Microsoft®
Training &
Certification

Microsoft Official
Curriculum

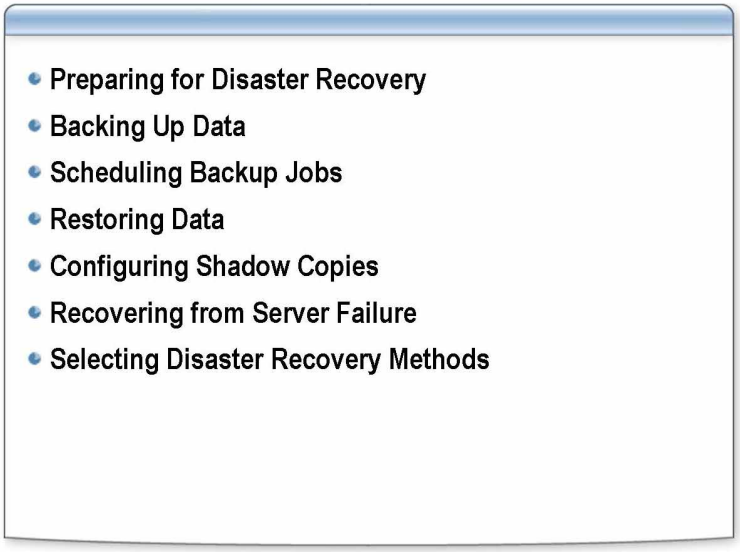
Module 7: Managing Disaster Recovery

Contents

Overview	1
Lesson: Preparing for Disaster Recovery	2
Lesson: Backing Up Data	7
Lesson: Scheduling Backup Jobs	25
Lesson: Restoring Data	34
Lesson: Configuring Shadow Copies	44
Lesson: Recovering from Server Failure	60
Lesson: Selecting Disaster Recovery Methods	76
What Are Server Disaster Recovery Tools?	77
Lab A: Managing Disaster Recovery	79

Microsoft®

Overview



Introduction

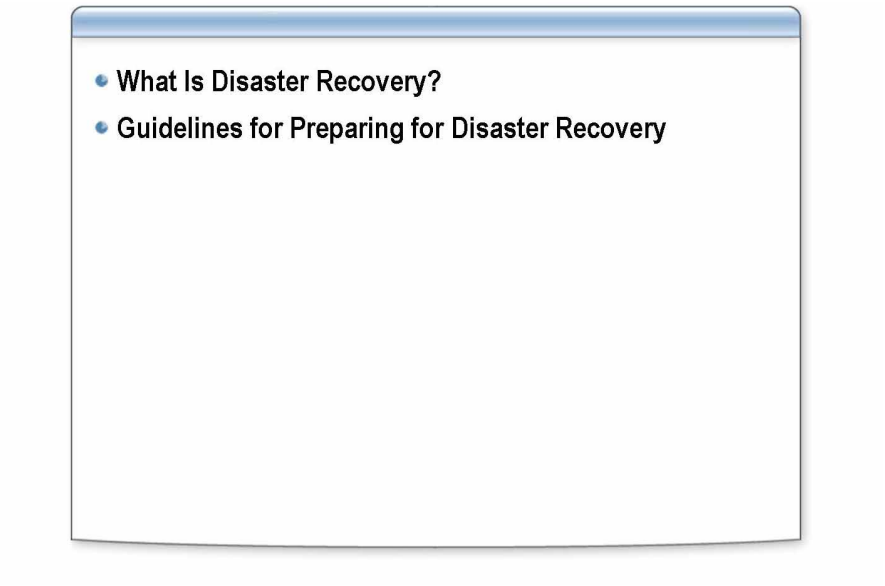
This module helps you prepare for a computer disaster by using the features in Microsoft® Windows® Server 2003 to prevent data loss and recover from data losses after they occur. Understanding these features is essential to developing and implementing an effective disaster protection and recovery plan.

Objectives

After completing this module, you will be able to:

- Prepare for disaster recovery.
- Back up data.
- Schedule backup jobs.
- Restore data.
- Configure a shadow copy.
- Recover from server failure.
- Select a disaster recovery method.

Lesson: Preparing for Disaster Recovery



Introduction

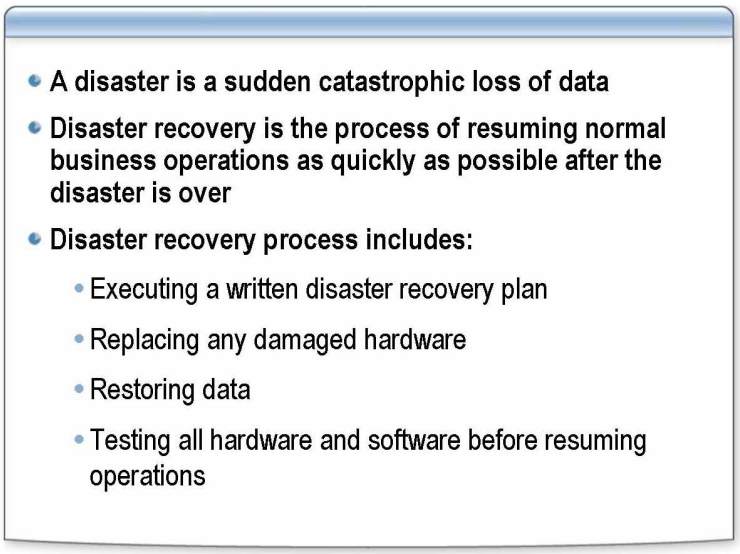
This lesson introduces the components of disaster recovery and the methods of recovering data after a disaster occurs. This lesson also provides recommended guidelines that will help you to develop your own disaster recovery plan.

Lesson objectives

After completing this lesson, you will be able to:

- Describe what to include in a recovery plan.
- Explain the guidelines to use when you create a disaster recovery plan.

What Is Disaster Recovery?



Introduction

A computer disaster is a sudden catastrophic loss of data. The business world depends on mission-critical data more than ever. As a result, organizations are placing a premium on protecting their information technology (IT) assets from data loss and server failure.

Disaster recovery

Disaster recovery is the process of resuming normal business operations as quickly as possible after the disaster ends. Ideally, you can use disaster recovery methods to restore data and services to the state they were in prior to the disaster.

Disaster recovery considerations

For each operating system and application that you introduce to your environment, answer the following questions about disaster recovery:

Disaster recovery method	Considerations
Recovery plan	• What are the possible failure scenarios? • What data is critical? • How often should you perform backups? • How long will you save the backups before reusing the medium? • Assuming failure, how much time will it take to restore from the most recent backup? Is that an acceptable amount of downtime? • Where will you store the backups, and do the appropriate people have access to them? • If the responsible systems administrator is gone, is there someone else who knows the proper passwords and procedures to perform backups and, if necessary, to restore the system?

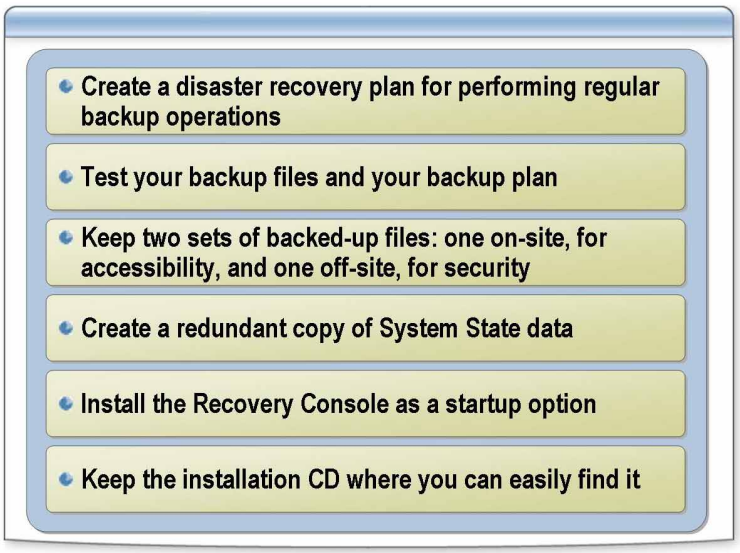
(*continued*)

Disaster recovery method	Considerations
Hardware	• How many, what kind, and where are individual computer components, such as hard disks and controllers, processors, and RAM? • How many, what kind, and where are external components such as routers, bridges, switches, cables, and connectors? • Are the critical hardware and services redundant?
Data restoration	• To what medium, such as tape, compact disc, or disk, will you send the backup? • Will you perform backups online, while users are working, or offline? • Will you perform the backups manually or schedule them to be performed automatically? • How long will you save the backups before reusing the medium? • Is the critical data redundant? How often is the critical data updated?
Testing	• If the backup is automated, how will you verify that it successfully occurred? • How will you ensure that the backups are usable?

Determine questions based on your situation

This is not a complete list—you must determine other questions based on your particular situation.

Guidelines for Preparing for Disaster Recovery



Introduction

You should develop and thoroughly test a disaster recovery plan. When you test, look for vulnerable areas by simulating as many possible failure scenarios as you can.

Guidelines

Use the following guidelines to prepare for disaster recovery:

- Create a disaster recovery plan for performing regular backup operations.

  Review and incorporate a plan for backing up all of your files on a regular basis. Keep a log of every update in your disaster recovery plan.

- Test your backup files and your backup plan.

  Testing your backup files and recovery plan is an important part of being prepared for disaster recovery. Testing must include the following tasks:

  - Test your uninterruptible power supply (UPS) on the computers running Windows Server 2003 and on hubs, routers, and other network components.
  - Perform full or partial restorations from your daily, weekly, and monthly backup media.

- Keep two sets of backed-up files: one on-site, for accessibility, and one off-site, for security.

  The backup should be accessible, such as on network shared folders or removable media, in case the data must be restored to another computer.

  If possible, make a copy of your backup sets every day and store them at both an on-site and off-site location. That way, if a catastrophic event, such as a fire, destroys all of your computers and on-site backup sets, you can restore all your data later. However, if all of your backups are off-site, every time you need to recover a file, you must get the backup files from the off-site location.

- Create a backup of the System State data.

  Create a backup copy of the System State data in the unlikely event that the hard disk on the server fails and cannot be recovered. This copy can help you restore your operating system to a new hard disk.

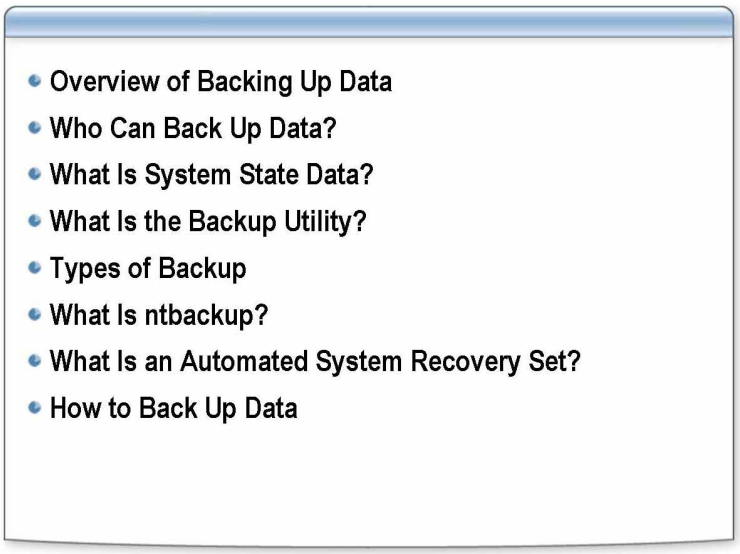
- Install the Recovery Console as a startup option.

  Install the Recovery Console on your computer to make it available in case you are unable to restart Windows Server 2003. You can then select the Recovery Console option from the list of available operating systems in safe mode.

- Keep the installation compact disc where you can easily find it.

  Keep the installation compact disc where you can find it easily. You can start the computer from the compact disc and then use the Recovery Console or Automated System Recovery.

Lesson: Backing Up Data



Introduction

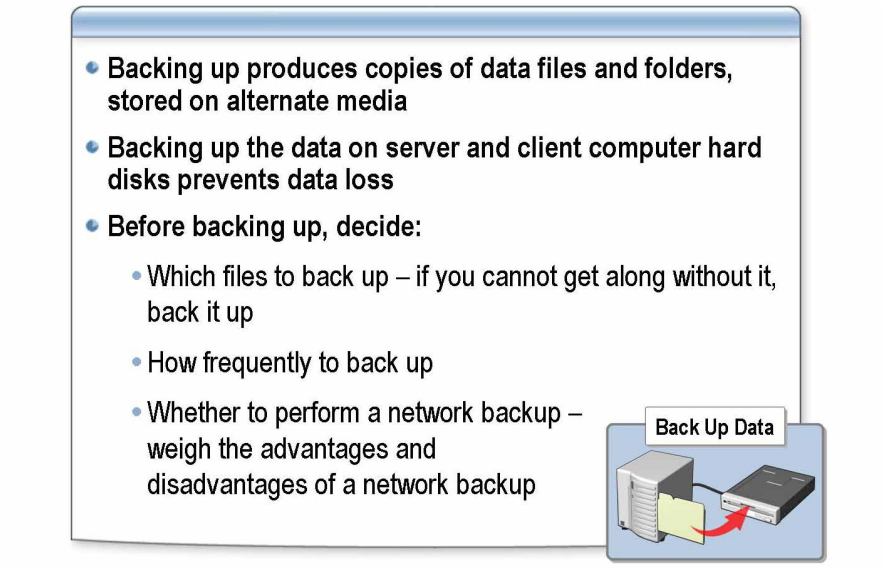
Backing up your data prevents data loss in case the original files are lost due to hardware or software failure. Windows Server 2003 includes a backup utility, Backup, that backs up data by copying designated files to storage media. You can also use Windows Server 2003 to back up your server by using Automated System Recovery.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the process of backing up data.
- Explain who can back up data.
- Explain the backup of System State data.
- Explain the Backup utility.
- Explain the various types of backup.
- Explain the **ntbackup** command-line tool.
- Explain an Automated System Recovery set.
- Describe guidelines for backup.

Overview of Backing Up Data



Introduction

Backup is a single process of copying files and folders from one location to another. Regularly backing up the data on server and client computer hard disks prevents data loss due to disk drive failures, power outages, virus infections, and other such incidents. If a data loss occurs, and you have performed regular backups based on careful planning, you can restore the lost data, whether it is in one file or on an entire hard disk.

There is a general backup rule: if you cannot get along without it, back it up.

When to use a network backup

Perform a network backup when the critical data is on multiple servers or you want to perform a backup over the network. The following table describes the advantages and disadvantages of a network backup.

Advantages	Disadvantages
Backs up the entire network	Users must copy their important files to the servers
Requires fewer tape drives or disks	Cannot back up the registry on remote computers
Less media to manage	Increases network traffic
One user can back up data	Requires greater planning and preparation

How frequently to back up

Backup frequency depends on the following conditions:

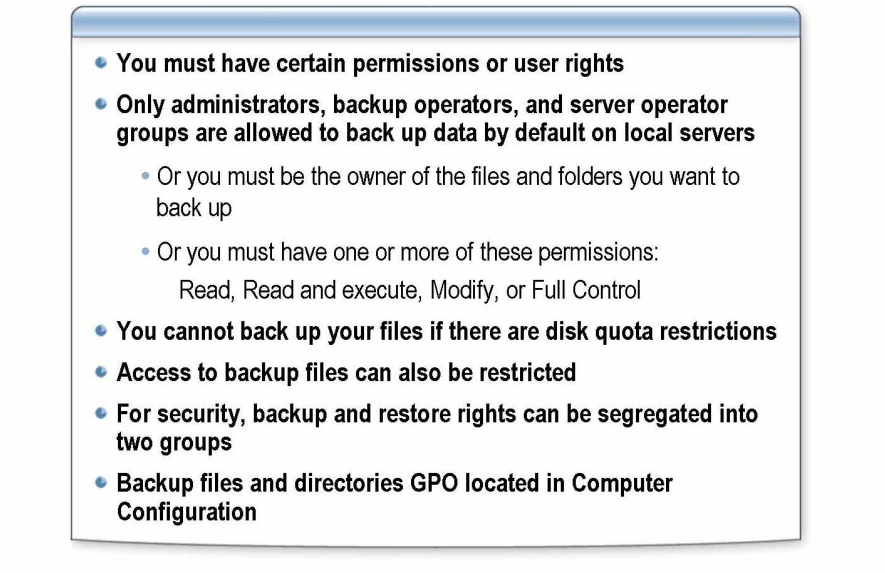
- How critical the data is to your organization. You back up critical data more often than data of low importance.
- How frequently the data changes. For example, if users create or modify reports only on Fridays, a weekly backup for the report files is sufficient.

Types of data to back up

System State data is a collection of data that defines the configuration of the operating system on a server. If accidental changes occur or if data is lost in any of the components that make up the System State data, you can restore System State data from a backup. This action restores your computer's configuration to a previously known good state.

Critical data is the data that your organization needs to survive. If you lose this data, which is typically stored on a server, your organization cannot conduct its business. If files are accidentally lost or corrupted, you can use the last known good backup files to restore this data.

Who Can Back Up Data?



Introduction

You must have certain permissions or user rights to back up and restore files and folders. If you are an administrator a backup operator or server operators in a local group, you can back up and restore any file or folder on the local server to which the local group applies.

Permissions and user rights

To successfully back up and restore data on a computer running Windows Server 2003, you must have the appropriate permissions and user rights, as described in the following list:

- All users can back up their own files and folders. They can also back up files for which they have the Read permission.
- Members of the Administrators, Backup Operators, and Server Operators groups can back up and restore all files, regardless of the assigned permissions. By default, members of these groups have the following user rights: Backup Files and Directories and the Restore Files and Directories as well as Modify and Full Control permissions.

No disk quota restrictions

You must also be certain that there are no disk quota restrictions that may restrict your access to a hard disk, thereby making it impossible for you to back up data. You can check whether there are any disk quota restrictions by right-clicking the disk that you want to save data to, clicking **Properties**, and then clicking the **Quota** tab.

Restrict access

You can also restrict access to a backup file by selecting **Allow only the owner and the Administrator access to the backup data** in the **Backup Job Information** dialog box. If you select this option, only an administrator or the person who created the backup file can restore the files and folders.

Separate backup and restore user rights

For security reasons, many organizations prefer to separate the backup and restore user rights into two groups as follows:

1. Create a Backup group and a Restore group by using Active Directory Users and Computers.
2. Add one set of members to the Backup group and another set of members to the Restore group.
3. Add the Backup group to the **Backup files and directories** Group Policy object (GPO).
4. Add the Restore group to the **Restore files and directories** GPO.

