Files and Folders

Introduction and/or Background

Tx-Rig would like to implement volume shadow copies, compression, and encryption to efficiently store and protect their sensitive files.

Objectives

In this project/lab the student will:

- Configure volume shadow copies
- Configure disk compression
- Enable encryption

Equipment/Supplies Needed

- VMWare Workstation Pro
- Windows Server 2019 Virtual Machine

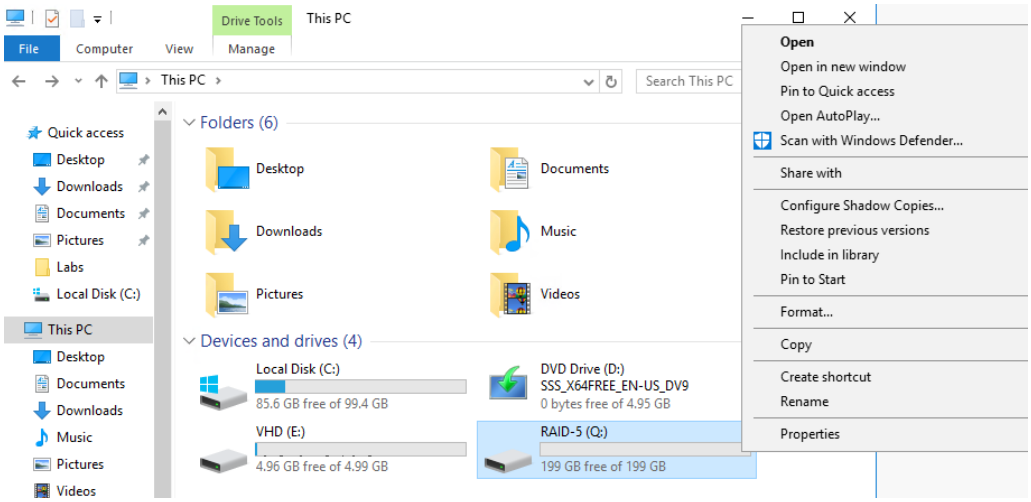
Assessment Criteria

- Take a screenshot of the restored RAID-5 text file (PrtScr#1).
- Take a screenshot showing the Test2 text file is no longer compressed (PrtScr#2).
- Take a screenshot showing who has access to the Encrypted2 file (PrtScr#3).
- Answer the Reflection questions in a text file

Assignment

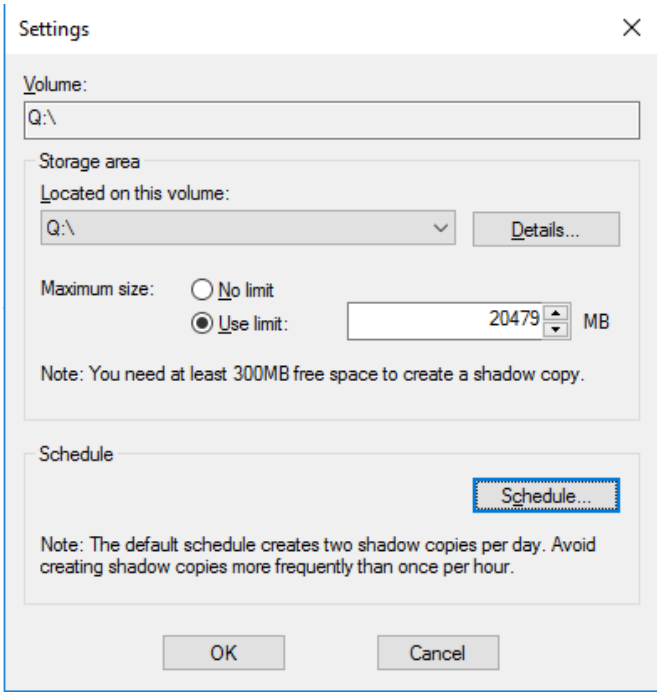
Purpose of Activity: In this activity, you will use the GUI to enable and configure Volume Shadow Copies on the Windows Server operating system.

1. Log on to your server as ***Administrator.***
2. Right-click **Start**, click **File Explorer**, click **This PC**. Right-click the **RAID-5** volume and click **Configure Shadow Copies**. (You can also open the volume's Properties dialog box and click the Shadow Copies tab.)

