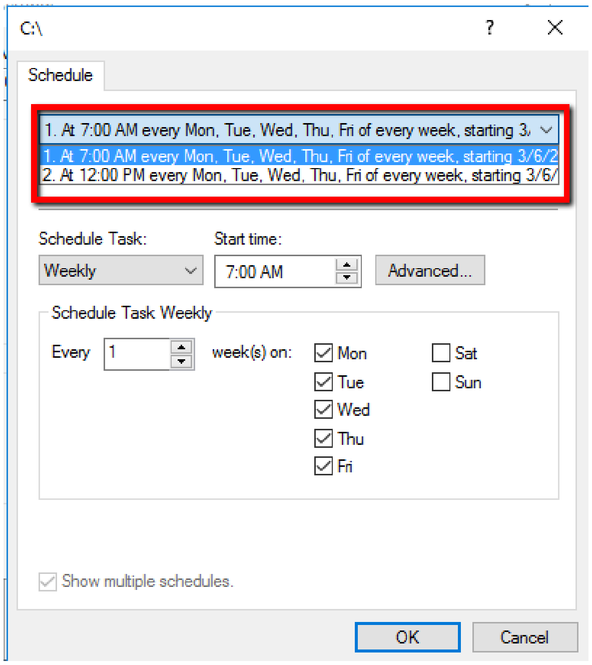
Schedule

Schedule...

Note: The default schedule creates two shadow copies per day. Avoid creating shadow copies more frequently than once per hour.

OK Cancel

Clicking on the drop-down menu reveals that there are 2 times shadow copies will be run, at 7AM and at 7PM every weekday starting now.



C:\

Schedule

1. At 7:00 AM every Mon, Tue, Wed, Thu, Fri of every week, starting 3/

1. At 7:00 AM every Mon, Tue, Wed, Thu, Fri of every week, starting 3/6/2
2. At 12:00 PM every Mon, Tue, Wed, Thu, Fri of every week, starting 3/6/

Schedule Task: Weekly

Start time: 7:00 AM

Advanced...

Schedule Task Weekly

Every 1 week(s) on: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

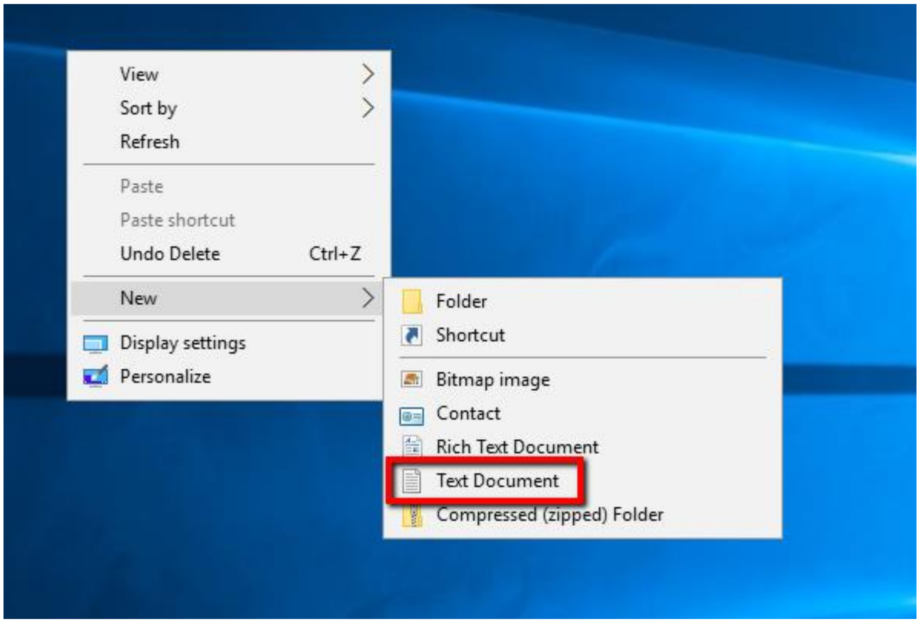
☑ Show multiple schedules.

