Backup Strategies

Before you can have a secure and effective plan for managing your data, you must incorporate a strategy that includes the following information:

- The importance of the data you are backing up
- How often to back up your system
- How many tapes you will use
- When you will use certain tapes
- How you will keep track of your backup information

Choosing a Backup Strategy

Several tape rotation schemes are described in this chapter. Prior to choosing a strategy to use with your Backup Exec system, you should examine the following questions.

How often should I back up?

While there is no set rule on how often to back up your data, there is one consideration that can help you decide for yourself: What is the cost of recreating data that was added or modified since the last backup?

Calculate the manpower, lost time and/or sales and other costs that would be incurred if your system crashed just before the next backup was to take place (always assume the worst-case scenario). If the cost is excessive, the strategy needs to be adjusted accordingly.

For example, if you have a database containing important customer information that you update several times a day, the cost to recreate that information would probably be quite substantial. On the other hand, the cost to recreate the data for one or two inter-office memos would be considerably less.

Ideally, you would want to do at least one Normal backup of all drives, directories, and files every day. Important files and directories that constantly change may need to be backed up several times a day. For safety reasons, a Normal backup should always be performed before adding new applications or changing your system's configuration.

How long does the data need to be stored?

The amount of time the data needs to be stored is directly related to the tape rotation scheme you use. For example, if you use one tape and back up every day, your backups will never be more than a day old.

Since tape media is relatively inexpensive when compared to the value of your data, it is a good idea to periodically backup your system on a tape not used in the tape rotation scheme and store it permanently.

The threat of viruses is an issue here also. Some viruses take effect immediately, while others may take days or weeks to cause noticeable damage. Because of this, you should have at least the following backups available to restore at any time:

- 3 daily backups (i.e., Monday, Tuesday, Wednesday)
- A one-week-old Normal backup
- A one-month-old Normal backup

  Having these backups available should allow you to restore your system prior to when it became infected.

Important: Be careful not to restore data you think may be infected to a drive that is not infected.

What is the life expectancy of a tape?

Tapes that are used over and over will eventually become old and worn out. When this happens, the success of restoring data from those tapes diminishes. Since tape media is relatively inexpensive, it is a good idea to periodically replace your older tapes with new tapes.

Set a standard as to how long you can use a tape before you replace it based on the backup strategy you use, the number of times you use the tape, and how long you plan to keep the tape. Also, if the quality and reliability of a tape becomes questionable (you begin to get tape errors during a backup operation), you should replace the tape.

Backup Methods

There are five backup methods:

Method	Description
Normal	Normal backups will back up all selected drives, directories, and files regardless of whether or not they have changed since the last backup (resets the archive bit).
Incremental	Incremental backups will back up only the files that have been created or changed since the last Normal or Incremental backup (resets the archive bit).
Differential	Differential backups will back up all files that have been created or changed since the last Normal backup (does not reset the archive bit).
Copy	Copy backups will back up all selected drives, directories, and files and does not affect subsequent Incremental or Differential backups.
Daily	The Daily Backup method backs up all files with today’s date (created or changed today) and does not affect the files’ backup status (does not reset the archive bit).

Before you can develop your tape rotation scheme, you will need to decide whether you want to do Normal, Incremental, Differential, or Daily backups or a combination. There are advantages and disadvantages to each method. Copy and Daily backups may be performed in addition to the tape rotation scheme selected.

Normal Backups

Advantages

Files are easy to find - Since Normal backups include all data contained on your hard drive, you do not have to search through several tapes to find a file that you need to restore.

There is always a current backup of your entire system on one tape or tape set - If you should need to restore your entire system, all of the most current information is located on the last backup.

Disadvantages

Redundant backups - since most of the files on your system rarely change, each backup following the first is just a copy of what has already been backed up.

Normal backups take longer to perform - Depending on how much data you are backing up, Normal backups can be time consuming.

Incremental Backups

Advantages

Better use of media - Only files that were created or changed since the last backup are included, so there is much less data storage space required.

Less time required for backup - Incremental backups take much less time than Normal backups to complete.

