Microsoft®
Training &
Certification

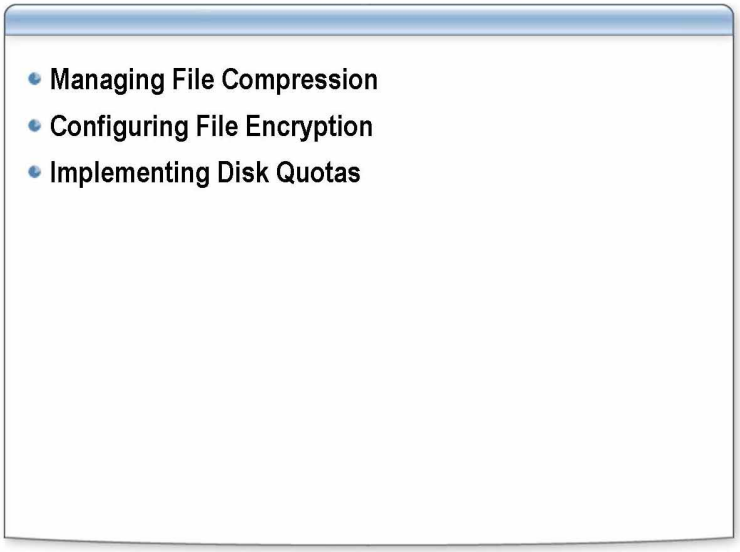
Microsoft Official
Curriculum

Module 6: Managing Data Storage

Contents

Microsoft®

Overview



Introduction

One of your tasks as a systems administrator is to manage the data that you will store on your network storage devices. To manage your data storage, you can compress files and folders to decrease their size and reduce the amount of space that they use on your drives or removable storage devices. In this module, you will learn when and how to compress files and folders.

To manage data, you must also understand encryption. In this module, you will learn about Encrypting File System (EFS), which stores data securely and protects your network.

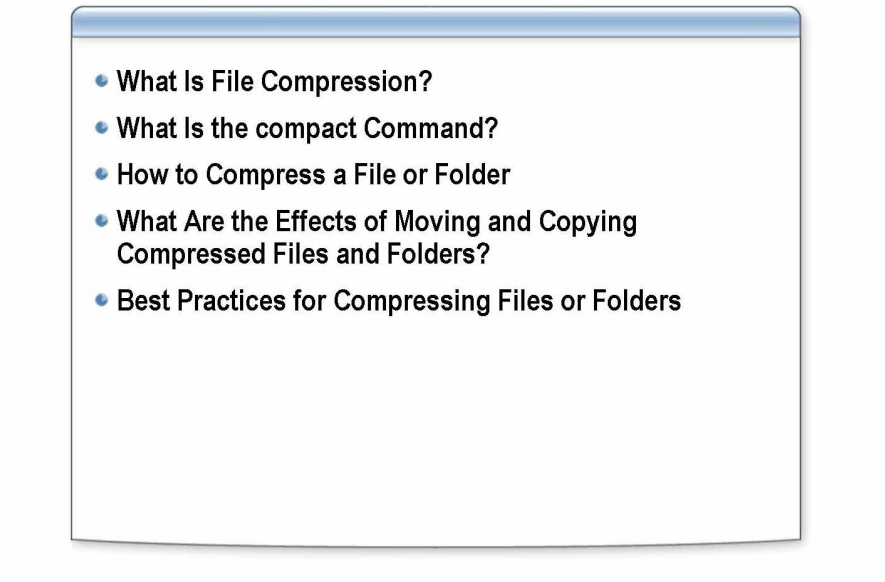
You will also learn how to administer disk quotas. You use disk quotas to limit the amount of storage space that is available to users.

Objectives

After completing this module, you will be able to:

- Manage NTFS file compression.
- Configure file encryption.
- Implement disk quotas.

Lesson: Managing File Compression



Introduction

Compressing files and folders decreases their size and reduces the amount of space they use on your drives and removable storage devices. Microsoft® Windows® Server 2003 supports two types of compression: NTFS compression and compression using the Compressed (zipped) Folders feature.

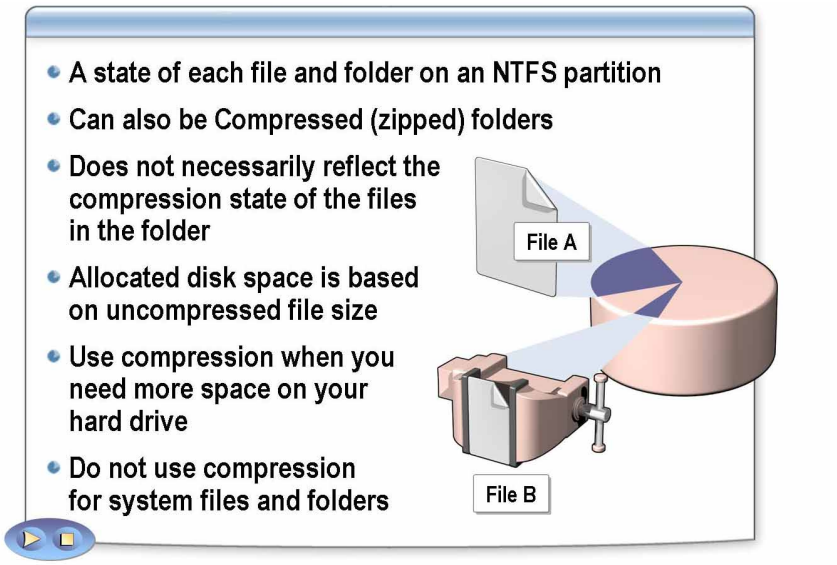
In this lesson, you will learn about these features and how to use them. You will also learn the best practices that are associated with compressing files and folders.

Lesson objectives

After completing this lesson, you will be able to:

- Describe file compression.
- Describe the **compact** command-line tool.
- Compress a file or folder on an NTFS partition.
- Explain the effects of moving and copying compressed files and folders.
- Describe the best practices for compressing files and folders.

What Is File Compression?



Introduction

Windows supports two types of compression: NTFS file compression and Compressed (zipped) Folders. You use Windows Explorer for both types.

Uses of compression

Use compression when you need more space on your hard disk drive. Compressing files, folders, and programs decreases their size and reduces the amount of space they use on drives or removable storage devices. You can also compress disk drives.

Files that can be compressed the most are text files, bitmap files, spreadsheets, and presentation files. Files that can be compressed the least are compressed graphics files and video files. Avoid compressing system folders and files because this affects the performance of the server.

NTFS file compression

Volumes, folders, and files on an NTFS volume are either compressed or uncompressed. The compression state of a folder does not necessarily reflect the compression state of the files in that folder. For example, you can selectively uncompress some or all of the files in a compressed folder.

When an application or an operating system command requests access to a compressed file, Windows Server 2003 automatically uncompresses the file. When you close or save a file, Windows Server 2003 compresses it again.

Space allocation

NTFS allocates disk space based on the size of the uncompressed file. If you copy a compressed file to an NTFS partition that does not have enough space for the uncompressed file, an error message notifies you that there is not enough disk space for the file.

Compressed (zipped) Folders

Files and folders that are compressed using the Compressed (zipped) Folders feature can be compressed on FAT, FAT32, and NTFS drives. A zipper icon identifies files and folders that are compressed by using this feature.

You can open files directly from these compressed folders, and you can run some programs directly from these compressed folders without uncompressing them. You can also move these compressed files and folders to any drive or folder on your computer, the Internet, or your network, and they are compatible with other file compression programs and files.