Location of the Backup files and directories GPO

The Backup files and directories GPO and Restore files and directories GPO are located in the following group policy:

Computer Configuration

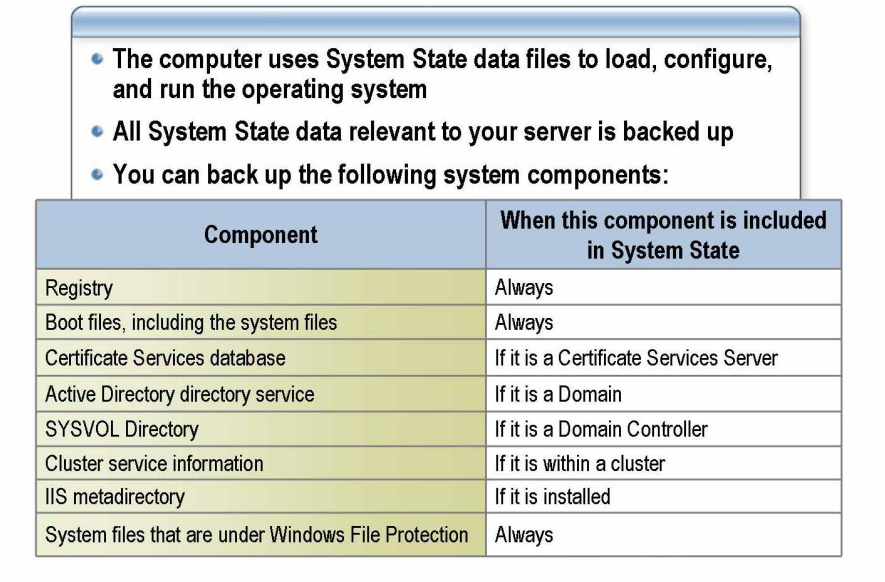
Windows Settings

Security Settings

Local Policies

User Rights Assignment

What Is System State Data?



Introduction

The System State is the collection of system-specific data maintained by the operating system that must be backed up as a unit. The computer uses these system files to load, configure, and run the operating system.

System State components

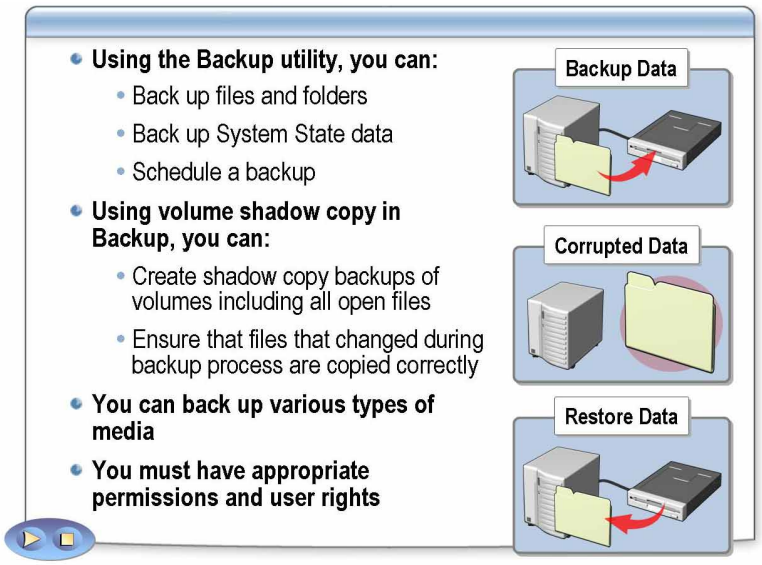
Backup refers to the following system files as the System State data.

Component	When included in System State
Registry	Always
Boot files, Com+ Class Registration, including the system files	Always
Certificate Services database	If it is a Certificate Services server
Active Directory® directory service	If it is a domain
SYSVOL directory	If it is a domain controller
Cluster service information	If it is within a cluster
IIS metadirectory	If it is installed
System files that are under Windows File Protection	Always

Back up System State data

When you back up or restore the System State data, all of the System State data that is relevant to your computer is backed up or restored. You cannot back up or restore individual components of the System State data because of dependencies among the System State components. However, you can restore the System State data to an alternate location. If you do this, only the registry files, SYSVOL directory files, Cluster database information files, and system boot files are restored to the alternate location. Active Directory, the Certificate Services database, and the COM+ Class Registration database are not restored if you designate an alternate location when you restore the System State data.

What Is the Backup Utility?



Introduction

The Windows Server 2003 backup utility, Backup, is designed to protect data from accidental loss resulting from the failure of your hardware or storage media. It is the graphical user interface (GUI) version of the Backup utility.

Use to manage backup

You can use Backup to:

- Back up files and folders.
- Back up System State data.
- Schedule a backup job.

You can use the Backup Wizard to back up the entire contents of a server, selected portions of the server contents, or the System State data.

Volume shadow copy

You can use Backup to create shadow copy backups of volumes and exact copies of files, including all open files. For example, databases that are held open exclusively and files that are open due to operator or system activity are backed up during a volume shadow copy backup. In this way, files that changed during the backup process are copied correctly.

Volume shadow copy backups ensure that:

- Applications can continue to write data to the volume during a backup.
- Open files are not omitted during a backup.
- Backups can be performed at any time, without locking out users.

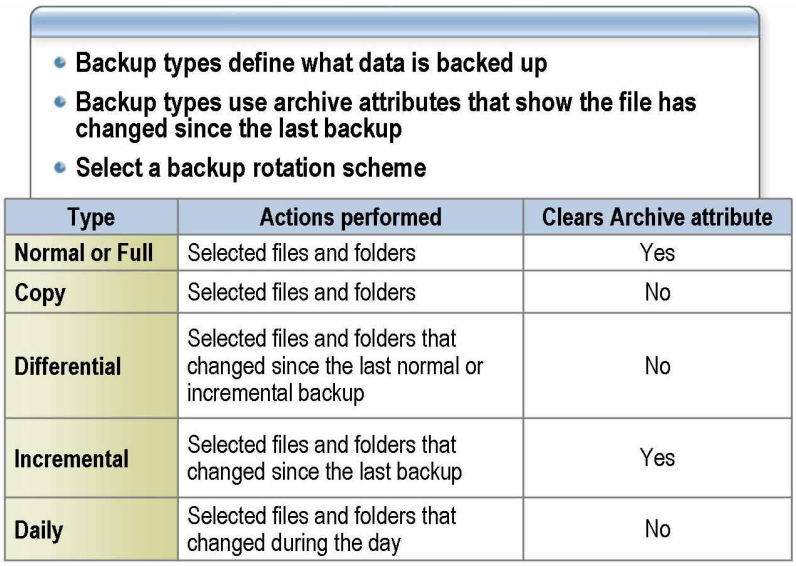
Some applications manage storage consistency differently while files are open, which can affect the consistency of the files in the backup. For critical applications, consult the application documentation or your provider for information about the recommended backup method. When in doubt, quit the application before performing a backup.

Volume shadow copy is enabled by default. If you disable this option, some files that are open or in use during the backup might be skipped. It is recommended that you do not disable this option.

Supports a variety of storage devices

The Backup utility supports a variety of storage devices and media, including tape drives, logical drives, removable disks, and recordable CD-ROM drives.

Types of Backup



Introduction

The Backup utility provides five backup types that specify what data is backed up, such as only files that have changed since the last backup.

Backup archive attributes

Some backup types use an archive attribute, which indicates that a file was modified since the last backup. When a file is modified, the archive attribute is set, and when you back up the file, the archive attribute is cleared or reset.

Backup types

Backup provides five backup types: normal, copy, differential, incremental, and daily. Each of these backup types targets specific categories of files for backup, such as files that have changed since the last backup or all files in a specific folder.

The following table presents the backup types, the function of each type, whether the backup type clears archive attributes, and tips for using the backup type.

Type	Description
Normal	Backs up all selected files, regardless of the setting of the archive attribute, and clears the archive attribute of all files that are backed up. If the file is modified later, the archive attribute is set, which indicates that the file needs to be backed up. Perform a normal backup the first time you create a backup set to set a baseline for future backup jobs.
Copy	Identical to a normal backup except that it does not change the archive attribute, which allows you to perform other types of backups on the files later. Use a copy backup to create an additional backup tape or disk without disturbing the archive attributes.

(*continued*)

Type	Description
Differential	Creates backup copies of files that have changed since the last normal backup. The presence of the archive attribute indicates that the file was modified and only files with this attribute are backed up. However, the archive attribute on files is not modified. This allows you to perform other types of backups on the files later. Because a differential backup does not clear archive attributes, if you perform two differential backups on a file, the entire file is backed up each time. Differential backups use more media than incremental backups, but when you restore the disk, you need only the media that contains the files from the normal backup and the most recent differential backup.
Incremental	Designed to create backups of files that have changed since the most recent normal or incremental backup. The presence of the archive attribute indicates that the file was modified, and only files with this attribute are backed up. When a file is backed up, the archive attribute is cleared. Because an incremental backup clears archive attributes, if you perform two incremental backups in a row on a file, the file is not backed up the second time. Incremental backups use the minimum amount of media and also save time by not copying all of the files that have changed since the last full backup. However, restoring a disk is inconvenient because you must change the media for each day of the week.
Daily	Backs up files by using the modification date on the file itself, and disregards the current state of the archive attribute. If a file was modified on the same day as the backup, the file is backed up. This type does not change the archive attributes of files.

Important Your backup plan can combine various backup types. If you combine backup types, archive attributes are critical. Incremental and differential backup types check for and rely on the archive attributes.

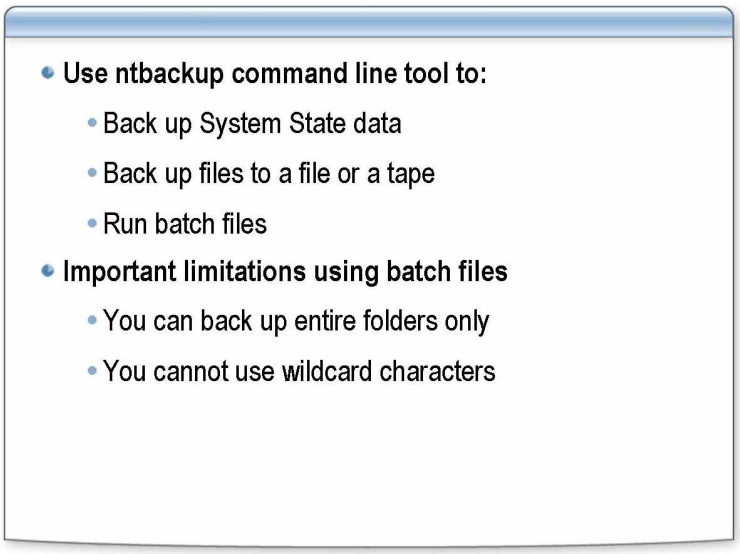
Backup scenarios

You perform a normal backup on Monday and incremental backups on Tuesday through Friday. If your disk fails on Saturday, you must restore the hard disk with Monday's tape and then complete the restore process by using the Tuesday-through-Friday tapes in the order that they were written.

You perform a normal backup on Monday and differential backups on Tuesday through Friday. If your disk fails on Saturday, you must restore the hard disk using Monday's tape followed by Friday's tape.

Workers in your organization are required to save their work to a server every hour. Management wants to limit the amount of data that is lost due to a server failure to one hour. To accomplish this, you perform a normal backup on Monday, a differential backup the other four days, and a daily backup every hour.

What Is ntbackup?



Introduction

In addition to Backup, Windows Server 2003 provides a command-line tool, **ntbackup**, that you can use to back up and restore data.

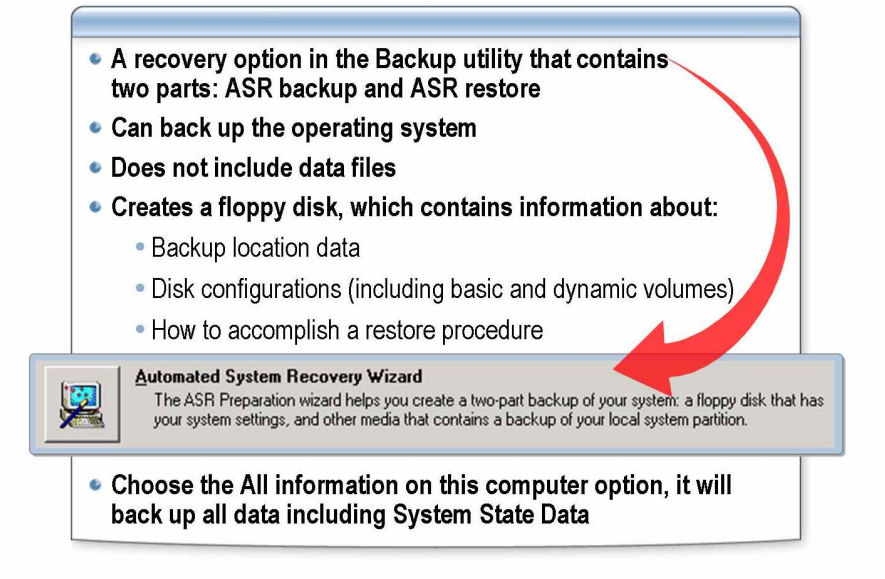
Use the command prompt or batch file

You can perform backup operations from a command prompt or from a batch file by using the **ntbackup** command, followed by various parameters.

There are two important limitations to using batch files to back up your data:

- When you use the **ntbackup** command, you must back up entire folders only. You cannot designate individual files for backup. However, you can designate a backup selection file (.bks file) from the command line, which contains a list of files that you want to back up. You must use the GUI version of the Backup utility to create backup selection files.
- The **ntbackup** command does not support the use of wildcard characters. For example, typing ***.txt** does not back up files with a .txt extension.

What Is Automated System Recovery?



Introduction

Automated System Recovery (ASR), in the Backup utility, helps you recover a system that does not start. ASR contains two parts: backup and recovery. ASR also creates a floppy disk that is used to store disk configurations during the ASR restore procedure.

ASR restores operating system

Typically, after installing or upgrading to Windows Server 2003, you create a set of ASR disks. The ASR process enables you to restore an installation of Windows Server 2003 to the condition of the operating system at the time that you created the ASR backup set.

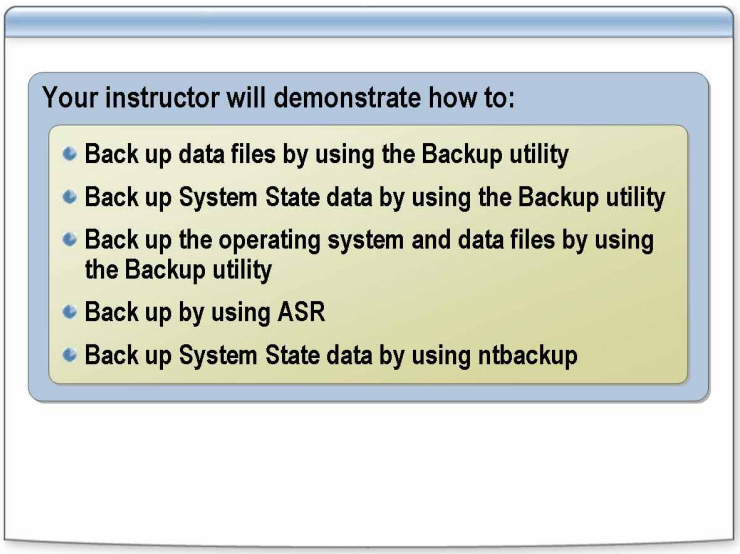
ASR Backup Wizard

The ASR Backup Wizard backs up the System State data, system services, and all disks that are associated with the operating system components, but it does not back up data files. The ASR Backup Wizard also creates a floppy disk, which contains information about the backup, the disk configurations, including basic and dynamic volumes, and the restore procedure.

Backup or Restore Wizard

The ASR Backup Wizard provides several backup options. The **All information on this computer** option backs up all data on the computer in addition to the System State data and the operating system components. This option also creates a system recovery disk that you can used to restore Windows in case of a disk failure.

How to Back Up Data



Introduction

You can use the Backup utility to make copies of your organization's most important data and your System State data. Use the Backup or Restore Wizard to back up those selected files. You can also use ASR to back up all the files, including program files and System State data files. Use the **ntbackup** command to create a batch file to back up System State data.

Procedure for backing up data files or System State using Backup

To back up files by using the Backup utility:

1. On the **Start** menu, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. On the **Welcome** page of the Backup or Restore Wizard, click the **Advanced Mode** link.
3. In the **Backup Utility** dialog box, on the **Backup** tab, on the **Job** menu, click **New**.
4. Under **Click to select the check box for any drive, folder or file that you want to back up**, click the box next to each file or folder that you want to back up, or click the box next to **System State**.
5. In the **Backup destination** box, do one of the following:
   - Select **File** if you want to back up files and folders to a file.
   - Select a tape device.
6. In the **Backup media or file name** box, do one of the following:
   - If you are backing up files and folders to a file, type the path and file name for backup (.bkf) file, or click **Browse** to find a file.
   - If you are backing up files and folders to tape, choose the tape you want to use.

7. To select backup options, on the **Tools** menu, click **Options**, and then select the options that you want to use, such as backup type and log file type.
8. Click **Start Backup**, and then make any changes in the **Backup Job Information** dialog box.

Procedure for backing up operating system and data by using Backup

To back up files by using the Backup or Restore Wizard:

1. On the **Start** menu, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. On the **Welcome** page of the Backup or Restore Wizard, click **Next**.
3. On the **Backup or Restore** page, click **Back up files and settings**, and then click **Next**.
4. On the **What to Back Up** page, click **All information on this computer**, and then click **Next**.
5. On the **Backup Type, Destination, and Name** page, click **Browse**.
6. In the **Save As** dialog box, in the **File name** box, type **D:\Complete.bkf** and then click **Save**.
7. Click **Next**, and then click **Finish**.

Procedure for backing up by using ASR

To store the ASR backup files to the disk:

1. On the **Start** menu, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. In the Backup or Restore Wizard, click **Advanced Mode**.
3. On the **Welcome** tab, click **Automated System Recovery Wizard**.
4. On the **Welcome to the Automated System Recovery Preparation Wizard** page, click **Next**.
5. On the **Backup Destination** page, select **File** in the **Backup media type** box, type **C:\backup.bkf** in the **Backup media or file name** box, and then click **Next**.
6. Click **Finish** and when prompted, insert a disk into drive A, and then click **OK**.
7. When prompted to remove the disk, click **OK**, and then close all windows.