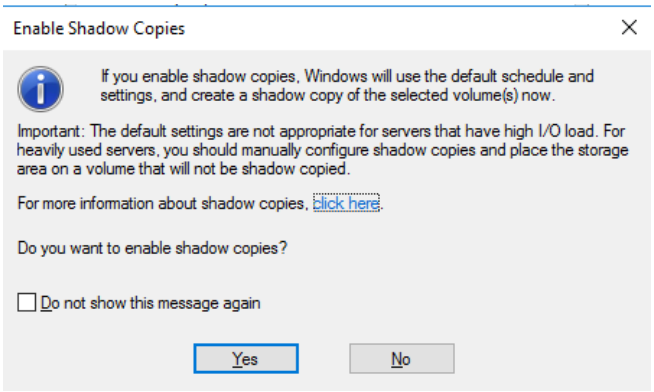


3. In the Select a volume list box, click **Q:** if it's not already selected. Each volume on the computer has an entry so that you can configure shadow copies for all volumes in one place. Each volume entry tells you the next scheduled run time for shadow copies, the number of shares on the volume, and how much space shadow copies are currently using.

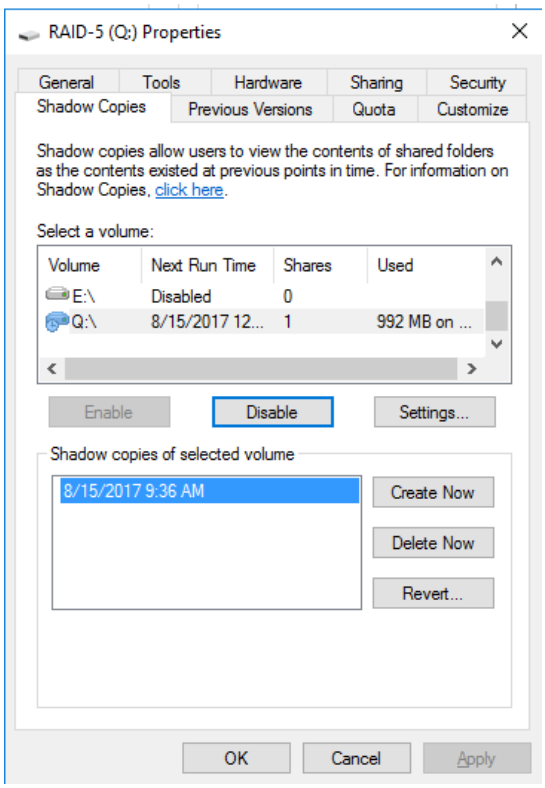
4. Click the **Settings** button. If necessary, you can change where shadow copies for this volume are stored. The Use limit option is set to 10% of volume size or 300 MB, whichever is higher. Click the **Schedule** button. The schedule currently contains two entries: one for 7:00 a.m. and one for 12:00 p.m. Monday through Friday. You can delete and add entries to the default schedule to create your own schedule. Click **Cancel**, and then click **OK**.



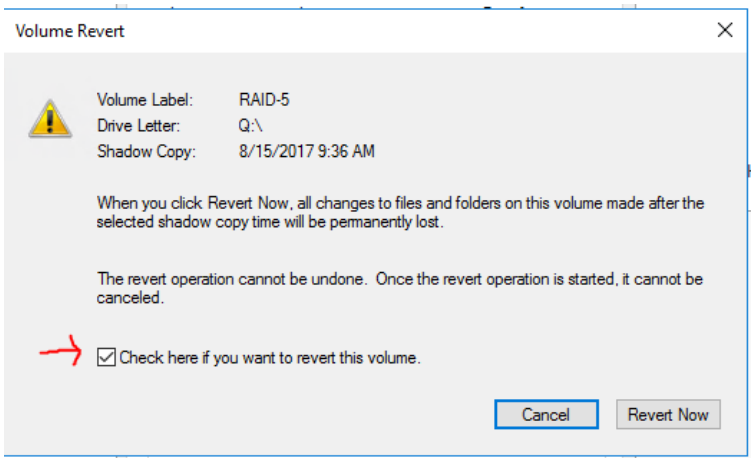
5. To enable shadow copies and create the first shadow copy, click to select the Q**:** volume, and then click the **Enable** button. Read the resulting message and click **Yes**.



6. Click the new entry in the Shadow copies of selected volume list box, and note that the Delete Now and Revert buttons are enabled.

