Microsoft TechNet

TechNet Home > Products & Technologies > Desktop Operating Systems > Windows XP Professional > Windows XP Professional Resource Kit

Windows XP Professional Resource Kit

Backing Up and Restoring Data

Published: November 3, 2005

Backup is a tool in Microsoft Windows XP Professional that allows users to back up and restore data. The ability to restore data from backup media in the event of an emergency is critical to the success of an organization.

Backup uses the Removable Storage feature to manage the storage devices attached to your system. Because backing up the data on your system is one of the most important aspects of data management, Windows XP Professional integrates Backup with Removable Storage to help you protect your data.

For information on how to obtain the Windows XP Professional Resource Kit in its entirety, please see http://www.microsoft.com/mspress/books/6795.asp.

On This Page

Related Information

- For more information about the NTFS file system and the file allocation table (FAT) file system, see Chapter 13, “Working with File Systems.”

Top of page

Overview

Regular backup of local hard disks prevents data loss from a disk or drive failure, disk controller errors, power outages, viruses, and other serious problems. Careful planning of backup operations and reliable equipment can make file recovery easier and faster.

Using Backup, you can back up data to tape, optical disc, or a compressed file. You can also store your backup files on a network share.

Backup Types

Deciding which type of backup to use depends on your organization’s needs. The two major considerations are the value of the data and the amount of data that has changed since the last normal or incremental backup.

You can perform any of the following types of backup:

Normal
A normal backup copies all selected files and marks each as having been backed up. Normal backups are the easiest to use for restoring files because you need only the most recent backup file or tape to restore all the backed-up files. Normal backups take the most time because every file that is selected is backed up, regardless of whether it has changed since the last backup.

Incremental
An incremental backup reduces the time required to complete the backup process by saving only files that have been created or changed since the last normal or incremental backups. It marks files so that you will know whether a specific file has been backed up. You need to create a complete normal backup of your system before you can run incremental backups. If you use a combination of normal and incremental backups to restore your data, you must have the last normal backup set of media as well as every incremental backup in chronological order since the last normal backup.

Differential
A differential backup can reduce the time required to complete the backup process by copying files that have been created or changed since the last normal or incremental backup. It does not mark files as backed up. You need to create a complete normal backup of your system before you run differential backups. If you use a combination of normal and differential backups, you must have the last normal backup media set and the last differential backup set to restore your data.

Copy
A copy backup copies all selected files, but it does not mark each copied file as backed up. Copying is a useful temporary method to back up files between normal and incremental backups; it does not affect other backup operations.

Daily
A daily backup copies all selected files that have been modified on the day that the daily backup is performed. The backed-up files are not marked as backed up.

Some backup types use a backup marker, also known as an "archive attribute," to track when a file has been backed up. When the file changes, Windows XP Professional marks the file to be backed up again. Files or directories that have been moved to new locations are not marked for backup. Backup allows you to back up only files with this marker set and to choose whether or not to mark files when they are backed up.

Caution Backup protects against data loss caused by a virus. Because some viruses take weeks to appear, keep normal backup tapes for at least a month to make sure that you can restore a system to its uninfected status.

Storage and Media

Windows XP Professional can back up files to a variety of storage devices. Data can be backed up to tape drives, disk volumes, removable disks, and network shares, or to a library of discs or tapes in a media pool controlled by a robotic changer. If you do not have a separate storage device, back up to a local hard disk or to floppy disks.

and File Systems
- Troubleshooting the Startup Process
- System Files Reference
- User Rights
- Tools for Troubleshooting
- Differences with Windows XP Home Edition
- Accessibility Tools

Storage Devices

Storage technology changes rapidly, so it is important to research the merits of various media before you make a purchase. When you select a storage device, consider storage device and media costs, as well as reliability and capacity. Ideally, a storage device has more than enough capacity to back up the combined data of all local hard disks and can detect and correct errors during backup-and-restore operations. For information about specific storage devices, see the Windows Catalog at http://www.microsoft.com/windows/catalog.

Tip To make sure that your storage devices and media work correctly, verify your backups by performing test restores.

Media Types

The most common medium is magnetic tape. Commonly used tape drives for backup include a quarter-inch cartridge, digital data storage (DDS), 8 mm cassette, Advanced Intelligent Tape (AIT), digital linear tape (DLT), and Super DLT (SDLT). High-capacity, high-performance tape drives typically use small computer system interface (SCSI) controllers. Other types of media include magnetic discs, optical discs, and CD-ROMs—recordable CD-ROM (CD-R) and rewritable CD-ROM (CD-RW).

Note Backup does not support backing up directly to CD-R or CD-RW devices. Back up to a file, and then copy that backup file to a CD-R or CD-RW. The restore process can be accomplished directly from the CD-R.

Security Considerations

Several steps are required to enhance the security and operation of your backup-and-restore operations. You need to take steps to secure your backup media.

When you develop a backup plan, consider the following methods:

- Secure both the storage device and the backup media. Data can be retrieved from stolen media and restored to another computer.
- Back up an entire volume by using the normal backup procedure. In case of a disk failure, it is more efficient to restore the entire volume in one operation.
- Always back up the System State data to prevent the loss of local user accounts and security information.
- Keep at least three current copies of backup media. Store one copy at an off-site location in a properly controlled, secure environment.

Backup and Restore Rights

In many cases, the local administrator performs backup and restore operations on Windows XP Professional systems. However, when Windows XP Professional is used as a file server in a peer-to-peer, local area network (LAN), backup and restore rights can be given to a user without granting full administrative privileges.

