Practical 4B – Advanced File System Management

Lab Requirements:

a) Ensure that the ***NYP-DC1*** and ***NYP-CL1*** virtual machines are running.
b) On the server NYP-DC1, set up another volume labeled as E: drive on another virtual disk, if not already done so. The disk size can be 10GB.
c) To allow a non-admin account (eg. user1-finance) to log in to NYP-DC1, add it as a member to Backup Operators group.

Practice 1

Objectives:

1. Use File Explorer to view and configure file and folder attributes.

Tasks:

1. Log on NYP-DC1 using your Administrator account. Open **File Explorer**.
2. Open drive **C**: to view its contents.
3. Click the **View** menu, and then click **Details**. This view displays the Name, Size, Type, Date Modified, and Attributes associated with files and folders. If the Attribute column is not displayed, click on **View → Add Columns** and select **Attribute** column. Review the letters listed in the Attribute column for the files and folders displayed. Each letter listed represents configured attributes for that folder. For example, the letters RHSA would designate a file or folder that has its read-only (R), hidden (H), system (S), and archive (A) attributes configured.
4. Go to **C:\Users** folder and view its contents. Make note of the folders that are visible in the C:\Users folder by default.
5. Click **View → Options → Change folder and search options**. The **Folder Options** window opens.
6. Click the **View** tab.
7. Click on **Show hidden files, folders, and drives.**
8. **Un-check** below settings:
   - Hide extensions for known file types.
   - Hide protected operating system files (Recommended). When the Warning dialog box appears, read the message it displays, and click **Yes**. Click **OK**
9. Click on Local **Disk (C:).** Note that there are hidden files or folders appearing in this list as a result of showing hidden files. Review the additional files and folders now displayed in the File Explorer interface, noting that each of the new files and folders now visible has its system and hidden attributes configured.
10. Right-click on the **bootmgr** file, and click **Properties**. On the **General** tab, notice that the Read-only check box is checked and can be changed, but that

the hidden attribute is unchecked and cannot be changed. The fact that the Hidden check box is not configurable is a function of the fact that this file also has its System attribute configured. Click **Cancel**.

11. Open drive **E:** to view its contents.
12. Click the **File** menu, select **New**, and then click **Text Document**. Name the new file **attribute-test**.
13. After creating the file, notice that it is automatically assigned the archive attribute by default.
14. Right-click on the **attribute-test** file and click **Properties**.
15. On the **General** tab, check both the Read-only and Hidden check boxes, and click **OK**.
16. Notice that the Attribute column now displays RHA, because the read-only, hidden, and archive attributes are configured for the file. Close all open windows.

Practice 2

Objectives:

1. View and change file attributes from the command line.

Tasks:

1. Right-click **Start**, and then click **Command Prompt** (Admin).
2. At the command line, type ***E:*** and press Enter.
3. Type ***mkdir attributes*** and press Enter to create a new directory called attributes. Leave the command prompt window open.
4. Open **File Explorer** and go to drive **E:** to view its contents, and then double-click on the **attributes** folder to open it. Create three new text files in the folder named **file1.txt, file2.txt**, and **file3.txt**. Once complete, close the File Explorer window.
5. In the command prompt window, type ***cd attributes*** and press Enter.
6. Type ***attrib file1.txt*** and press Enter. Notice that the output of the command displays the letter A (meaning the archive attribute is set) and the path to the file.
7. Type ***attrib –A file1.txt*** and press Enter. This removes the archive attribute from file1.txt.
8. Type ***attrib file1.txt*** and press Enter. Notice that the output no longer displays any attributes for file1.txt.
9. Type ***attrib +A +H +R +S file1.txt*** and press Enter. This command adds the archive, hidden, read-only, and system attributes to file1.txt. Close the command prompt window.
10. Open **File Explorer** and go to drive **E:** to view its contents, and then double-click on the attributes folder to open it. Notice that all three files are visible in the Window Explorer interface, along with their associated attributes. Notice also that file1.txt uses a transparent icon, since its hidden attribute is set.

11. Click **View → Options → Change folder and search options**, and check the **Hide protected operating system files** (Recommended) check box, and click **OK**.
12. Notice that **file1.txt** no longer appears in the list of files in File Explorer. This is because file1.txt has both the system and hidden attributes set, and as such is hidden from display because it is treated like a protected operating system file as configured in Step 11.
13. Close the My Computer window.