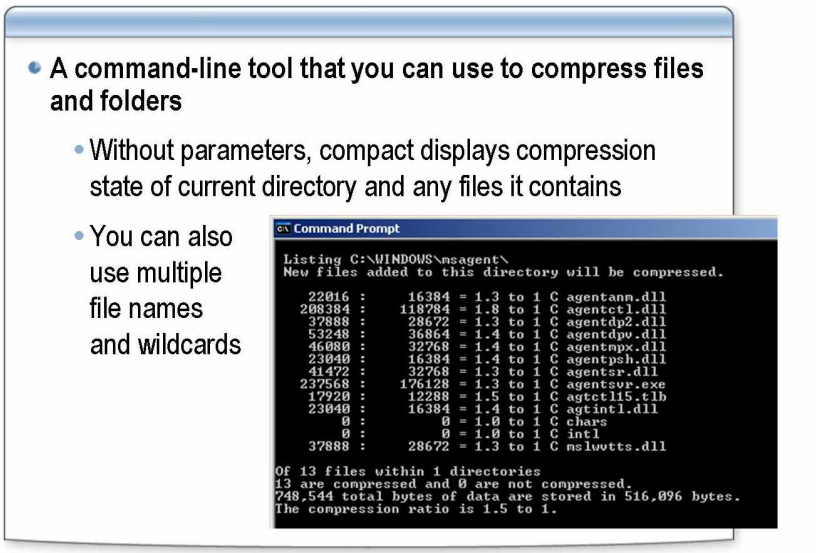
Compressing folders by using Compressed (zipped) Folders does not affect the overall performance of your computer. Performance is affected only when Compressed (zipped) Folders is accessed to compress a file.

Comparison of compression methods

The two compression methods are compared in the following table.

Attribute	NTFS file compression	Compressed (zipped) Folders
File system	NTFS	NTFS or FAT, FAT32
Compressible objects	Files, folders, and drives	Files and folders
Performance	Decrease	No decrease
Password protection	No	Yes
Encrypt	No	Yes
Change display color	Yes	No

What Is the compact Command?



Introduction

In addition to using Windows Explorer to compress files and folders, you can use the **compact** command-line tool.

Displays compression state of directory

When used without parameters, **compact** displays the compression state of the current directory and any files that it contains. For example, you can use the following command line to compress all files and folders in the IIS directory:

compact /c c:*IIS**.***

Example using multiple parameters

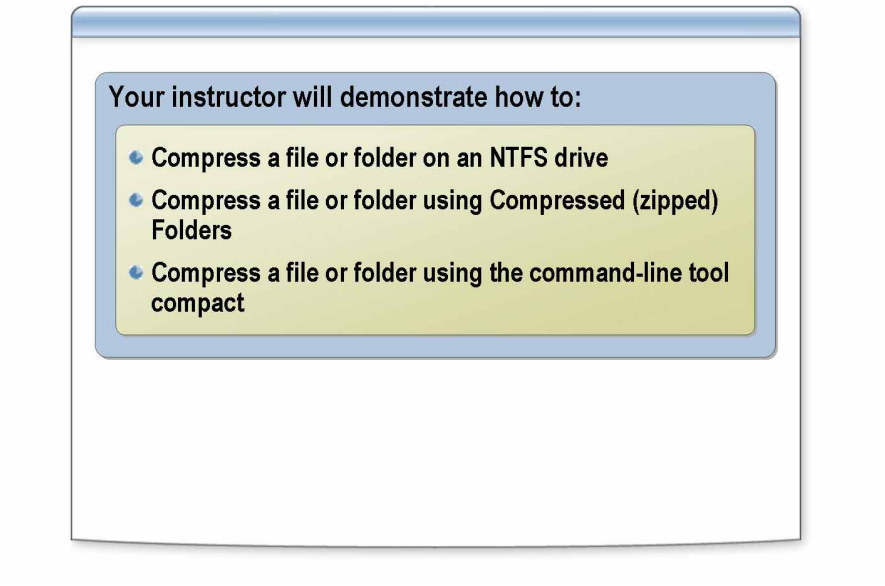
You can use multiple file names and wildcards with **compact**. You must, however, put spaces between multiple parameters, as shown in the following example:

compact /C | **/U**] [**/S**[:*dir*]] [**/A**] [**/I**] [**/F**] [**/Q**] [*filename* [...]

Each parameter is listed and described in the following table.

Parameter	Description
/C	Compresses the specified files. Directories are marked so that files added afterward are compressed.
/U	Uncompresses the specified files. Directories are marked so that files added afterward are not compressed.
/S	Performs the specified operation on files in the specified directory and all subdirectories. Default value is the current directory.
/A	Displays files with the hidden or system attributes. These files are omitted by default.
/I	Continues performing the specified operation even after errors occur. By default, **compact** stops when an error is encountered.
/F	Forces the compress operation on all specified files, even those that are already compressed. Already-compressed files are skipped by default.
/Q	Reports only the most essential information about the specified pattern, file, or directory. Specifies a pattern, file, or directory.

How to Compress a File or Folder



Introduction

You can use Windows Explorer to compress files and folders by using NTFS file compression or Compressed (zipped) Folders. You can also compress files and folders by using the **compact** command.

Procedure for using NTFS file compression

To use NTFS file compression to compress files or folders on an NTFS drive:

1. In Windows Explorer, right-click the file or folder that you want to compress, and then click **Properties**.
2. In the **Properties** dialog box, on the **General** tab, click **Advanced**, select the **Compress contents to save disk space** check box, and then click **OK**.
3. In the **Properties** dialog box, click **OK**.
4. In the **Confirm Attribute Change** dialog box, click **OK**.

Procedure for using Compressed (zipped) Folders

To compress files or folders by using Compressed (zipped) Folders:

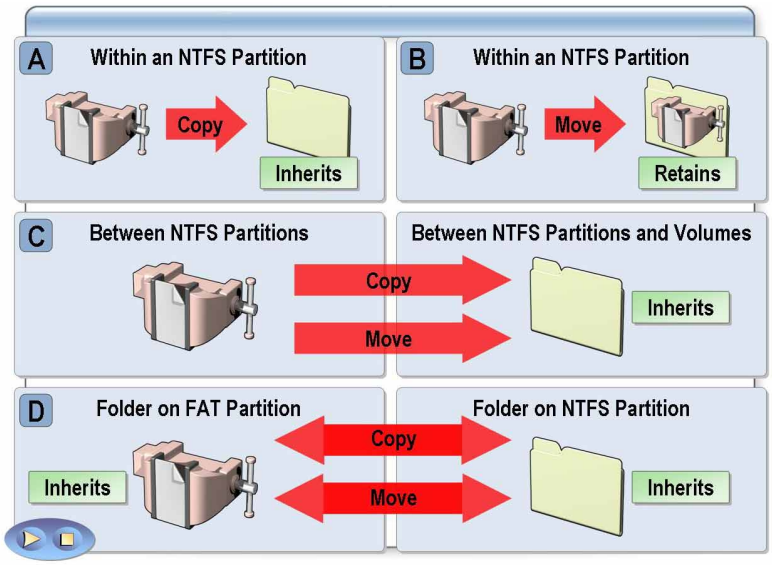
1. In Windows Explorer, in the details pane, right-click any open area, click **New**, and then click **Compressed (zipped) Folder**.
2. Move or copy files to the new folder to compress them.

Procedure for using compact

To compress files, folders, or directories using the **compact** command:

1. Open a command prompt.
2. Type **compact** */c c:***MOC***.* and then press ENTER.

What Are the Effects of Moving and Copying Compressed Files and Folders?



Introduction

Moving and copying files and folders on disk volumes can change their compression state, depending on the compression state of these files and folders and on the file system in which they were created. The compression state of a file or folder created in an NTFS partition is controlled by its compression attribute.

Copy within an NTFS partition

As shown in section A of the illustration, when you copy a file or folder within an NTFS partition, the file or folder inherits the compression state of the target folder. For example, if you copy a compressed file or folder to an uncompressed folder, the file or folder is automatically uncompressed.

Move within an NTFS partition

As shown in section B, when you move a file or folder within an NTFS partition, the file or folder retains its original compression state. For example, if you move a compressed file or folder to an uncompressed folder, the file remains compressed.

Copy between NTFS partitions

As shown in section C, when you copy a file or folder between NTFS partitions, the file or folder inherits the compression state of the target folder.

Section C illustrates copying a file or a folder to a folder. The file or folder takes on the compression attribute of the target folder. For example, if you copy a compressed file to an uncompressed folder, the file is uncompressed when it is copied to the folder.

Move between NTFS partitions

As shown also in section C, when you move a file or folder between NTFS partitions, the file or folder inherits the compression state of the target folder. Because Windows Server 2003 treats a move between partitions as a copy and then a delete operation, the files inherit the compression state of the target folder.