OK Cancel

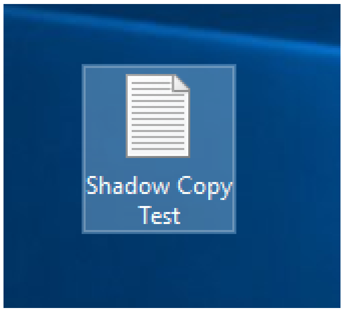
Click OK.

Next let's perform a test of what shadow copies can do for us.

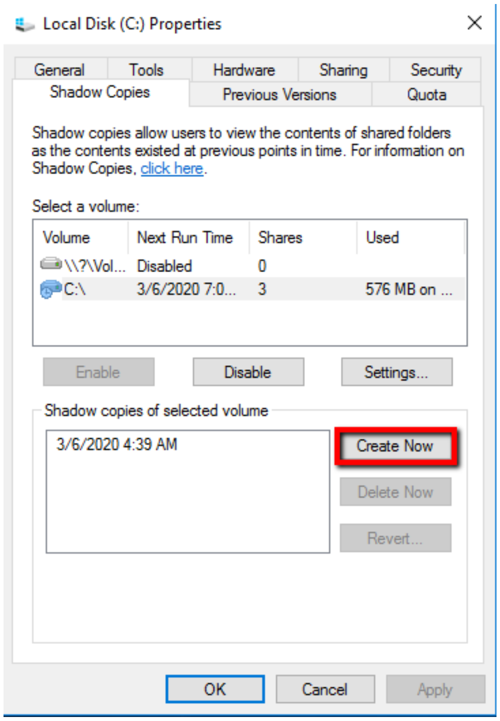
On the Desktop create a new text file.



Name the file “Shadow Copy Test”.



Navigate back to the C: drive Properties window and under the “Shadow Copies” tab click the “Create Now” button to create a new shadow copy.



Local Disk (C:) Properties

Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.

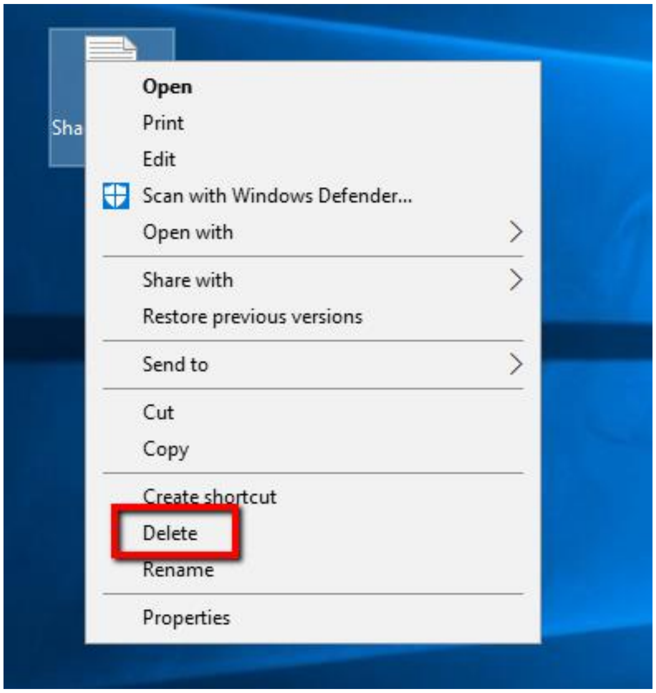
Select a volume:

Volume	Next Run Time	Shares	Used
\\?\Vol...	Disabled	0	
C:\	3/6/2020 7:0...	3	576 MB on ...