Practice 3

Objectives:

1. Configure a folder to compress its contents.

Tasks:

1. Open **File Explorer** and go to drive **E:**. Create a new folder called **Compress**. Go to **C:\Windows** folder and find any .**bmp** file. Copy the .bmp file to the **Compress** folder. (eg. BGInfo.bmp)
2. Right-click the **Compress** folder and click **Properties**. Note both the Size and Size on disk information provided on the **General** tab.
3. Click the **Advanced** button to open the Advanced Attributes dialog box.
4. In the Compress or Encrypt attributes section, click the **Compress contents to save disk space** check box and then click **OK**.
5. Click **OK** to exit the properties of the Compress folder.
6. When the Confirm Attribute Changes dialog box opens, ensure that the **Apply changes to this folder, subfolders and files** radio button is selected and then click **OK**.
7. In the File Explorer, notice that the **Compress** folder is now listed in blue text, which designates it as having its compression attribute set.
8. Open the **Compress** folder, right-click on the .**bmp** file, and click **Properties**. Notice that while the Size value has not changed, the Size on disk value is now significantly reduced from its original value.
9. Close all open windows.

Practice 4

Objectives:

1. Implement and test file encryption security using EFS.

Tasks:

1. On NYP-DC1, log on using **user1-finance** account.

2. Open **File Explorer** and create a new folder on drive **E**: named **Encrypted**.
3. Right-click the **Encrypted** folder and click **Properties**.
4. On the **General** tab, click the **Advanced** button to open the folder's advanced attributes settings.
5. Check the **Compress** contents to save disk space check box, and then check the **Encrypt contents to secure data** check box. Notice that only one of these two options can be selected at any time. Select the **encryption mode**.
6. Click **OK** to exit the Advanced Attributes window, and then click **OK** again to exit the properties of the Encrypted folder. After encryption is successful, continue with the steps below.
7. Open the Encrypted folder and create a new text file within it called **encrypted.txt.** In the encrypted.txt file, type **this is an encrypted file**, then save your changes and close the file. Notice the file has a extra **lock icon** to indicate it as encrypted. Access the **Advanced** Attributes of this file to ensure that the Encrypt contents to secure data check box is checked. Close the Advanced Attributes dialog box and the Properties dialog box.
8. Close all open windows and then log off. Log on as the **user1-it** (user1-it must be a member of the Backup Operators) with the password Pa$$w0rd.
9. Open File Explorer and attempt to open the **E:\Encrytped folder**.
10. Attempt to open the **encrypted.txt** file by double-clicking on it. Notice that access is denied because User1 IT does not have the private key necessary to decrypt the file. Close all open windows.
11. Log off and then log on again as **Administrator** with the password Pa$$w0rd.
12. Open the **E:\Encrypted** folder and attempt to open the file encrypted.txt. Notice that the file opens because the domain Administrator account is the default recovery agent. Close all open windows.
13. Log off and then log on again using your Administrator account.

Practice 5

Objectives:

1. Encrypt files using the CIPHER utility.

Tasks:

1. Login to NYP-DC1 as Administrator.
2. Open **File Explorer** and double-click on drive **E**: to view its contents.
3. Click the **File** menu, select **New**, and the click **Folder**. Name the new folder **ciphertest** and open it.
4. Create 3 text files called - **file1.txt, file2.txt** and **file3.txt**. Close the Explorer window.
5. Open a Command Prompt (Admin).
6. Type **E:** and press Enter.
7. Type **cd ciphertest**, and press **Enter**.

8. Type **cipher** and press Enter. All files in the ciphertest folder should currently be listed as unencrypted, as designated by the letter **U** that precedes their file names.
9. Type **cipher /e /a file1.txt** and press Enter. This action encrypts file1.txt only.
10. Type **cipher** and press Enter. Notice that file1.txt is now preceded with the letter **E**, meaning the file is encrypted.
11. Type **cipher /e /a *.txt** and press Enter. This command encrypts all currently unencrypted text files in the ciphertest folder.
12. Type **cipher** and press Enter to confirm that all files in the folder are currently encrypted.
13. Close the command prompt window.