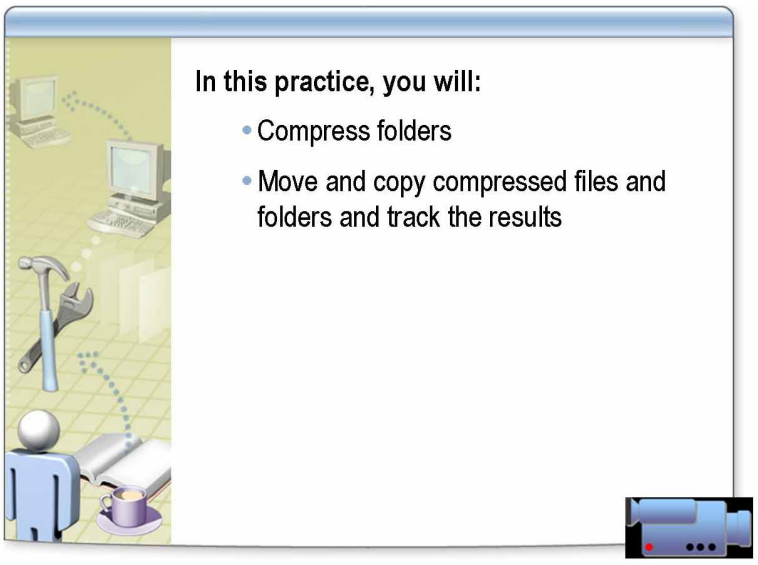
Copying files or folders on NTFS volumes

When you copy a file to a folder that already contains a file of the same name, the copied file takes on the compression attribute of the target file, regardless of the compression state of the folder.

Moving and copying files between FAT16, FAT32, and NTFS volumes

Similar to files that are copied between folders on an NTFS volume, section D shows that files that are moved or copied from a folder on a FAT volume to a folder on an NTFS volume inherit the compression attribute of the target folder. Because compression is supported only on NTFS volumes, compressed files that are moved or copied from an NTFS volume to a FAT volume are automatically uncompressed. Similarly, compressed files that are copied or moved from an NTFS volume to a floppy disk are automatically uncompressed.

Practice: Managing File Compression



Objective

In this practice, you will:

- Compress folders.
- Move and copy compressed files and folders, and track the results.
- Identify the effects of moving and copying compressed files and folders.

Scenario

You are the systems administrator for an organizational unit on a large network. The accounting department manager complains to you about the amount of free disk space left on his server's hard disk drive. He wants at least 20 percent more free space without having to move any of the files to tape.

The folder structure of his drive is primarily made up of tax returns from 1997 to 1999. You need to compress the \data\taxes\199*x* folders to create additional free space.

Practice: Compressing the files

► **Compress the files**

1. Log on to the domain as *Computer***User** with a password of **P@ssw0rd**.
2. Open Windows Explorer.
3. Browse to **C:\MOC\2275\Practices\Mod06\Data\Taxes**.
4. Open the **Properties** dialog box for **Taxes**.
5. Note the Size on disk parameter: _____
6. Click **Advanced**.

7. Select the **Compress contents to save disk space** check box, and then click **OK**.
8. In the **Taxes Properties** dialog box, click **Apply**, and then confirm that you want the changes to be made to this folder and all subfolders and files.
9. How much room did you gain by compressing the tax folders? _____%.
10. Click **OK**, and then close all windows.

Practice: Moving compressed files and folders (Exercise 1)

► **Move the files**

1. On the Student Materials compact disc, under **Multimedia**, open *Managing NTFS File Compression and Encryption*, and then select **Compression Move**.
2. Move the files and folders to various locations on the page, and record the results in the following table.

   The drives in the exercise represent NTFS-formatted drives on the same computer.

Move to:	On same drive		On different drive	
	Compressed folder	Uncompressed folder	Compressed folder	Uncompressed folder
Compressed file				
Compressed folder				
Uncompressed file				
Uncompressed folder				
Use C to indicate compression and U to indicate no compression.				

Practice: Copying compressed files and folders (Exercise 2)

► **Copy the files**

1. On the Student Materials compact disc, under **Multimedia**, open *Managing NTFS File Compression and Encryption*, and then select **Compression Copy**.
2. Copy the files and folders to various locations on the page, and record the results in the table below.

   The drives in the exercise represent NTFS-formatted drives on the same computer.

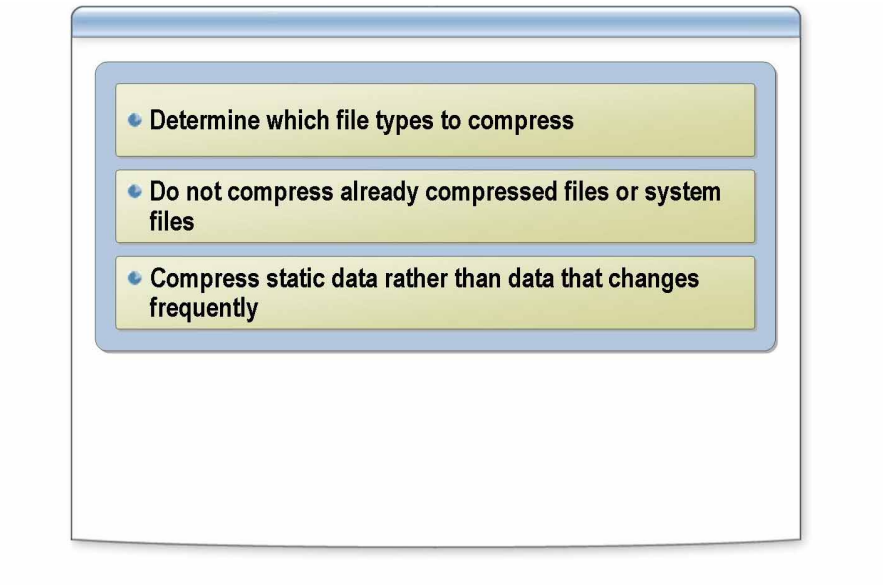
Copy to:	On same drive		On different drive	
	Compressed folder	**Uncompressed folder**	**Compressed folder**	**Uncompressed folder**
Compressed file				
Compressed folder				
Uncompressed file				
Uncompressed folder				

Use C to indicate compression and U to indicate no compression.

Challenge

When you use the **Compression Move**, can you compress all of the files and folders by using the Move operation? Can you uncompress all of the files and folders by using the Move operation?

Best Practices for Compressing Files or Folders



Introduction

Consider the following best practices for managing compression on NTFS partitions.

Determine which file types to compress

Because some file types can be compressed more than others, determine which file types to compress based on the anticipated size of the compressed file. For example, because Windows bitmap files contain more redundant data than application executable files, this file type can be compressed more than an .exe file. Bitmaps can often be compressed to less than 50 percent of the original file size, whereas an application file can rarely be compressed to less than 75 percent of the original size.

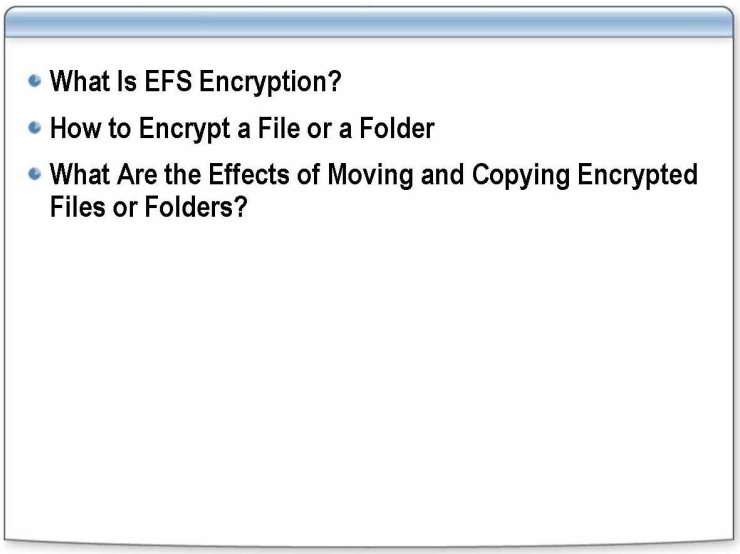
Do not compress already compressed file

Do not compress already compressed files or system files. Windows Server 2003 attempts to compress the file even more, which wastes system time and yields no additional disk space.

