Server
Enterprise

CHAPTER

15

Backing Up and Restoring Data

Backing Up Files and Folders 561
What to Back Up 561
Backup Types 562
Backup Strategies 563
Security considerations 564
Tape rotation 565
Documenting backups 566
Performing a Backup Using Windows NT Backup 566
Using the Schedule Service to Automate Backups 570
Restoring Files and Folders 571
Test Your Backup with a Trial Restore 571
Performing a Restore Using Windows NT Backup 571
Key Point Summary 574
Applying What You've Learned 576
Instant Assessment 576
Hands-on Lab Exercise 577
Lab 15.24: Performing a backup 577

About Chapter 15

This chapter covers the basics of backing up and restoring your Windows NT computer's data.

Chapter 15 begins by explaining the importance of performing and testing regular backups. Various backup types, such as normal, differential, and incremental are considered; and common backup strategies are presented. Security considerations are presented, as well as tape rotation schemes and tips for documenting backups.

Next, the chapter takes you through the steps to perform a backup using Windows NT Backup. Backing up the local Registry is included in this section. Finally, the chapter outlines the steps to perform a restore by using Windows NT Backup.

This chapter includes one hands-on lab that requires the use of a tape drive. In this lab you practice using Windows NT Backup to back up files and folders on your Windows NT computer.

If you're reading this book, it's probably important for you to know how to back up and restore data. That said, this chapter can be considered optional if you're preparing for only the Workstation exam, but is absolutely essential if you're preparing for either the Server or Enterprise exams. This chapter maps to various fault tolerance and Registry backup objectives in the Troubleshooting section in the Server and Enterprise exams' objectives.

Backing Up Files and Folders

Backing up files and folders is an important part of your network fault tolerance plan. Planning and adhering to a regular backup schedule can make recovering from a corrupt file or a failed hard drive a straightforward, if somewhat painful, task. Failing to make regular backups of your system's critical data can be harmful (or even fatal) to your business and/or to your employment status.

A tape backup is *not* a replacement for other fault tolerance methods, such as disk mirroring and striping with parity. It is an additional safety precaution to use when other fault tolerance methods fail. I don't recommend that you rely solely on disk mirroring, striping with parity, or tape backup. A comprehensive fault tolerance policy typically should include two or more of these strategies.

Always remember that a tape backup is your last line of defense against data loss. If the data on the tape is too old to be of value, or if it is corrupt, or if the tape has been damaged due to fire or other causes, then you have nothing. And having nothing is very hard to explain to upper management.

It's been my sorry duty, on more than one occasion, to have to explain to a client that both disks in a mirrored pair have failed, *and* that their most recent tape backup is corrupt. I can't stress enough the importance of carefully performing regular tape backups and periodically testing the validity of those backups. If you've ever experienced a partial or total disk failure, you know why I'm saying this. Have a hard disk fail on you—and you will never regret the time it takes you to perform backups again.

This chapter covers the basics about backing up and restoring data, including what to back up, backup types, using Windows NT Backup to perform a backup, using the Schedule service to automate backups, and restoring files and folders.

What to Back Up

Before you can create a backup strategy, you need to determine which data on your network will be backed up. I recommend that all network data be backed up regularly to tape. This includes operating systems, applications, the Registry, and user-created data files.

In general, operating systems and applications need to be backed up less frequently than user-created data files. You may find it sufficient to back up operating systems and applications once a week, once a month, or even less often. I recommend that you back up operating systems and applications, on separate tapes, initially and every time you modify the operating system or install a new application.

Depending on the importance of the data, user-created data files can be backed up once a week, once a day, once an hour, or at any frequency that meets your organization's needs. When determining which files to back up and how often, the main question you need to ask yourself is *how much data can you afford to lose?* For example, if you decide to back up only once a week, can you afford to lose six days of sales information and other employee-created data?

Backup Types

Before the specific backup types are presented, a short discussion on the archive attribute, and how the operating system and backup programs use this attribute, is in order.

The *archive attribute* is a marker that the operating system automatically assigns to all files and folders when they are first installed or created. Depending on the backup type, backup programs *remove* the archive attribute from a file or folder to indicate that the file or folder has been backed up. If a file or folder is modified after it is backed up, the operating system reassigns the archive attribute to it.