Shadow copies of selected volume

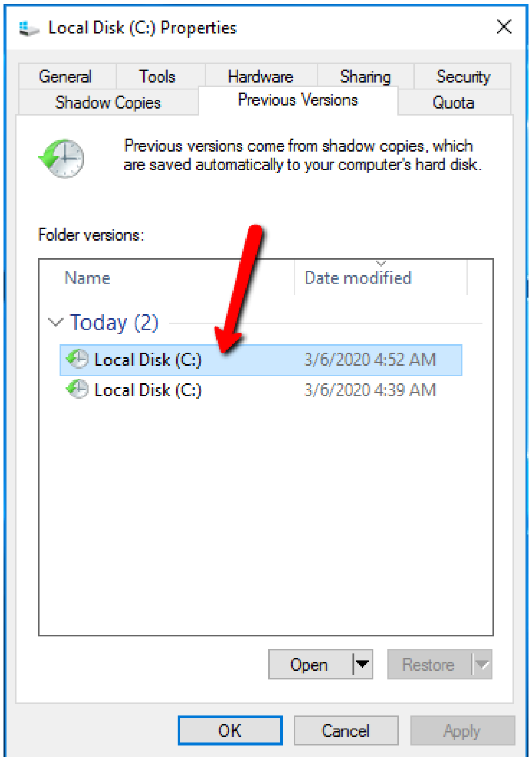
3/6/2020 4:39 AM

After it has run, delete the “Shadow Copy Test” text file.



Navigate to the “Previous Versions” tab and select the most recent shadow copy.

Click Open

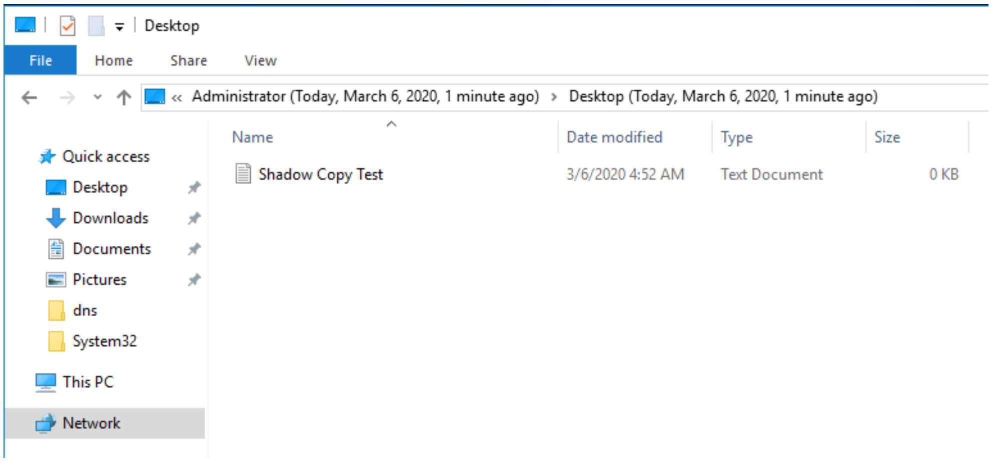


Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

Folder versions:

Name	Date modified
Today (2)	
Local Disk (C:)	3/6/2020 4:52 AM
Local Disk (C:)	3/6/2020 4:39 AM