Compress static data

Compress static data rather than data that changes frequently. Compressing and uncompressing files incurs some system overhead. By choosing to compress files that are accessed infrequently, you minimize the amount of system time that is dedicated to compression and uncompression activities.

Lesson: Configuring File Encryption



Introduction

An intruder who has physical access to a computer can easily install a new operating system and bypass the security of the existing operating system. Thus, sensitive data is left exposed. You can add an effective layer of security by encrypting these files with Encrypting File System (EFS). When the files are encrypted, the data is protected even if an intruder has full access to the computer's data storage.

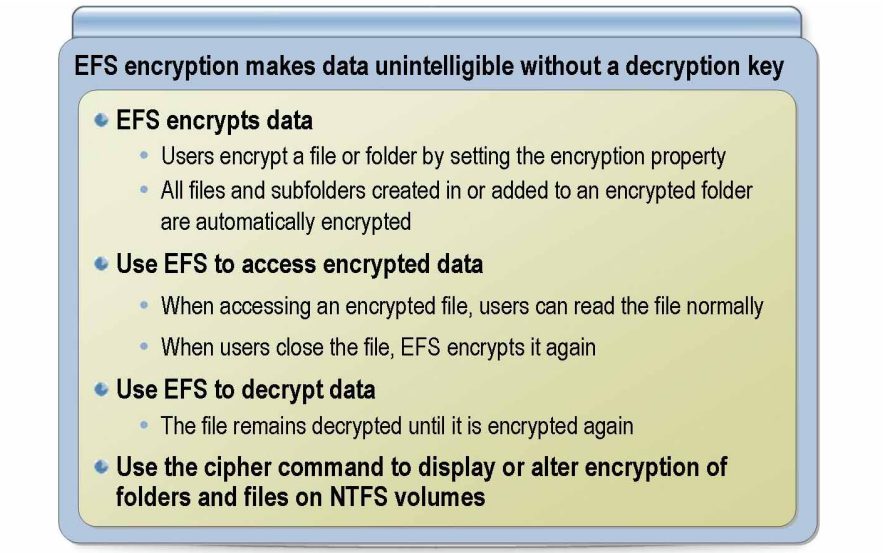
In this lesson, you will learn about encryption, as well as how to manage encryption. You will also learn the effects of moving and copying encrypted files.

Lesson objectives

After completing this lesson, you will be able to:

- Describe EFS file encryption.
- Encrypt a file or a folder.
- Describe the effects of moving and copying encrypted files or folders.

What Is EFS Encryption?



Introduction

An attacker can gain access to a shared system by starting a different operating system. An attacker can also steal a computer, remove the hard disk, install the disk in another system, and gain access to the stored files. Files that are encrypted by using Encrypting File System (EFS), however, appear as unintelligible characters when the attacker does not have the decryption key.

EFS provides file level encryption

EFS provides file-level encryption for files created on NTFS volumes. By using EFS, you can ensure that sensitive or confidential data is more secure and cannot be easily read or decrypted by another user.

Use EFS to encrypt data

Encryption and decryption are the primary tasks of EFS. The default configuration of EFS requires no administrative effort—users can begin encrypting files immediately. EFS automatically generates an encryption key pair for a user if one does not exist.

Encryption and decryption options available

Several encryption and decryption options are available to users. Users can encrypt and decrypt files by using Windows Explorer, by using the **cipher** command, or by using the shortcut menu accessed by right-clicking a file or folder.

Encrypted folder contents

Folders that are marked for encryption are not actually encrypted. Only the files in the folder are encrypted, as well as any new files that are created in or moved to the folder.

Use EFS to access encrypted data

Using EFS, users access encrypted files just as they do unencrypted files. Thus, when a user accesses an encrypted file that is stored on disk, the user can read the contents of the file in the normal way. When the user saves the file on disk again, EFS saves the changes as encrypted.

Use EFS to decrypt data

You can decrypt a file by clearing the **Encryption** check box in the **Properties** dialog box for the file. After it is decrypted, the file remains decrypted until you encrypt it again. There is no automatic re-encryption of a file, even if it exists in a directory marked as encrypted.

Users can decrypt a file either by clearing the **Encryption** check box in the **Properties** dialog box for the file, or by using the **cipher** command.

Display or alter encryption on NTFS volumes with cipher

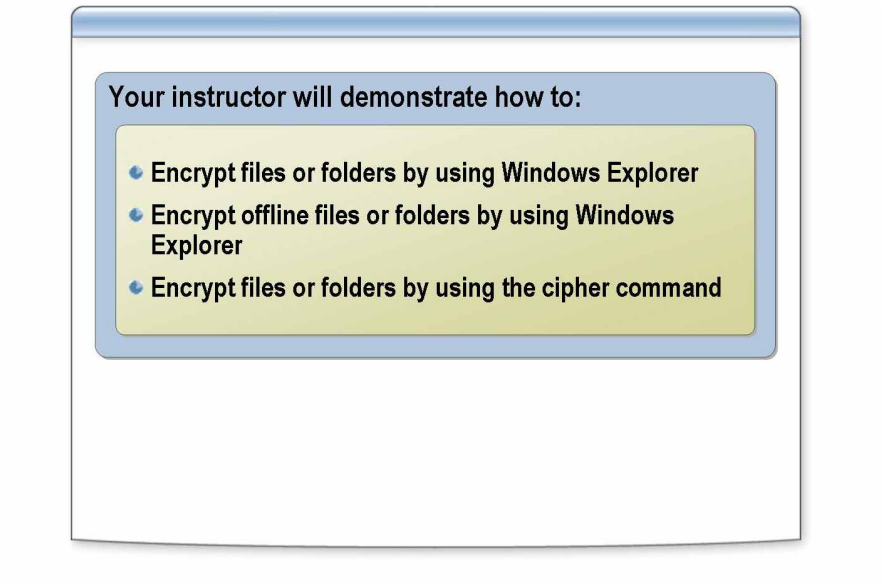
Use the **cipher** command to display or alter the encryption of folders and files on NTFS volumes. Used without parameters, **cipher** displays the encryption state of the current folder and any files it contains.

Parameters of cipher

You can use the **cipher** command with the parameters in the following table to perform the listed tasks.

Parameters	Task description
Use **cipher** with no parameters or with the name of a specific file or folder.	Display the encryption status of files and folders
/e	Set the encryption attribute for folders in the current directory
/e /a	Encrypt files in the current directory
/d	Remove the encryption attribute from folders in the current directory
/d /a	Decrypt files in the current directory
/?	Display all of the options that are available with **cipher**

How to Encrypt a File or Folder



Introduction

Use EFS to encrypt files that must be protected, especially those files that will be shared across the network or over the Internet. Encrypting an offline file helps to ensure that you can protect all of the files on your network.

Procedure for encrypting a file

To encrypt a file or folder by using Windows Explorer:

1. In Windows Explorer, right-click the file or folder you want to encrypt, and then click **Properties**.
2. In the **Properties** dialog box, on the **General** tab, click **Advanced**.
3. In the **Advanced Attributes** dialog box, select the **Encrypt contents to secure data** check box.
4. The encrypted file text within the folder changes color, denoting the encrypted state of the file.

Procedure for encrypting an offline file or folder

Note Remote Desktop must be disabled for the following procedure to work.

To encrypt an offline file or folder by using Windows Explorer:

1. In Windows Explorer, on the **Tools** menu, click **Folder Options**.
2. On the **Offline Files** tab, select the **Encrypt offline files to secure data** check box.

