# Chapter 1  Welcome to Backup Director

## Overview

This chapter describes:

- Backup Director product features
- Automatic and custom backup operations
- SMS Architecture
- Media libraries
- Media scheduling
- Backup Director databases
- Types of files and file systems protected

## Contents

# What is Backup Director?

Backup Director provides high-performance backup, restore, and media management functionality with an easy-to-use interface. Backup Director provides superior departmental and enterprise-wide protection for Novell NetWare LANs and a variety of client/server environments, including Macintosh, DOS, OS/2, and Oracle.

## Intelligent Storage Management

Backup Director is unique because it intelligently handles all of the tasks involved with managing your network's data storage challenges:  daily backups, restoration of files, and file management. Using its unique rules-based system, the program software lets you establish protection criteria for your system. The program then automates the procedures necessary to accomplish those goals.

## Reliability and Flexibility

Backup Director provides two methods of backing up your data.

- Automatic jobs−Backup Director determines which operation(s) to perform, which files to back up, and which media to use. Most parameters are configurable.

- Custom jobs−You select the resource(s), the operation, and the media. At the file level, you select the directories and/or files located on a resource that you want to back up.

You can schedule either type of job to run whenever you want.

Most likely, you will want to rely on automatic jobs for the majority of your backup operations, while using custom jobs for special situations such as backing up project data or cloning resources for branch offices.

### Saves Time and Media

Backup Director manages your backups for you by automatically launching the appropriate backup each day; you never have to manually submit a job.

Most backup products routinely back up the same version of files at every backup. Backup Director saves time and media by using its unique file-tracking databases to copy only the files requiring backup. This results in faster backups without compromising the integrity of your system's data protection.

# Key Components of Backup Director

Backup Director uses client/server architecture to manage the protection of your data.

Three primary components make up this architecture:

- Client-side Windows interface

- Server-based backup and restore engines

- Server-based job queue and job server

## Client-side Windows Interface

The Windows-based user interface is easy-to-use and allows you quickly access to all protected resources, configured devices, media sets, and job-related information. The interface consists of a suite of “managers,” each with a specific function that can be accessed from anywhere within Network.

For example, you are viewing your resources through Resource Manager but want to view your configured devices; click the Device Manager icon to access this manager.

The tasks you can perform within each manager are briefly described below.

**Control Console**

- Respond to alert notification or other messages. For example, the program may notify you to retrieve media from an off-site vault or investigate a backup device error.

- View and edit jobs in the job queue.

- Monitor jobs being processed.

- View the System Messages window.

**Resource Manager**

- Perform backup and restore operations on selected resources (both servers and resources). For example, perform monthly backups on specific resources or back up a resource after a project has been completed.

- Edit your Protected Resource List, including adding, deleting, de-activating, renaming, and changing the tracking name space of the selected resource.

**File Manager**

- Perform backup and restore operations on selected directories or files. For example, you can back up individual files, rather than wait for the automatic operation to complete on all protected resources.

- Determine how specific files or those matching a filename pattern are backed up.

**Media Manager**

- View the media journal, which describes the contents of media.

- Restore directories or files.

- Perform media utility operations, such as copying, erasing, and formatting.

**Device Manager**

- View configured tape drives, autoloaders, and host adapters.

- Add, delete, and rename devices.

- Perform tests on device drives and autoloaders.

**Configuration Manager**

- Define the media rotation schedule, automatic operations, and other system parameters.

- Add and delete users.

- Install other Palindrome products.

## Backup and Restore Engines

The backup and restore engines manage the protection and recovery of your data. The engines are actually NetWare Loadable Modules (NLMs) that reside on your installation server and are loaded into server memory when called to process a job.

Because the job server handles all of the jobs, you can create custom jobs or define the automatic job from your workstation and then exit the program. The workstation is then free to do other tasks while the program processes the job.

### Other Functions of the Backup Engine

Backup Director also uses the backup engine to perform database maintenance, which updates media records and verifies the database integrity.

### Job Queue and Job Server

Every backup and restore request is placed into the job queue. The job queue stores jobs until they are processed by the job server (an NLM that remains loaded in server memory and constantly monitors the job queue). Backup Director processes jobs in the order in which they are submitted to the job queue.

If it detects a job in the queue, the job server launches the associated NLM to process the job at the appropriate time. The job server distinguishes between scheduled jobs, which are only eligible for processing after a certain time or event, and unscheduled jobs, which are immediately eligible for processing. The automatic job is a scheduled job.