There are five standard types of backups that you can perform:

- **Normal (full):** A *normal backup* backs up all selected files and folders. It removes the archive attribute from the backed up files and folders. A normal backup is a full, complete backup—it is the backbone of your backup plan or strategy.
- **Differential:** A *differential backup* backs up all selected files and folders that have changed since the last normal (full) backup. A differential backup does *not* remove the archive attribute from any files or folders. A differential backup is a *cumulative* backup since the last normal (full) backup. Because the differential backup does not remove the archive attribute, if a normal backup is performed on Sunday, and differential backups are performed Monday through Friday, Monday's differential backup will contain all changes made to data on Monday; Tuesday's

differential backup will contain all changes made to data on Monday and Tuesday, Wednesday's differential backup will contain all changes made to data on Monday, Tuesday, and Wednesday, and so on. A differential backup is often used in between normal backups, because it takes less time to perform a differential backup than a normal backup.

- **Incremental:** An *incremental backup* backs up all selected files and folders that have changed since the last normal or incremental backup. An incremental backup removes the archive attribute from the backed up files and folders. An incremental backup is *not* cumulative like a differential backup. It contains only changes made since the last normal or incremental backup. If a normal backup is performed on Sunday, Monday's incremental backup will contain all changes made to data on Monday; Tuesday's incremental backup will contain all changes made to data only on Tuesday; Wednesday's incremental backup will contain all changes made to data only on Wednesday, and so on. Because less data is backed up, an incremental backup takes even less time to perform than a differential backup.
- **Copy:** A *copy backup* backs up all selected files and folders. It does not remove or otherwise affect the archive attribute. The copy backup can be performed without disrupting the normal backup schedule, because it does not affect the archive attribute. You could use a copy backup to create an extra backup to store off-site**.**
- **Daily:** A *daily backup* backs up all selected files and folders that have changed during the day the backup is made. It does not remove or otherwise affect the archive attribute.

Companies often use a combination of the standard backup types in their backup strategy.

Backup Strategies

There are a number of acceptable backup strategies, and three fairly common ones:

- *Perform a normal (full) backup every day*. This is the most time-consuming of the three common strategies. However, should a restore be necessary, only the last normal backup is required, and restore time is generally less than either of the other two strategies.

- *Perform a weekly normal backup and daily differential backups.* As the week progresses, the time required to perform the differential backups increases. However, should a restore be necessary, only two backups will be needed—the most recent normal backup, and the most recent differential backup. (This is because the most recent differential backup contains *all* files and folders that have changed since the last normal backup.) The restore can be accomplished relatively quickly.
- *Perform a weekly normal backup and daily incremental backups.* Incremental backups tend to take about the same amount of time each day, and are considered the fastest backup method. However, should a restore be necessary, multiple backup sets will be required—the most recent normal backup, and *every* incremental backup since the most recent normal backup. (This is because the incremental backups each contain different data and are not cumulative.) The restore will typically take more time than if a differential backup had been used.

When planning your backup strategy, the big trade-off you need to consider is time—the time it takes to perform backups versus the time it takes to restore data.

Security considerations

When planning your company's backup strategy, there are a few security considerations to take into account:

- If the data is of a sensitive nature, consider physically securing the tape drive and the backup tapes. While your server may require a password and permissions to access confidential data, when a backup tape is taken and restored on another server, your server's security measures are defeated.
- Consider rotating backup tapes to an off-site location. This can prevent or minimize data loss due to a single catastrophic event, such as a theft, fire, flood, or earthquake. Consider using a third-party company that will store your data tapes in a secure, climate-controlled environment.
- If you store backup tapes in a fireproof safe, remember that *fireproof* does not necessarily mean that heat or smoke can't destroy magnetic tapes. Make sure the safe is capable of protecting magnetic media as well as papers and other important items.

- Finally, depending on your organization's security needs, consider who should perform backups. In very high-security environments, consider allowing only administrators to perform backups. In medium-to-low-security situations, consider separating the backup and restore functions by designating certain personnel to perform only backups, and other employees to perform only restores.

Tape rotation

Most organizations rotate their magnetic tapes in order to reduce the cost of backups. Instead of using a new tape every day, tapes are reused in a systematic manner.