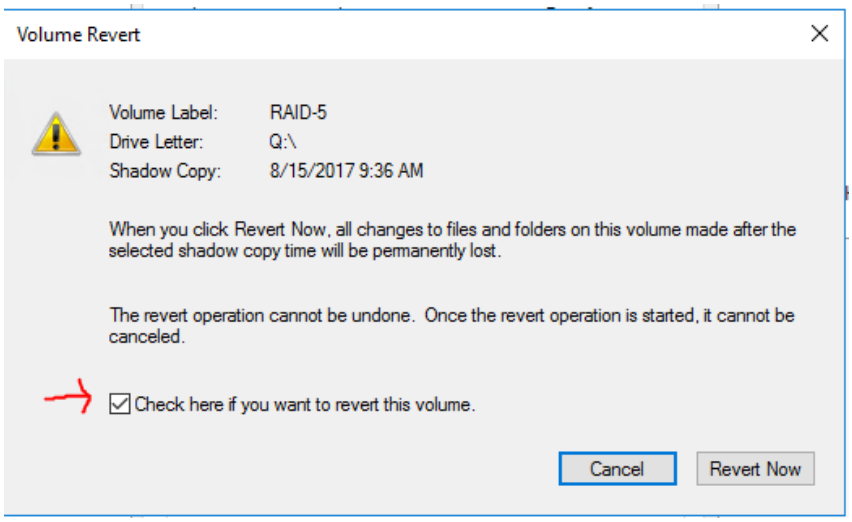


7. Click the **Revert** button, and read the Volume Revert message. Click **Check here if you want to revert this volume**, and then click **Revert Now**. The shadow copy entry is deleted because this instance was used to revert the volume.

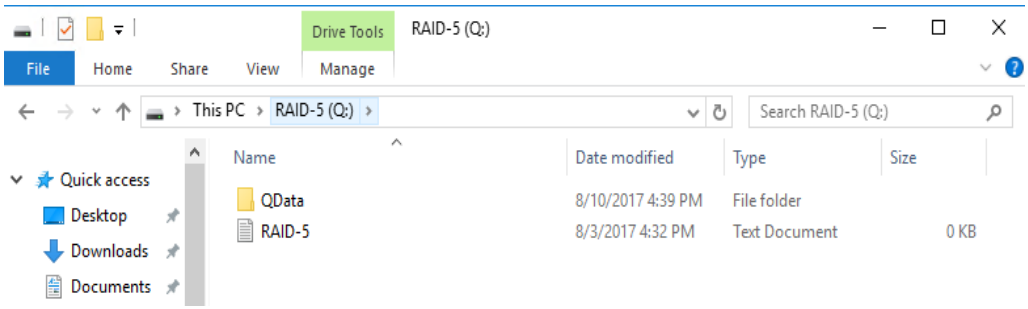


8. Click **Create Now**. A new shadow copy entry is created. Click **OK**.
9. Open the **RAID-5 (Q:)** volume and delete the RAID-5 text file.
10. Open the **Q:** volume's **Properties** dialog box again, and click the **Shadow Copies** tab. If necessary, click the **Q:** volume. Click the entry in

the Shadow copies of the selected volume list box, and then click **Revert**. Click **Check here if you want to revert this volume**, and then click **Revert Now**. Click **OK**.



11. In File Explorer, navigate to the **RAID-5 (Q:)** drive in the left pane, if necessary. Right-click empty space and click **Refresh**. Notice that the RAID-5 text file has been restored.
12. Take a screenshot of the restored RAID-5 text file (PrtScr#1).



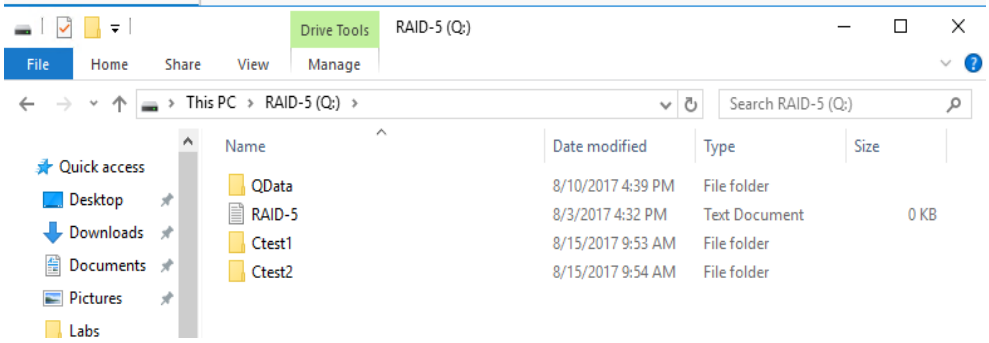
13. Close all open windows but remain logged on for the next activity.