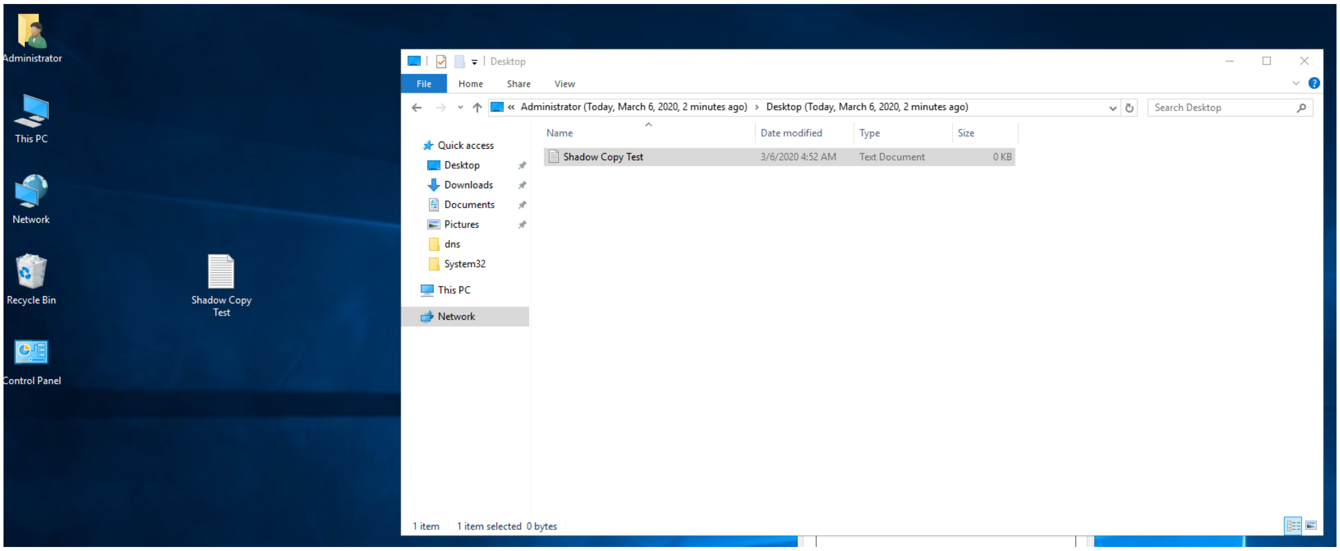
The shadow copy of the C: drive will now open. This is a version of the drive as it was when the shadow copy was created. From this previous version let’s see if we can retrieve the “Shadow Copy Test” file we just deleted. Navigate to Users -> Administrator -> Desktop. You should see the “Shadow Copy Test” file appear.



« Administrator (Today, March 6, 2020, 1 minute ago) › Desktop (Today, March 6, 2020, 1 minute ago)

Name	Date modified	Type	Size
Shadow Copy Test	3/6/2020 4:52 AM	Text Document	0 KB

Either drag the file or copy and paste it back to the Desktop.



Name	Date modified	Type	Size
Shadow Copy Test	3/6/2020 4:52 AM	Text Document	0 KB

The file has now been recovered from the shadow copy.

Next we will look at the “Quota” tab.

NTFS Quotas are used to set storage limits for users for a particular volume. A user who exceeds this limit can be issued a warning or denied access. The storage limit is used by the size of files that a user creates or owns.

Navigate to the “Quota” tab.

Here we will make some changes.

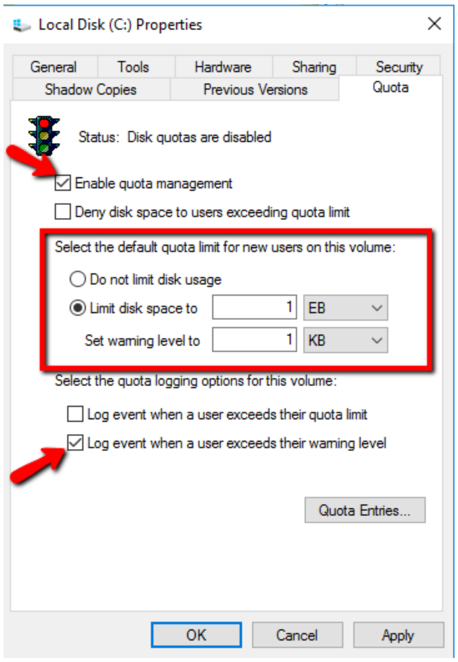
Click the button to “Enable quota management”.

Next select limit disk space and change the KB option to EB. This changes the disk space limit from 1 kilobyte to 1 exabyte.

Leave the warning level at 1 KB.

Finally check the box next to “Log event when a user exceeds their warning level”

Click OK.