There are probably almost as many tape rotation methods as there are network administrators. Consider the following tape rotation example, which is illustrated in Table 15-1.

TABLE 15-1 SAMPLE BACKUP TAPE ROTATION SCHEME

MONDAY	*TUESDAY*	*WEDNESDAY*	*THURSDAY*	*FRIDAY*
Tape # 1	Tape # 2	Tape # 3	Tape # 4	Tape # 5
Tape # 1	Tape # 2	Tape # 3	Tape # 4	Tape # 6
Tape # 1	Tape # 2	Tape # 3	Tape # 4	Tape # 7
Tape # 1	Tape # 2	Tape # 3	Tape # 4	Tape # 8-Archived

This example requires eight tapes for a four-week period. Tapes one through four are reused each week, with the Monday tape used again the following Monday, and so on. Depending on the amount of data backed up and the tape's capacity, the data from the previous backup can be appended or replaced. The eighth tape is permanently archived and removed from the tape rotation scheme.

When choosing a tape rotation method, consider the following:

- The useful life of a tape. Tapes need to be eventually removed from the rotation scheme and replaced with new tapes. The number of times a magnetic tape can be reused depends on the tape's quality and storage conditions.

- Tape cost versus the cost of lost data. Many tapes are guaranteed for life—but for only the cost of the tape. The cost of lost data is not guaranteed.
- Removing a tape from the rotation schedule weekly, monthly, or quarterly to provide a permanent, long-term archive of your data.

Documenting backups

Documenting your backups will make restoring after a failure a much easier task.

You should consider keeping a backup log book that documents each backup procedure performed. You should record the date and time the backup was performed, a brief description of the data backed up, the name of the person who performed the backup, the tape number used, and its storage location. You can also include a detailed or summarized printed log of the backup. If you have this information readily available, the person performing the restore will be able to quickly identify and locate the most recent backup tape(s) needed.

Most backup programs can be configured to create detailed logs that list the individual files and folders backed up. These logs can be quite helpful if a user tells you that he or she has accidentally deleted an important file, and asks you to restore it from tape. A log (either printed, or written to a file on disk) will enable you to locate the appropriate tape needed to restore the file quickly and easily.

Performing a Backup Using Windows NT Backup

Windows NT ships with a backup program called *Windows NT Backup*. NT Backup is a basic tape backup program that gives you full capability to back up and restore a Windows NT computer, including the local Registry. It does not back up the Registry on computers other than the one in which the tape device is installed. NT Backup does not provide the extensive scheduling and automation features included in more sophisticated third-party backup programs.

In order to perform a backup, you need a tape drive that is compatible with NT (check the *Windows NT Hardware Compatibility List* [HCL]). If possible, select a tape drive that has the capacity to back up your entire server on a single tape. This is a big help, especially if you perform unattended tape backups.

Before you perform a tape backup using Windows NT Backup, you need to install a tape device and driver, if you haven't already done so, by using the Tape Devices application in Control Panel. Also, make sure that you have the appropriate user rights to perform a backup — you need to either be a member of the Administrators, Backup Operators, or Server Operators groups; or, you need to have the "Back up files and directories" user right assigned to you.

Consider the time of day when performing backups. Because of the utilization of processor and memory during backup, it's normally best to perform backups during the periods of lowest server and/or network usage — often after business hours.

TO PERFORM A BACKUP USING WINDOWS NT BACKUP, FOLLOW THESE STEPS:

1. Place a tape in the tape drive.
2. Start ➪ Programs ➪ Administrative Tools (Common) ➪ Backup.
3. The Backup dialog box appears. Select Window ➪ Drives.
4. Maximize the Drives dialog box. Select the drive(s) and/or files and/or folders that you want to back up.
   - To back up an entire drive, select the check box next to the drive.
   - To back up individual files and folders, double-click the drive that contains those files and folders, and then select the check boxes next to the files and/or folders that you want to back up. Click the Backup command button.
5. The Backup Information dialog box appears, as shown in Figure 15-1. Notice the various backup configuration options available.
   - **Tape Name:** In the Tape Name text box, either accept the default name listed or type in a new name for the tape.
   - **Verify After Backup:** Select the check box next to Verify After Backup if you want Windows NT Backup to verify the files and folders it has backed up. It's a good idea to verify after a backup, even though selecting this option approximately doubles the time the backup takes.
   - **Backup Local Registry:** Select the check box next to Backup Local Registry (if it is not grayed out) if you want Windows NT Backup to include the Registry on the computer that the tape drive is installed on in its backup. In order to back up the Registry, you must select at least one file or folder for backup on the drive on which Windows NT is installed.