Part 2

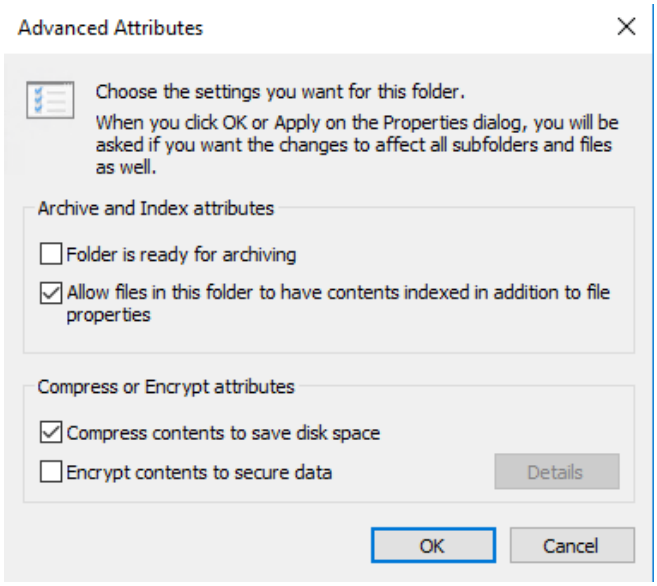
Purpose of Activity: In this activity, you will use the GUI to enable and configure Disk Compression on the Windows Server operating system.

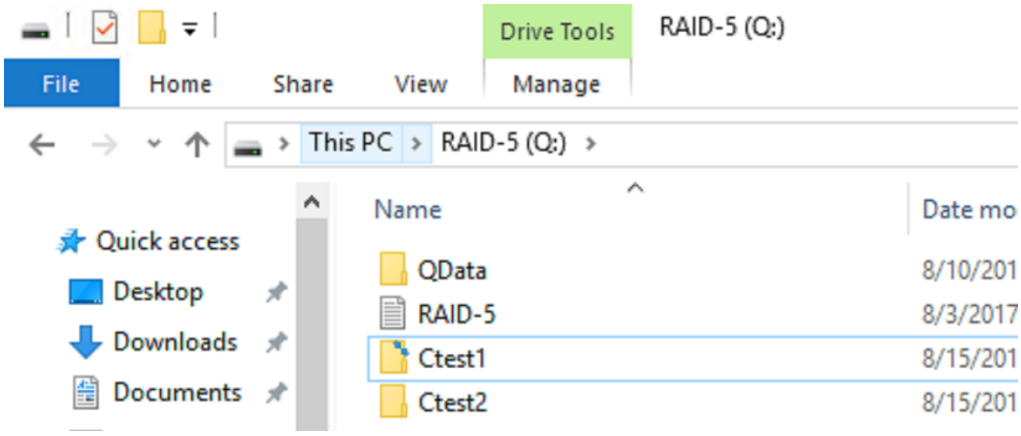
1. Log on to your server as ***Administrator.***

2. Open **File Explorer**, and click to open the **RAID-5** volume. Create two folders named **Ctest1** and **Ctest2**.

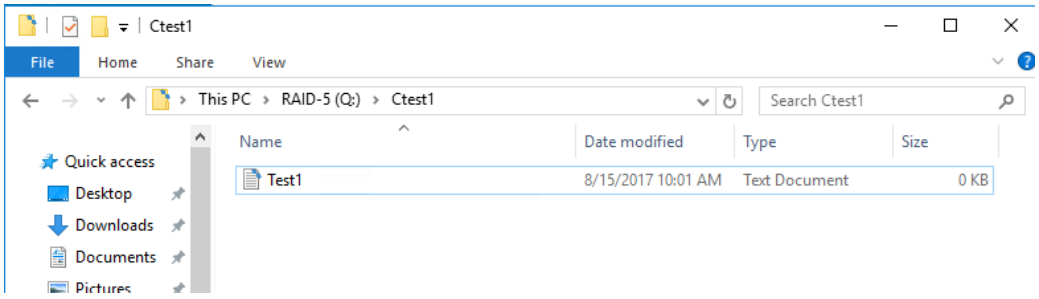


3. Right-click **Ctest1** and click **Properties**. Click **Advanced**. In the Advanced Attributes dialog box, click the **Compress contents to save disk space** check box, and then click **OK** twice. Note that the **Ctest1** folder's icon has 2 small blue arrows pointing to each other in the right corner.