Procedure for backing up System State data using ntbackup

To back up files by using **ntbackup**:

- At the command line prompt, type:

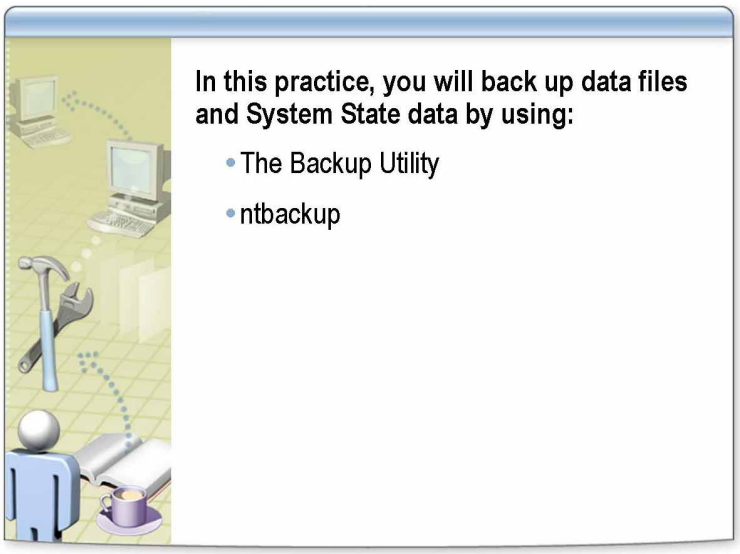
  ntbackup backup [systemstate] "@bks *file name*" **/J** {"*job name*"} [**/P** {"*pool name*"}] [**/G** {"*guid name*"}] [**/T** { "*tape name*"}] [**/N** {"*media name*"}] [**/F** {"*file name*"}] [**/D** {"*set description*"}] [**/DS** {"*server name*"}] [**/IS** {"*server name*"}] [**/A**] [**/V:**{**yes**|**no**}] [**/R:**{**yes**|**no**}] [**/L:**{**f**|**s**|**n**}] [**/M** {*backup type*}] [**/RS:**{**yes**|**no**}] [**/HC:**{**on**|**off**}] [**/SNAP:**{**on**|**off**}]

Parameter	Definition
systemstate	Specifies that you want to back up the System State data. When you select this option, the backup type is forced to normal or copy.
@bks *file name*	Specifies the name of the backup selection file (.bks file) to be used for this backup operation. The at (@) character must precede the name of the backup selection file. A backup selection file contains information about the files and folders you have selected for backup. You must create the file by using the graphical user interface (GUI) version of Backup.
/J {"*job name*"}	Specifies the job name to be used in the backup report. The job name usually describes the files and folders you are backing up in the current backup job.
/P {"*pool name*"}	Specifies the media pool from which you want to use media. This is usually a subpool of the Backup media pool, such as 4mm DDS. If you select this parameter, you cannot use the **/A**, **/G**, **/F**, or **/T** command-line options.
/G {"*guid name*"}	Overwrites or appends to this tape. Do not use this switch in conjunction with **/P**.
/T {"*tape name*"}	Overwrites or appends to this tape. Do not use this switch in conjunction with **/P**.
/N {"*media name*"}	Specifies the new tape name. Do not use **/A** with this switch.
/F {"*file name*"}	Logical disk path and file name. Do not use the following switches with this switch: **/P /G /T**.
/D {"*set description*"}	Specifies a label for each backup set.
/DS {"*server name*"}	Backs up the directory service file for the specified Microsoft Exchange server.
/IS {"*server name*"}	Backs up the Information Store file for the specified Microsoft Exchange server.
/A	Performs an append operation. Use either **/G** or **/T** with this switch. Do not use this switch in conjunction with **/P**.
/V:{**yes**|**no**}	Verifies the data after the backup is complete.
/R:{**yes**|**no**}	Restricts access to this tape to the owner or members of the Administrators group.
/L:{**f**|**s**|**n**}	Specifies the type of log file: **f**=full, **s**=summary, **n**=none (no log file is created).

(*continued*)

Parameter	Definition
/M {*backup type*}	Specifies the backup type. It must be one of the following: normal, copy, differential, incremental, or daily.
/RS:{**yes**|**no**}	Backs up the migrated data files located in Remote Storage. The **/RS** command-line option is not required to back up the local Removable Storage database that contains the Remote Storage placeholder files. When you back up the %systemroot% folder, Backup automatically backs up the Removable Storage database as well.
/HC:{**on**|**off**}	Uses hardware compression, if available, on the tape drive.
/SNAP:{**on**|**off**}	Specifies whether the backup should use a volume shadow copy.

Practice: Backing Up Data



Objective

In this practice, you will back up data files by using:

- The Backup utility
- The **ntbackup** command

Scenario

You are the systems administrator for an organizational unit on a large network. Your department manager is relying on you to be able to quickly restore the C:\MOC folder on the department server in case it is corrupted. The backup must be stored as D:\MOC.bkf.

Practice: Starting the Backup utility using Run as

► **Start the Backup utility by using Run as, and back up a folder**

1. Log on to the domain as *Computer***User** with a password of **P@ssw0rd** (where *Computer* is the name of your computer).
2. Open Windows Explorer, open the C:\Moc\2275\Practices\Mod03 folder, and then delete all swap.***** files.
3. On the **Start** menu, point to **All Programs**, point to **Accessories**, point to **System Tools**, right-click **Backup**, and then click **Run as**.
4. In the **Run as** dialog box, use **nwtraders/administrator** for the account name and **P@ssw0rd** for the password.
5. Click **Advanced Mode**, click the **Backup** tab, expand **Local Disk (C:)**, and then select the **MOC** check box.
6. Back up the C:\MOC folder as **D:\MOC.bkf**.
7. When the backup is complete, close all windows.

Practice: Backing up a folder by using ntbackup

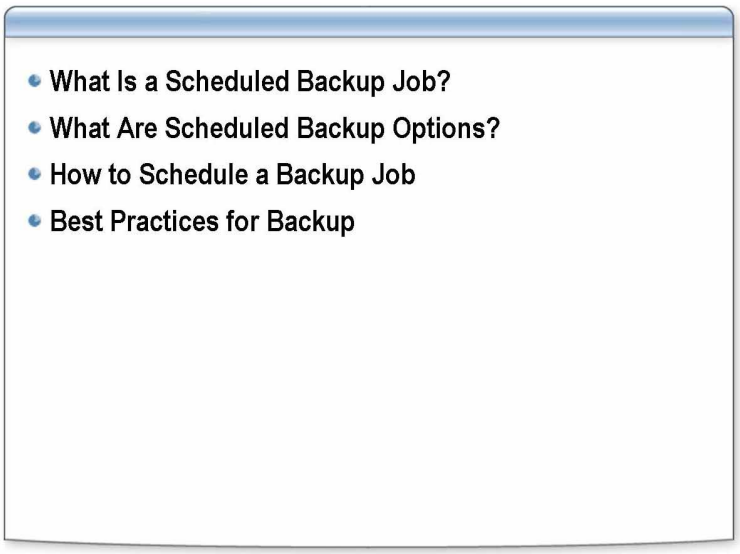
► **Back up a folder by using a ntbackup**

1. Open a command prompt with administrator credentials using the **runas** command.
2. In the command window, type:

   ntbackup backup C:\MOC /j ntbackup /f d:\MOC2.bkf

   This command backs up the C:\MOC folder as **D:\MOC2.bkf**.
3. When the backup is complete, close all windows and log off.

Lesson: Scheduling Backup Jobs



Introduction

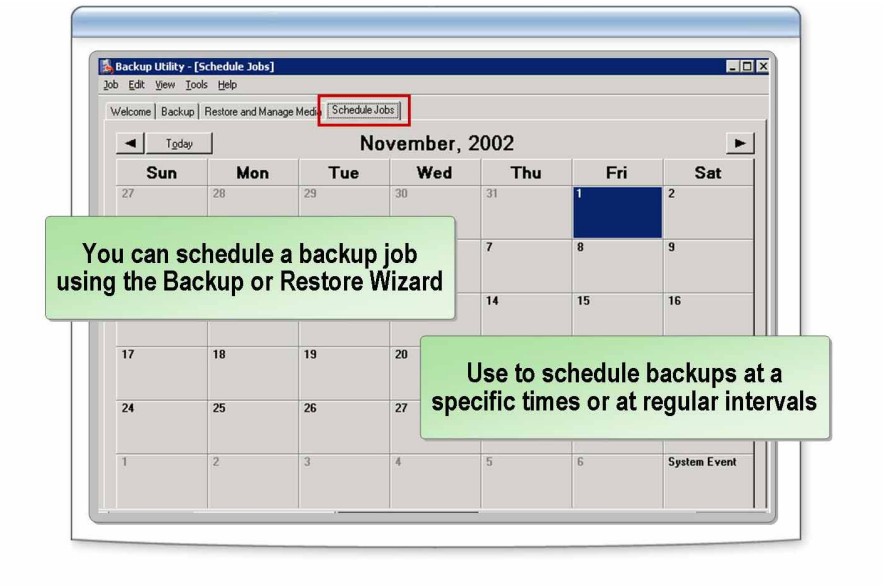
In addition to backing up files and folders, the responsibility of a systems administrator includes scheduling backups. Using your organization's backup plan, schedule your backups so that they contain the most complete and up-to-date set of files by using the least time-consuming method.

Lesson objectives

After completing this lesson, you will be able to:

- Explain a scheduled backup job.
- Describe backup schedule options.
- Schedule a backup job by using Backup.

What Is a Scheduled Backup Job?



Introduction

To keep backup files up-to-date without having to remember to back them up, you can schedule backup jobs. When you schedule a backup, you can always be sure that the backup copy is available for restoring the data if the original data is lost. You can set up a schedule when you create a backup job or you can create a schedule for an existing backup job.

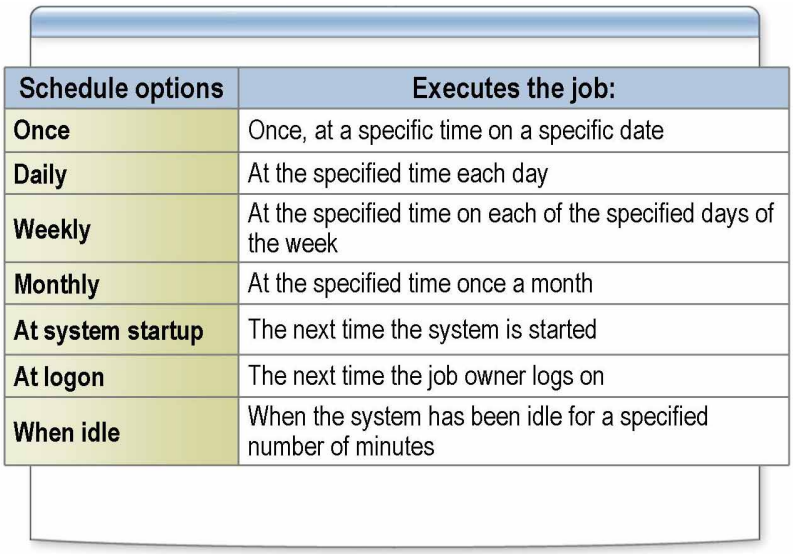
Two ways to schedule a backup job

Try to schedule a backup job to occur at regular intervals or during periods of relative inactivity on a network.

You can schedule a backup job two ways:

- When you create a new backup job in Backup.
- By using the **Scheduled Jobs** tab in Backup to schedule an existing backup job.

What Are Scheduled Backup Options?



Schedule options	Executes the job:
Once	Once, at a specific time on a specific date
Daily	At the specified time each day
Weekly	At the specified time on each of the specified days of the week
Monthly	At the specified time once a month
At system startup	The next time the system is started
At logon	The next time the job owner logs on
When idle	When the system has been idle for a specified number of minutes

Introduction

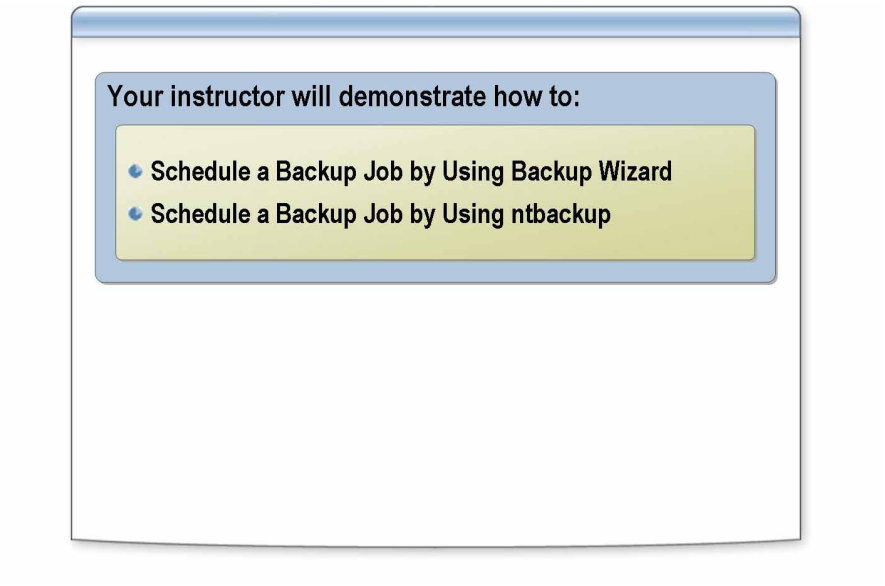
Windows Server 2003 provides several options to help you schedule your backup job.

Backup options

The following table describes the options that are available for scheduling backup jobs.

Schedule options	Executes the job:
Once	Once at a specific time on a specific date
Daily	At the specified time each day
Weekly	At the specified time on each of the specified days of the week
Monthly	At the specified time once a month
At system startup	The next time the system is started
At logon	The next time the job owner logs on
When idle	When the system has been idle for a specified number of minutes

How to Schedule a Backup Job



Introduction

You can schedule regular backups by using the Backup or Restore Wizard to keep your archived data up-to-date. You must be logged on as an administrator or a backup operator to schedule a backup job.

Procedure for scheduling a backup job using Backup or Restore Wizard

To schedule a backup job by using the Backup or Restore Wizard:

1. Open Backup, and then on the **Welcome** page of the Backup or Restore Wizard, click the **Advanced Mode** link.
2. In the **Backup Utility** dialog box, on the **Backup** tab, on the **Job** menu, click **New**.
3. Under **Click to select the check box for any drive, folder or file that you want to back up**, click the box next to each file or folder that you want to back up.
4. In the **Backup** destination box, do one of the following:
   a. Select **File** if you want to back up files and folders to a file.
   b. Select a tape device.
5. To select backup options, on the **Tools** menu, click **Options**, and then select the options that you want to use, such as backup type and log file type.
6. On the **Job** menu, click **Save Selections** to save your selections as a backup job file.
7. Click **Start Backup**, make any changes you want in the **Backup Job** Information dialog box, and then click **Schedule**.
8. In the **Set Account Information** dialog box, enter the user name and password that you want the scheduled backup to run under.
9. In the **Scheduled Job Options** dialog box, in the **Job name** box, type a name for scheduled backup job, and then, on the **Schedule data** tab, click **Properties** to set the date, time, and frequency parameters for the scheduled backup.

Procedure for scheduling a backup job by using ntbackup

To schedule a backup by using **ntbackup**:

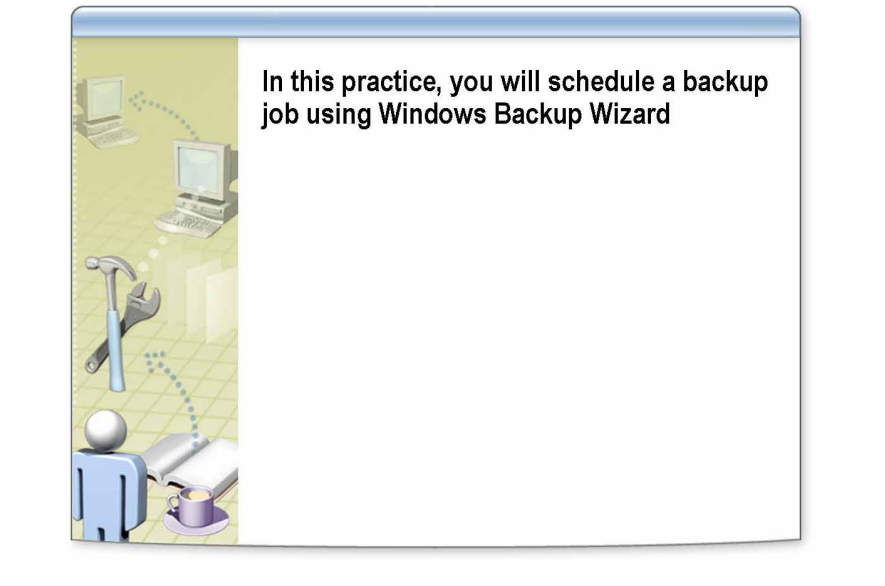
1. Open Notepad.
2. Type the following command:

   ntbackup backup "C:" /j "Command line backup 1"/f "d:\full.bkf"
3. Save the file as **backup.bat**.
4. Close Notepad.
5. Open a command prompt, and then type the following command:

   at 18:00 /every:M,T,W,TH,F backup.bat

   This command causes drive C to be backed up to D:\full.bkf on the server at 6:00 P.M. every Monday through Friday.

Practice: Scheduling a Backup Job



Objective

In this practice, you will schedule a backup job by using the Backup or Restore Wizard.

Scenario

You are the systems administrator for an organizational unit on a large network. Your manager wants you to schedule a backup of the C:\MOC folder every night at 11:30 P.M. You want to perform a test run during the day so that you can familiarize yourself with scheduling backups.

Practice

► **Schedule a backup job by using the Backup Wizard**

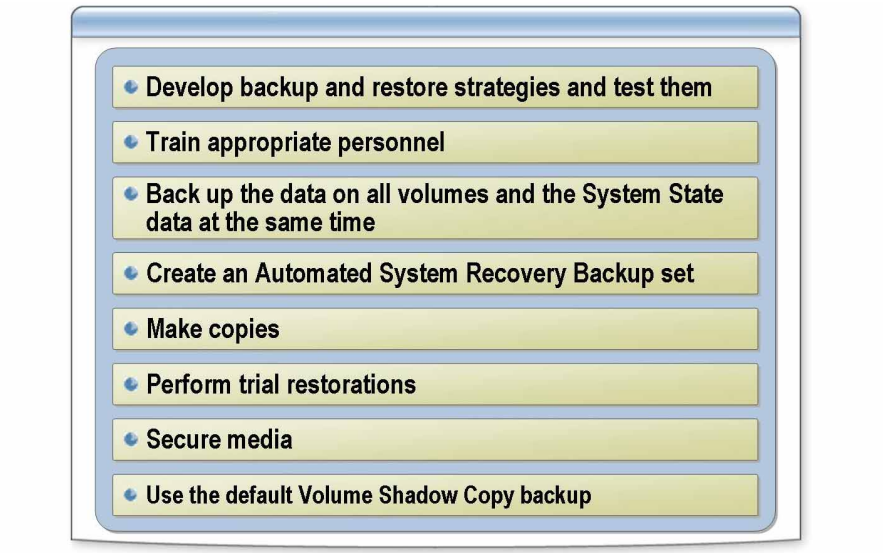
1. Log on to the domain as Administrator with a password of **P@ssw0rd**.
2. Start the Backup utility.
3. Click **Advanced Mode**, and then click **Backup Wizard**.

4. Use the following table to select the appropriate responses.

On the Backup Wizard page	Select
What to Back Up	**Back up selected files, drives, or network data**
Items to Back Up	Expand **My Computer**, expand **Local Disk (C:)**, and then select **MOC**
Backup Type, Destination, and Name	**Browse**
Save As	**Save in:** New Volume (D:)
	File name: MOC3.bkf
Completing the Backup Wizard	Click **Advanced**
Type of Backup	**Normal**
How to Back Up	**Verify data after backup**
Backup Options	**Replace the existing backups**
When to back up	When do you want to run the back up? **Later**
	Job name: **MOC3**
	Click **Set Schedule**
Schedule	Set the start time to begin 5 minutes from now
Set account information	Run as: nwtraders\administrator
	Password: **P@ssw0rd**
	Confirm password: **P@ssw0rd**
Completing the Backup Wizard	**Finish**

5. Use Microsoft Windows Explorer to verify that D:\MOC3.bkf is created.
6. Close all windows and log off.

Best Practices for Backup



Introduction

You can protect your organization from data loss by using a set of best practices when you develop your backup plan.