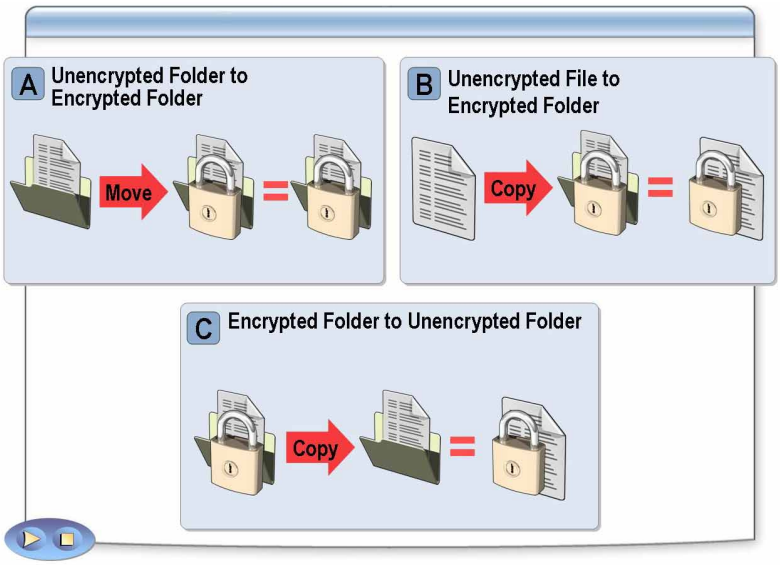
Procedure for encrypting a file using cipher

To encrypt a file by using **cipher**:

1. Open a command prompt.
2. Type the following command to encrypt a *filename* folder, its subdirectories and its files:

   cipher /e /a /s:\Secret

What Are the Effects of Moving and Copying Encrypted Files and Folders?



Introduction

All files and folders that are created in a folder marked for encryption are automatically encrypted. Moving and copying encrypted files and folders can change the encryption state of the file or folder, depending upon the situation.

Effect of moving encrypted files

As shown in section A in the illustration, if you move a file from an unencrypted folder to an encrypted folder, the file remains encrypted.

Effect of copying encrypted files

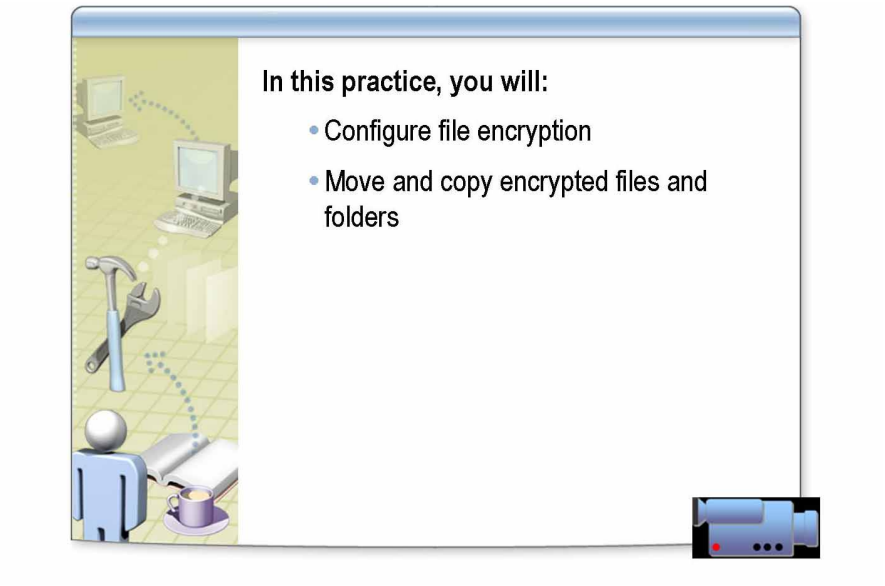
As shown in section B, if you copy an unencrypted file to an encrypted folder, the copied file is encrypted. If you copy an encrypted file from an encrypted folder to an unencrypted folder, the file remains encrypted.

If you copy an encrypted file from an NTFS volume to a FAT or FAT32 volume, the file becomes unencrypted. If you copy a file from a FAT volume to an encrypted folder on an NTFS volume, the file becomes encrypted.

When you encrypt a folder, all files and subfolders that are added to the folder in the future will be encrypted when they are added.

Note For more information about encryption, see the white paper, *EFS*, under **Additional Reading** on the Student Materials compact disc.

Practice: Configuring File Encryption



Objective

In this practice, you will:

- Configure file encryption.
- Move and copy encrypted files.
- Identify the effects of moving and copying compressed files and folders.

Scenario

You are the systems administrator for an organizational unit on a large network. The Research and Development (R&D) department has a server that can be accessed by all of the employees in the department. Although the department manager has configured NTFS permissions on most folders to restrict unauthorized users from looking at the files, he wants you to encrypt the R&D folder.

Practice: Encrypting the folder

► **Encrypt the R&D folder**

1. Log on to the domain as *Computer***User** with a password of **P@ssw0rd**.
2. Open Windows Explorer.
3. Browse to C:\MOC\2275\Practices\Mod06\Data\R&D.
4. Open the **Properties** dialog box for the R&D folder.
5. Click **Advanced**.
6. Select the **Encrypt contents to secure data** check box, and then click **OK**.
7. In the **Confirm Attribute Changes** dialog box, confirm that you want the changes to be made to this folder and all subfolders and files.
8. Close all windows and log off.

9. Log on to the domain as **Administrator** with a password of **P@ssw0rd**.
10. Open Windows Explorer and browse to C:\MOC\2275\Practices\Mod06\Data\R&D.
11. Open the file named Tiger Lily. What happens?
12. Close all windows and log off.

Practice: Moving encrypted files and folders (Exercise 1)

► **Move encrypted files and folders**

1. On the Student Materials compact disc, under **Multimedia**, open *Managing NTFS File Compression and Encryption*, and then select **Encryption Move**.
2. Move the files and folders to various locations on the page, and record the results in the table below.

   The drives in the exercise represent NTFS-formatted drives on the same computer.

Move to:	On same drive		On different drive	
	Encrypted folder	**Unencrypted folder**	**Encrypted folder**	**Unencrypted folder**
Encrypted file				
Encrypted folder				
Unencrypted file				
Unencrypted folder				

Use E to indicate encryption and U to indicate no encryption.

Practice: Copying encrypted files and folders (Exercise 2)

► **Copy encrypted files and folders**

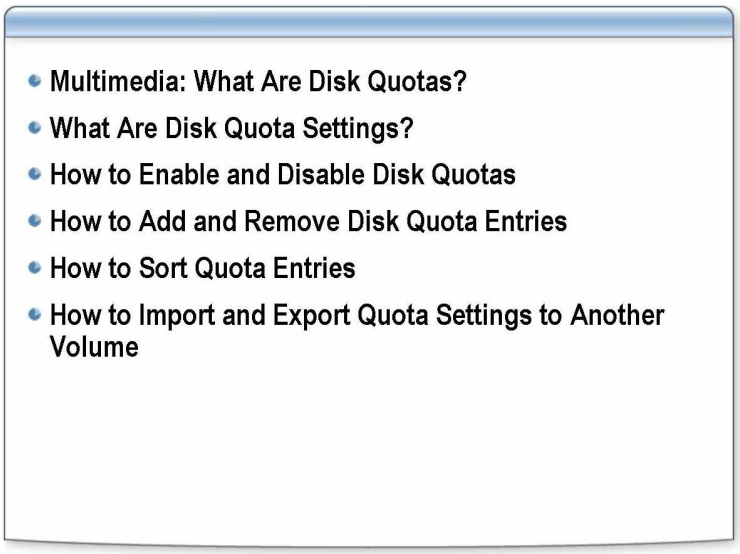
1. On the Student Materials compact disc, under **Multimedia**, open *Managing NTFS File Compression and Encryption*, and then select **Encryption Copy**.
2. Copy the files and folders to various locations on the page, and record the results in the table below.

   The drives in the exercise represent NTFS-formatted drives on the same computer.

Copy to:	On same drive		On different drive	
	Encrypted folder	**Unencrypted folder**	**Encrypted folder**	**Unencrypted folder**
Encrypted file				
Encrypted folder				
Unencrypted file				
Unencrypted folder				

Use E to indicate encryption and U to indicate no encryption.