- **Restrict Access to Owner or Administrator:** Select the check box next to Restrict Access to Owner or Administrator if you want Windows NT Backup to only enable the owner of the tape, an Administrator, or a member of the Backup Operators group to read, write, or erase the tape using Windows NT Backup.
- **Hardware Compression:** Select the check box next to Hardware Compression if you want the backup data compressed as it is backed up, and if your tape backup hardware supports this feature.
- **Operation:** In the Operation section, you have two options: you can choose to have this backup appended to the last backup on the tape, or you can choose to have Windows NT Backup write over (replace) any existing data on the tape. (Replace is the default operation.)
- **Backup Set Information:** In the Backup Set Information section, you can type a description of the backup. I recommend that you enter the date, a brief description of the data backed up, and the type of backup performed.
- **Backup Type:** In the Backup Type drop-down list box, select the backup type you want to perform: Normal, Copy, Differential, Incremental, or Daily.
- **Log Information:** In the Log Information section, Windows NT Backup shows the location to which it will write a backup log. Modify this location if necessary.
- **Log Options:** Select the radio button next to one of the three log options, depending on the type of log you want NT Backup to create: Full Detail, Summary Only, or Don't Log. (Summary Only is the default log option.) Click OK.

6. The Backup Status dialog box appears. If the tape has been used before, a Replace Information dialog box appears. These dialog boxes are shown in Figure 15-2. Click the Yes command button to have Windows NT Backup replace the data on the tape with the backup you are preparing to perform.
7. Windows NT Backup performs the backup. (This process takes several minutes to several hours, depending on the amount of data being backed up and your tape drive speed.)
8. The Verify Status dialog box appears if you selected Verify After Backup. Windows NT Backup verifies that all files and folders were backed up correctly. (This process takes approximately the same amount of time as the backup.) Figure 15-3 shows the Verify Status dialog box after the verify has been completed. Notice the information presented in the Summary list box. Click OK after the verify is completed.