Disadvantages

Files are more difficult to find - Incremental files may be spread across all tapes used since the last Normal backup. You may be required to search several tapes to find the file you want to restore (this is typically not a problem if you use full cataloging and Backup Exec's Advanced File Selection feature).

Full restoration of your hard drive may be time consuming - Restoring a hard drive will probably require the restoration of data from more than one tape. This can take more time than if all data was on a single tape.

Differential Backups

Differential backups include backing up all files that were created or changed since the last Normal backup. For example, let's say you perform a Differential backup on Monday following Friday's Normal backup. When you perform a Differential backup again on Tuesday, the backup will include the data you backed up Monday, as well as any files that were changed on Tuesday. If you had performed an Incremental backup on Monday and Tuesday, Tuesday's backup would include only files that were created or changed since Monday's backup.

Advantages

Files are easy to find - Restoring a system backed up under the Differential backup strategy requires a maximum of two tapes--the latest Normal backup tape and the latest Differential backup tape. This potentially represents a considerable time savings over backup strategies which require the latest Normal backup tape and all Incremental backup tapes created since the Normal backup.

Less time required for backup - Differential backups take much less time to complete than Normal backups.

Disadvantages

Redundant backups - The amount of data backed up each day following a Normal backup gets greater and greater. For example, let's say you are performing a Normal backup on Friday, and Differential backups Monday through Thursday. Redundancy occurs because the same information backed up on Monday will be backed up again three times (Tuesday, Wednesday, and Thursday).

Copy Backups

Copy backups may be performed in addition to the tape rotation scheme selected. Copy backups allow you to perform a backup to meet a specific purpose (e.g., create a special tape, backup specific data, etc.).

Daily Backups

Daily backups may be performed in addition to the tape rotation scheme selected. The Daily Backup method backs up all files with today's date (created or changed today). The Daily Backup method does not affect the files' backup status (does not reset the archive bit).

Tape Rotation Schemes

There are many different tape rotation schemes. They differ mostly by the number of tapes they require and how long the tapes are kept before they are rotated back into the schedule. The tape rotation schemes described here are:

- Son
- Father/Son
- Grandfather
- Ten Tape

Backup Strategies

Password Protection

Stick to the Schedule

To realize the maximum benefits of your tape rotation scheme, stick to the schedule. If the schedule is not followed regularly, mistakes could take place that would render all backup efforts useless. Make sure that backups of your system are performed on schedule.

The tape rotation schemes described here are generic. Depending on the value and quantity of your data, you may want to adjust a schedule to better fit your needs. For example, if you are using the Grandfather scheme, you may want to perform a Copy backup on the last Saturday of the month to rotate off-site for permanent storage.

Son Scheme

Number of tapes required: 1
Maximum Storage life: last backup

This tape rotation scheme simply involves doing a Normal backup every day. Although the Son scheme is simple to manage, backing up with a single tape is not an effective backup strategy due to the fact that magnetic media eventually wears out after many uses and the data you can restore only dates back to your last backup.

Father/Son Scheme

Number of tapes required: 6
Maximum Storage life: Two weeks

The Father/Son tape rotation scheme uses a combination of Normal and Incremental backups for a two week schedule.

In the Father/Son scheme, four tapes are used Monday through Thursday for Incremental or Differential backups. The other two tapes containing Normal backups are rotated out and stored off-site every Friday.

The Father/Son scheme is easy to manage and allows you to keep data longer than the “Son” scheme.

Note: If you choose to perform Differential backups, you can use 3 tapes instead of six. For example, you can perform Differential backups with Tape 1 on Monday through Thursday, and use Tapes 2 and 3 for your Friday Normal backups.

To implement the Father/Son scheme, perform the following steps:

1. Label your tapes and perform a Normal backup on Tape 5 (Incremental) or Tape 3 (Differential) on Friday.

2. Follow the schedule shown above for performing backups Monday through Thursday.

3. Rotate tapes 5 and 6 (Incremental) or 2 and 3 (Differential) off-site for maximum protection.

Grandfather Scheme

Number of tapes required: 19
Maximum Storage life: One Year

The Grandfather scheme is one of the most common tape rotation schemes. It is simple to manage and comprehensive enough to find files easily when they need to be restored.