Best practices

Apply the following best practices when you develop your backup plan:

- Develop backup strategies and test them.

  A good plan ensures that you can quickly recover your data if it is lost.

- Train appropriate personnel.

  On minimum-security and medium-security networks, assign backup rights to one user, by using Group Policy, and assign restore rights to a different user. Train personnel with restore rights to perform all of the restore tasks if the administrator is unavailable.

  On a high-security network, only administrators should restore files.

- Back up the data on all volumes and the System State data at the same time. This action allows you to be prepared in the unlikely event of a disk failure.

- Create an Automated System Recovery backup set.

  Always create an Automated System Restore (ASR) backup set when the operating system changes, for example, whenever you install new hardware and drivers or apply a service pack. An ASR backup set can help you to recover from a server failure. ASR protects only the System State files; you must back up data volumes separately.

- Create a backup log.

  Always create a backup log for each backup, and then print the logs for reference. Keep a book of logs to help you locate specific files. The backup log is helpful when you restore data; you can print it or read it from any text editor. Also, if the media containing the backup set catalog is corrupted, the printed log can help you locate a file.

- Make copies.

  Keep at least three copies of the media. Keep at least one copy off-site in a properly controlled environment.

- Perform trial restorations.

  Perform a trial restoration periodically to verify that your files are properly backed up. A trial restoration can uncover hardware or media corruption problems that do not show up when you verify software.

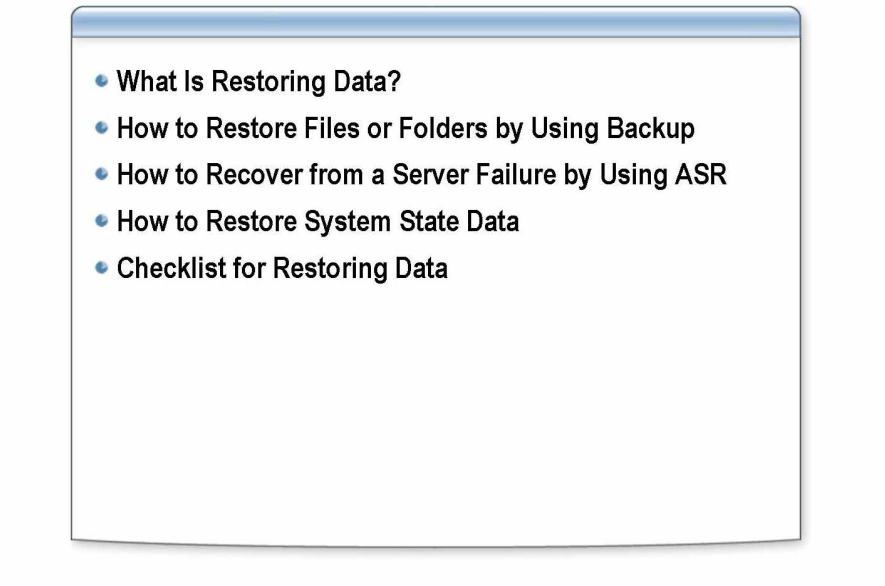
- Secure media.

  Secure the media. It is possible for someone to access the data from a stolen medium by restoring the data to another server for which they are an administrator.

- Use the default Volume Shadow Copy backup.

  Do not disable the default Volume Shadow Copy backup method. If you disable this method, open files that are being used by the system during the backup process will be skipped during the backup.

Lesson: Restoring Data



Introduction

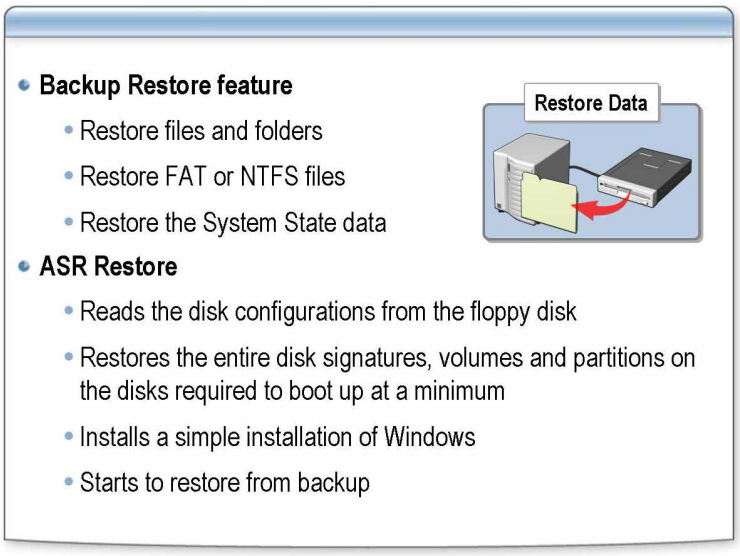
The second part of the disaster recovery process involves restoring the data that you backed up during the first part of the process.

Lesson objectives

After completing this lesson, you will be able to:

- Explain how to restore data.
- Restore System State data.
- Restore files and folders by using Backup.
- Restore data by using ASR.
- Explain guidelines for restoring data.

What Is Restoring Data?



Introduction

When you use Backup to create a duplicate copy of the data on your hard disk and then archive the data on another storage device, such as a hard disk or a tape, you can use the Restore feature in Backup to easily restore the data.

Restore files and folders

Using Backup, you can restore the archived files and folders to your hard disk or any other disk that you can access.

Back up and restore data on FAT or NTFS

You can use Backup to back up and restore data on either FAT (file allocation table) or NTFS file system volumes. However, if you backed up data from an NTFS volume that is used in Windows Server 2003, it is recommended that you restore the data to an NTFS volume used in Windows Server 2003. If you do not, you may lose data and some file and folder features, such as permissions, Encrypting File System (EFS) settings, disk quota information, mounted drive information, and Remote Storage information.

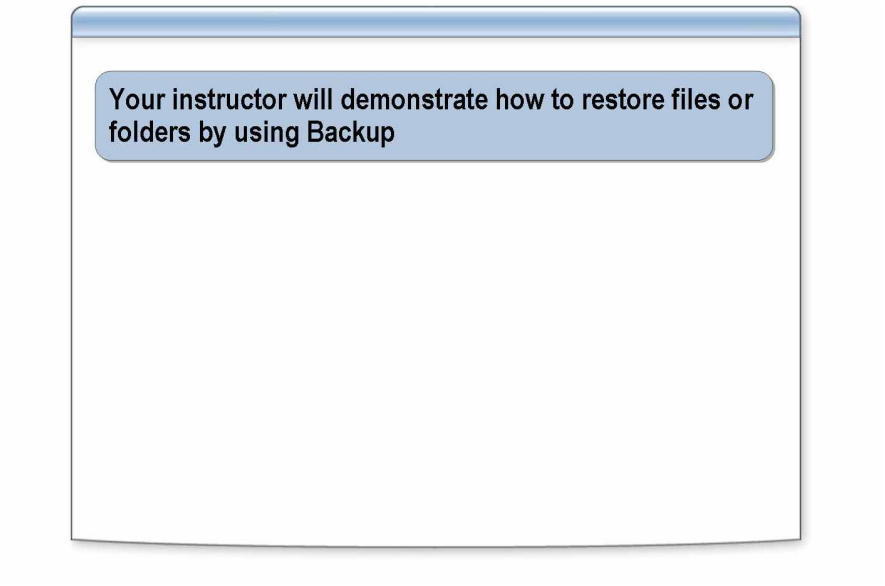
Restore System State data

You can use Backup to restore the System State data. If the System State data was backed up on a computer and that computer system fails, you can rebuild the computer with the original Windows Server 2003 compact disc and the System State data.

ASR Restore

You can access the restore part of ASR by pressing F2 when prompted in the text mode portion of Windows setup. ASR reads the disk configurations from the floppy disk and restores the entire disk signatures, volumes, and partitions on the disks that are required to start the computer. ASR then installs a simple installation of Windows and automatically starts to restore from backup by using the ASR backup set that you created by using the ASR wizard.

How to Restore Files or Folders by Using Backup



Introduction

In Backup, when you click the **Restore and Manage Media** tab, the tapes, files, and backup sets from which you can restore data are displayed in a tree view. You can restore complete sets of folders and files or individual files and folders.

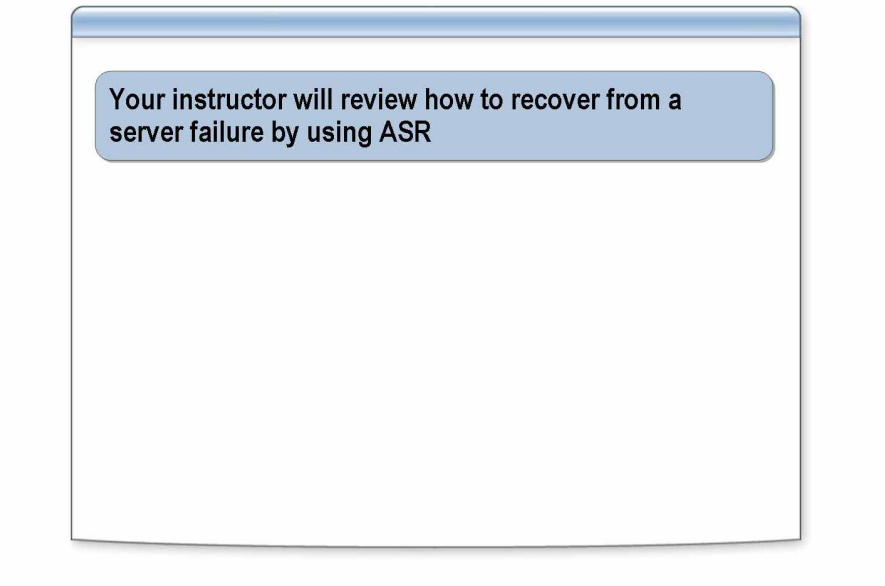
Procedure

To restore files or folders by using Backup:

1. Open Backup, and then on the **Welcome** page of the Backup or Restore Wizard, click the **Advanced Mode** link.
2. In the Backup Utility–[Untitled] window, click the **Restore and Manage Media** tab.
3. In the left pane, expand **File**, expand the desired media item, and then select the check box for the items to be restored.
4. In the **Restore files to** box, do one of the following:
   a. Click **Original location** if you want the backed up files and folders to be restored to the folder or folders they were in when they were backed up.
   b. Click **Alternate location** if you want the backed up files and folders to be restored to a folder that you designate. This option preserves the folder structure of the backed up data; all folders and subfolders appear in the alternate folder that you designate.
   c. Click **Single folder** if you want the backed up files and folders to be restored to a folder that you designate. This option does not preserve the folder structure of the backed up data; the files appear only in the folder that you designate.

5. If you selected **Alternate location** or **Single folder**, type a path for the folder under **Alternate location**, or click **Browse** to find folder.
6. On the **Tools** menu, click **Options**, and then on the **Restore** tab, do one of the following:
   - Click **Do not replace the file on my computer**.
   - Click **Replace the file on disk only if the file on disk is older**.
   - Click **Always replace the file on my computer**.
7. Click **OK** to accept the restore options that you have set.

How to Recover from a Server Failure by Using ASR



Introduction

During backup, ASR creates a floppy disk that you can use to restore disk signatures, volumes, and partitions on the disks that are required to start the computer. By using the ASR floppy disk, you can install a simple installation of Windows. Backup automatically begins to restore your operating system by using the ASR wizard after the simple Windows installation is complete.

Remember that ASR does not include data files. After you restore your operating system, you can restore data files by using the backup files that you created during your scheduled backups.

Procedure

To recover from a server failure by using ASR:

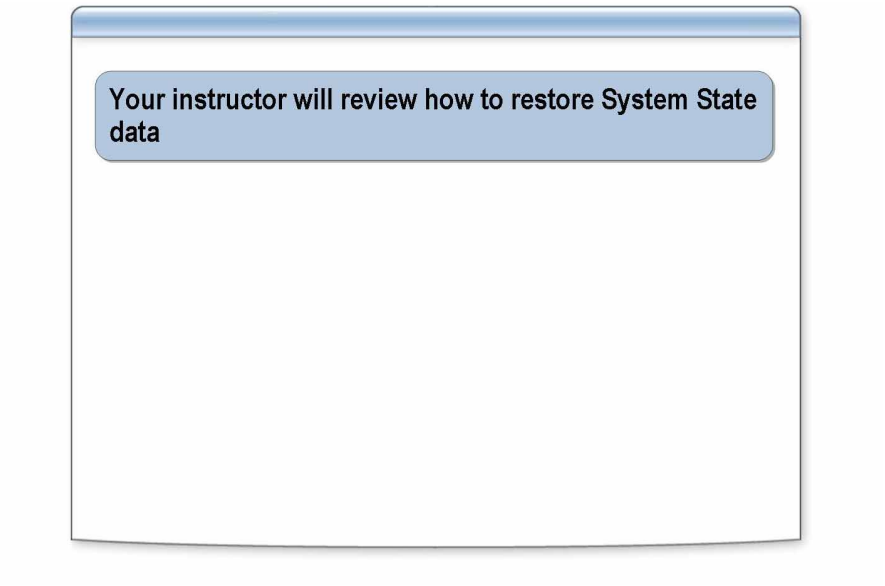
1. Make sure the following items are available before you begin the recovery procedure:
   - Previously created ASR floppy disk.
   - Previously created backup media.
   - Original installation compact disc for the operating system.
   - If you have a mass storage controller and an updated driver (different from the driver on the Setup compact disc) is available from the manufacturer, before you begin this procedure, obtain the updated driver on a floppy disk.
2. Insert the original installation compact disc for the operating system into your CD-ROM drive.
3. Restart your computer. If prompted to press a key to start the computer from the compact disc, press the appropriate key.
4. If you have a separate driver file as described in step 1, use the driver as part of Setup by pressing F6 when prompted.

5. At the beginning of the text-only mode section of Setup, press F2 when prompted.

   You are prompted to insert the ASR floppy disk that you previously created.

6. Follow the directions on the screen.
7. If you have a separate driver file as described in step 1, press F6 a second time when prompted after the system restarts.
8. Follow the directions on the screen.

How to Restore System State Data



Introduction

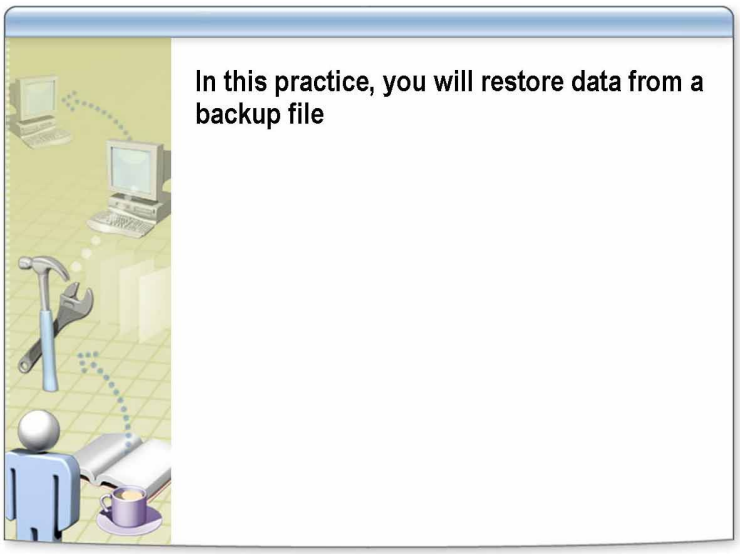
When you restore System State data, the current version of your System State data is replaced with your restored version. Also, you cannot choose where to restore the System State data. Backup determines the appropriate location for restoring the System State data based on the location of your current systemroot directory.

Procedure

To restore System State data by using Backup:

1. Open Backup, and then on the **Welcome** page of the Backup or Restore Wizard, click the **Advanced Mode** link.
2. On the **Restore and Manage Media** tab, expand the desired media item, and then click the box next to **System State**.

Practice: Restoring Data



Objective

In this practice, you will restore data from a backup file.

Scenario

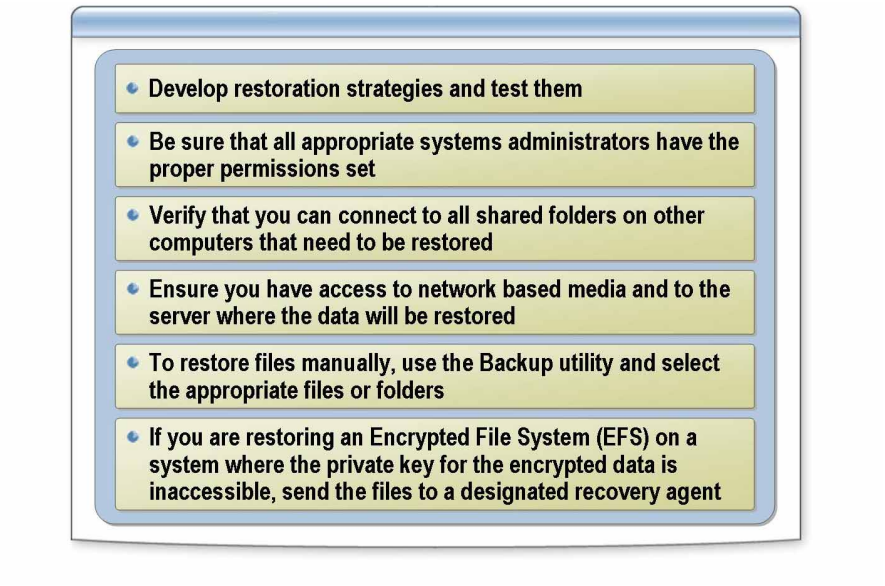
You are the systems administrator for an organizational unit on a large network. You receive an emergency call from a manager, because one of his users accidentally deleted most of the files in a database folder named VSS. You must restore the deleted files as soon as possible.

Practice

► **Restore the data from the backup file**

1. Log on to the domain as *Computer***User** with a password of **P@ssw0rd**.
2. Open Windows Explorer, and then delete the C:\MOC folder.
3. Start Backup by using **Run as**, and then click **Advanced Mode**.
4. On the **Restore and Manage Media** tab, expand **File**, expand **MOC.bkf**, select the **C:** check box, and then click **Start Restore**.
5. When "Restore is complete" appears in the **Restore Progress** dialog box, click **Close**, and then close the Backup utility.
6. In Windows Explorer, press F5 to refresh the screen, and then verify that the MOC folder appears under **Local Disk (C:)**.
7. Close all windows and log off.

Checklist for Restoring Data



Introduction

After you back up your files to the storage media and follow the best practices for developing a backup plan, you must create a restoration plan. It is recommended that you use the following checklist when you create your organization's restoration plan.

Checklist for restoring data

Apply the following best practices when you create a restoration plan:

- Develop restoration strategies and test them.