If you are the system administrator of a networked computer with shared volumes or of a publicly used computer, you need to extend backup and restore rights only to users who are responsible for backing up the computer. Do this by adding users to the Backup Operators local group. In a high-security environment, only you need the ability to restore files, although it is a good idea to train personnel to perform all restore tasks in the event that you are unavailable.

To add a user to the Backup Operators group

1. In **Control Panel**, double-click **Administrative Tools**.
2. Double-click the **Computer Management** icon.
3. In the console tree, click **Local Users and Groups**, and then double-click **Groups** in the details pane.
4. Double-click the **Backup Operators** group, and then click **Add**.
5. Enter the user's name, and then click **OK**.

   Caution A user who does not have permission to write to a file might have permission to restore the file. During a restore operation, such permission conflicts are ignored and the existing file can be overwritten.

File Permissions

In Windows XP Professional, access to NTFS files is limited by NTFS file and folder permissions, share permissions, and file attributes. You cannot back up or restore NTFS files to which you do not have access rights unless you are a member of either the Administrators or Backup Operators local group.

Note Neither of the file allocation table (FAT) file systems (FAT16 and FAT32) provides file permissions.

Backup Media Storage

Store some data off-site for long-term storage or to have available in the event of a disaster; however, other data needs to be readily available.

Caution Tape cartridges last longer in cool, humidity-controlled locations. Your storage area must also be free of magnetic fields, such as those near telephone equipment and the backs of computer terminals.

Daily backups—full and incremental

Store media in a fireproof safe or cabinet to protect against natural disaster, theft, and sabotage.

Copies of cartridges

If more than one copy of a software program is purchased, store one off-site if possible. If you have only one copy, back it up to a cartridge, label it as a backup, and store the original off-site. If you have to reinstall software, you can restore it from the backup cartridge to a computer that is running Windows XP Professional.

For highly confidential data that must be stored off-site, consider assistance from a company that specializes in secure data storage. If the cost or logistics of such protection is too great, use an alternative solution, such as a safe-deposit box or an off-site fireproof safe that is designed to protect magnetic media.

For maximum security, store the following items off-site:

- A full, normal backup of the entire system, performed weekly.
- Original software that is installed on computers. (Keep only copies on-site.)
- Documents that are required for processing an insurance claim, such as purchase orders or receipts.
- Information that is required to get network hardware reinstalled or reconfigured.

- Information that is required to reconfigure your storage subsystem.

  Tip Make sure that your off-site storage location is bonded. That is, the agreement you have with the facility is guaranteed by a bond. It does not mean that your materials are insured.

Top of page

Establishing a Backup Plan

When you develop your backup plan:

- Keep spare hardware and media on hand in case of a failure. To avoid a problem, compare the spare hardware with the original hardware in advance to make sure that the firmware revision is the same as the original equipment. For more information about firmware revisions, check the documentation provided by the manufacturer.
- Test backed-up data regularly to verify the reliability of your backup procedures and equipment.
- Include stress testing of backup hardware (storage drives, optical drives, and controllers) and software (backup program and device drivers).

Several different system configurations can affect your backup strategies. At one end of the range is a simple, stand-alone computer with one user. At the other end is a workgroup network with a computer that is hosting a network public file share.

Caution Backup does not back up files on computers running Microsoft MS-DOS, unless you create a share that Backup can access over the network. Consider reserving space on a network share so that users of MS-DOS and Microsoft Windows version 3.1 can copy important files. Files on the network share can be backed up during regular file server backups.

You can work out a backup solution by doing these four tasks:

1. Research and select a storage device. When considering new backup hardware, be sure to consider its reliability, speed, capacity, cost, and compatibility with Windows XP Professional. The media must provide more than enough space to back up all your data.
2. If necessary, install a controller card in the computer. If you choose to use a SCSI-based tape drive, put the tape drive on its own controller.
3. Connect your new storage device to the computer so that you can back up the System State data. If you are using an external SCSI drive, start the drive before you start the computer so that the driver can be loaded properly.
4. Establish a backup media rotation schedule. You need to continue making backups as long as data is created or changed.

Over a period of time, you need to use several separate discs or tapes when you run your backup regimen. By using multiple discs or tapes instead of repeatedly using the same disc or tape, you gain additional benefits with your backup program:

- It preserves access to multiple versions of data files in case a user needs to restore an older copy of a data file.

- If the last backup is unsuccessful as a result of a bad cartridge, you have a backup from the previous process.
- You extend the useful life span of each cartridge.

Tip Have several extra, new, blank, formatted media available in case of media failure. Regularly scan the Backup log for errors that might indicate that a backup cartridge is beginning to fail.
Make sure to clean a tape drive's recording heads regularly. Failure to do so can lead to unusable backups and the premature failure of the tape drive. See the tape drive manufacturer's recommendations for the proper method and frequency of cleaning.

Stand-Alone Computer

You need to choose a backup medium to use. If the quantity of data that you need to back up is small, a removable hard disk or rewritable DVD disc (DVD RAM) might be all that you need. However, for more flexibility and capacity for growth, a tape cartridge is still the backup medium of choice.

To back up to a CD-R or CD-RW, you must back up to a file first and then copy that file to the CD-R or CD-RW. You can then restore the file directly from the CD-R or CD-RW. Because space on CD-R or CD-RW is limited from 650 to 700 MBs, you might have to divide your backups into smaller jobs.