In the Grandfather scheme, four tapes are used Monday through Thursday for Incremental backups. Another three tapes are used every Friday for Normal backups. The remaining 12 tapes are used for monthly Normal backups (January through December) and are kept off-site.

The Grandfather scheme is recommended because it offers a good tape number to storage life ratio (19 tapes/1 year). It is also easy to modify should you want to incorporate more tapes. For example, you could perform a Normal backup on the last Saturday of the month to store permanently.

Ten Tape Scheme

Number of tapes required: 10
Maximum Storage life: 12 weeks

Some tape rotation schemes result in excessive wear on the tapes that are used most often in the schedule. For example, a scheme may require the same four tapes to be used for Incremental backups on Monday through Thursday, every week. The Ten Tape scheme eliminates this by rotating tapes in a way that allows each tape to be used the same number of times over a 40 week period.

The cycle begins with a Normal backup on each Friday, and Incremental backups Monday through Thursday. On the fourth Friday of each four-week cycle, a Normal back up is performed and rotated off-site.

The scheme is divided into ten, four week intervals. The same four tapes are used Monday through Thursday in a given cycle, but change the next cycle. A different tape is used each Friday of the four-week cycle.

When you first implement the Ten Tape scheme, you will need to perform a Normal backup on Tape 10 before backing up to Tape 1 on Monday. This will ensure that you have a four-week-old copy of your data at the end of the first four week cycle.

The main benefit of the Ten Tape scheme is that all tapes are used equally during the cycle. This scheme is more difficult to manage than others described in this chapter. Although less tapes are required than the Grandfather scheme, storage life is reduced to 12 weeks.

Keep a Backup Chart

Although Backup Exec’s cataloging is extremely useful for keeping track of tapes, a chart should be kept that includes at least the date, time, and contents of each tape. This way, if you need to restore data in a disaster situation, you will have a chart to use for reference.

Disaster Preparation

What is a Disaster?

A disaster is any event that interrupts computer operations. Disasters can range from earthquakes to overflowed toilets, and disasters can be divided into two categories: natural and man-made.

Disasters caused by nature (earthquakes, hurricanes, floods, etc.) are out of our realm of control, but the precautions presented in this chapter can make recovering from them much easier.

Not all man-made disasters are committed intentionally, but unfortunately, some are. The threat of man-made disasters can not be completely alleviated, however, there are precautions that can be taken to help prevent them.

Here are several types of disaster situations and some suggestions for minimizing their damage.

Acts of Nature

Floods, extreme temperatures, earthquakes, tornadoes, hurricanes, and thunderstorms have impacted computer users who either did not backup regularly, or ever at all. Many companies are opting to use off-site storage for backups because of nature-related disasters.

Fire

Off-site storage should be part of your backup strategy because of the threat of fire. Fire-proof containers are not alternatives to off-site storage; they reach extremely high temperatures inside and could cause magnetic media to fail.

Crime

Computer crime can take several forms: unauthorized changing of files, embezzlement, fraud, hackers, illicit code, industrial espionage, logic bombs (code that causes negative consequences and are triggered by a future event, like a date), malicious damage, mischief, sabotage, tampering, theft, etc. Major corporations have been victimized by computer crime and have lost millions of dollars because the proper safety precautions were not in place. Make sure you have a secure environment and that you strictly enforce password protection and rights if you are on a network. Do not forget to back up regularly!

Magnetic Fields

Be careful about choosing a location for your backup tapes. Magnetic fields can destroy data on tape media. Try to keep your tapes away from such electronic devices as video monitors, analog telephones, etc.

Backup Strategies

Operator error, Accident, Omission

Most data is lost accidentally. Make sure important data is backed up often.