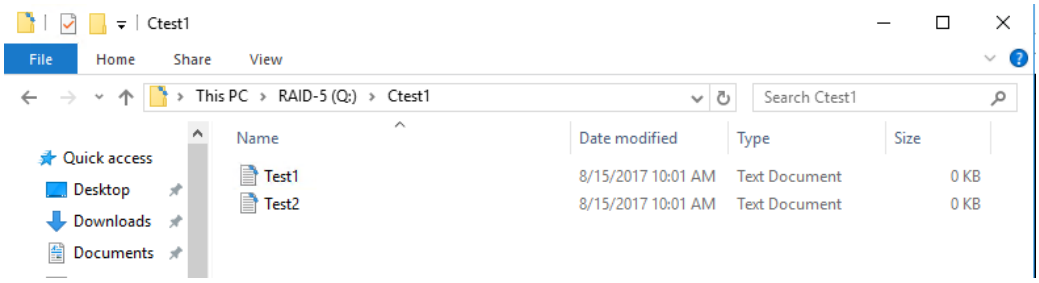




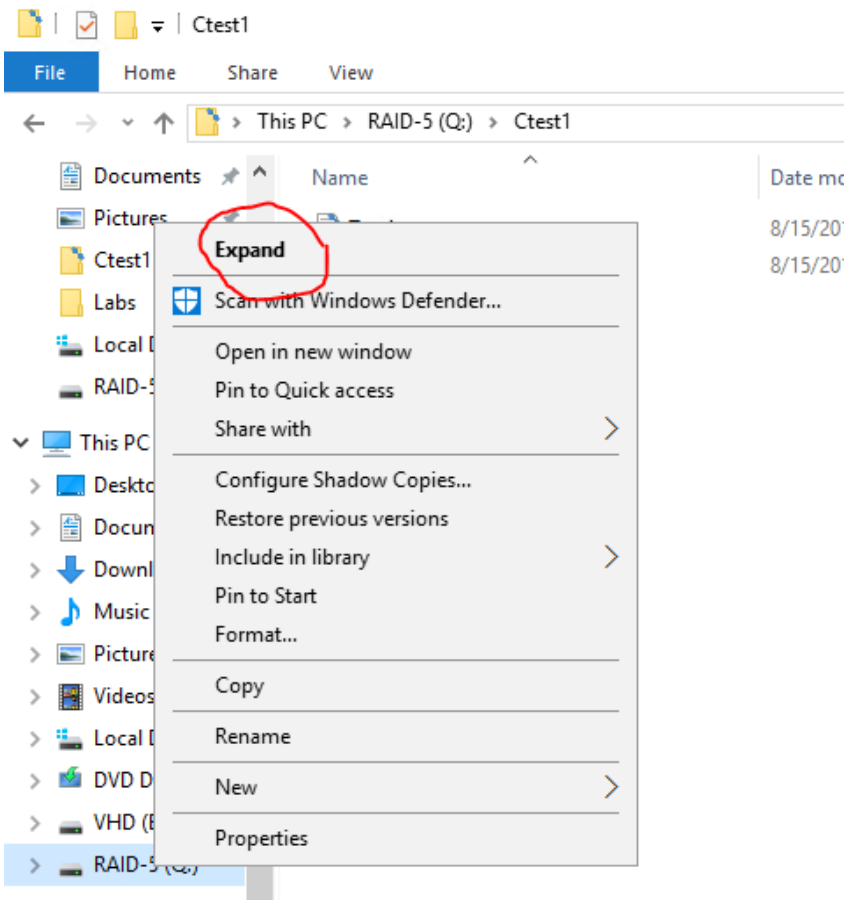
4. Double-click to open the **Ctest1** folder, and create a text document in it named **Test1**. Note that the Test1 filename has the same 2 little blue arrows in the right corner, indicating that it's compressed. Open **Test1**, type your name, and then save and close the file. Access to the compressed file is transparent, meaning you didn't have to do anything special to open it.



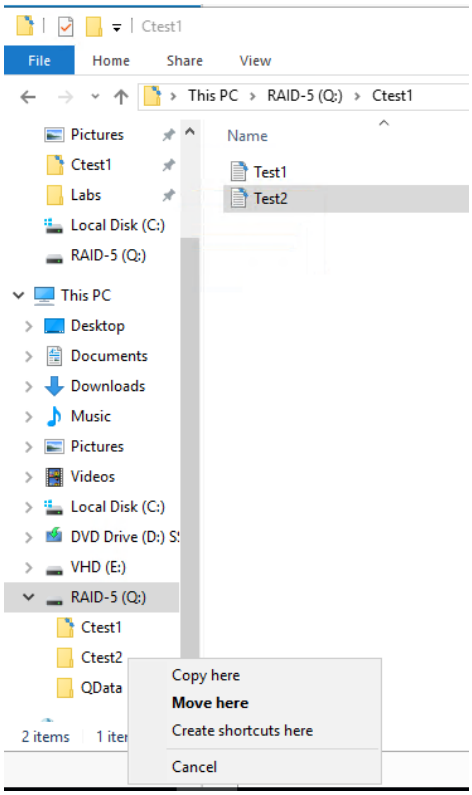
5. Copy **Test1** and paste it in the same folder. Rename this file **Test2**.