Local Disk (C:) Properties

Status: Disk quotas are disabled

☑ Enable quota management

☐ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

○ Do not limit disk usage

● Limit disk space to 1 EB

Set warning level to 1 KB

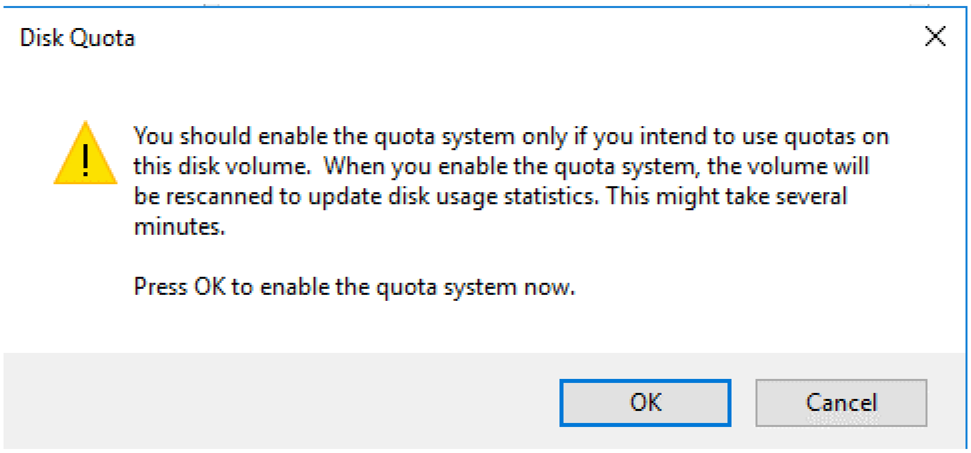
Select the quota logging options for this volume:

☐ Log event when a user exceeds their quota limit

☑ Log event when a user exceeds their warning level

A warning window will appear saying that the quota system should only be activated on this drive if quotas are expected to be used and that the volume will be now scanned for usage stats.

Click OK.



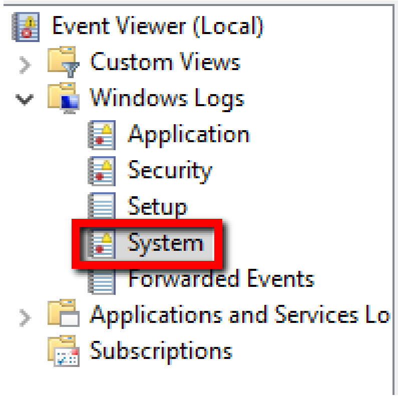
Disk Quota

You should enable the quota system only if you intend to use quotas on this disk volume. When you enable the quota system, the volume will be rescanned to update disk usage statistics. This might take several minutes.

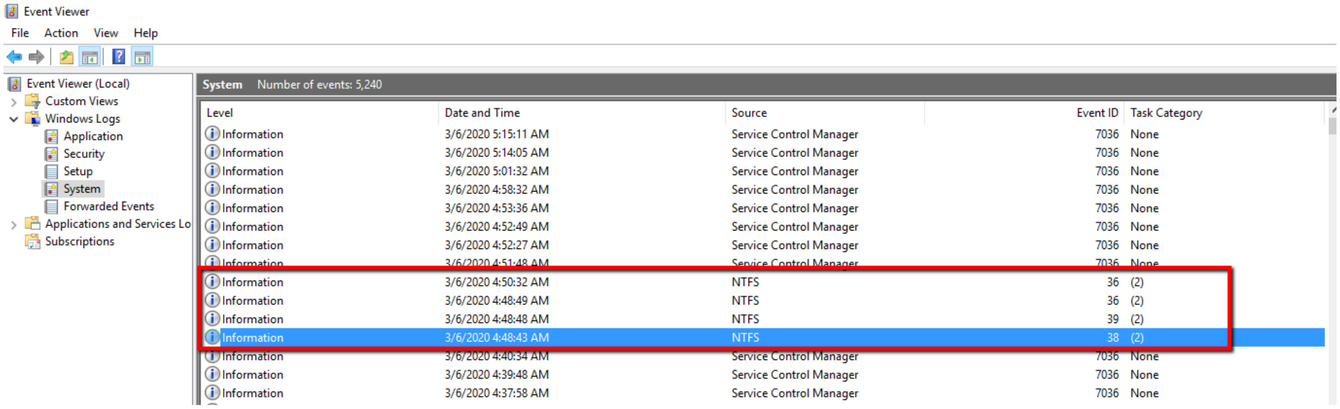
Press OK to enable the quota system now.