After your storage device is installed, decide on a backup schedule and the type of backup. If the data that is created on a daily basis is irreplaceable, daily backups are necessary. If the data is less valuable, the frequency of backups can be less often. Recognize, however, that the longer the period between backups, the greater the potential for loss. Just as it is unwise to work on a document all day without periodically saving the file, it is unwise to work on a document all week without backing it up. The value of the data helps you determine the appropriate frequency of backups.

The type of backup you make determines how easy or difficult it is to restore the data in an emergency. The compromise is between security and convenience. If you choose to run full, normal backups every day, you can restore lost data easily, but the backups can take a substantial amount of time (depending upon the quantity of data to be backed up and the data transfer speed of the storage device). If you choose to make incremental backups for a month after making a full backup, you save substantial time in the backup process. However, fully restoring a corrupted hard disk might require you to restore the normal backup and then each incremental backup in succession. Substituting a differential backup for the incremental backup shortens the restore process, but as the backup process takes more time each day, the total accumulation of changed files continues to grow, so the time you gain by using a differential backup might be minimal. You must also use a separate cartridge for each differential backup to prevent losing the ability to retrieve earlier versions of files.

Stand-Alone Method One

Computers that contain frequently changing data that is hard to replace or reproduce or computers that provide a public network share need to be backed up daily. Run a full, normal backup every Friday. Every Monday through Thursday run a differential backup to a different tape or disc. After the second Friday, when a second full backup has been successfully made, store the first full backup as a temporary archive. Then after every following Friday's full backup, alternate the full backups as temporary archives. On every eighth Friday, save the full backup as a permanent archive, which needs to be stored in a secure, off-site location. Over the course of a year, this method uses at least 14 tapes or discs.

Note If a computer is used seven days a week, add a Saturday and Sunday differential backup to the schedule.
Use new tapes if you choose to make permanent archives on tape.

Stand-Alone Method Two

If the computer is used less often or if the data is not as valuable, consider making one incremental backup each week for three weeks and one full, normal backup every fourth week. Alternating the full backups between two cartridges ensures that at least one always exists. This reduces the amount of time spent creating backups, but it also reduces protection against data corruption or erasure. Over the course of a year, this method uses at least fives tapes or discs.

LAN Workgroups

The following scenario illustrates a possible approach for backing up a small network that consists of a computer that is running Windows XP Professional and that is hosting a public file share for 20 other client computers.

Connect a storage device to the share host computer. From the share host computer, you can back up user files on remote computers that are running the following operating systems: Microsoft Windows for Workgroups, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT 4.0, Microsoft Windows 2000, Microsoft Windows Server™ 2003, and Windows XP Professional. (See the two suggested methods for doing this that follow.) Establish a media rotation schedule. If conserving media is a requirement, back up clients less frequently than you back up the share host and encourage users to copy critical files to the network share at the end of the day.

Volume shadow copies cannot be used on remote shares. The success of your backup is more reliable if it is run on an individual Windows XP Professional–based computer and saved to the server that you are backing up. Using this method provides a shadow copy of the data volumes, and you can then schedule periodic system state backups. However, this backup method must be managed and scheduled for each computer individually, which is not practical if you manage many computers.

In the descriptions of the following methods for backing up remote computers, the computer that contains the data to be backed up is called "Data." The computer that runs the backup process is called "Target."

Workgroup Method One

Back up Data locally to disk. Use Backup over the network or the **xcopy** command to move the resulting backup file to Target. Make sure you run a backup verification pass that compares the data on Data and the data on Target on a regular basis. Typical transfer speeds for Ethernet or Token Ring are approximately 1 megabyte (MB) per second if the network is not busy. Use this transfer rate and the total amount of data being transferred to estimate the transfer time. If the transfer time is too long, you might need to use a faster network connection or a different backup method.

For more information about using the **xcopy** command, type the following at the command prompt:

```
    xcopy /?
```

Workgroup Method Two

Copy the data that you want to back up to another disk or disks on Data. Bring Data online, and copy the data by using the data storage device that is connected to Data. You can also back up Data over the network to Target. Whether to perform the backup from Data or from Target depends on the following factors:

- Availability of a target computer
- Policies requiring backups on designated computers
- Time and cost of performing backup from Data
- Time and cost of transferring files to Target

LAN Backup Schedule

After you have determined the best method for giving Target access to the data it needs to back up, begin your backup schedule plan. On Target, run a full, normal backup every Friday. Every Monday through Thursday, run a differential backup to a different tape. Run this program for four weeks before you reuse tapes in the backup program. On every fourth Friday, save the full backup as a permanent archive stored in a secure, off-site location. Over the course of a year, this method uses at least 31 tapes.

Note To allow users access to even older versions of document files, lengthen the backup schedule to six weeks before tapes are reused. This increases the number of tapes used in a year to at least 41.
If a computer is used seven days a week, add a Saturday and Sunday differential backup to the schedule.

Documenting Backup-and-Restore Procedures

Keeping accurate backup records is essential for locating backed-up data quickly, particularly if you have accumulated a large number of backup cartridges. Thorough records include cartridges labels, catalogs, and online log files and log books.

Cartridge labels

Labels for write-once cartridges need to contain the backup date, the type of backup (normal, incremental, or differential), and a list of contents. If you are restoring from differential or incremental backups, you need to be able to locate the last normal backup and either the last differential backup or all incremental backups that have been created since the last normal backup. Label reusable media, such as tapes or removable discs, sequentially and keep a log book in which you note the content of cartridges, the backup date, the type of backup, and the date the medium was placed in service. If you have to replace a defective cartridge, label the new cartridge with the next unused sequential ID and record it in the log book.