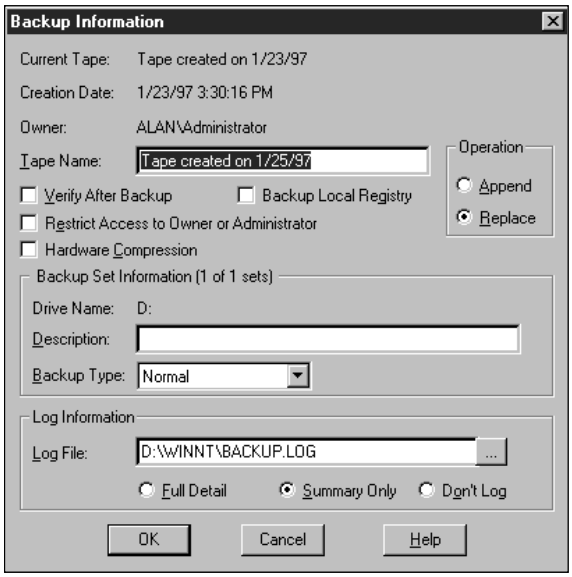


FIGURE 15-1 **Configurable options in Windows NT Backup**

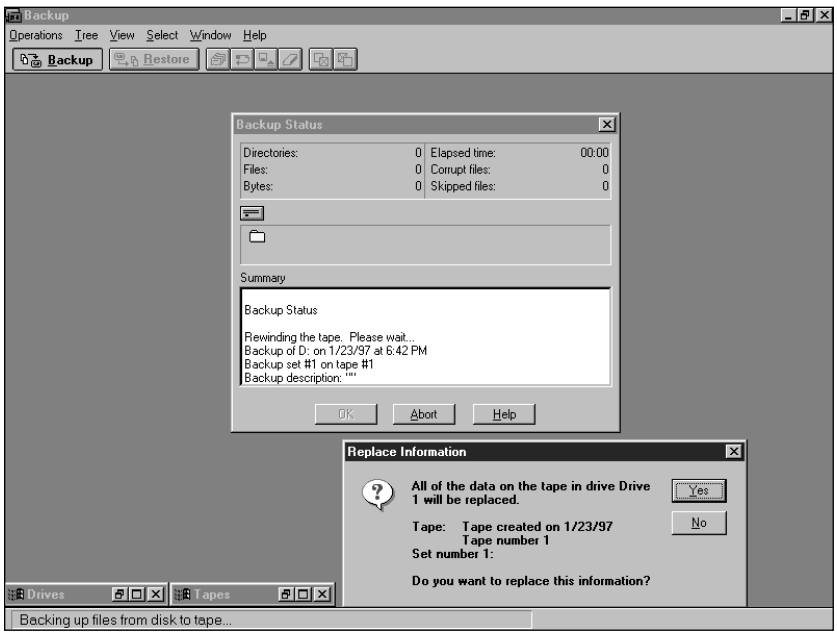


FIGURE 15-2 **Performing a backup using Windows NT Backup**

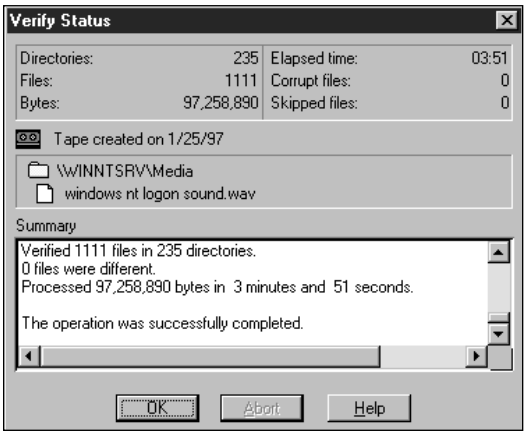


FIGURE 15-3 **Windows NT Backup verification completed**

9. Exit Windows NT Backup.

Using the Schedule Service to Automate Backups

You can use the Schedule service in Windows NT to schedule unattended (automated) backups.

To do this, you must first configure the Schedule service to start automatically (by default, it is started manually) by using the Services application in Control Panel.

Then you must use the `At.exe` command-line utility to schedule and configure the unattended backup. All options of Windows NT Backup can be configured and scheduled by using this utility in conjunction with the `NTBackup.exe` (Windows NT Backup) utility's command-line switches.

concept link

A detailed discussion of the command-line syntax and switches is beyond the scope of this book. For more information on the `At.exe` command-line utility, type at /? at the command prompt. For more information on the `NTBackup.exe` utility's command-line switches, type ntbackup /? at the command prompt. You might also want to check out the Command Scheduler, a graphical scheduler utility on the compact disc that ships with the *Microsoft Windows NT Server Resource Kit* (Microsoft Press, 1996). Command Scheduler is a graphical version of the `At.exe` command-line utility.

Restoring Files and Folders

Hopefully, you'll never have to restore files and folders after a catastrophic data loss. Nevertheless, it's a good practice to be comfortable with the process of restoring data to your system, just in case.

For this reason, and also to ensure that your backup tapes contain valid copies of your data files, you should periodically test your backup by performing a trial restore.

The following sections discuss testing your backup with a trial restore and performing a restore using Windows NT Backup.

Test Your Backup with a Trial Restore

To test the validity of the data contained on a backup tape, you should restore at least one folder that contains several data files to a *different* folder than it was originally backed up from. The folder you restore to is a test folder, and shouldn't contain other files. For example, you could restore the `D:\Public` folder to `D:\Public2` or to `E:\Public2`. This process verifies that the tape can be read, and that files and folders can be restored from it.

Once you've restored the folder, compare its contents with the original folder (on your hard drive) to find out whether the files are the same by using the `Comp.exe` command-line utility. If there are no differences between the files compared, then presumably all of the files on the backup tape are valid and not corrupt.

Another resource you can use to compare files is the `Windiff.exe` graphical utility that ships with the *Microsoft Windows NT Server Resource Kit*. An advantage to using `Windiff.exe` is that it enables you to specify *multiple files and folders* for comparison; as opposed to `Comp.exe`, which only enables you to specify a single file at a time for comparison.