  Remember to keep a record of your backup and restoration plans to refer to in the event of data loss.
- Be sure that all appropriate systems administrators have the proper permissions set.
- Verify that you can connect to all shared folders on other computers that must be restored.

  You can use the default user rights of the Backup Operators group to restore your organization's data and system files, or you can segregate backup and restore permissions by individuals.
- Test all shared folders on all servers for which you are responsible to make sure that you can restore data contained in them.
- Ensure that you have access to network-based media and to the server where the data will be restored.

  As part of your restoration plan, be sure that you test your access to the storage media where you backed up your files.

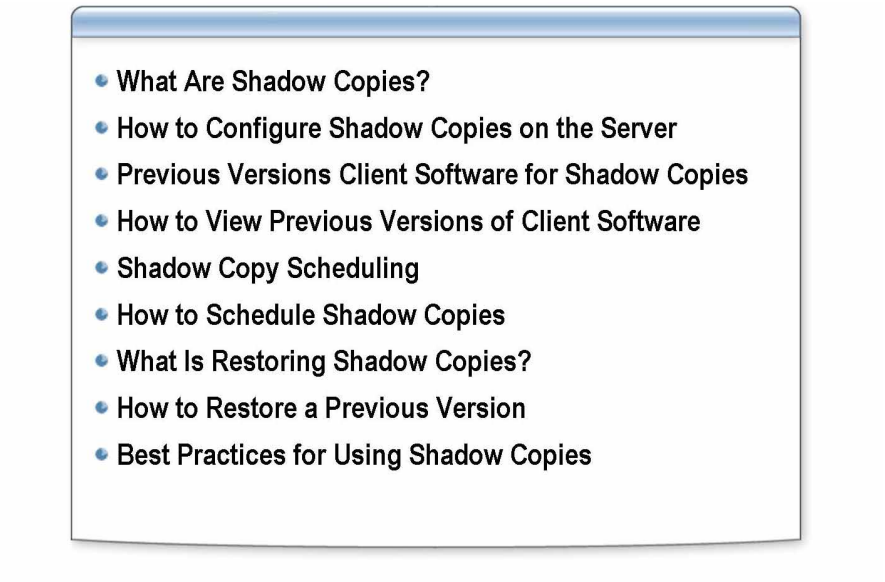
- To restore files manually, use the Backup utility and select the appropriate files or folders.

  Because you may need to restore only certain files, test the procedure that you will use to select and restore only those files, using the Backup utility.

- If you are restoring EFS files on a system where the private key for the encrypted data is inaccessible, send the files to a designated recovery agent.

  For files that are encrypted for security and are therefore inaccessible, perform a test by sending the files to a designated recovery agent. Ensure that you can copy and open all files.

Lesson: Configuring Shadow Copies



Introduction

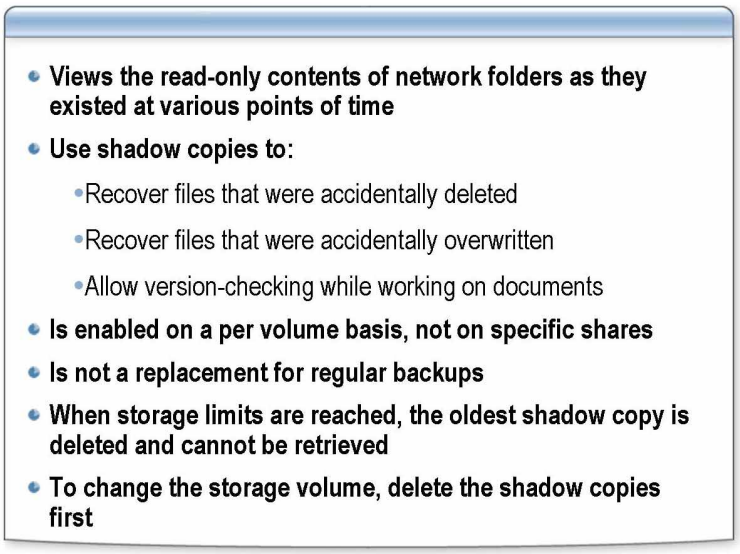
In Windows Server 2003, you can use Shadow Copies of Shared Folders as a data recovery tool. You can use shadow copies to view and restore shared files and folders as they existed at previous points in time.

Lesson objectives

After completing this lesson, you will be able to:

- Explain shadow copies.
- Configure a shadow copy.
- Describe the Previous Versions client software for shadow copies.
- View previous versions of client software.
- Explain scheduling shadow copies.
- Create a shadow copy schedule.
- Explain restoring shadow copies.
- Restore a previous version.
- Explain best practices for using shadow copies.

What Are Shadow Copies?



Definition

A shadow copy is a feature of the Windows Server 2003 family that provides point-in-time, read-only copies of files on network shares. With Shadow Copies of Shared Folders, you can view the contents of network folders as they existed at various points in time. To view Shadow Copies of Shared Folders, you must install the client software.

Shadow copy scenarios

You can use shadow copies in the following three scenarios:

- Recover files that were accidentally deleted.

  This scenario is the network equivalent of a short-term local backup and restore. If a user accidentally deletes a file, the user can open a previous version of the file and copy it to a safe location.

- Recover files that were accidentally overwritten.

  Shadow Copies of Shared Folders can be very useful in environments where new files are commonly created by opening an existing file, making modifications, and then saving the file with a new name. For example, you might open a financial modeling spreadsheet, make modifications based upon new assumptions, and then save the spreadsheet with a new name to create a new spreadsheet. The problem arises when you forget to save the file by using a new name, thereby erasing the original work. You can use Shadow Copies of Shared Folders to recover the previous version of the file.

- Allow version-checking while working on documents.

  You can use Shadow Copies of Shared Folders during the normal work cycle to check the differences between two versions of a file. For example, you might want to know "What did this paragraph say this morning before I started to rewrite it?"

Shadow copy characteristics

The following characteristics apply to shadow copies:

- Configuring shadow copies is not a replacement for creating regular backups.
- Shadow copies are read-only. You cannot edit the contents of a shadow copy.
- Shadow copies are enabled on a per volume basis. You cannot enable shadow copies on specific shared resources.
- After shadow copies are enabled on a volume, shadow copies are enabled for all shared folders on that volume.

Shadow copies storage

The minimum amount of storage space for shadow copies is 100 megabytes (MB). The default maximum storage size is 10 percent of the source volume or the volume being copied, but you can change the maximum size at any time. When the storage limit is reached, the oldest versions of the shadow copies are deleted and cannot be restored.

Allocate storage space

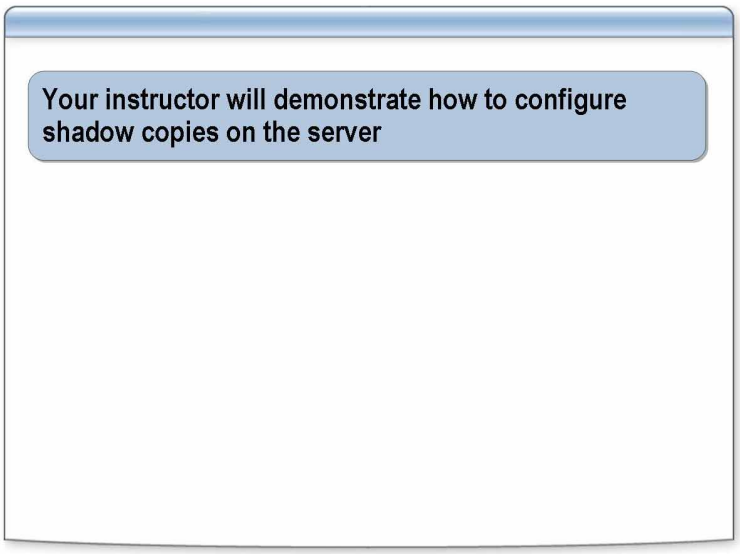
When determining the amount of space to allocate for storing shadow copies, you must consider both the number and size of files that are being copied, as well as the number of times that the shadow copies are to be copied to the disk.

Store shadow copies on a different volume

You can also store shadow copies on a different storage volume. However, changing the storage volume deletes the shadow copies. To avoid this problem, verify that the storage volume that you initially select is large enough to handle your growing business needs.

Note For more information about shadow copies, go to the Microsoft Technet Services Web site at http://www.microsoft.com/windowsserver2003/docs /VolumeShadowCopyService.swf.

How to Configure Shadow Copies on the Server



Introduction

By default, shadow copies are disabled. You can enable shadow copies on the server by completing the following steps, but shadow copies is not enabled on the client computer until the client software for shadow copies is installed on the client computer.

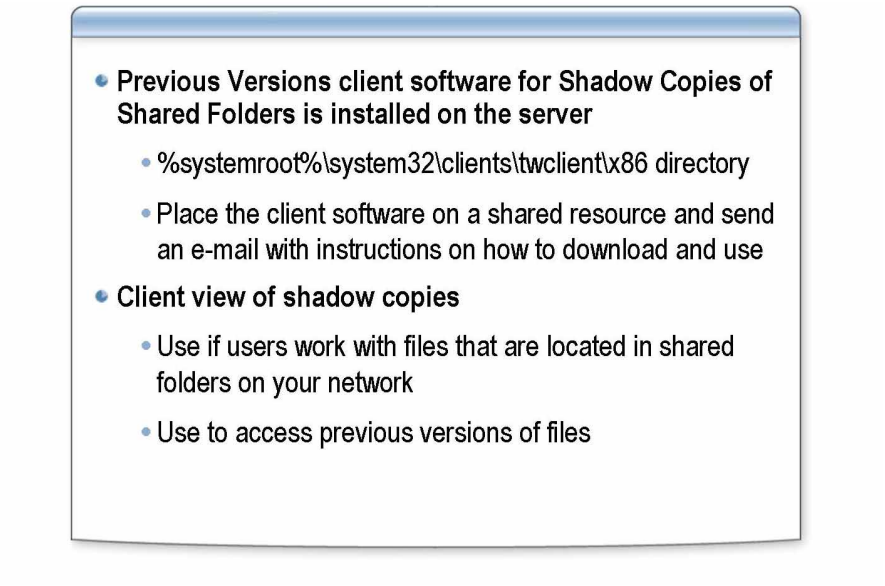
Before you deploy Shadow Copies of Shared Folders, it is recommended that you create a plan that specifies the location and storage limits of the shadow copies. The default storage size is 10 percent of the source volume.

Procedure

To configure shadow copies:

1. In Computer Management (Local), in the console tree, right-click **Shared Folders**, point to **All Tasks**, and then click **Configure Shadow Copies**.
2. Select the volume where you want to enable Shadow Copies of Shared Folders, click **Enable**, and then click **Yes** when prompted to enable shadow copies.

Previous Versions Client Software for Shadow Copies



Introduction

Before users can use and access shadow copies, they must install the client software for shadow copies. The client software allows users to access previous versions of their files and folders from a shared folder.

Previous versions on client computers

Shadow copies are copies of files that are located on the server and appear as previous versions on the client computers. Shadow copies can be used on both servers and clients to view and locate previous versions of files. Both views are created by the systems administrator.

Locations of shadow copy views

The locations of the shadow copies for both views are as follows:

- The server portion of Shadow Copies of Shared Folders is located on the **Shadow Copies** tab of the **Local Disk Properties** dialog box.
- The client view of the shadow copies is referred to as **Previous Versions** and is located in the **Properties** dialog box of the shared folder.

Client software for shadow copies

The client software for shadow copies is installed on the server in the %systemroot%\system32\clients\twclient\x86 directory. You can distribute the client software in a variety of ways; consider the various options before deployment. Windows Server 2003 provides several tools, such as Group Policy, that can make deploying and maintaining the client software easier.

Alert users

It is recommended that you place the client software on a shared resource and then send an e-mail message to users that describes the function of the software and how to install it.

For example, you may want to inform users that:

- A new feature, Previous Versions, is enabled on the following file server: *server**sharedresource*.
- Files are scheduled to be copied at 7:00 A.M. and noon, Monday through Friday. Remember that these are copies of the files as they exist at these times and do not reflect any changes that are made to the files after these times.
- Saving your work frequently is still the best way to ensure that your work is not lost.
- To install the software, go to *server**sharedresource* and double-click **twclient.msi**.

Helps recover files for users

Accessing previous versions of files is useful because you can:

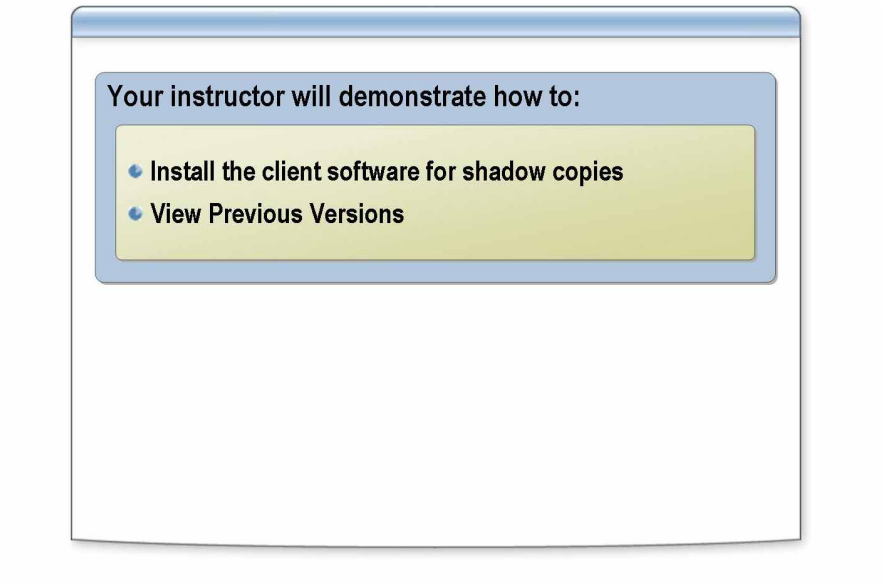
- Recover files that were accidentally deleted. If you accidentally delete a file, you can open a previous version and copy it to a safe location.
- Recover files that were accidentally overwritten. If you accidentally overwrite a file, you can recover a previous version of the file.
- Compare versions of file while working. You can use previous versions when you want to check what has changed between two versions of a file.

Other distribution methods

You can use Group Policy to install the client software for shadow copies.

Note For more information about installing software using Group Policy, see Course 2279*, Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*.

How to View Previous Versions of Client Software



Introduction

Before a user can view a previous version of a file or folder, you must install the client software for shadow copies on the user's computer. Use the following procedures to install the client software and view the previous versions.

Procedure for installing Previous Versions client software

To install client software for shadow copies on a client computer:

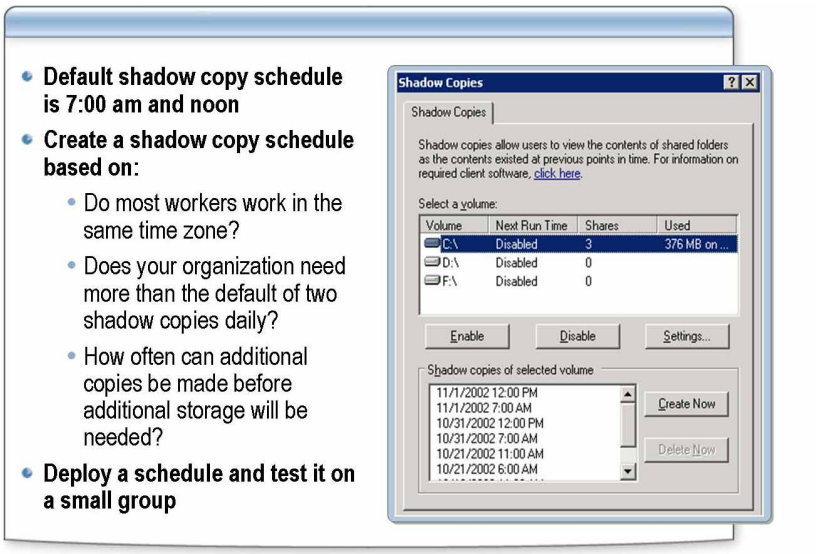
1. On the command line, type **\windows\system32\clients\twclient\x86\twcli32.msi** and then press ENTER.
2. In the Previous Versions Client Setup Wizard, click **Finish**.

Procedure for viewing previous versions

To view the previous version of a file or folder:

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type *Computername***Share** (where *Computername* is the name of the server hosting shadow copies).
3. Right-click any file or folder, and then click **Properties**.
4. Click the **Previous Versions** tab.

Shadow Copy Scheduling



Introduction

When you enable Shadow Copies of Shared Folders, a default schedule is also created. Although this schedule may work for your organization, evaluate the work habits of your users before you use the default schedule.

Create a shadow copy schedule

When you create a shadow copy schedule, consider the location of your users. The default schedule is 7:00 A.M. and noon, daily. If users are located across multiple time zones, you probably need to create more than the default of two shadow copies per day.

If you increase the number of scheduled shadow copies, consider how often copies can be added without requiring additional storage. Before deploying Shadow Copies of Shared Folders, it is recommended that you create a plan that specifies where to store the shadow copies and what the storage limits are. You can store up to 64 shadow copies per volume. When this limit is reached, the oldest shadow copy is deleted and cannot be retrieved.

Deploy a small test group

You may want to create an initial schedule and deploy it for a small group to test whether your schedule creates enough shadow copies while staying within your storage limits. Also, consider asking your users about their work habits and when they think that a shadow copy would be beneficial. For example, knowing that they make most of their errors in the late afternoon or first thing in the morning can help you determine the best schedule for your specific users.

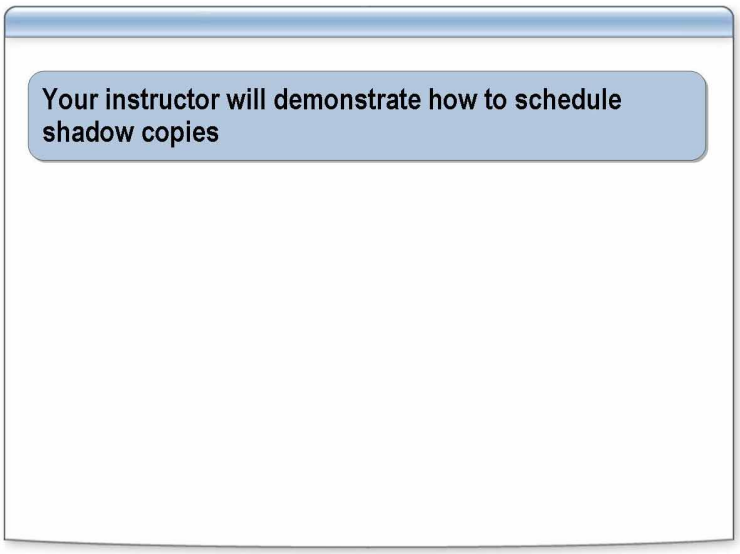
Scenario

You have enabled Shadow Copies for Shared Folders on all file servers and are using the default schedule. Your organization has a flexible schedule that allows employees to work any time between 8:00 A.M. and 6:00 P.M., as long as they work 8 hours a day. Many users create files between noon and 6:00 P.M.

Question: Are these files protected by shadow copies if users save them every hour?