Catalogs

Most backup software includes a mechanism for cataloging backup files. Backup stores catalogs on a backup cartridge and temporarily loads them into memory. Catalogs are created for each backup set or for each collection of backed-up files from one drive.

Log files
Log files include the names of all backed-up and restored files and folders. A log file is useful when you are restoring data because you can print or read this file from any text editor. Keeping printed logs in a notebook makes it easier to locate specific files. For example, if the tape that contains the catalog of the backup set is corrupted, use the printed logs to locate a file. Carefully review log files following each backup session to ensure that the session completes successfully.

Verify Operations

A verify operation compares the files on disk to the files on the backup media. It occurs after all files are backed up or restored, and it takes about as long as the backup procedure. Recommended times for performing verify operations follow:

- After every backup, especially if you back up to a set of cartridges for long-term storage
- After a file restore operation

Choosing a verify operation while backing up system files might cause the verify operation to falsely report files that are in use by the operating system and continuously changing.

If a verify operation is unsuccessful for a particular file, check the date that the file was last modified. If the file changes between a backup operation and a verify operation, the verify operation is unsuccessful. A change in the size of a file or corruption of data on the backup disc or cartridge also might make a verify operation unsuccessful.

⇧ Top of page

Backing Up System State Data

System State data includes the following:

- Boot files, including the system files
- Files protected by Windows File Protection (WFP)
- The registry
- Performance counter configuration information
- The Component Services class registration database

The System State data does not represent the entire system. To restore a system to an operational condition, the boot files, system volumes, and System State must all be restored together.

Restoration of the System State replaces boot files first and commits the system hive of the registry as a final step in the process.

System State backup and restore operations include all System State data. You cannot choose to back up or restore individual components because of dependencies among the System State components. However, you can restore System State data to an alternate location in which only the registry files and system boot files are restored. The Component Services class registration database is not restored to the alternate location.

Although you cannot change which components of the System State are backed up, you can back up all system-protected files at the same time as the System State data by setting advanced backup options.

The system-protected files only change if you install a service pack or application, or upgrade your operating system. Typically, the system-protected files represent a very large portion of System State data—the default, including the protected files, is about 180 MB. Include these system-protected files only if new programs have been installed. Otherwise, a restore causes the new application to fail.

To back up System State data

1. From the **Start** menu, point to **All Programs**, **Accessories**, **System Tools**, and then click **Backup**.
2. Click **Advanced Mode**.
3. Click the **Backup** tab, and then select the **System State** check box.
4. Click **Start Backup**.

This backs up the System State data along with any other data that you have selected for the current backup operation. Keep the following in mind when you are backing up System State data:

- You must be an administrator or a backup operator to back up files and folders.
- You can back up the System State data only on a local computer.
- You must also back up the Boot and System volumes to ensure that the system starts properly.
- You can use the Backup Wizard to back up System State data.
- You cannot use an incremental backup while backing up System State data.

Boot and System Files

Backup depends on the functionality of WFP when backing up and restoring boot and system files. System files are backed up and restored as a single entity. In Microsoft Windows NT version 4.0 and earlier, backup programs can selectively back up and restore operating system files as they do data files, allowing for incremental backup and restore operations of most operating system files. Windows XP Professional, however, does not allow incremental restoration of operating system files.

The advanced backup options give you additional backup choices. Descriptions of the options and information about setting them follow.

To set advanced backup options

1. Open Backup, and then click **Advanced Mode**.
2. In the **Backup Utility** dialog box, click the **Backup** tab and then select the files and folders that you want to back up.
3. Click **Start Backup**.

4. In the **Backup Job Information** dialog box, click **Advanced**.
5. Set the advanced backup options that you want, and then click **OK**.

The advanced backup options are described in Table 14-1.

Table 14-1 Advanced Backup Options

Option	Description
Back up migrated Remote Storage data	Backs up data that has been designated for Remote Storage. You can restore Remote Storage data only to an NTFS volume that is used with Windows 2000, Windows Server 2003, and Windows XP Professional. Note that Remote Storage is available only on Windows 2000–based and Windows Server 2003–based computers.
Verify data after backup	Verifies that the backed-up data is exactly the same as the original data. This can substantially increase the time it takes to perform a backup.
Use hardware compression, if available	Compresses the data you are backing up so that you can save more data on a tape. If this option is disabled, you do not have a tape drive on your computer or your tape drive cannot compress data.
Automatically back up system-protected files along with the System State	Backs up all system files in your systemroot directory in addition to the boot files included with the System State data. This option is available only if you are backing up the System State.
Disable volume shadow copy	Allows you to disable volume shadow copy technology. This option is not available if you are backing up the System State.

Top of page

Using the Backup Tool

Backup is a graphical tool that is used with a variety of storage media to back up and restore files on volumes using any file system supported by Windows XP Professional. Backup also simplifies archiving and allows you to schedule jobs to automate backups.

Note The Backup utility is not included in a default installation of Windows XP Home Edition. See article 302894, "How to Install Backup from the CD-ROM in Windows XP Home Edition," in the Microsoft Knowledge Base at http://support.microsoft.com for information on how to manually install Backup from the Valueadd folder on the Windows XP Home Edition CD-ROM.

Removable Storage does tasks such as mounting and dismounting a tape or disc. It tracks and controls backup cartridges, which are typically organized into pools, on storage devices, and it allows applications such as Backup to share robotic changers and cartridge libraries. After Removable Storage is started, it is transparent, so you only need access to it when you change cartridges, not when you perform a backup or restore operation.