Lesson: Implementing Disk Quotas



Introduction

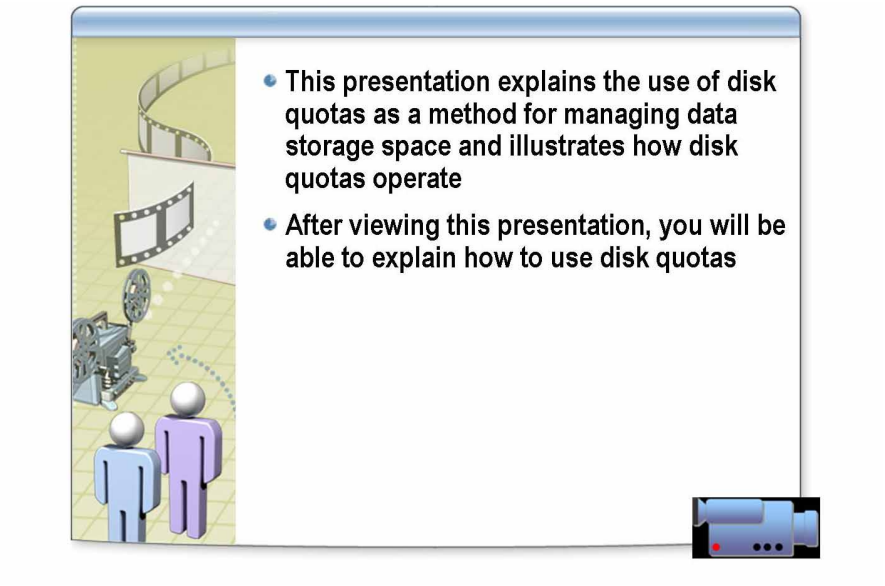
Use disk quotas to manage server resources by limiting storage space for users. You can also use disk quotas to track disk usage by users or groups. In this lesson, you will learn how to use disk quotas and how to set up disk entries.

Lesson objectives

After completing this lesson, you will be able to:

- Explain disk quotas.
- Describe disk quota settings.
- Enable and disable disk quotas.
- Add and remove disk quota entries.
- Sort disk quota entries.
- Import and export disk quota settings to another volume.

Multimedia: What Are Disk Quotas?

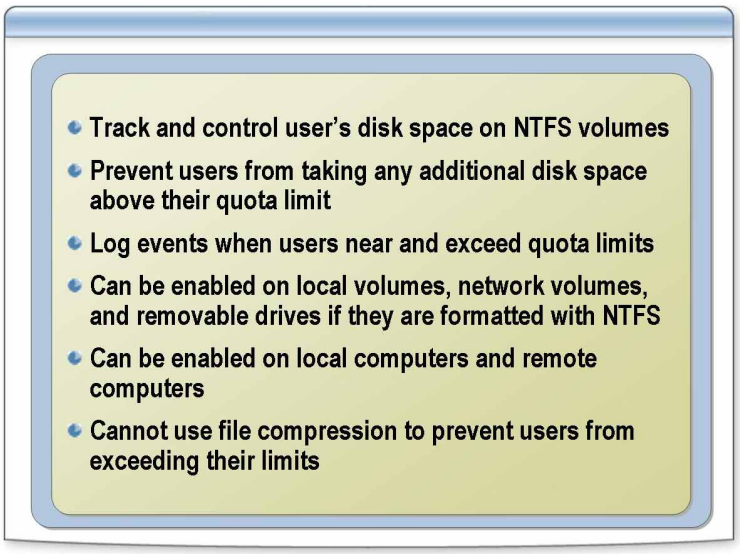


File location

To view the *What Are Disk Quotas?* presentation, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Do not open this presentation unless the instructor tells you to.

What Are Disk Quota Settings?



Introduction

You can use disk quota settings to prevent users from writing additional data to a disk volume after they exceed their assigned quota limit.

Use disk quotas to track disk space

You can also enable quotas without limiting disk space when you do not want to deny users access to a volume but want to track the disk space use of each user. You can also specify whether to log an event when users exceed either their quota limit or their quota warning level.

Enable quotas on volumes

You can enable quotas on local volumes, network volumes, and removable drives if they are formatted by using NTFS. Also, network volumes must be shared from the volume's root directory, and removable drives must be shared. This is not file sharing, but administrative sharing. When you enable disk quotas for a volume, volume usage is automatically tracked for all users from that point on.

File compression does not prevent exceeding quota limits

You cannot use file compression to prevent users from exceeding their quota limits because compressed files are tracked based on their uncompressed size. For example, for a 50-megabyte (MB) file that is 40 MB after it is compressed, Windows counts the file's original 50-MB size toward the quota limit.

CPU overhead and administration

Enabling disk quotas requires a minimal amount of CPU overhead and no additional administration other than the initial configuration.

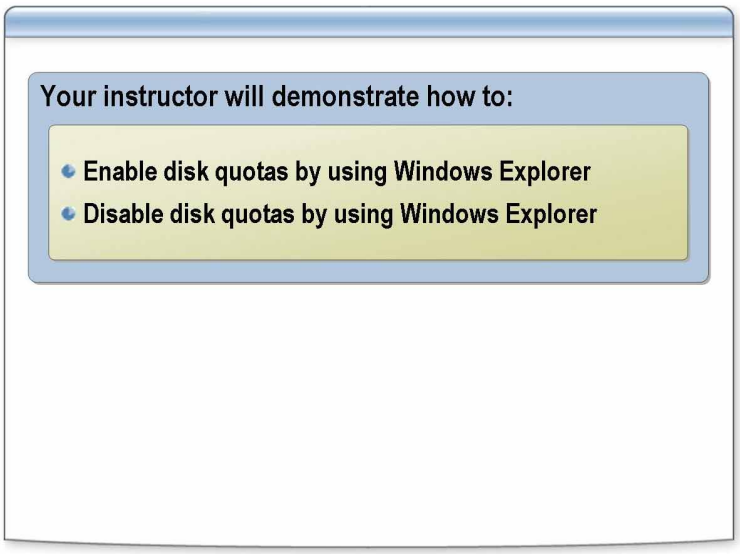
Local and remote implementations of disk quotas

You can enable disk quotas on local computers and remote computers. On local computers, use quotas to prevent users from using excessive disk space on a shared folder on your computer, and limit the amount of space that is available to users who log on to the local computer. For remote computers, quotas can ensure that disk space on public servers is not consumed by one or a few users, and that those users are accountable for the use of shared disk space by using public disk space only for necessary files.

Set quotas on remote volumes

You can set quotas on a remote volume by mapping to it by using Windows Explorer or My Computer. You can manage NTFS volumes on remote computers running Windows 2000 and Windows Server 2003. The volumes must be formatted by using NTFS and must be shared from the root folder of the volume.

How to Enable and Disable Disk Quotas



Introduction

Use the following procedures to enable and disable disk quotas.

Procedure for enabling disk quotas

To enable disk quotas:

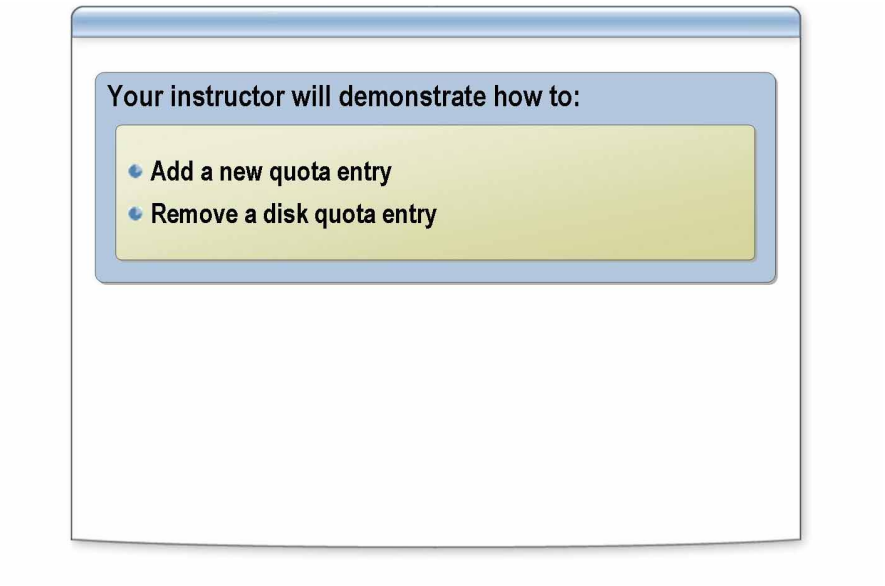
1. In Windows Explorer, right-click the disk volume for which you want to enable disk quotas, and then click **Properties**.
2. In the **Properties** dialog box, on the **Quota** tab, select the **Enable quota management** check box.
3. Select one or more of the following options:
   a. **Deny disk space to users exceeding quota limit**
   b. **Limit disk space to _____**
   c. **Log event when a user exceeds their quota limit**
   d. **Log event when a user exceeds their warning level**

Procedure for disabling disk quotas

To disable disk quotas:

1. In Windows Explorer, right-click the disk volume for which you want to disable disk quotas, and then click **Properties**.
2. In the **Properties** dialog box, on the **Quota** tab, clear the **Enable quota management** check box.