Answer: The files of users who modify and save their files between noon and 6:00 P.M. are not saved by shadow copies until 7:00 A.M. the next day. To protect their files, set up a schedule to create shadow copies of their files every hour from 8:00 A.M. to 6:00 P.M. every weekday. Depending on storage limits, this schedule provides the users with up to five days of shadow copies.

How to Schedule Shadow Copies



Introduction

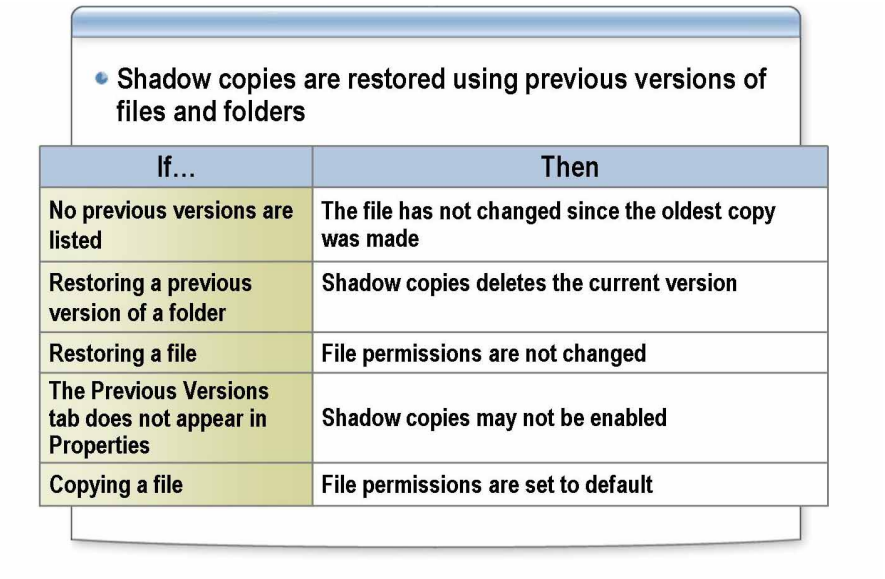
You can create a shadow copy schedule to automatically provide copies of files as they appear at various points of time. You can use shadow copies as another option for providing a backup of files that you can to recover from data loss.

Procedure

To create a shadow copy schedule:

1. In Computer Management, in the console tree, right-click **Shared Folders**, point to **All Tasks**, and then click **Configure Shadow Copies**.
2. Under **Select a volume**, click the volume for which you want to create a schedule, and then click **Settings**.
3. In the **Settings** dialog box, click **Schedule**, and then change the settings as appropriate.

What Is Restoring Shadow Copies?



Introduction

After you create a shadow copy, you can use it to restore shared files and folders to a previous version.

Note You can only restore a shadow copy from a client.

Restored files and folders using previous versions

If no previous versions are listed on the Previous Versions tab, the file has not changed since the oldest copy was made.

When you restore a previous version of a folder, files in the current folder that were not in the previous version of the folder are overwritten. If you do not want to delete the current version, use **Copy** to copy the previous version to a different location.

Example of a previous version folder

For example, the current version of a folder contains files A, B, and C. The previous version of the folder contained only files A and B. After you restore the previous version, the folder contains the previous version of file A, the previous version of file B, and the current version of file C.

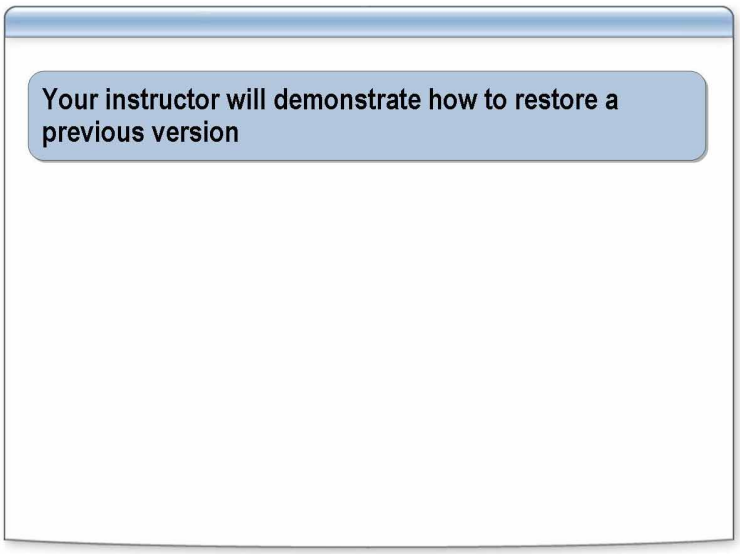
File permissions are not changed

When you restore a file, the file permissions are not changed. Permissions remain the same as they were before you restored the file. When you copy a previous version of a file, the permissions are set to the default permissions for the directory where the copy of the file is placed.

Restoring overwrites the current version

Restoring a previous version overwrites the current version. If you restore a previous version of a folder, the folder is restored to its state at the date and time that you selected. Any changes that you made to files in the folder before that time are lost.

How to Restore a Previous Version



Introduction

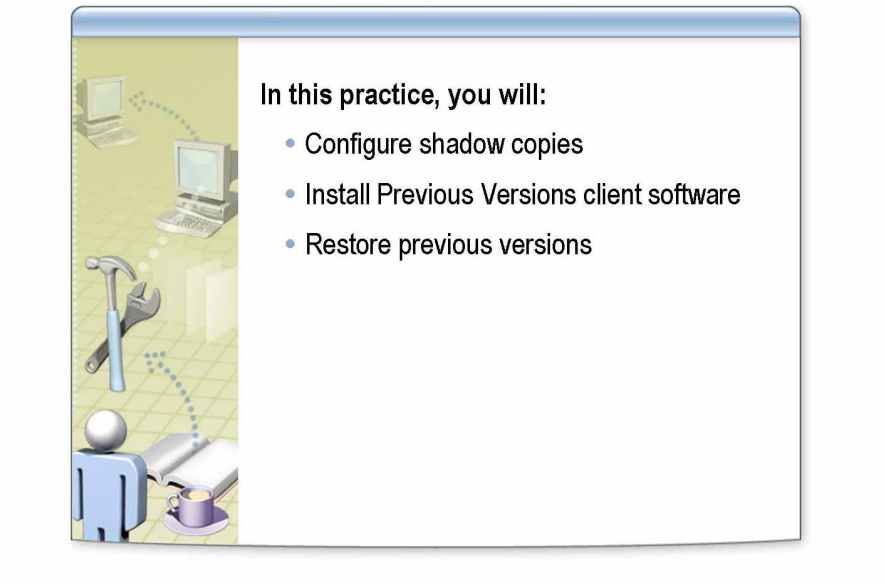
You can restore data from previous versions of files and folders, assuming that the client software is installed on a computer running Windows XP (client) or Windows Server 2003, and you configured the volumes for which you want to create shadow copies.

Procedure

To restore shadow copies:

1. In Windows Explorer, locate the file or folder that you want to restore, right-click the icon, and then click **Properties**.
2. In the **Properties** dialog box, on the **Previous Versions** tab, select the version that you want to restore, and then click **Restore**.

Practice: Configuring Shadow Copies



Objective

In this practice, you will:

- Configure shadow copies
- Install Previous Versions client software
- Restore previous versions

Scenario

You are the systems administrator for an organizational unit on a large network. Users who work with shared folders on the department server frequently complain about file corruption caused by other users.

For example, a user who is working on a Microsoft PowerPoint® presentation asks a colleague to review the presentation. After the colleague reviews the presentation, the user reopens the file and finds that some of the slides are corrupted or missing. The IT department cannot restore the file, so the user must re-create the missing slides. To provide users a way to recover previous versions of their work, you decide to configure a shadow copy of the shared folder to solve the problem.

Practice: Configuring shadow copies

► **Configure shadow copies on drive C**

1. Log on to the domain as *Computer***User** with a password of **P@ssw0rd**.
2. In the **Run** dialog box, use the **runas** command to start Computer Management with administrator privileges by typing:

   runas /user:nwtraders\administrator "mmc %windir%\system32 \compmgmt.msc"
3. Expand **Computer Management**, expand **System Tools**, right-click **Shared Folders**, point to **All Tasks**, and then click **Configure Shadow Copies**.
4. Enable shadow copies for the C:\ volume.
5. Click **Settings**, click **Schedule**, click **Advanced**, schedule shadow copies to made every minute of every day, and then save your changes.

6. In Computer Management, expand **Shared Folders**, right-click **Shares**, and then click **New Share**.
7. Share the C:\MOC\2275\Practices\Mod07 folder as **Mod07**.
8. In Computer Management, click **Shares**, right-click **Mod07**, and then click **Properties**.
9. Allow *Computer***User** to have full control on the Mod07 folder for both share permissions and NTFS permissions.

Practice: Installing Previous Versions client software

► **Install Previous Versions client software**

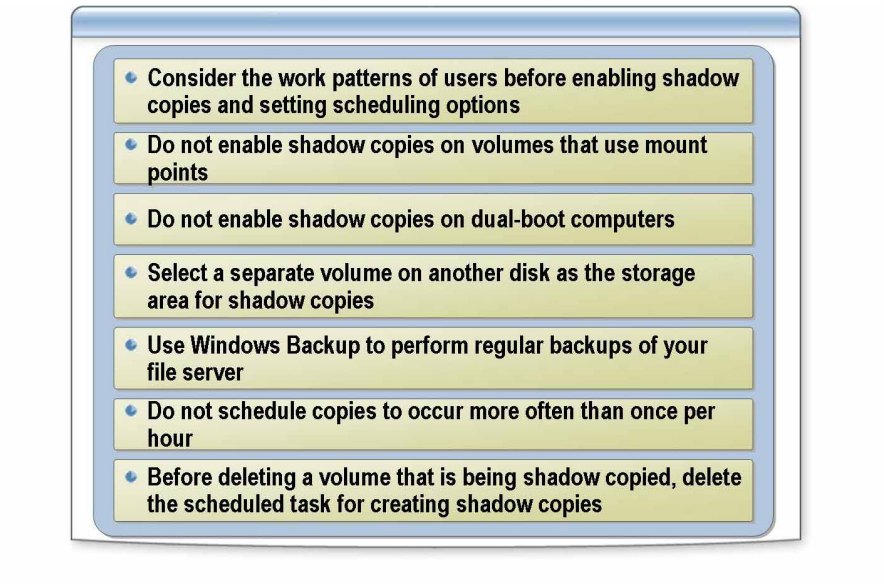
1. Using **runas**, start a command prompt with administrator privileges.
2. Install the Previous Versions client software, located at windows\system32\clients\twclient\x86\twcli32.msi.

Practice: Restoring a previous version

► **Restore a previous version**

1. Open the **Run** dialog box.
2. Open Mod07 by using the Universal Naming Convention (UNC) for your computer, by typing *Computer***Mod07** and then pressing ENTER.
3. Open the Test folder, and then open Shadow.txt.
4. On the first line, replace “Best practices” with “changed text”.
5. Save your work, and then close Shadow.txt.
6. Open the **Properties** dialog box for Shadow.txt.
7. On the **Previous Versions** tab, restore the previous version of the file and then close the dialog box.
8. Open Shadow.txt and verify that “Best practices” appears in the first line of the restored version of the file.
9. Close all windows and log off.

Best Practices for Using Shadow Copies



Introduction

Shadow copies can help you restore lost or corrupted data files. It is still a good idea, however, to maintain your regular backup file schedules.

Best practices

Consider the following best practices when you configure shadow copies and create a shadow copy schedule:

- Adjust the shadow copy schedule to fit the work patterns of your users.
- Do not enable shadow copies on volumes that use mounted drives.

  The mounted drives are not included when shadow copies are made. Enable shadow copies only on volumes without mount points or when you do not want to make shadow copies of the shares on the mounted volume.
- Do not enable shadow copies on computers with a dual-boot configuration.

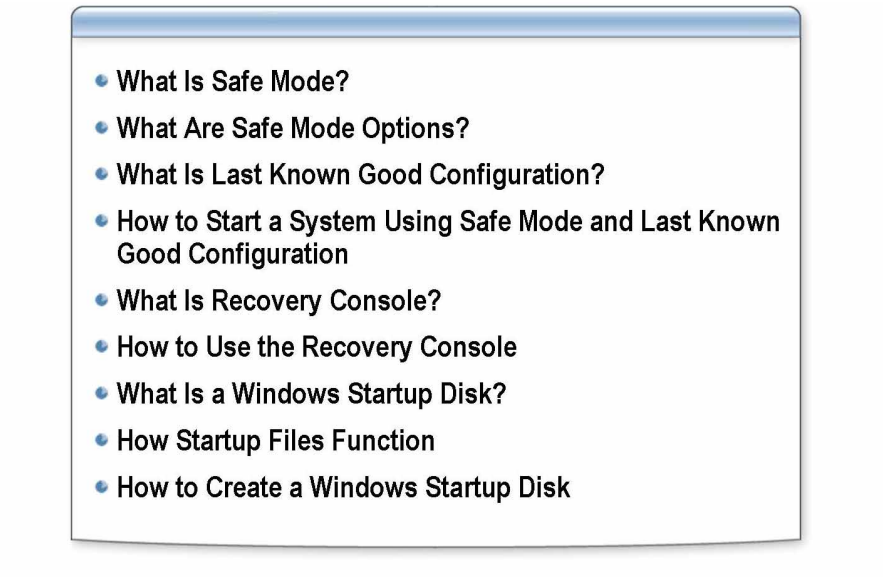
  If you have enabled a dual-boot configuration on a computer running an earlier operating systems (such as Microsoft Windows NT® 4.0) the shadow copies that persist during the reboot may be corrupted and unusable when the computer is started in Windows Server 2003.
- Select a separate volume on another disk as the storage area for shadow copies.

  Using a separate volume on another disk provides better performance and is recommended for heavily used file servers.
- Creating shadow copies does not replace performing regular backups.

  Use Backup in coordination with shadow copies to provide your best restoration scenario.

- Do not schedule copies to occur more often than once per hour. The default schedule is set for 7:00 A.M. and noon. If you decide that you need copies to be made more often, make sure you allot enough storage space and that you do not schedule copies to be made so often that server performance is degraded.
- If you delete the volume but not the shadow copy task, the scheduled task fails and an Event ID: 7001 error is written to the event log. Delete the shadow copy task before deleting the volume to avoid filling the event log with these errors.

Lesson: Recovering from Server Failure



Introduction

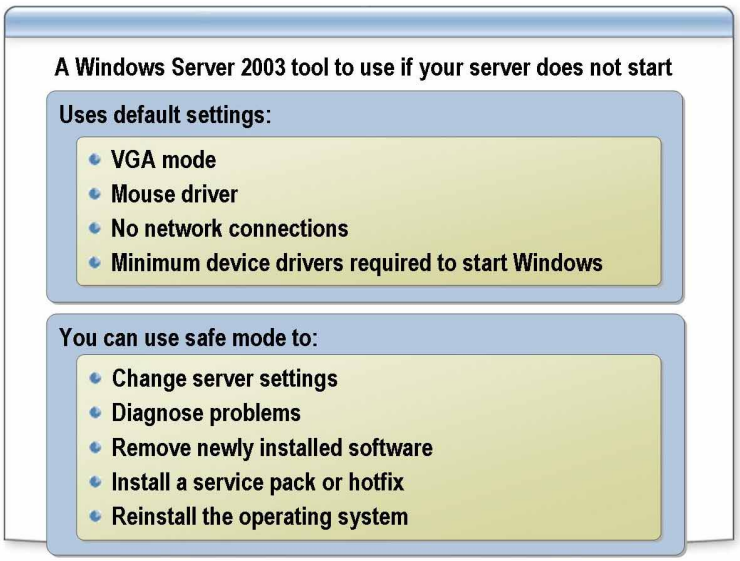
If a server fails, Windows Server 2003 provides several options that you can use to restore the computer. Understanding these options and their functions can help you to restore a server to working condition.

Lesson objectives

After completing this lesson, you will be able to:

- Explain safe mode and when to use it.
- Describe safe mode options.
- Explain Last Known Good Configuration and when to use it.
- Start a computer by using safe mode and Last Known Good Configuration.
- Explain the Recovery Console and when to use it.
- Use the Recovery Console.
- Describe the Windows startup disk.
- Describe how startup files function.
- Create a Windows startup disk.

What Is Safe Mode?



Definition

If your computer does not start, you may be able to start it in safe mode. In safe mode, Windows uses default settings, video graphics adapter (VGA) mode, the mouse driver, no network connections, and the minimum device drivers that are required to start Windows.

There are three safe mode options. You must log on in all modes, either by using the domain administrator account or by using the local Security Accounts Manager administrator account, depending on which safe mode option you select. Network connections are available in safe mode depending on the option that you use.

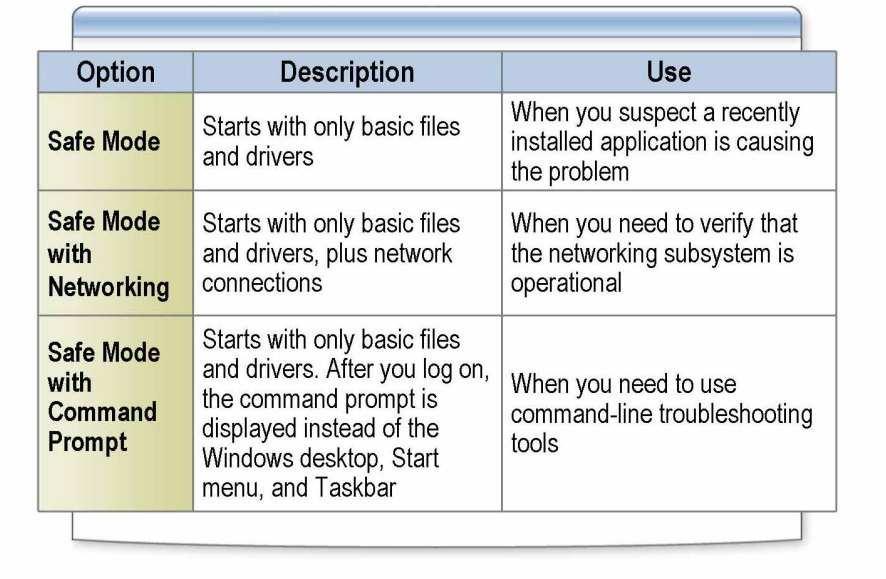
Start a computer using Safe Mode

If your computer does not start after you install new software, new hardware, or a new driver, you may be able to start it with minimal services in safe mode and then change your computer settings, remove the newly installed software, or remove new hardware that is causing the problem. You can reinstall a service pack or the entire operating system, if necessary.

Use Safe Mode to diagnose problems

Safe mode helps you diagnose problems. If a symptom does not reappear when you start in safe mode, you can eliminate the default settings and minimum device drivers as possible causes. If a newly added device or a changed driver is causing problems, you can use safe mode to remove the device or reverse a change.

What Are Safe Mode Options?