Note Removable Storage does not manage backing up to files on a random access medium, such as a hard disk or removable disk.

Because of Removable Storage technology in Windows XP Professional, target media of Backup are not drive-oriented as in the past. In versions of Backup included in Windows NT 4.0, backup data was written to drives (for example, tape or disc drives).

In Windows XP Professional, Backup uses cartridges in media pools to store backed-up data. Backup still writes backup data to tapes or files on discs but Removable Storage, which references media instead of drives, manages the media. Backup determines whether each cartridge to which it gains access is a member of an existing media pool or unallocated media. The significance of this change can be seen when a user sets up a regular backup schedule.

In the past, users scheduled Backup to run on specified days, and they could use any cartridge for that day's job. Removable Storage tracks the use of all cartridges, so it does not allow indiscriminate use of unrecognized cartridges by the applications that use Removable Storage to manage the media associated with their respective applications.

Each cartridge that Backup uses is added to Backup's application media pool, and you must identify a cartridge for each job you schedule. If you choose to back up your data to a different cartridge each night over the course of a week, you have to create seven scheduled jobs, or one job for each tape. This is because the job scheduler you can use with Backup requires that you specify a cartridge name in the scheduled job. (Each cartridge has a unique name recorded in the header of the data area.) If you place the Tuesday cartridge in the recording drive on Friday, the scheduled job is unsuccessful because the criteria required for completing the job are not met.

To improve your chances of success, run the backup manually the first time the cartridge is used and assign the cartridge a unique name (such as "Monday"). After you give each cartridge a unique name, create a set of scheduled backup jobs.

This feature is very important to pay attention to using a scheduled backup to a single drive (a drive that does not include a changer). In this case, Removable Storage cannot load the proper media into the drive. If the media left in the drive is not the expected media, the job will fail. Backup running in scheduled mode has no way of reporting failures to the user on an interactive basis; therefore, the backup log is the only way to determine whether failures of this type have occurred. If you do not review the backup logs, failures could prevent any backup from occurring during that session.

A new feature Windows XP Professional offers is the ability to view the media pools directly from Backup. In Windows 2000, you must view media pools by opening the Removable Storage snap-in in Microsoft Management Console (MMC).

For more information about Removable Storage, see "Removable Storage" later in this chapter.

Note If you use a multicartridge library device (such as a tape drive that contains a magazine of tapes) and set Backup to always draw cartridges from the free media pool, you need to schedule only one job. However, data on each previously used cartridge must be deleted, which places the cartridge back into the free media pool to be used again.

Files Skipped During Backup

Using volume shadow copy technology in Windows XP Professional, you can reduce the number and type of files skipped during backup. If the volume shadow copy fails, Backup defaults to non–shadow copy techniques used in previous editions of Windows.

If non–shadow copy technology is used, Backup skips the following files:

- Files that are open in other applications
- Files that Backup skips by default

Files Skipped by Default

Files that Backup skips by default include temporary files, such as Pagefile.sys, Hiberfil.sys, the ASR log file, the ASR error file, temporary files, and other files. These files are neither backed up nor restored by Backup. To display or configure which files Backup skips during a backup operation, do the following:

1. Open Backup, and then click **Advanced Mode**.
2. In the **Backup Utility** dialog box, select **Tools** and then **Options**.
3. Select the **Exclude Files** tab.

Backup also skips files on remote computers that are on a network share if the files are in use at the time of the backup.

Volume Shadow Copy Technology

Volume shadow copy technology provides an instant copy of the original volume. A shadow copy of the volume is made at the time a backup is initiated. Data is then backed up from the shadow copy instead of from the original volume. The original volume continues to change as the process continues, but the shadow copy of the volume remains constant. This is helpful if users need access to files while a backup is taking place.

Other important advantages of this technology include the following:

- A computer can be backed up while applications and services are running.
- Files are not skipped during the backup process.
- Files open at the time of the shadow copy appear closed on the shadow copy volume.
- The need for scheduling a *backup window* is eliminated. A backup window requires that applications be shut down to ensure a successful volume backup.

Using volume shadow copy technology, Windows XP Professional works with running applications to determine when a volume shadow copy occurs. The Volume Shadow Copy service then allows a backup application to access the volume and back it up. Applications continue running uninterrupted on the actual volumes. After the backup is completed and the data is saved on the backup media, the shadow copy is deleted.

By default, Windows XP Professional uses free disk space on any NTFS volume to store a record of the differences between the original volume and the shadow copy volume. The data on the shadow copy volume exists only while the shadow copy is being taken. The amount of disk space temporarily consumed depends on how much file data on the volume has changed during backup.

If sufficient temporary disk space is not available, Windows XP Professional cannot complete a volume shadow copy and Backup skips open files. Thus you must provide sufficient disk space to create a shadow copy of open files. Applications that can use Backup can register writer interfaces, which help coordinate the backup activity with the backup application.

Windows XP Professional uses volume shadow copy technology by default. If you only want to back up a few files or directories, you might want to disable shadow copies to avoid delays.

For more information about volume shadow copy technology, see Windows XP Professional Help and Support Center.

Note Volume shadow copies require that you use NTFS for your file system.

Automated System Recovery

The Automated System Recovery (ASR) tool, an advanced option of the Backup Tool (NTBackup.exe), is new in Windows XP Professional. The ASR feature replaces the Emergency Repair Disk found in Windows 2000 and Windows NT 4.0. Use ASR to restore your system only if other disaster recovery tools are unavailable.