How to Add and Remove Disk Quota Entries



Introduction

Use the following procedures to add and remove disk quota entries. Each new user is considered a quota entry.

Procedure for adding a new disk quota entry

To add a new disk quota entry:

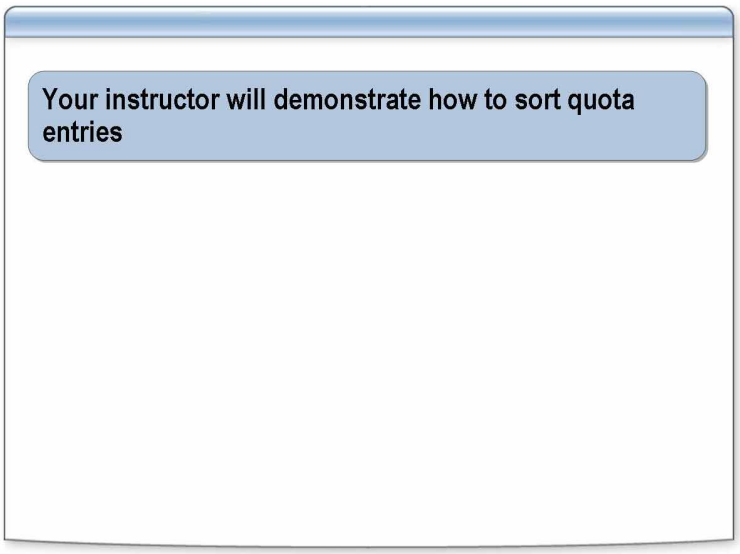
1. In Windows Explorer, right-click the volume for which you want to add a new disk quota entry, and then click **Properties**.
2. In the **Properties** dialog box, on the **Quota** tab, click **Quota Entries**.
3. In the Quota Entries window, on the **Quota** menu, click **New Quota Entry**.
4. In the **Select Users** dialog box, in the **Enter the object names to select** text box, type the domain or workgroup name, followed by a backslash (\) and the username of the user for which you want to impose quotas, and then click **OK**.
5. In the **Add New Quota Entry** dialog box, specify one of the following options:
   a. **Do not limit disk usage**
   b. **Limit disk space to**

Procedure to remove disk quota entries

To remove disk quota entries:

1. In Windows Explorer, right-click the volume for which you want to add new disk quota entries, and then click **Properties**.
2. In the **Properties** dialog box, on the **Quota** tab, click **Quota Entries**.
3. In the Quota Entries window, click the entries for the users you want to delete, and then on the **Quota** menu, click **Delete Quota Entry**.
4. If the **Disk Quota** dialog box appears, click **Yes**, click the files or folders that you want to take action on, and then click one of the following buttons: **Delete**, **Take Ownership**, **Move**.

How to Sort Quota Entries



Introduction

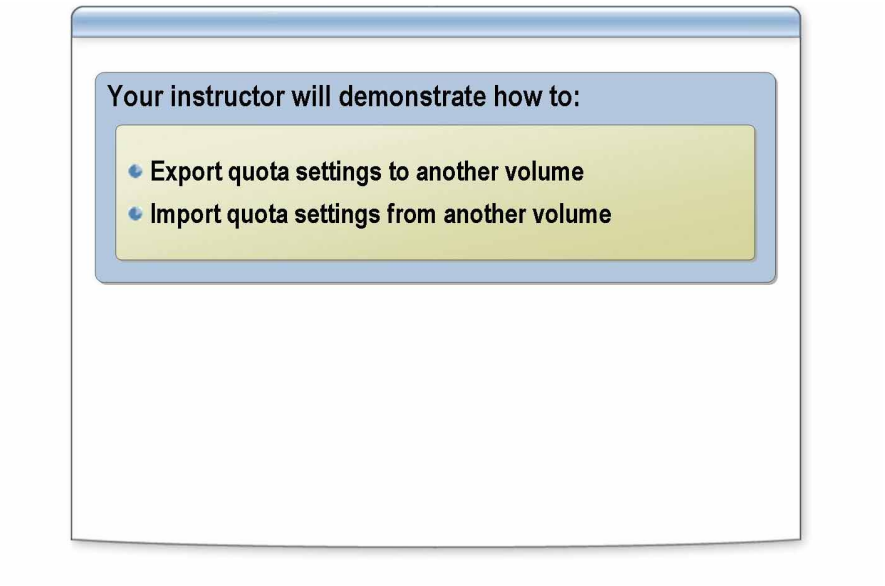
After setting up the list of users who are using disk quotas, you can use the following steps to sort the results of disk quotas.

Procedure for sorting quota entries

To sort quota entries:

1. In Windows Explorer, right-click the volume for which you want to sort quota entries, and then click **Properties**.
2. In the **Properties** dialog box, on the **Quota** tab, click **Quota Entries**.
3. In the Quota Entries window, on the **View** menu, point to **Arrange Items**, and then click one of the following options:
   a. **By Folder**
   b. **By User Name**
   c. **By Logon Name**
   d. **By Status**
   e. **By Amount Used**
   f. **By Quota Limit**
   g. **By Warning Level**
   h. **By Percent Used**

How to Import and Export Quota Settings to Another Volume



Introduction

By using the list of disk quota users you have set up for one volume, you can save time and effort by importing the settings to other volumes. Use the following steps to export quota settings from one volume and import them to another volume.

Procedure for exporting quota settings

To export quota settings to another volume:

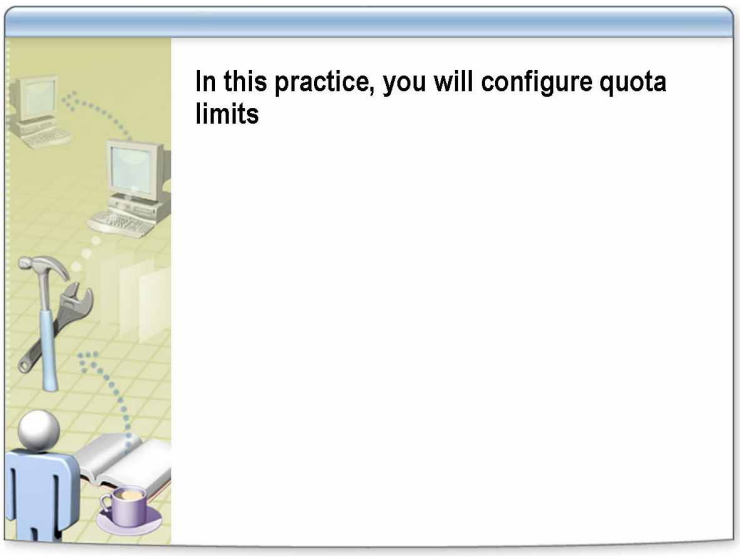
1. In Windows Explorer, right-click the volume to which you want to import quota settings, and then click **Properties**.
2. In the **Properties** dialog box, on the **Quota** tab, make sure the **Enable quota management** check box is selected, and then click **Quota Entries**. Click the user quota settings you want to export.
3. On the **Quota** menu, click **Export**. In the **Export Quota Settings** dialog box, specify a destination folder, type the file name for the saved settings, and then click **Save**.

Procedure for importing quota settings

To import quota settings from another volume:

1. In Windows Explorer, right-click the volume to which you want to import quota settings, and then click **Properties**.
2. In the **Properties** dialog box, on the **Quota** tab, click **Quota Entries**, and then in the Quota Entries window, on the **Quota** menu, click **Import**.
3. In the **Import Quota Settings** dialog box, select the name of the file that contains the quota settings you want to import, and then click **Open**.
4. When you import quota settings a dialog box appears if imported settings will overwrite existing settings for a volume user. Specify whether you want to overwrite the existing user settings.

Practice: Configuring Quota Limits



Objective

In this practice, you will configure quota limits.