6. Right-click on the **RAID-5** volume and select **Expand**.

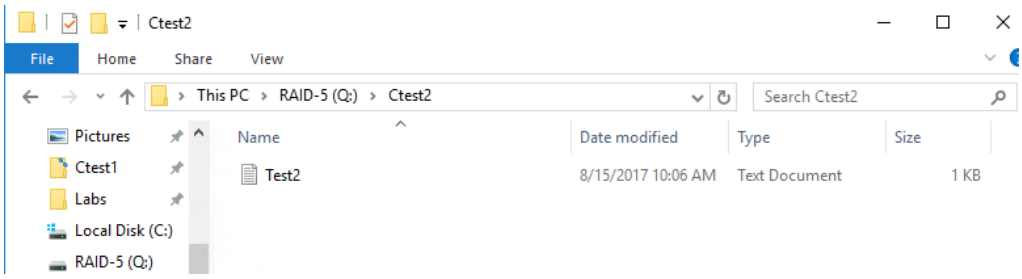


7. Right-click and drag **Test2** to the **Ctest2** folder. Release the right mouse button and click **Move Here**.



8. Click to open the **Ctest2** folder. Note that **Test2** is still compressed.
9. Press **Ctrl**+**Z** to undo the last action. Test2 is moved back to the Ctest1 folder.

10. Right-click and drag **Test2** to the **Ctest2** folder. Release the right mouse button and click **Copy Here**. Click the **Ctest2** folder. Notice that Test2 is not compressed because copied files inherit the compression attribute from their parent folders, and moved files retain their compression attribute (unless moved to a different volume).



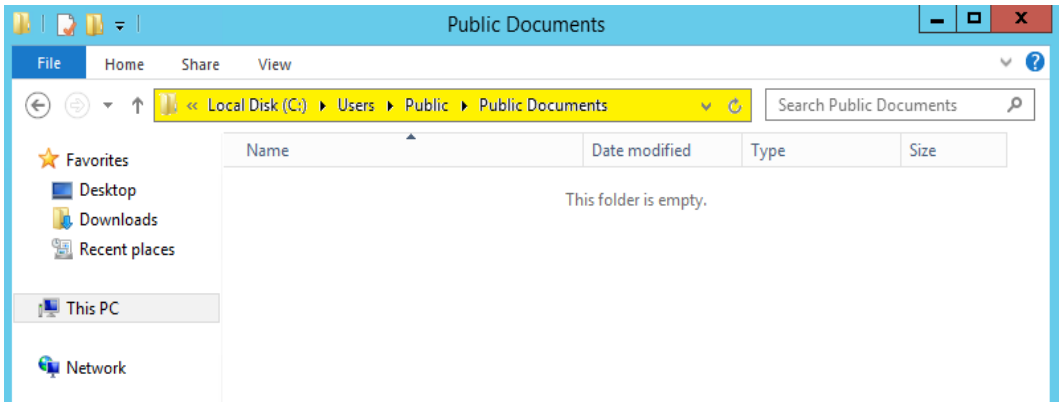
11. Take a screenshot showing the Test2 text file is no longer compressed (PrtScr#2).
12. Close all open windows but remain logged on for the next activity.

Part 4

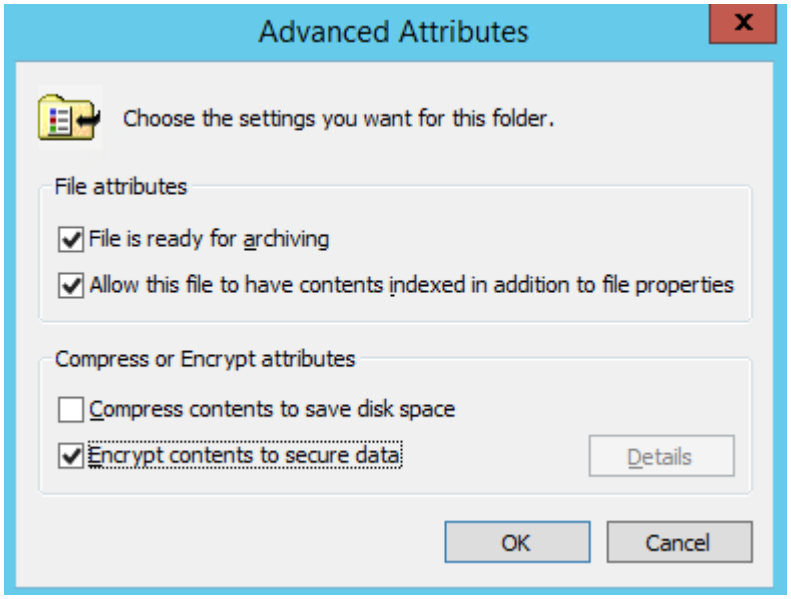
Purpose of Activity: In this activity, you will use the GUI to enable and configure File Encryption on the Windows Client operating system.