ASR allows you to restore the operating system to a previous state so that you can start Windows XP Professional when other recovery methods do not work. For example, disk damage might prevent you from starting Windows XP Professional in normal or safe mode, or it might prevent you from using Recovery Console and Last Known Good Configuration. ASR gives you another way to start your system.

ASR consists of two parts that automate the process of saving and restoring system state information: ASR backup and ASR restore. To learn more about disaster recovery tools, see Appendix C, “Tools for Troubleshooting.”

ASR Backup

The ASR Wizard guides you through the process of saving ASR backups to removable media. When using the wizard to create an ASR backup, you need to decide where to store the ASR backup data and have a blank floppy disk available.

To locate the ASR wizard

1. In **All Programs**, point to **Accessories**, **System Tools**, and then click **Backup**.

2. Click **Advanced Mode**, and then click **Automated System Recovery Wizard**.

On the floppy disk, the wizard saves only hard-disk configuration information (not user data), such as disk signatures, the partition table, and volume data. If you run the ASR restore operation later, ASR restore configures disks by using the saved data on the ASR floppy disk. The ASR backup operation scans your system and lists files to save for an ASR restore.

ASR Restore

The ASR restore text-mode process relies on Windows XP Professional Setup along with the information stored on an ASR floppy disk. Before you begin, gather the following items:

- The most recent ASR floppy disk
- The Windows XP Professional operating system CD
- The most recent ASR backup media set, typically removable media such as data tape cartridges

To restore your system by using ASR

1. Insert the Windows XP Professional operating system CD, and then restart your computer.
2. At the **Press any key to boot CD** prompt, press any key.
3. At the **ASR** prompt, press **F2**.
4. At the prompt, insert an ASR floppy disk.
5. At the prompt, insert ASR backup media (typically one or more pieces of removable media such as data tape cartridges).
6. At the prompt, provide a destination folder, such as C:\Windows or C:\Winnt.

ASR checks the backup media. To avoid application configuration issues, give the destination folder the same directory name that you used when you created the ASR backup.

Restoring from network shares is not an ASR option. Therefore, you must use locally attached devices such as the following devices attached to ATA or SCSI adapters:

- Tape backup drives
- Removable disks, including CDs
- Other hard disks

ASR considerations

ASR is not a replacement for regular backups in which files stored on one or more volumes are saved to backup media. Because ASR saves only the files necessary to restore system state, data loss might occur. Therefore, always consider other recovery options before using ASR.

For more information about Recovery Console, see Appendix C, "Tools for Troubleshooting."

Before using ASR, consider the following points:

- ASR formats the *systemdrive* partition as part of the restore process. When you have dedicated space for user data files on the system partition (*systemdrive*), personal data or application files are not restored, and data loss is possible.
- ASR restores only operating system files that it determines need repair. However, ASR might initialize operating system volumes that also contain users' personal files. Therefore, there is a risk to user files stored on these volumes.

  ASR is different from the System Restore feature. ASR is a recovery tool that

- backs up all files on the system partition and is used to bring a system back online if startup fails. System Restore saves only incremental changes, or shadow copies, and lets you start Windows XP Professional in normal or safe mode. Always try System Restore before resorting to ASR.
- ASR supports FAT16 volumes up to 2.1 GB only. ASR does not support 4 GB FAT16 partitions that use a cluster size of 64 kilobytes (KB). If your system contains 4 GB FAT16 partitions, convert them from FAT16 to NTFS before using ASR. For more information about volumes and clusters, see Chapter 13, “Working with File Systems.”

For more information about Automated System Recovery, see Windows XP Professional Help and Support Center.

Top of page

Removable Storage

Removable Storage provides services to applications and system administrators that facilitate the use, sharing, and management of removable media devices, such as tape drives and robotic storage libraries. The availability of Removable Storage technology eliminates the need for independent software vendors (ISVs) to develop customized solutions and support for these devices on a per-device basis. More importantly, Removable Storage enables multiple storage applications to share expensive removable media storage devices. Thus the focus of storage applications can be directed to customer features rather than hardware issues.

As shown in Figure 14-1, Removable Storage provides a single set of application programming interfaces (APIs) that allow applications to catalog all removable media (except floppy disks and similar small-capacity media), such as disc, tape, and optical media, which are either stored on shelves (offline) or in libraries (online). Also, by disguising the complexities of underlying robotic library systems, Removable Storage lowers the costs of developing and operating storage applications and provides consistency for customers who purchase these applications.

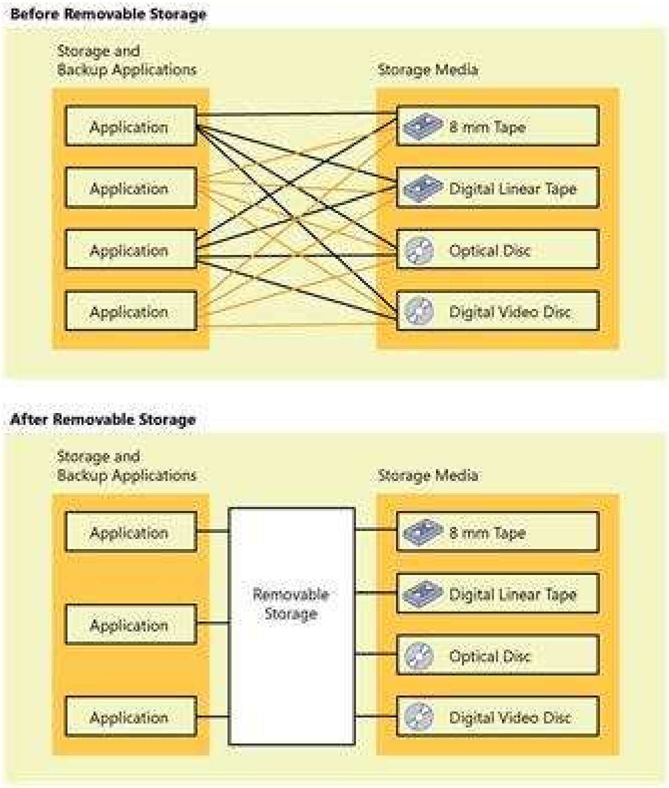

Figure 14-1 Removable media with and without Removable Storage
See full-sized image