Scenario

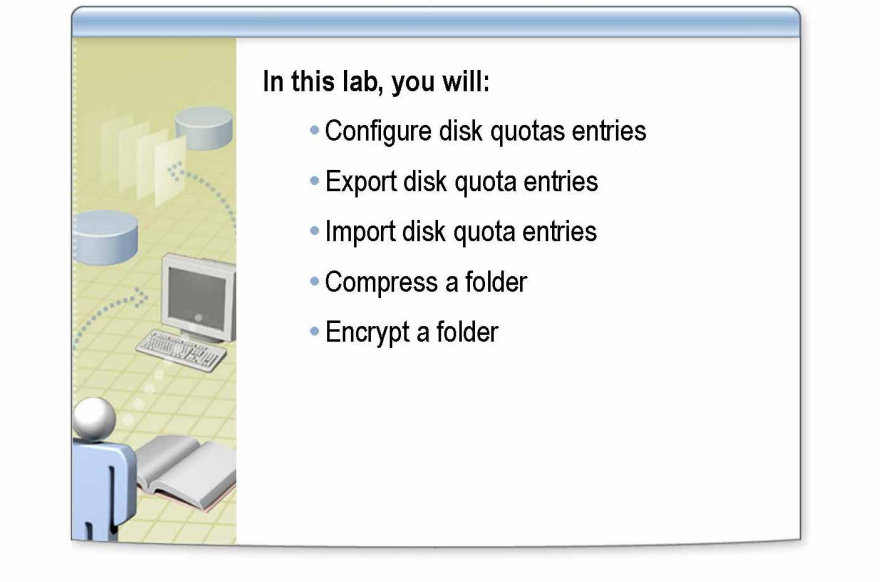
You are the systems administrator for an organizational unit on a large network. The department manager has decided to allocate space on the department server for employees' personal files. However, the manager has asked you to put a 10-MB limit on the amount of personal data that each user is allowed to store on the server. You will need to configure disk quotas to limit the amount of space each user is allowed on the D drive.

Practice

1. Log on to the domain as Administrator with a password of **P@ssw0rd**.

   You must log on as Administrator in this practice, because Windows Explorer cannot be started using the **Run As** command.
2. In Windows Explorer, open the **Properties** dialog box for the D drive.
3. On the **Quota** tab, select the **Enable quota management** check box.
4. Enable the following options:
   a. Deny disk space to users exceeding quota limit
   b. Limit disk space to 10 MB
   c. Set the warning level to 9 MB
   d. Log event when a user exceeds their quota limit
   e. Log event when a user exceeds their warning level
5. Close all windows and log off.

Lab A: Managing Data Storage



Objectives

After completing this lab, you will be able to:

- Configure disk quotas entries.
- Export disk quota entries.
- Import disk quota entries.
- Compress a folder.
- Encrypt a folder.

Prerequisites

Before working on this lab, you must have:

- Completed the labs and practices from Module 5, "Managing Disks," in Course 2275, *Maintaining a Microsoft Windows Server 2003 Environment.*

  If you have not completed those labs and practices, you must run the following batch file: C:\MOC\2275\Labfiles\Lab06\Mod5.bat.
- Run the setperm script in C:\MOC\2275\Labfiles.

Scenario

You are the systems administrator for an organizational unit on a large network. After arriving at work one morning, you receive the following requests from your manager:

- The organization has decided to implement disk quotas on all of the volumes on its servers. To test this plan, you have been asked to configure disk quota entries on your drive D and then export them to a file. Next, you will import them to your drive E and verify the quota configuration. You will use *Computer*User and GlasgowUser for your testing.
- The marketing department wants you to compress the 5,000 graphics files on its server. The files are in a folder named Graphics.
- The Human Resources department has decided to encrypt all of the personnel files. The HR director wants you to show her how to do this.

Estimated time to complete this lab: 10 minutes

Exercise 1
Configuring Disk Quota Entries

You need to configure disk quota entries for *Computer*User and GlasgowUser for your testing.

Tasks	Specific instructions
1. Log on using the domain user account.	▪ Log on to the domain as *Computer***User** with a password of **P@ssw0rd**.
2. Start Computer Management with administrative credentials.	▪ In the **Run** dialog box, use **runas** to start Computer Management: **runas /user:nwtraders\administrator "mmc %windir%\system32\compmgmt.msc"**
3. Configure disk quota entries.	**a.** In Disk Management, open the **Properties** dialog box for drive D. **b.** On the **Quota** tab, select the following entries: **Enable quota management**, **Deny disk space to users exceeding quota limit**, **Log event when a user exceeds their quota limit**, and **Log event when a user exceeds their warning level**. **c.** Configure a quota entry for *Computer*User. **d.** In the **Limit disk space to** box, type **10 MB** and then in the **Set warning level to** box, type **9 MB**
4. Add GlasgowUser quota entries.	▪ Repeat step 3 for GlasgowUser.

Exercise 2
Exporting Disk Quota Entries

In this exercise, you will export the disk quota entries that you created to a binary file.

Tasks	Specific instructions
1. Export disk quota entries to a binary file.	▪ In Disk Management, highlight the new quota entries that you created in the previous exercise, and then on the **Quota** menu, click **Export**.
2. Save the quota entries file.	▪ Name the quota entries file **export.bin** and then save the file in **C:\MOC\2275\Labfiles**.
3. Close the Quota Entries window.	▪ Close the Quota Entries for New Volume (D:) window, close the **New Volume (D:) Properties** dialog box, and then click **OK** to close the remaining dialog boxes.

Exercise 3
Importing Disk Quota Entries

In this exercise, you will import the disk quota entries on drive E.

Tasks	Specific instructions
1. Import disk quota entries to another drive.	**a.** In Computer Management, open the **Properties** dialog box for New Volume (E:) drive. **b.** On the **Quota** tab, select the **Enable quota management** check box, and then open the Quota Entries window. **c.** Open the **Import Quota Settings** dialog box, and then import the export.bin file.
2. Verify that the three quota entries are displayed.	▪ In the Quota Entries for New Volume (E:) window, verify that the three quota entries are displayed in New Volume (E:).
3. Close the windows.	**a.** Close the Quota Entries for New Volume (E:) window. **b.** Close the dialog box by clicking **OK**.
4. Test the quota entries.	**a.** In Windows Explorer, browse to C:\Moc\2275\Labfiles\Lab06, and then double-click **diskhog**. A command prompt window opens, and the text starts scrolling. Diskhog is a program that creates a small file and then doubles its size repeatedly until there is no more disk space. Notice that the text stops scrolling, and the size of the file is displayed. **b.** How big was the junk.txt file before diskhog stopped? _____ **c.** Close all windows.

Exercise 4
Compressing a Folder

In this exercise, you will compress the C:\MOC\2275\Labfiles\Lab06\Data\Graphics folder.

Tasks	Specific instructions
1. Select the file to be compressed.	**a.** In Windows Explorer, browse to C:\MOC\2275\Labfiles\Lab06\Data\Graphics. **b.** Open the **Properties** dialog box for the Graphics folder, and then click **Advanced**.
2. Compress the folder.	**a.** Using **Compress or Encrypt attributes**, compress the folder. **b.** Close all dialog boxes by clicking **OK**.

Exercise 5
Encrypting a Folder

In this exercise, you will encrypt the C:\MOC\2275\Labfiles\Lab06\Data\Personnel folder.

Tasks	Specific instructions
1. Select the file to be encrypted.	**a.** In Windows Explorer, browse to C:\MOC\2275\Labfiles\Lab06\Data\Personnel. **b.** Open the **Properties** dialog box for the Personnel folder, and then click **Advanced**.
2. Encrypt the folder.	**a.** Using Compress or Encrypt attributes, encrypt the folder. **b.** Close all dialog boxes by clicking **OK**. **c.** Close all windows and log off.
3. Verify that the contents of the Personnel folder are secure.	**a.** Log on the domain as Administrator with a password of **P@ssw0rd**. **b.** Open Windows Explorer, and browse to C:\MOC\2275\Labfiles\Lab06\Data\Personnel. **c.** Double-click **people**. **d.** Close all windows and log off.

Course Evaluation

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

At a convenient time before the end of the course, please complete a course evaluation, which is available at http://www.CourseSurvey.com.