1. Log on to your **Win10-XX VM as *Sguthridge.***

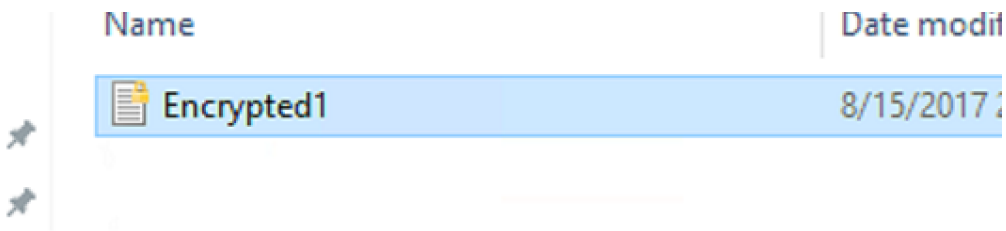
2. Right-click **Start**, click **File** Explorer, click **This PC, Local Disk (C:), Users, Public, Public Documents** to open the Public Documents folder.



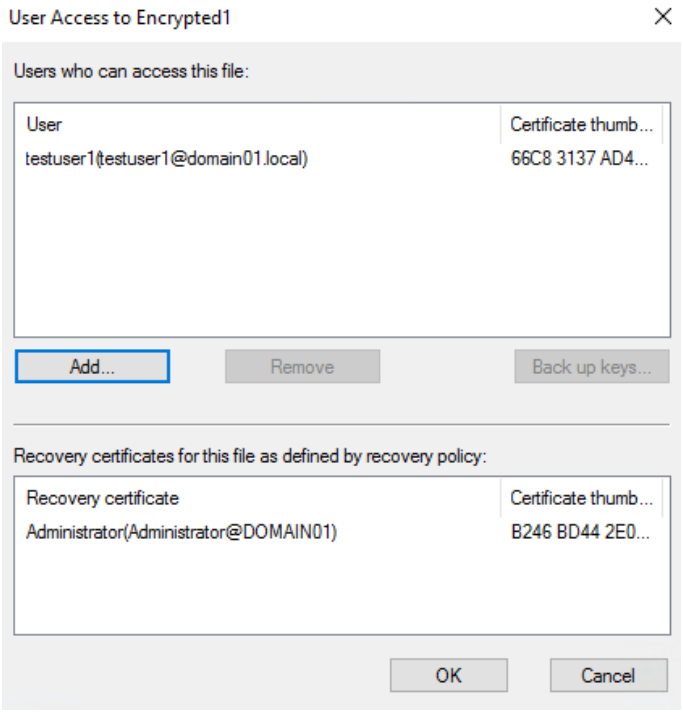
3. Create a text file in the **Public Documents** folder, and name it **Encrypted1**.
4. Right-click **Encrypted1** and select **Properties**.
5. Click the **Advanced** button to open the Advanced Attributes dialog box for Encrypted1, click the **Encrypt contents to secure data** check box, and then click **OK** twice.



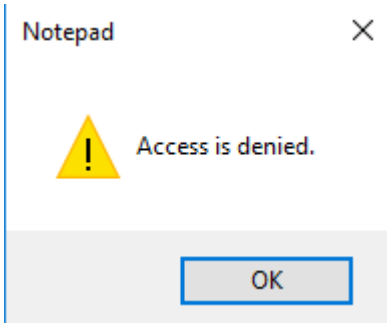
6. When you get the Encryption Warning message, click the **Encrypt the file only** option button and **Always encrypt only the file** check box, and then click **OK**. Notice the file icon has a yellow lock in the right corner indicating the file is encrypted.



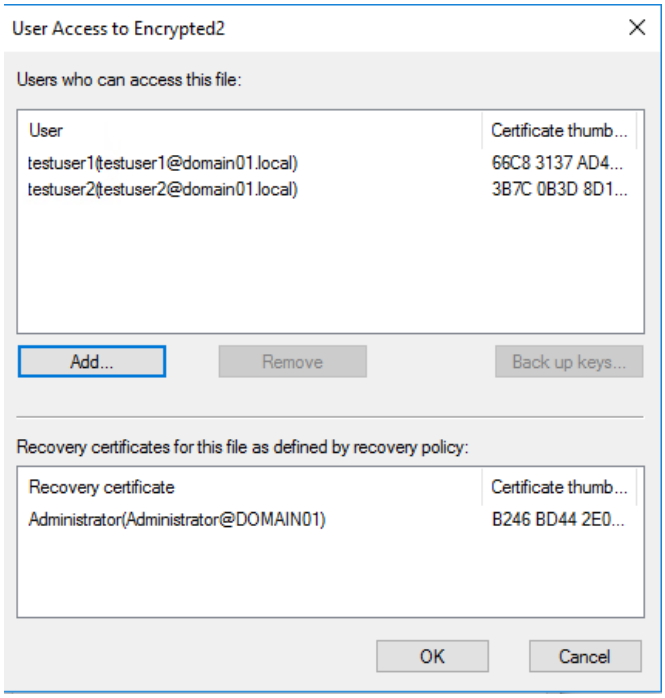
7. Double-click **Encrypted1** and open the file in Notepad and type your name in it. Save the file, and exit Notepad.
8. Right-click **Encrypted1** and select **Properties**.
9. Click the **Advanced** button to open the Advanced Attributes dialog box for Encrypted1, and click the **Details** button. Notice that Sguthridge is listed as a user who can access the file, and Administrator is listed as a recovery agent. Click **Cancel** and then click **OK** twice.