Power

Electrical current changes can manifest themselves in several ways, any of which can disable a computer and destroy data. Local power failures, blackouts, power fluctuations, power surges, and utility failures are among the most common causes of data disaster. File servers should always have uninterruptible power supplies and have their electrical outlets monitored occasionally. Surge protectors on all servers and workstations are also recommended.

Viruses

Viruses can be introduced a number of ways: by disgruntled employees, by competitors, or by accident. Always use a virus detection and/or protection program, and strictly prohibit users on the network from downloading software from non-accredited bulletin boards.

Now that you know more about the types of disaster that can occur, you can proceed in putting a Disaster Preparation Plan in place.

What is Disaster Preparation Planning?

Disaster preparation planning is the implementation of strategies and procedures that will minimize damage in the event a catastrophe destroys your data. While things can be done to minimize the effects of this type of occurrence (surge protectors, password protection, etc.), there is nothing that can safeguard your data 100%.

The purpose of a Disaster Preparation Plan (DPP) is to be able to return to an operational status as soon as possible. Backup Exec is a crucial component of the DPP and this section discusses how to apply this powerful data management tool to your DPP.

Key Elements of a Disaster Preparation Plan

The DPP you put in place with your Backup Exec system should be tailored to your system environment. While environments will vary in different organizations, there are five elements that should be covered to have a comprehensive DPP. They are:

- Hardware protection
- The ability to maintain business operations during a disaster period
- A sound backup strategy
- Off-site storage of backup tapes
- Effective DPP management

Password Protection

Backup Strategies

Physical Security

Hardware Protection

The hardware devices on your network (CPUs, drives, video) are susceptible to damage from many disaster situations.

Here is a list of equipment most often used today to protect hardware:

- Uninterruptible power supplies (UPS) on file servers
- Surge protectors
- Security monitoring devices

If you do not already have these items in place, you should consider installing them. The initial investment could be justified many times over in the event of a disaster.

The Ability to Maintain Business Operations During a Disaster Period

Make sure that proper precautions are taken to implement plans for interruptions. For example, the phones in the sales department will continue to ring even though the server is down, so orders may have to be handwritten until the server is up again. Each department or computer user should work out strategies for such occurrences. If the proper precautions are taken, your system will be up and running in no time and operations can still continue.

A Sound Backup Strategy

A well-designed backup strategy should be implemented. It should include a tape rotation scheme that allows you to quickly restore your system.

Off-site Storage of Backup Tapes

It is imperative that backed up data be moved off-site regularly. This ensures that if something happens to your facility, all of your backup tapes will not be destroyed. Depending on the importance of your data, you may choose to use several off-site storage facilities. There are companies that provide off-site storage services that will pick up and deliver tapes when they are to be rotated.

Effective DPP Management

The last element (and possibly the most important) is proper management of your DPP strategy. A person or group of people should be assigned the responsibility of constantly supervising your organization’s disaster preparation efforts. Someone needs to install and maintain hardware protection devices, make sure all departments have a plan if the file server goes down temporarily, and make sure that backups are made and rotated off-site regularly. Also, it is a good idea to document your Disaster Prevention Plan for reference, review, and updating purposes.

Security Planning

The first step towards security planning is to become familiar with the Windows NT security model. Read the chapter called How Network Security Works in the Windows NT Server Concepts and Planning Guide that was included with Windows NT Server.

Backing up, archiving, and restoring a Windows NT Server or workstation share requires special backup and restore rights. Windows NT provides several built-in groups that contain these rights. These groups include:

- Administrators
- Backup Operators
- Server Operators (only on Windows NT Servers)

  In order for Backup Exec to back up and restore these Windows NT servers, you must have backup and restore rights.

Physical Security

Physical security of a network is an important consideration. When using Backup Exec, physical security of tape media becomes an even more important consideration. Limiting physical access to tape drives and tape media is something that should be carefully considered.

The highest level of physical security is keeping all tape drives and tape media in a locked computing room where access can be restricted.

You may also be able to lock the workstation before leaving it unattended.

Password Protection

In addition to physical security, Backup Exec provides the ability to password protect your tape media. You may also be able to limit access to the workstation using password protection on the screen saver.