To find the logs we enabled in the “Quota” tab open Event Viewer.

The logs will appear under Windows Logs -> System.



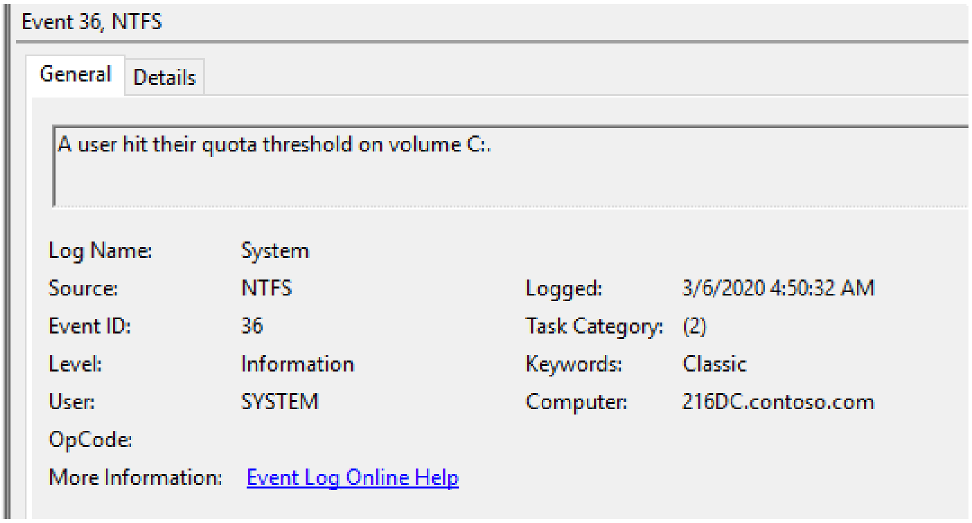
Look for the Event ID of 36. This will correspond to our warning for a user exceeding their quota warning level.



System Number of events: 5,240

Level	Date and Time	Source	Event ID	Task Category
Information	3/6/2020 5:15:11 AM	Service Control Manager	7036	None
Information	3/6/2020 5:14:05 AM	Service Control Manager	7036	None
Information	3/6/2020 5:01:32 AM	Service Control Manager	7036	None
Information	3/6/2020 4:58:32 AM	Service Control Manager	7036	None
Information	3/6/2020 4:53:36 AM	Service Control Manager	7036	None
Information	3/6/2020 4:52:49 AM	Service Control Manager	7036	None
Information	3/6/2020 4:52:27 AM	Service Control Manager	7036	None
Information	3/6/2020 4:51:48 AM	Service Control Manager	7036	None
Information	3/6/2020 4:50:32 AM	NTFS	36	(2)
Information	3/6/2020 4:48:49 AM	NTFS	36	(2)
Information	3/6/2020 4:48:48 AM	NTFS	39	(2)
Information	3/6/2020 4:48:43 AM	NTFS	38	(2)
Information	3/6/2020 4:40:34 AM	Service Control Manager	7036	None
Information	3/6/2020 4:39:48 AM	Service Control Manager	7036	None
Information	3/6/2020 4:37:58 AM	Service Control Manager	7036	None

Clicking on one of these logs will provide some details.



Event 36, NTFS

A user hit their quota threshold on volume C:.

Log Name:	System		
Source:	NTFS	Logged:	3/6/2020 4:50:32 AM
Event ID:	36	Task Category:	(2)
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	216DC.contoso.com
OpCode:			
More Information:	Event Log Online Help		

This concludes PIAT - File and Share Access Configuration.