10. Log off and log on as **Clong**. Hint: Select **Other user.** Navigate to the **Public Documents** folder as you did in Step 3. Double-click **Encrypted1** to open it. You get an Access Denied message. Click **OK**, and then exit Notepad.

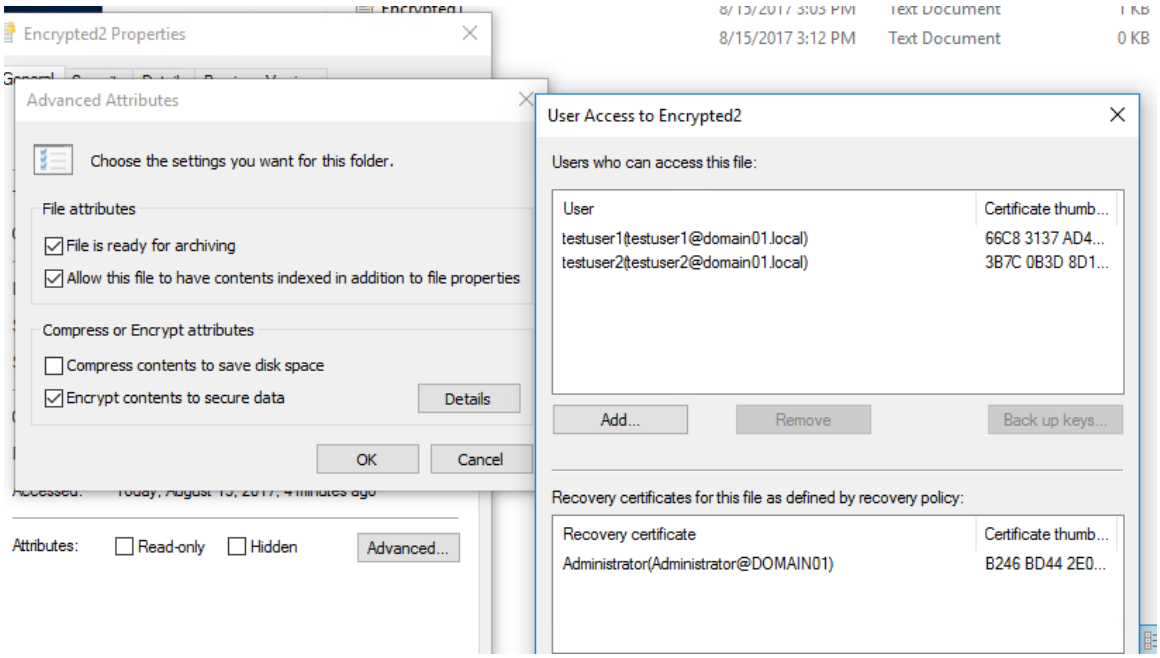


11. Create a text file named **Encrypted2**. Set the encryption attribute on the file as you did in Step 6, and then click **OK** until all Properties dialog boxes are closed. Open the **Advanced Attributes** dialog box for **Encrypted2**. Click **Details**, and then click **Add**. Note that Sguthridge, and Clong are listed. Click **Sguthridge**, and then click **OK**. Click **OK** three more times.



12. Logoff and log on again as **Sguthridge**. Click to open the **Public Documents** folder. Verify that you can open **Encrypted2** without error, and then close the file.

13. Copy **Encrypted2** to the **desktop**. Verify that the new file remains encrypted by opening the **Advanced Attributes** dialog box.



14. Take a screenshot showing who has access to the Encrypted2 file (PrtScr#3).
15. Close all open windows and sign out of the Windows 10 client computer.

Reflection

1. What happens to the Test1 text document if you copy it to the C drive on your Window 10 client computer?

2. What is the purpose of the lab?

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 restored RAID-5 text file (PrtScr#1) (20 points)	
	Criteria #2:Take a screenshot showing the Test2 text file is no longer compressed (PrtScr#2) (30 points)	

	Criteria #3: Take a screenshot showing who has access to the Encrypted2 file (PrtScr#3) (30 points)	
	Criteria #4: Answer the Reflection questions in a text file (20 points)	