Option	Description	Use
Safe Mode	Starts with only basic files and drivers	When you suspect a recently installed application is causing the problem
Safe Mode with Networking	Starts with only basic files and drivers, plus network connections	When you need to verify that the networking subsystem is operational
Safe Mode with Command Prompt	Starts with only basic files and drivers. After you log on, the command prompt is displayed instead of the Windows desktop, Start menu, and Taskbar	When you need to use command-line troubleshooting tools

Introduction

Windows Server 2003 includes advanced startup options that you can use when you troubleshoot and repair startup problems and when you connect the computer to a debugger. These startup options enhance your ability to diagnose and resolve driver incompatibility and startup problems.

Note To display the advanced startup options, press F8 during the operating system selections phase of the startup process in Windows Server 2003.

Advanced startup options

The following table describes the Windows Server 2003 advanced startup options.

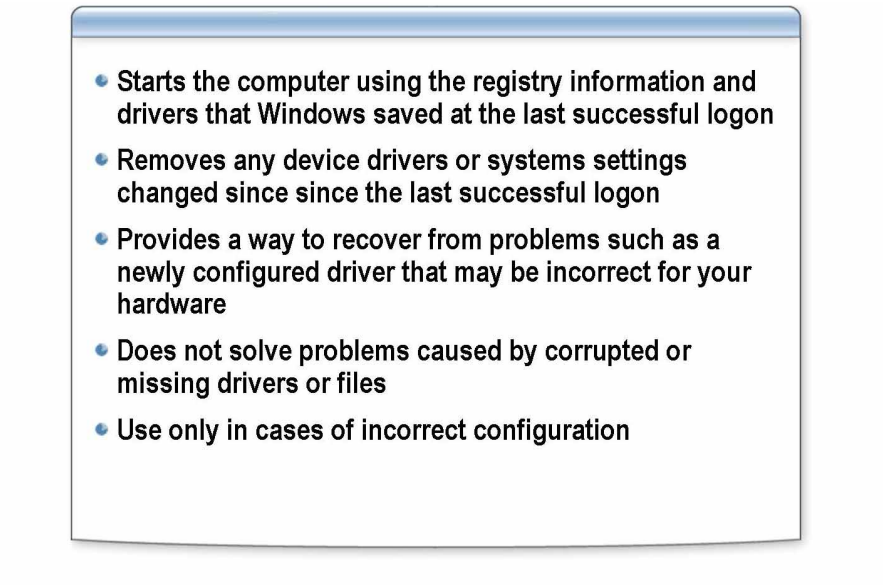
Option	Description
Safe Mode	Loads only the basic devices and drivers that are required to start the computer, including the mouse, keyboard, mass storage devices, base video, and the standard, default set of system services. This option also creates a log file.
Safe Mode with Networking	Loads only the basic devices and drivers that are required to start the computer and enable networking. This option also creates a log file.
Safe Mode with Command Prompt	Same as safe mode but starts a command prompt instead of the graphical user interface. This option also creates a log file.

Safe Mode examples

The following examples describe when to use the Safe Mode options.

- *Safe Mode*. Use this mode when you suspect that a recently installed application is causing the problem.
- *Safe Mode with Networking.* Use this mode when you must verify that the networking subsystem is operational and when you need access to the network to obtain the files.
- *Safe Mode with Command Prompt.* Use this mode when you must use command-line troubleshooting tools. You can use this mode when the other modes fail to start the computer.

What Is Last Known Good Configuration?



Definition

The Last Known Good Configuration startup option uses the registry information and drivers that Windows saved at the last successful logon. When you use this option to start a server, any changes made to driver settings or other system settings since the last successful logon are lost. Use this option only in cases of incorrect configuration.

Recover from newly added incorrect drivers

You can use the Last Known Good Configuration startup option to recover from a problem by reversing driver and registry changes that you made since you last started Windows Server 2003. Windows Server 2003 does not update Last Known Good Configuration information in the registry until the operating system successfully restarts in normal mode and a user logs on and is authenticated.

Restores information for the registry

Using Last Known Good Configuration restores information for the registry subkey HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet. Also, if you updated any device drivers, using Last Known Good Configuration restores the previous drivers.

Resolves startup or stability problems

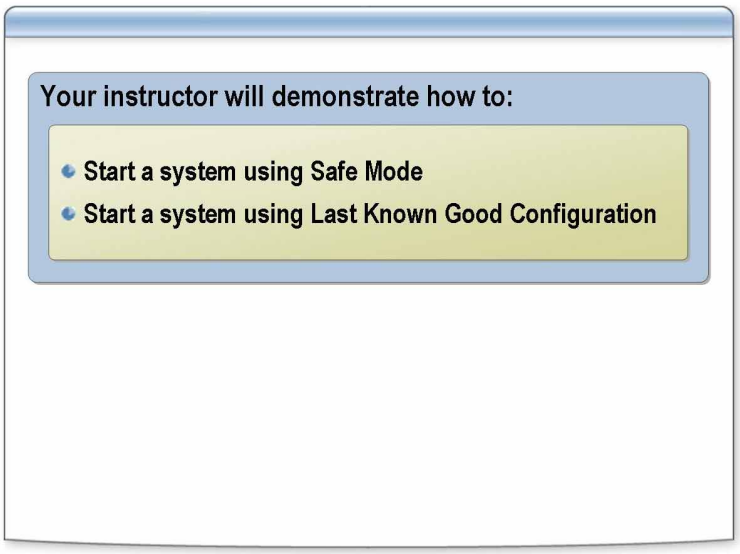
Using Last Known Good Configuration can help you resolve startup or stability problems. For example, if a Stop error occurs immediately after you install a new application or device driver, you can restart the computer and use Last Known Good Configuration to recover from the problem.

Using Last Known Good Configuration can help you recover from problems such as a newly added driver that may be incorrect for your hardware. It does not solve problems that are caused by corrupted or missing drivers or files.

Use with Safe Mode

When you suspect that a change you made to your computer is causing a problem, it is recommended that you use Last Known Good Configuration before you try other options, such as safe mode. However, even if you decide to use safe mode first, logging on to the computer in safe mode does not update the Last Known Good Configuration. Therefore, using Last Known Good Configuration remains an option if you cannot resolve your problem by using safe mode.

How to Start a System Using Safe Mode and Last Known Good Configuration



Objective

Safe Mode and Last Known Good Configuration options load a minimal set of drivers. You can use these options to start Windows so that you can modify the registry or load or remove drivers.

Procedure for starting a system using Safe Mode

To start your system by using Safe Mode:

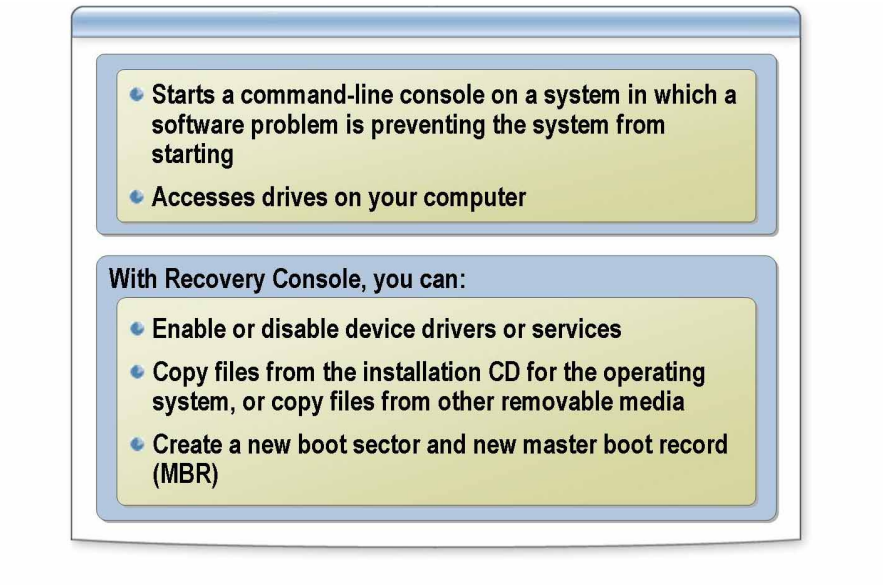
1. Restart your computer.
2. When you see the message "Please select the operating system to start," press F8.
3. Use the arrow keys to highlight the appropriate Safe Mode option, and then press ENTER.
4. Use the arrow keys to highlight an operating system, and then press ENTER.

Procedure for starting a system using Last Known Good Configuration

To start your system using Last Known Good Configuration:

1. Restart your computer.
2. When you see the message "Please select the operating system to start," press F8.
3. Use the arrow keys to highlight **Last Known Good Configuration**, and then press ENTER.
4. Use the arrow keys to highlight an operating system, and then press ENTER.

What Is the Recovery Console?



Definition

The Recovery Console in Windows Server 2003 is a command-line console that you can start from the Windows Server 2003 Setup program. The Recovery Console is particularly useful if you must repair a system by copying a file from a disk or compact disc to the hard disk, or if you must reconfigure a service that is preventing a computer from starting properly.

Specify which installation of Windows

When you start the Recovery Console, you must specify the installation of Windows Server 2003 to log on to, even on a server with a single-boot configuration. You then must log on using the local Administrator account.

Minimal version of Windows Server 2003 operating system

The Recovery Console is a minimal version of the Windows Server 2003 operating system that you can use to start Windows Server 2003 when all other startup options fail. By using the minimal set of commands in the Recovery Console, you can repair damaged system components, such as a damaged boot sector, that prevent you from starting the computer any other way.

Use to perform repair tasks

You use the Recovery Console to perform the following repair tasks:

- Enable and disable services that prevent Windows Server 2003 from starting.
- Read and write files on a local drive, including drives that are formatted with the NTFS file system. The Recovery Console recognizes and enforces NTFS permissions.
- Format hard disks.
- Repair a boot sector.
- Copy files and system files from a floppy disk or compact disc.

To use the Recovery Console

When using the Recovery Console, you must log on by using the local built-in Administrator account that resides in the local security database. On a domain controller, this is a minimal database that Windows Server 2003 creates when you install Active Directory. This database contains only the Administrator user account that you use to perform repair tasks on a domain controller when Active Directory is not available, such as when you run the Recovery Console.

Note If you choose not to install the Recovery Console, or if it does not start because the partition on which you installed it is inaccessible, you can start the Recovery Console from the Windows Server 2003 compact disc. Start the computer by using the Windows Server 2003 compact disc or Setup boot disks. When prompted to choose whether to set up Windows Server 2003 or repair an existing installation, select the repair option..

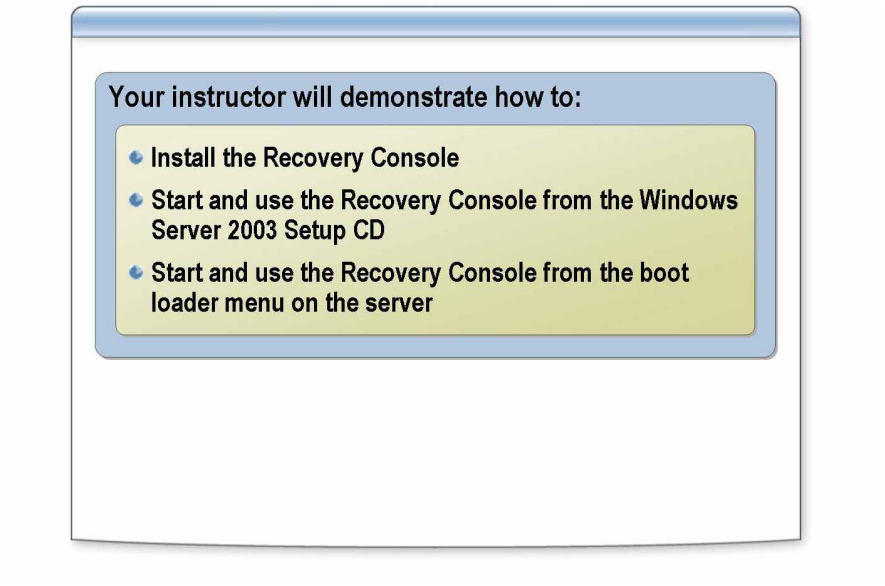
Recovery Console commands

When you run the Recovery Console, you can get help on the available commands by typing **help** at the command prompt and then pressing ENTER.

The following table describes the commands available in the Recovery Console.

Command	Description
attrib	Displays the attributes of the files in the current folder
batch	Executes commands specified in a text file
bootcfg	Repairs boot configuration and recovery
chdir (cd)	Displays the name of the current folder or changes the current folder
chkdsk	Checks a disk and displays a status report
cls	Clears the screen
copy	Copies a single file to another location
delete (del)	Deletes one or more files
dir	Displays a list of files and subfolders in a folder
disable	Disables a system service or a device driver
diskpart	Manages partitions on your hard disks
enable	Starts or enables a system service or a device driver
exit	Exits the Recovery Console and restarts your computer
expand	Expands a compressed file
fixboot	Writes a new partition boot sector onto the system partition
fixmbr	Repairs the master boot record of the partition boot sector
format	Formats a disk
help	Displays a list of the commands that you use in the Recovery Console
listsvc	Lists all available services and drivers on the computer
logon	Logs on to a Windows Server 2003 installation
map	Displays the drive letter mappings
mkdir (Md)	Creates a folder
more	Displays a text file
rmdir (rd)	Deletes a folder
rename (ren)	Renames a single file
systemroot	Sets the current folder to the systemroot folder of the system that you are currently logged on to
type	Displays a text file

How to Use the Recovery Console



Introduction

You should install the Recovery Console before you need to use it so that it is on the hard disk when you do need it. You install the Recovery Console from a Windows Server 2003 compact disc.

Procedure for installing the Recovery Console

To install the Recovery Console:

1. In a command prompt, change to the I386 folder on the Windows Server 2003 compact disc.
2. At the command prompt, type **winnt32 /cmdcons** and then press ENTER.
3. Click **Yes**, and then click **OK**.

Procedure for starting and using the Recovery Console from the Setup compact disc

To start and use the Recovery Console from the Windows Server 2003 Setup compact disc:

1. Insert the Setup compact disc and then restart the computer from the CD-ROM drive.
2. When prompted for the Windows installation, type **1** and then press ENTER.
3. When the text-based part of Setup begins, follow the prompts; select the repair or recover option by pressing R.
4. When prompted, type the Administrator password.
5. At the system prompt, type the appropriate Recovery Console commands.

   For information about commands, type **help** for a list of commands, or type **help** *commandname* for help on a specific command.
6. To exit the Recovery Console and restart the computer, type **exit**

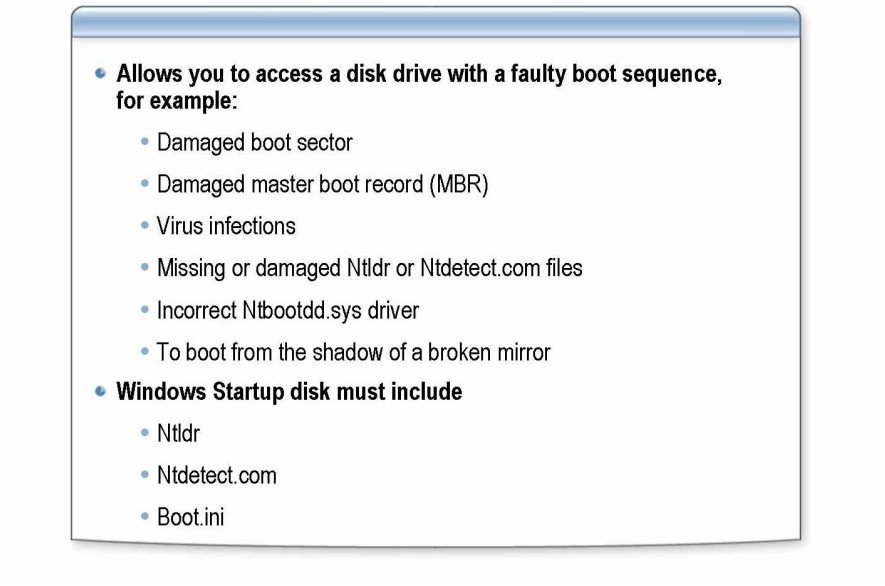
Procedure for starting and using the Recovery Console from the server

To start and use the Recovery Console from the operating system boot menu on the server:

1. Start the computer, on the boot loader menu select **Microsoft Windows Recovery Console**, and then press ENTER.
2. When prompted for the Windows installation, type **1** and then press ENTER.
3. Type the password for the local Administrator account, and then press ENTER.
4. At the command line, type **help** to display all of the available commands. You can use these commands to repair the server.

   For instructions on how to use a specific command, at the command line, type **help** *commandname.*

What Is a Windows Startup Disk?



Definition

A Windows startup disk allows you to access a disk drive that has a faulty boot sequence. You may also be able to use a Windows startup disk to start the operating system on a computer running Windows Server 2003.

Use a Windows startup disk to work around the following startup problems:

- Damaged boot sector
- Damaged master boot record (MBR)
- Virus infections
- Missing or damaged Ntldr or Ntdetect.com files
- Incorrect Ntbootdd.sys driver

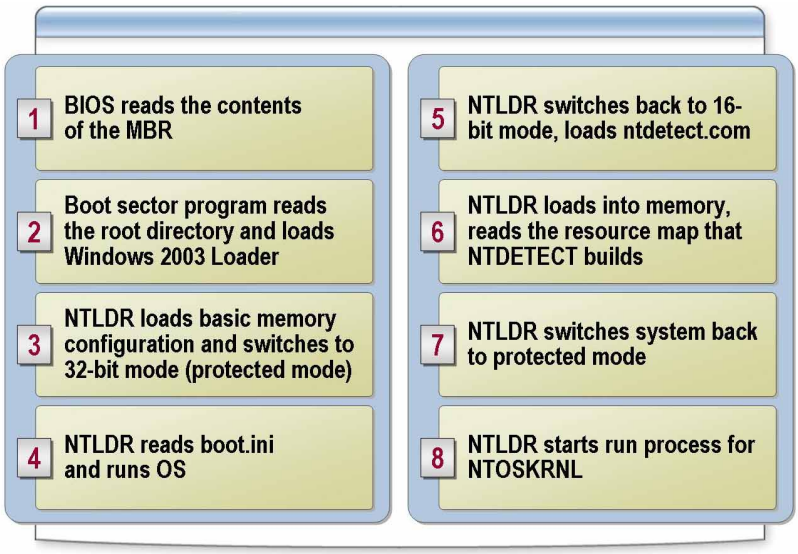
The Windows startup disk must include the Ntldr, Ntdetect.com, and Boot.ini files, and may require ntbootdd.sys, which is the device driver for your hard disk controller renamed to ntbootdd.sys.

Note The attributes of the Ntldr, Ntdetect.com, and Boot.ini files are typically set to system, hidden, and read-only. You do not have to reset these attributes for the startup disk to work, but you must reset them if you copy these files to the hard disk.

Using the Windows startup disk

If you must replace a corrupted boot file on drive C, start the Recovery Console. At the Recovery Console command prompt, insert the Windows startup disk and copy the appropriate boot file to the root directory on drive C.