Performing a Restore Using Windows NT Backup

You can use Windows NT Backup to perform a full or partial restore of data from a tape backup created by using NT Backup.

TO PERFORM A RESTORE USING WINDOWS NT BACKUP, FOLLOW THESE STEPS:

1. Place the backup tape that contains the data you want to restore in the tape drive. (If the tape backup consisted of more than one tape, insert the *last* tape in the backup set into the tape drive, because NT Backup wrote a catalog of the backup to this tape.)
2. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ Backup.
3. The Backup dialog box appears. Select Window ≥ Tapes.
4. Maximize the Tapes window that is displayed. If you want to perform a full restore, select the check box next to the backup set you want to restore in the right-hand window. If you want to perform a partial restore, double-click the backup set in the right-hand window. Windows NT Backup loads a catalog list of the files and folders in the backup. Then select the check boxes next to the individual files and folders you want to restore.

   Click the Restore command button.
5. The Restore Information dialog box appears, as shown in Figure 15-4. Notice the available configuration options.

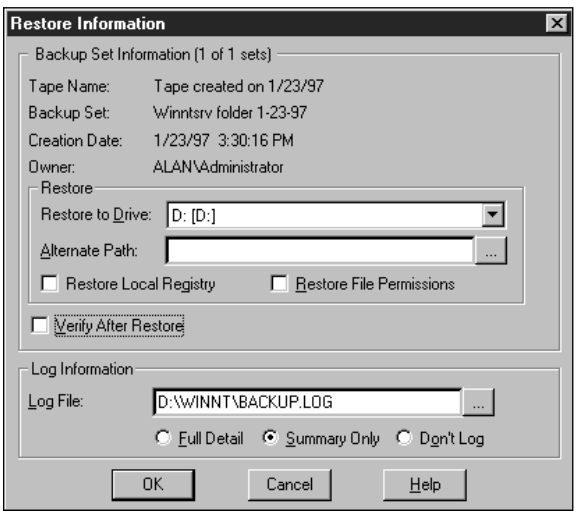


FIGURE 15-4 **Restore options available in Windows NT Backup**

- **Restore to Drive and Alternate Path:** If you want the selected files to be restored to their original drive location, accept the default in the Restore to Drive drop-down list box. Otherwise, you can specify a new drive letter, and then specify a folder that you want the files restored to in

the Alternate Path text box. (You might want to do this if you're doing a trial restore to test your backup.)

- **Restore Local Registry:** Select the check box next to Restore Local Registry only if you want the current Registry on your server replaced with the Registry on the backup tape. Use great caution when exercising this option.
- **Restore File Permissions:** Select the check box next to Restore File Permissions if you want to keep the file permissions as they were stored on the tape backup. Otherwise, the restored files will be assigned their file permissions based on the permissions of the folder to which they are restored.
- **Verify After Restore:** Select the check box next to Verify After Restore if you want NT Backup to verify files after it restores them. (Selecting this option approximately doubles the time it takes to perform a restore.)
- **Log Information:** Configure the Log Information section. (The options are the same for performing restores as they are for performing backups.) Click OK.

6. The Restore Status dialog box appears. NT Backup rewinds the tape and restores the files and/or folders selected, and verifies the files and folders selected if configured to do so. (This process can take a while.) The Restore Status dialog box, after the restore is completed, is shown in Figure 15-5. Notice the information presented in the Summary list box. Click OK.

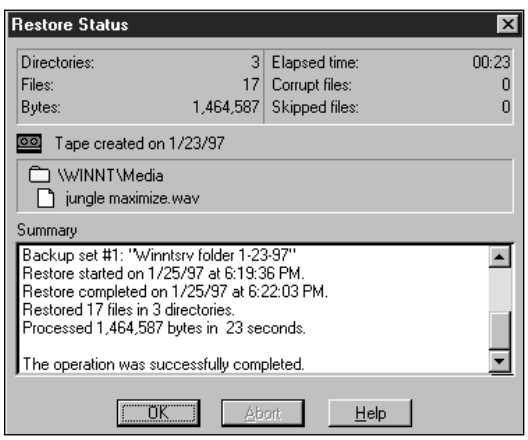


FIGURE 15-5 **Restore completed**

7. Exit Windows NT Backup.

Key Point Summary

This chapter covered the importance of backing up files and folders, how to decide which data to back up, and various backup types and strategies. Performing a backup using Windows NT Backup and utilizing the Schedule service were also outlined. Finally, Chapter 15 covered restoring files and folders.