Practice 6

Objectives:

1. Enable and manage disk quotas settings.

Tasks:

1. Log into NYP-DC1 as Administrator.
2. Open **File Explorer** and right-click drive **E:** and then click **Properties**.
3. Click the **Quota** tab. Notice that the status notice and icon both point out disk quotas are currently disabled for the partition.
4. Click the **Enable quota management** check box.
5. Click the **Limit disk space to** radio button, then type **100** in the text box and select **MB** in the drop-down box.
6. In the **Set warning level to** text boxes, type **80** and select **MB.**
7. Check the **Log event when a user exceeds their quota limit** check box.
8. Check the **Log event when a user exceeds their warning level** check box.
9. Review all of the choices selected. Notice that although quota information is tracked for this volume, the option to Deny disk space to users exceeding quota limit was not selected. As such, these quotas settings would be considered "**soft**" because they do not actually deny disk space to users and would instead be used for monitoring purposes. Click **OK**.
10. When the Disk Quota dialog box opens, read the message and then click **OK**. Allow a few minutes for the disk to be rescanned and quota information gathered if necessary.
11. Open the **Properties** of drive **E**: and click the **Quota** tab. Notice that the Disk quota system is now active and that the quota icon has changed.
12. Click the **Quota Entries** button.
13. In the Quota Entries dialog box, double-click the entry that appears for the **Administrator** user account to view its properties. Note the quota used and quota remaining information provided.
14. Change the quota entry for Administrator such that the quota limit and warning level are both set to **1KB**. Click **OK**. Notice that the icon next to the

quota entry changes to warning because this user is now over their quota limit.

15. Close all open Windows.

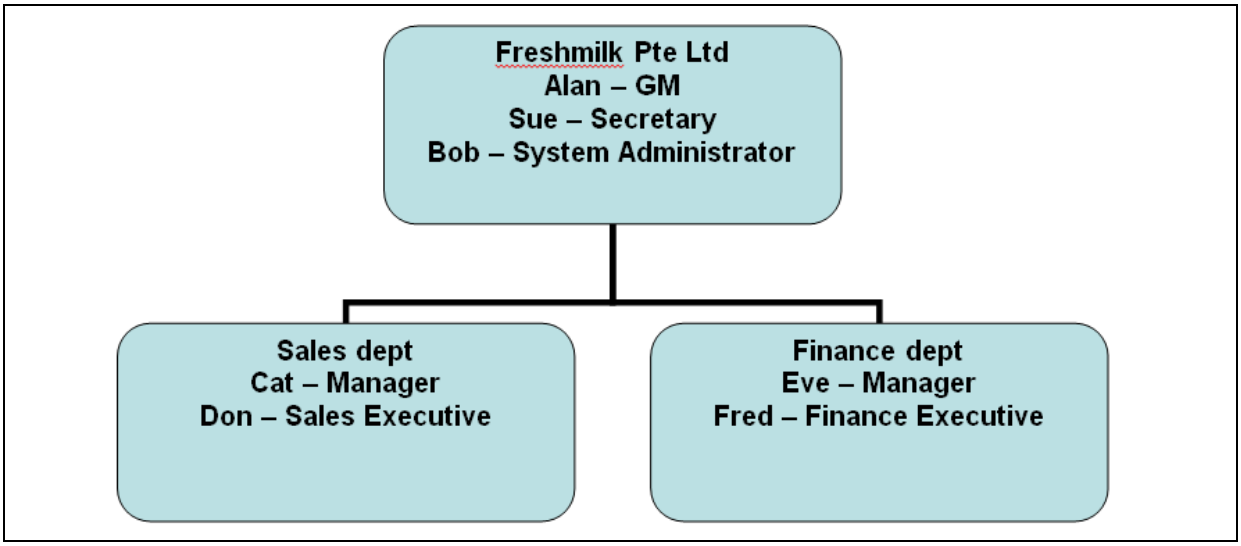
(Note: check if only new accounts are affected by the quota setting)

Exercise 4B

In Freshmilk Pte Ltd, one physical hard disk of 20 GB is to be shared equally between Sales Dept and Finance Dept (ie. each dept has about 10 GB). Implement the following disk quota for the 2 departments:

- Sales dept – all users: limit to 2 GB, warning set at 1 GB
- Finance dept – all users: limit to 1 GB, warning set at 500 MB
- Prevent users from exceeding the limit.

Only users from respective dept can access the disk (ie. only sales staff can use the disk assigned to sales dept. No other users should be able to access it).
Configure the disk and disk quota and test it out.
Can disk quota be implemented thru a Group Policy?



[THE END]