How Startup Files Function



Introduction

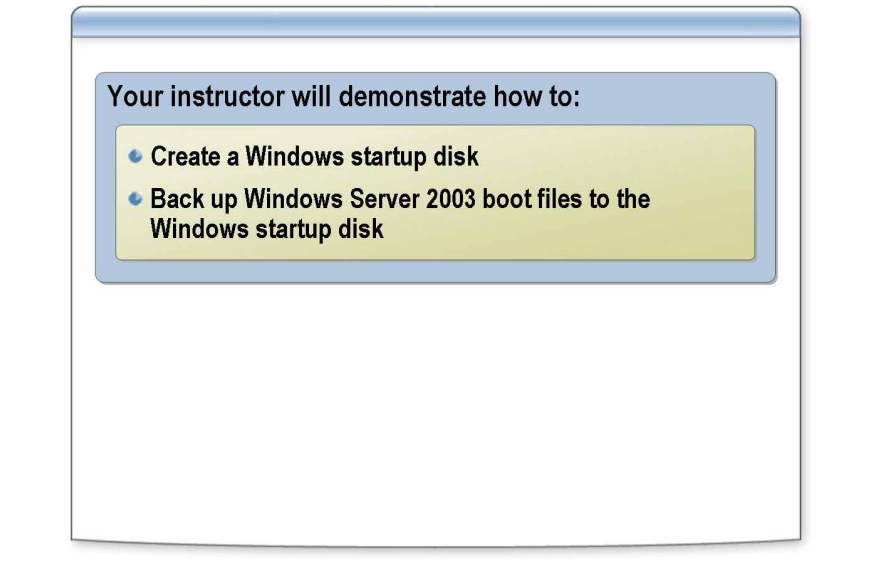
If your server fails to start, and you must start the computer temporarily, start it by using the Windows startup disk. If the problem is caused by one of the three boot files, you will be able to run the server normally.

Function of the boot files

The boot files function as follows.

1. After the power-on self test (POST) loads the system BIOS into memory, the BIOS reads the contents of the Master Boot Record (MBR). The MBR takes control and reads the contents of each partition's various boot sectors to find a bootable sector.
2. The bootsector program reads the root directory and loads Windows Server 2003 Loader (NTLDR).
3. NTLDR loads the basic memory configuration and switches to 32-bit mode (protected mode). NTLDR then places itself into high memory to free up as much memory space as possible.
4. NTLDR reads boot.ini and runs the operating system. If boot.ini is not present, NTLDR assumes that Windows Server 2003 is in the \Windows directory on the C drive.
5. NTLDR switches back to 16-bit mode and loads ntdetect.com, which is a 16-bit application. NTDETECT determines the computer’s physical environment. This determination occurs every time Windows Server 2003 starts, so the environment can change for each boot.
6. NTLDR loads into memory and reads the resource map that NTDETECT builds.
7. NTLDR switches the system back to protected mode. NTLDR then sets up the ring 0 mode for the kernel and loads the proper kernel (NTOSKRNL) for the computer. NTLDR pulls in the proper Hardware Abstraction Layer (HAL) and all boot drivers. Everything that NTDETECT collects becomes the HKEY_LOCAL_MACHINE/HARDWARE Registry key.
8. NTLDR starts the run process for NTOSKRNL.

How to Create a Windows Startup Disk



Introduction

You may encounter a situation when it is not possible to start Windows or any other operating system on your computer. This situation can occur when Windows is installed on a computer that has an Intel x86-based processor, and the boot record for the active partition or files that are required to start Windows becomes corrupted.

Use the following procedures to create and use a Windows startup disk. A Windows startup disk contains only the files that are necessary to start the operating system with the remainder of the Windows system files installed on the hard disk drive.

Procedure for creating a Windows startup disk

To create a Window startup disk:

1. Place a blank floppy disk in drive A.
2. On the **Start** menu, click **Windows Explorer**.
3. In Windows Explorer, expand **My Computer**.
4. Right-click **3½ Floppy (A:)** and then click **Format**.
5. In the **Format 3 ½ Floppy (A:)** dialog box, click **Quick Format**, click **Start**, and then click **OK**.
6. In the **Formatting 3 ½ Floppy (A:)** dialog box, click **OK**, and then click **Close**.

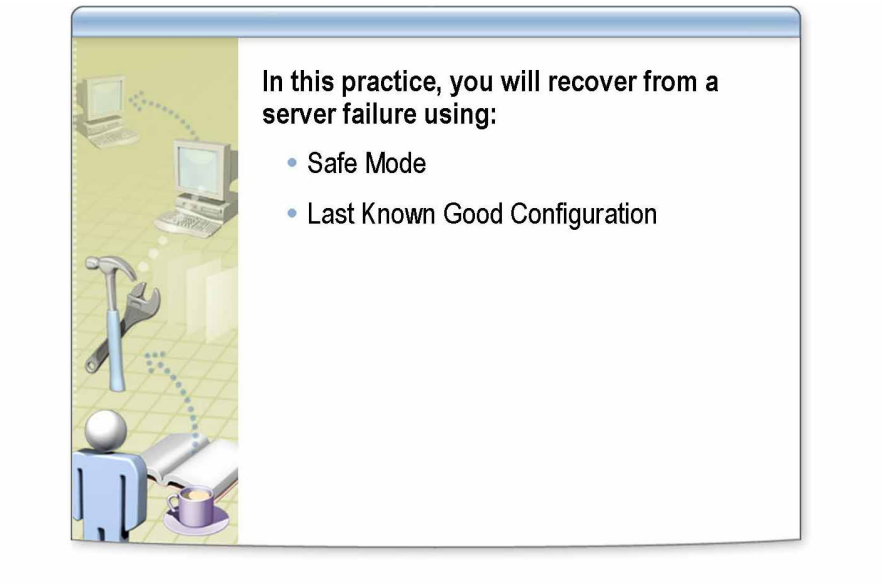
Procedure for backing up boot files

To back up Windows Server 2003 boot files to the Windows startup disk:

1. In Windows Explorer, click **Local Disk (C:)**.
2. On the **Tools** menu, click **Folder Options**.
3. On the **View** tab, clear the **Hide protected operating system files (Recommended)** check box.
4. In the **Warning** box, click **Yes**, and then click **OK**.
5. Copy the following files to drive A:
   - Boot.ini
   - Ntdetect.com
   - Ntldr

   If either the Bootsect.dos or the Ntbootdd.sys file resides in the system partition, also copy these files to the boot disk.
6. Open a command prompt, type **attrib –h –s –r a:*.*** and then press ENTER.
7. On the **Tools** menu, click **Folder Options**.
8. On the **View** tab, select the **Hide protected operating system files (Recommended)** check box, and then click **OK**.
9. Remove the disk from the drive, and label it **Windows startup disk**.

Practice: Recovering from Server Failure



Objective

In this practice, you will recover from a server problem by using:

- Safe Mode
- Last Known Good Configuration

Scenario

You are the systems administrator for an organizational unit on a large network. You install a new software package on a server. After installation is complete, you restart the computer. After you log on, the computer malfunctions. You will fix this problem by using Last Known Good Configuration and Safe Mode.

Practice

► **To start your computer using Last Known Good Configuration and Safe Mode**

1. Log on as Administrator with a password of **P@ssw0rd**.
2. Open the **Run** dialog box, type **\MOC\2275\Practices\Mod07\install.bat** and then click **OK**.
3. After the computer restarts, log on as Administrator.
4. Note the unusual behavior. What does the computer do?

_____

5. When the computer restarts, use Last Known Good Configuration to start Windows Server 2003.
6. Log on as administrator.
7. Did this work? Why or why not?

_____

8. When the computer restarts, use Safe Mode to start Windows Server 2003.
9. Log on as administrator.

10. Did this work? Why or why not?

    _____

11. On the **Start** menu, click **Search**.
12. In the **Search Results** dialog box, search for all bootme files. Delete any bootme files in the Windows folder.
13. Restart your computer, and then log on as Administrator. What happens?

    _____

14. Log off, and then log on again. Does the problem appear to be solved?

    _____

Lesson: Selecting Disaster Recovery Methods

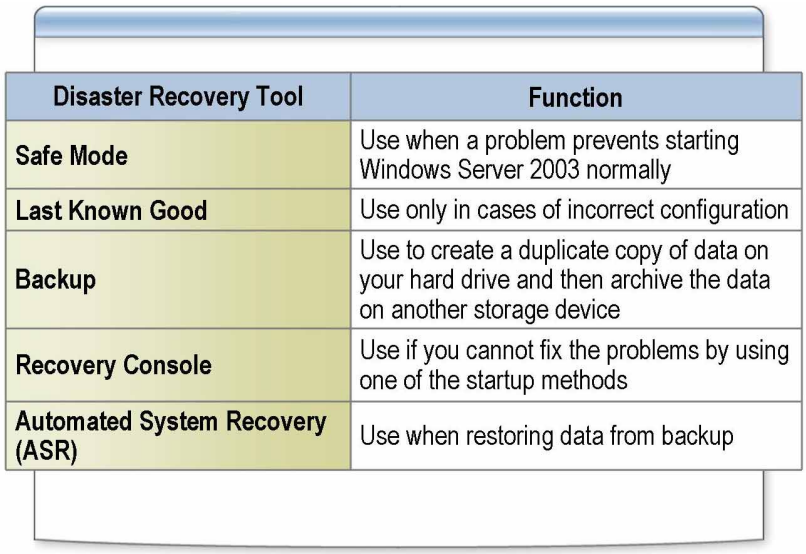
Introduction

By using the system recovery tools, backup, and restore, you can implement a disaster recovery method for most common data losses.

Lesson objective

After completing this lesson, you will be able to determine which disaster recovery solutions to use to recover data during a server failure.

What Are Server Disaster Recovery Tools?



Disaster Recovery Tool	Function
Safe Mode	Use when a problem prevents starting Windows Server 2003 normally
Last Known Good	Use only in cases of incorrect configuration
Backup	Use to create a duplicate copy of data on your hard drive and then archive the data on another storage device
Recovery Console	Use if you cannot fix the problems by using one of the startup methods
Automated System Recovery (ASR)	Use when restoring data from backup

Introduction

To recover your system, you can use Safe Mode, Last Known Good Configuration, Backup, Recovery Console, ASR, or some combination of these tools, as well as others such as shadow copies. Follow the recommended best practices when you use these disaster recovery solutions.

Disaster recovery tools

The following table lists disaster recovery tools in the preferred order of use, from tools that present little or no risk to data, to those that might cause data loss. Safe Mode and Backup are available in both safe and normal startup modes.

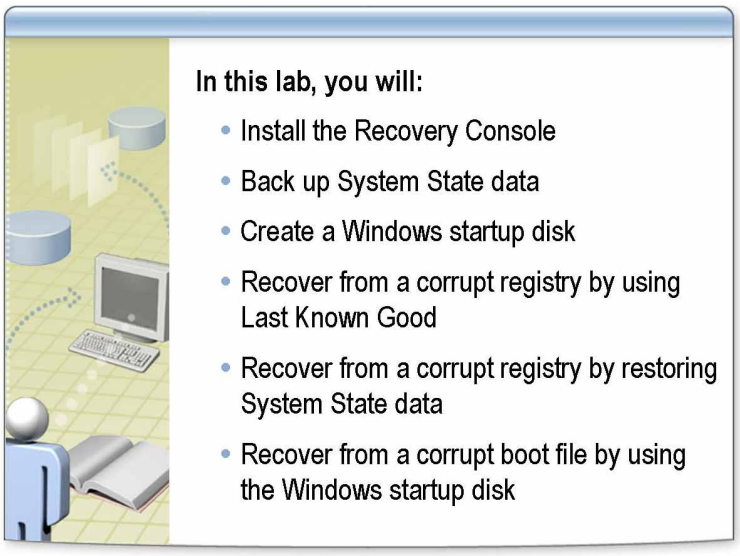
Disaster recovery tool	Function
Safe Mode	Use when a problem prevents Window Server 2003 from starting normally. Safe mode is a startup option that disables startup programs and nonessential services to create an environment that is useful for troubleshooting and diagnosing problems.
Last Known Good Configuration	Use only in cases of incorrect configuration. By using Last Known Good Configuration, you can recover by reversing the most recent driver and registry changes made since the last time you logged on to Windows Server 2003.
Backup	Use to create a duplicate copy of data on your hard drive and then archive the data on another storage device. Backup is a tool for saving data, such as System State data. Before you troubleshoot problems, attempt workarounds or apply updates.

(*continued*)

Disaster recovery tool	Function
Recovery Console	Use if you cannot fix the problems by using one of the startup methods. In addition to Last Known Good Configuration and safe mode, users can use Recovery Console to attempt manual recovery operations.
Automated System Recovery (ASR)	Use when restoring data from backup. Use this option instead of reinstalling Windows because ASR restores system settings and critical files on the system and boot partitions. Because the ASR process formats disks, consider this a last resort when using Last Known Good Configuration, Backup, restoring system state data, or Recovery Console does not solve the problem.

Note For more information about how to select the correct recovery tool or combination of tools to correct the specific disaster you encounter, see Appendix H, "Which Recovery Tool Do I Use?"

Lab A: Managing Disaster Recovery



Objectives

After completing this lab, you will be able to:

- Install the Recovery Console.
- Back up System State data.
- Create a Windows startup disk.
- Recover from a corrupt registry by using Last Known Good.
- Recover from a corrupt registry by restoring System State data.
- Recover from a corrupt boot file by using the Windows startup disk.

Estimated time to complete this lab: 45 minutes

Exercise 1
Installing the Recovery Console

In this exercise, you will install the Recovery Console.

Tasks	Specific instructions
1. Log on to your computer.	▪ Log on to the domain using the administrator account.
2. Install the Recovery Console.	**a.** Insert the Windows Server 2003 compact disc into the CD-ROM drive. **b.** Close the Welcome screen. **c.** Open a command prompt and change to the I386 folder on the Windows Server 2003 compact disc. **d.** At the command prompt, type **winnt32 /cmdcons** and then press ENTER. **e.** Follow the on-screen directions for installing the Recovery Console. **f.** Remove the Windows Server 2003 compact disc from the CD-ROM drive.

Exercise 2
Backing Up the System State Data

In this exercise, you will use the Backup Wizard to back up the System State data for your computer on your drive C.

Tasks	Specific instructions
▪ Start the Backup Wizard and back up the System State data.	**a.** In the **Run** dialog box, type **ntbackup** **b.** Click **Advanced Mode** and then start the Backup Wizard. **c.** Select the following option: Only back up the System State data. **d.** On the **Backup Type, Destination and Name** page, browse to C:\MOC\2275\Labfiles\Lab07. **e.** Use **SysState** as the filename. **f.** Close all windows when the backup is completed.

Exercise 3
Creating a Windows Startup Disk

In this exercise, you will create a Windows startup disk.

Tasks	Specific instructions
1. Format a disk.	**a.** Insert a floppy disk into the drive. **b.** Using Windows Explorer, format the disk.
2. Copy Windows Server 2003 boot files to the disk.	**a.** In Windows Explorer, expand **Local Disk (C:)**. **b.** On the **Tools** menu, click **Folder Options**. **c.** On the **View** tab, clear the **Hide protected operating system files (Recommended)** check box. **d.** Use Windows Explorer to copy the following files to the disk: • Boot.ini • Ntdetect.com • Ntldr • If either the Bootsect.dos or the Ntbootdd.sys file resides in the system partition, also copy these files to the disk. • Open a command prompt and type **Attrib –h –s –r a:*.*** **e.** On the **Tools** menu, click **Folder Options**. **f.** On the **View** tab, select the **Hide protected operating system files (Recommended)** check box. **g.** Remove the disk and label it “Windows startup disk.”

Exercise 4
Recovering from a Corrupt Registry (Part One)

In this exercise, you will recover from a non-responsive computer. The cause of this problem was the installation of a software package that modified the registry. (The source for this exercise is the Microsoft Knowledge Base article at http://support.microsoft.com/kbid=317246.)

Tasks	Specific instructions
1. Install the software.	▪ Using Windows Explorer, browse to **C:\MOC\2275\Labfiles\Lab07** and then double-click **inst_01.bat**.
What happens when the computer restarts?	
What do you need to do to recover from this disaster?	
2. Recover from a corrupt registry.	**a.** Restart your computer, and then press F8 to open the Windows **Advanced Options** menu. **b.** Select the option that you can use to recover from a corrupt registry.

Exercise 5
Recovering from a Corrupt Registry (Part Two)

In this exercise, you will recover from a non-responsive mouse. The cause of this problem was the installation of a software package that modified the registry. (The source for this exercise is the Microsoft Knowledge Base article at http://support.microsoft.com/kbid=317246.)

Tasks	Specific instructions
1. Log on to your computer.	▪ Log on to the domain using the administrator account.
2. Install the software.	**a.** Open Windows Explorer, browse to C:\MOC\2275\Labfiles\Lab07, and then double-click **inst_04.bat**. **b.** When the computer restarts, log on to the domain as an administrator.
What do you need to do to recover from this disaster? _____	
3. Recover from a corrupt registry using Last Known Good Configuration.	**a.** Shut down, and then restart the computer. **b.** Press F8 go open the Windows **Advanced Options** menu. **c.** Select **Last Known Good Configuration** to resolve this problem. **d.** Log on to the domain using the administrator account. Did this resolve the problem? _____
4. Recover from a corrupt registry by restoring System State data using the keyboard. Use the following keys to navigate in the Backup program: ALT + TAB CTRL + ESC TAB ENTER CTRL + TAB SPACEBAR Up arrow Down arrow Right arrow Left arrow	**a.** Log on to the domain using the administrator account. **b.** Open the **Start** menu by pressing the _____ + _____ keys. **c.** Use the arrow keys to select **Run**, and then open the **Run** dialog box by pressing _____. **d.** In the **Run** dialog box, type **ntbackup** and then press _____. **e.** In the **Backup or Restore Wizard** dialog box, use the _____ key to select **Advanced Mode** and then press _____. **f.** In the Backup Utility – [Untitled] window, use the _____ + ____ keys to select **Restore and Manage Media**. **g.** In the **Restore and Manage Media** page, use the _____ key to highlight **File** in the tree view pane, and then use the _____ key to open the tree. **h.** When the tree is open, use the _____ key to traverse the tree until you get to the **Systate.bkf** entry, and then use the _____ key to view the **System State** check box. **i.** When the System State check box is displayed, use the _____ key to highlight it, and then use the _____ key to select **the System State** check box. **j.** Start the system restore process by pressing the _____ key, and then press the _____ key twice to confirm your choice. **k.** When the restore process is complete, close the **Restore Progress** dialog box by pressing the _____ key, and then restart the computer.

Exercise 6
Recovering from a Corrupt Boot File

In this exercise, you will recover from a corrupt boot.ini file.

Tasks	Specific instructions
1. Log on to your computer.	▪ Log on to the domain using the administrator account.
2. Install the software.	▪ Using Windows Explorer, browse to C:\MOC\2275\Labfiles\Lab07, and then double-click **inst_03.bat**.
What do you need to do to recover from this disaster?	
3. Recover from a corrupt boot file.	**a.** Insert the Windows startup disk in drive A, and then restart the computer. **b.** Log on to the domain using the administrator account. **c.** Use Windows Explorer to copy the a:\boot.ini file to C:\. **d.** Remove the Windows startup disk. **e.** Shut down, and then restart the computer.