- *Backup is an important part of your network fault tolerance plan.* Backup is not a substitute for other fault tolerance methods, such as disk mirroring and striping with parity, but is an additional safety precaution. A tape backup is your last line of defense against data loss.
- *All network data should be regularly backed up to tape,* including: operating systems, applications, the Registry, and user-created data files. It's a good idea to back up operating systems and applications on separate tapes, and separately from data file backups, to make the restore process easier. Determining the frequency of backup is often based on the answer to the question: How much data can you afford to lose?
- The *archive attribute* is a marker that, when removed from a file or folder, indicates that the file or folder has been backed up.
- There are five standard types of backups:
  - **Normal (full):** Backs up all selected files and folders, and removes the archive attribute from the backed up files and folders.
  - **Differential:** Backs up all selected files and folders that have changed since the last normal backup, and does *not* remove the archive attribute from files or folders. A differential backup is a *cumulative* backup, and because of this fact, takes more time to perform than an incremental backup, but less time to perform than a normal backup.
  - **Incremental:** Backs up all selected files and folders that have changed since the last normal or incremental backup, and removes the archive attribute from the backed up files and folders. An incremental backup is *not* cumulative, and because of this fact, takes less time to perform than a differential backup.
  - **Copy:** Backs up all selected files and folders, and does *not* remove the archive attribute. This backup type can be used without disrupting the normal backup schedule.

  - **Daily:** Backs up all selected files and folders that have changed during the day the tape backup is made, and does *not* remove the archive attribute.
  - Often, a combination of the standard backup types is used.
- There are three fairly common backup strategies. The trade-off that needs to be considered, when planning a backup strategy, is the time it takes to perform backups versus the time it takes to restore data.
  - One strategy is to perform a normal backup every day. This strategy is time consuming in terms of backup, but requires the least amount of effort should a restore be necessary, because only the most recent normal backup is required.
  - A second strategy is to perform a weekly normal backup and daily differential backups. This strategy takes more backup time than performing daily incremental backups, but requires only the last normal backup and the most recent differential backup should a restore be necessary.
  - A third strategy is to perform a weekly normal backup and daily incremental backups. This strategy takes the least amount of time in terms of backup, and potentially the most amount of time to perform a restore, because the last normal backup, in addition to *all* incremental backups since the last normal backup, are required.
- When planning a backup strategy and procedure, remember to take into account *security considerations*, *tape rotation*, and the *documentation* you should keep on your backups. It is beneficial to keep a detailed logbook that contains the date and time each backup was performed, a brief description of the data backed up, the person who performed the backup, the tape number used, and its storage location. It's also helpful to keep a detailed log of each backup so that individual files can be restored from tape quickly and easily.
- You can use Windows NT Backup to backup and restore data.
- Performing a tape backup requires the use of a tape drive device. Make sure to use a tape drive that is on the HCL, and if possible, one that has the capacity to back up your entire server on a single tape.
- You can use the Schedule service and the `At.exe` command-line utility in conjunction with Windows NT Backup `(NTBackup.exe)` command-line switches to configure and schedule unattended backups.

- To ensure that your backup tapes contain valid copies of your data, you should periodically test your backup by performing a trial restore. When performing a trial restore, restore files from a backup tape to a different folder (that is only used as a test folder and that contains no other files). Then compare the files to the original files (on your hard disk) using the `Comp.exe` command-line utility (or `Winndiff.exe`, a graphical utility included in the *Microsoft Windows NT Server Resource Kit*). If there are no differences between the files compared, then presumably all of the files on the backup tape are valid, and not corrupt.

Applying What You've Learned

Now it's time to regroup, review, and apply what you've learned in this chapter.

The Instant Assessment questions bring to mind key facts and concepts. The hands-on lab exercise will reinforce what you've learned, and allow you to practice some of the tasks tested by the Microsoft Certified Professional exams.