Removable Storage uses media pools to organize media. Media pools control access to media, group media into media types according to use, allow media to be shared across applications, and allow Removable Storage to track application sharing.

Basic Concepts

Removable Storage can be described in terms of five basic concepts: media units, media libraries, media pools, work queue items, and operator requests. The first item in this list, *media*, is fundamental and affects all others. The remaining four items in the list are the top-level nodes in the Removable Storage snap-in.

Media Units

Media are classified into media units (also known as cartridges or discs) of a certain type, such as 8mm tape, magnetic disc, optical disc, or CD-ROM.

While both sides of double-sided media must be contained in the same library, the state of each side can be different. For example, one side can be allocated, and the other side can be available.

Media Libraries

Removable Storage manages two classes of libraries: online libraries and offline media physical locations. Libraries include both cartridges and the means to read and write them. The offline media physical location is a special holder for cartridges that are cataloged by Removable Storage but do not reside in a library.

Online libraries

In its simplest form, a *library* consists of the following components:

- A data storage cartridge
- A means of reading and writing to the cartridge

For example, a CD-ROM drive is a simple library with one drive, no slots, an insert/eject port, and no transport.

In comparison, a robotic-based tape library can hold up to several thousand tapes, have one or more tape drives, and have a mechanical means of moving tapes into and out of the drives.

Robotic library

A robotic library can contain any of the following components: cartridges, slots to hold the cartridges, one or more drives, a transport, and either a door or an insert/eject port. No user intervention is required to place a cartridge in a library in one of its drives.

Stand-alone drive library

In a stand-alone drive library (also known as a stand-alone drive), the user or a transport must place a cartridge in a drive. The CD-ROM drive on most desktop computers is a stand-alone drive library. Removable Storage treats any drive that has an insert/eject port as a stand-alone library.

Offline media physical location

In an online library, the location of a cartridge is the library in which it resides. Cartridges that are not in an online library, such as archived backup tapes on a shelf, are offline media that reside in an offline media physical location. When a user or administrator moves an offline medium into an online library, Removable Storage tracks its location to the library into which it is placed. When a cartridge is taken out of an online library, Removable Storage designates its location as the offline media physical location.

Media Pools

A media pool is a logical collection of cartridges that share some common attributes. A media pool contains media of only one type, but a media pool can contain more than one library. Both sides of a two-sided cartridge are always in the same pool.

Each media pool can control access to the media that belong to it. Although a media pool does not control access to the data that is contained on the cartridges, it does control how the cartridges are manipulated, including an application’s ability to move a cartridge from the pool or to allocate a cartridge for its own use.

Media pools can be used hierarchically to hold other media pools or to hold cartridges. An application that needs to group media of several types into one collection can create one application media pool for the whole collection and additional media pools within the original pool—one for each media type. A *free pool* contains a media pool for each media type. Media pools are categorized into two classes: system media pools and application media pools. The system and application media pools are defined as follows:

- System pools, which are created by Removable Storage for its own use, include free pools, import pools, and unrecognized pools.
- Application pools, which are created by applications to group media, allow

several applications to share the libraries attached to a system.

System pools
The following three kinds of system pools hold cartridges when they are not in use:

- **Free pool.** Holds unused cartridges that are available to applications
- **Import pool.** Temporarily holds cartridges newly placed in a library
- **Unrecognized pool.** Temporarily holds unidentifiable cartridges newly placed in a library

Free pool
Free pools support sharing cartridges among applications. The pools contain blank or recycled cartridges that are available to any application. An application can draw cartridges from the free pools, and it can return cartridges to the free pools when the cartridges are no longer needed.

Import pool
When a cartridge is placed in a library, if Removable Storage can identify the format or the application that is associated with it, but has not seen it before, Removable Storage places the cartridge in the import pool. For example, if an administrator places a tape written by Backup on one computer into a library that is attached to a second computer, Removable Storage on the second system recognizes that the tape was written using Microsoft Tape Format (MTF) and places it in the import pool for its media type.

Unrecognized pool
When a cartridge is placed in a library, if Removable Storage cannot identify the format or the application that is associated with it and has not seen the cartridge before, Removable Storage places the cartridge in the unrecognized pool for its media type. Blank cartridges are treated this way. Cartridges in unrecognized pools might have data on them, but Removable Storage cannot read data on these cartridges and cannot catalog them. Cartridges in the unrecognized pool are not available for backup media. Instead, they must be moved to the free pool to be used by Backup. When Backup first starts, it checks the unrecognized pool for media. If media is found there, Backup offers the user the option to move the media to the free pool.

Caution Moving media to the free pool deletes all data contained on the media.

Application Pools
Each application that uses cartridges managed by Removable Storage uses one or more application pools. Applications can create these pools, or you can create them by using Removable Storage. You can set permissions for application pools that allow applications to share pools or that assign each application its own set of pools.