Instant Assessment

1. Which Windows NT utility can you use to perform backups and restores?
2. What is the archive attribute, and how can it be affected during backup?
3. Briefly list and describe the five standard types of backups.
4. What two items should be considered when selecting a tape drive device?
5. What should you do periodically to ensure that your backup tapes contain valid copies of your data?
6. Which backup combination listed below, A or B, takes more time *in terms of the amount of time it takes to perform backups*?
   - **A.** A weekly normal backup and daily differential backups
   - **B.** A weekly normal backup and daily incremental backups

7. Which backup combination listed below, A or B, typically takes more time *in terms of amount of time it takes to perform restores?*

   A. A weekly normal backup and daily differential backups

   B. A weekly normal backup and daily incremental backups

8. How does selecting the Verify After Backup option in Windows NT Backup affect the amount of time it takes to perform a backup?

9. Which Windows NT Service must be configured before an unattended backup can be performed using Windows NT Backup?

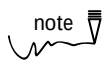
10. What can you do to minimize data loss from a single catastrophic event, such as a theft, fire, flood, or earthquake?

For answers to the Instant Assessment questions see Appendix D.

Hands-on Lab Exercise

The following hands-on lab exercise provides you with an opportunity to apply the knowledge you've gained in this chapter about backing up and restoring data.

Lab 15.24 *Performing a backup*



This lab is optional because it requires a tape drive.

Server Enterprise

The purpose of this lab is to give you hands-on experience using Windows NT Backup to back up files and folders on a Windows NT computer. You will also view the detailed log created during the backup by using Windows NT Explorer and Notepad.

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator. If you haven't already done so, install a driver for your tape drive by using the Tape Devices application in Control Panel. Place a tape in the tape drive.

FOLLOW THE STEPS BELOW CAREFULLY:

1. Start ≥ Programs ≥ Administrative Tools (Common) ≥ Backup.
2. The Backup dialog box appears. Select Window ≥ Drives.

3. Maximize the Drives dialog box. Double-click the C: drive (or the drive that you have installed Windows NT Server on). Select the check box next to the `Winntsrv` folder. (If you wanted to back up the entire C: drive instead of selected folders only, when the Drives dialog box first appears, select the check box next to the C: drive instead of double-clicking it.)

   Click the Backup command button.

4. The Backup Information dialog box appears. Select the check boxes next to the following: Verify After Backup, Hardware Compression (if the box is not grayed out), and Backup Local Registry.

   In the Operation section, ensure that the radio button next to Replace is selected.

   In the Description text box, type **Winntsrv folder *current_date* normal backup**.

   In the Backup Type drop-down list box, select Normal.

   In the Log Information section, select the radio button next to Full Detail.

   Click OK.

5. The Backup Status dialog box appears. If the tape has been used before, a Replace Information dialog box appears. Click the Yes command button to have Windows NT Backup replace the data on the tape with the backup you are preparing to perform.

6. Windows NT Backup performs the backup. (This process takes several minutes.)

7. The Verify Status dialog box appears. Windows NT Backup verifies that all files and folders were backed up correctly. (This process also takes several minutes.) After the verify is completed, click OK.

8. The Backup - (Drives) dialog box appears. Select Window ≥ Tapes.

9. The Backup - (Tapes) dialog box appears. Double-click the + sign next to the C: in the right-hand window (or the letter of the drive on which you installed Windows NT Server).

10. Double-click the `Winntsrv` folder in the left-hand window.

11. Windows NT Backup displays the contents of the `Winntsrv` folder from the tape backup that you just created. Notice that, for restore purposes, you can select individual files and subfolders by selecting the check boxes next to the files and subfolders that you want to restore.

    Exit Windows NT Backup.

12. To view the log for the backup you just created, select Start ≥ Programs ≥ Windows NT Explorer.

13. In the Exploring dialog box, click the + sign next to the C: drive (or the drive on which you installed Windows NT Server). Highlight the `Winntsrv` folder. In the 'Contents of Winntsrv,' double-click `Backup.log`.
14. View the backup log that is displayed in Notepad. Exit Notepad.
15. Exit Windows NT Explorer.