Work Queue Items
When applications make a library request, Removable Storage places the request in a queue and processes it as resources become available. For example, a request to mount a tape in a library results in a mount work queue item, which might wait until a drive or slot is available.

Operator Requests
Sometimes, even with robotic libraries, manual assistance is required to complete a request or perform maintenance. If an application requests that a cartridge in an offline location be mounted, the cartridge must be manually entered into the online library. This generates a request to the administrator or

an operator to enter the cartridge.

Available Backup Media

Backup displays a list of all available storage devices in the **Backup destination** list on the **Backup** tab. If Backup does not detect any external storage devices, you can back up data to a file on the hard disk. If you want to back up to a medium that Removable Storage does not manage, make sure that you load the medium in the appropriate storage device.

When you back up data to cartridges that are managed by Removable Storage, make sure that Removable Storage is running. (You can confirm this in the Services console of the MMC.) To back up to new cartridges, first make the cartridges available in the media pool. In an existing media pool, cartridges must be loaded in a library.

Locked Files

In Windows XP Professional, you can back up local files that the operating system locks, such as event logs and registry files. However, Backup skips event logs and registry files if they are open in other applications and you do not use the shadow copy method to back up files.

To minimize the number of files that are not backed up, use the default method of backing up files, which uses volume shadow copy technology. If you choose to use another method of backing up files, avoid running applications while Backup is running.

Encrypted Files

Encrypted files remain encrypted when they are backed up. Therefore, it is important to ensure that user keys, particularly the recovery agent keys, are also stored safely on backup cartridges. The Certificates console provides methods for exporting keys to floppy disks or to other removable media so that they can be secured.

For information about Encrypting File System (EFS), see Chapter 13, “Working with File Systems.”

Backing Up Files on Your Local Computer

Using Backup, you can back up any file on your local hard disk.

Because most changes on a server occur as users add, modify, or delete files from their computers, back up changes to users’ folders daily.

Some users keep most of the files that they want backed up on network shares. Other users require that data on local computers be backed up. Your backup procedures need to take both situations into account.

Network users primarily use applications such as Microsoft Word. You can reinstall the executable files from the original distribution medium, but the time and productivity that is lost doing this make the approach less than ideal. In addition, if you have customized the applications to suit the needs of your organization, reproducing those settings can be more difficult than reloading the programs themselves. Because the applications rarely change, backing them up as part of your backup procedure uses minimal offline storage space and ensures that the latest version is always available.

Backing Up Files on Remote Computers

You can use Backup on any computer to which you can connect remotely. This allows a single-medium drive to be shared across an entire network and one backup policy to be in effect for the entire network.

You cannot back up System State data directly from a remote computer by using Backup. You can back up files and folders on a remote computer only by using a shared folder.

To back up the System State data of a remote computer

1. Run Backup locally on the remote computer to save the System State data to a file on a shared volume.
2. Back up the System State data file remotely to the shared volume.

To restore the System State data of a remote computer

1. Restore the System State data file remotely to the shared volume.
2. Restore the System State data file locally on the local computer.

   Tip See article 315412, "How to Back Up the System State Data of a Remote Computer in Windows 2000," in the Microsoft Knowledge Base at http://support.microsoft.com for more information on how to schedule backup of System State information on a remote computer.

Top of page

Restoring Data

If files or directory services are not accessible, you must restore them. Restore operations are possible only if you have used Backup or another program to back up the files. Using Backup, you can restore the entire backup medium, one or more backup sets, or individual files. After the restore operation starts, you can restore the System State data as well.

Typically, all catalog information is maintained on the corresponding medium for that backup set.

When you insert a backup medium to restore data, only information about the first backup set is displayed. To restore the entire medium, first load the catalog by right-clicking the media and selecting **Catalog**. Otherwise, when you select a medium, you select only the displayed sets.

Restoring System State Data

When you restore the System State data, all System State data that is relevant to your computer is restored. However, as a result of dependencies among the system state components, you cannot back up or restore individual components of the System State data.

To restore System State data

1. Log on to the computer as the administrator.
2. Start **Backup**.
3. Click the **Restore** tab, and then select the check box for any drive, folder, or file that you want to restore.
4. Select the **System State** check box to restore the System State data and any other data you selected for the current restore operation.

   Caution If you restore the System State data and you do not designate an alternate location for the restored data, Backup replaces the System State data on your computer with the System State data you are restoring.

Files from Third-Party Backup Programs

You can use Backup to restore data from a tape that was backed up by using a program other than Backup if the tape is in Microsoft Tape Format (MTF). Although the tape might not have the full on-tape catalog information that Backup produces, it must have equivalent information. Also, some older tape backup devices might not support creating full on-tape catalogs by using Backup. Contact the vendor if you suspect that your tape backup device does not support creating a full on-tape catalog.

File Security Settings

Backup preserves permissions, ownership, and audit flags on files restored to NTFS volumes, but not on files restored to FAT volumes. It is not possible to secure that type of information on FAT volumes.

When you restore files to a new computer or hard disk, you do not have to restore security information. The files inherit the permissions of the NTFS directory in which they are placed. If the directory has no permissions, the file retains its previous permissions, including ownership.

Top of page

Additional Resources

These resources contain additional information and tools related to this chapter.

Related Information

- Chapter 13, “Working with File Systems”
- Chapter 27, “Understanding Troubleshooting”
- Appendix C, “Tools for Troubleshooting”

Top of page ◄ 14 of 29 ►

Manage Your Profile