# Product Features

### File Management

Backup Director tracks time stamp and size changes of each file and records all Backup Director operations in a relational database. Unless you have configured it otherwise, the program copies evolving files (files that are changing frequently) at every automatic backup job. At every backup, the program compares all files and backs up only those files that changed.

### Backup Operations (Backups)

Backup Director performs a backup at every automatic operation. The program erases previous backup sessions on rotation day.  Typically, automatic operations run daily, although they can be performed as frequently as desired.

#### Types of Backups

A **full backup** is the default backup operation on a rotation day and makes a backup copy of all eligible files on all resources.

An **incremental backup** is the default backup operation on non-rotation days. An incremental backup operation writes copies of all files that have changed since the previous full or incremental backup operation.

A **differential backup** operation makes a backup copy of every file that has changed since the most recent full backup.

Each of the above backup operations rely on the File History Database to determine what files to copy to media.

## Submitting Backup Jobs

There are two methods of submitting backup jobs: automatic jobs and custom jobs.

### Automatic Jobs

Automatic jobs are the foundation of your data protection strategy and make Backup Director unique. Automatic jobs are defined through the Configuration Manager. **Automatic** means Backup Director automatically determines:

- Which operation to perform−Automatic jobs can perform one of several backup operations on the entire Protected Resource List.

- Which managed media to use−Backup Director automatically labels and uses managed media.

- When to perform the backup.

- When you should rotate media sets on- and off-site.

### Custom Backup Jobs

A custom backup job is any backup operation that you define through either the Resource Manager or File Manager. For example, backing up selected resources through the Resource Manager is a custom backup job.

Custom backup jobs are useful for additional disaster recovery protection and/or making “snapshots” of your system for storing off-site or system maintenance operations.

## Concurrent Backup Operations

Backup Director's backup engine can perform multiple backup operations within the same job. When concurrency is enabled, the job server launches the appropriate NLMs to process multiple resources at one time.

If you have two backup devices, you can simultaneously run two backup operations on two different resources submitted by a single job.

Similarly, if you have three devices, a single job can allow three resources to be backed up concurrently. As with any backup operation, concurrent operations depend on the proper media being available.

## Restore Operations

Backup Director's restore engine enables you to quickly copy a file, several files or an entire resource, from media to the file's original location or to a new location on disk.

### Restoring Previous File Versions

Backup Director uses a File History Database to locate versions and simplify the selection of files for resource- or file-level restores. You can highlight the version desired, and during the restore operation, Backup Director identifies all of the backup media that contain a copy of that version of the file. You can then insert any of these backup media, and Backup Director restores the file.

### Restoring Entire Resources

Backup Director can easily rebuild entire resources. You can restore all files for which the program has media records. The program automatically updates these records at every rotation day. In addition to restoring files residing on a particular resource, Backup Director also restores the resource's File History Database(s) (if necessary), directories, and trustees.

# Media Libraries

## Libraries

The collection of backup media you use to back up your system is called a library. You may maintain two types of libraries: managed and non-managed. The **managed library** contains the media used for all of your automatic backup jobs. You can also write sessions produced by other jobs. You can assign a unique name to this library, which Backup Director adds to the label of each media it creates.

Backup Director's intelligence tells you which media to use at every automatic job. If a tape fills, if an administrator didn't change media, or if the size of your network has increased, Backup Director always tells you which media you should use.

The **non-managed library** contains media that is never used for automatic jobs; only custom jobs can write to media in this library.

## Media Sets

Your library consists of media sets, which are cataloged alphabetically. A **media set** is a group of media that the program requires for a specific job. When you add new managed media, the program automatically labels it. The media label format is:

**Library:Set:Media Number**

For example, for the Tower of Hanoi rotation pattern, the program might label managed media as follows:

**ADMIN:A:1**

**ADMIN:B:1**

....

“ADMIN” is the media library name
“A” is the media set
“1” is the number of the backup media in the A media set. In a Tower of Hanoi rotation pattern, Backup Director labels managed media sets A through ZZ. Each media set can have up to 999 backup media.

If the rotation pattern is Grandfather-Father-Son, the program labels the managed media as follows:

ADMIN:MONDAY:1, ADMIN:TUESDAY:1 ...
ADMIN:WEEK1:1, ADMIN:WEEK2:1 ...
ADMIN:JANUARY:1, ADMIN:FEBRUARY:1 ...
ADMIN:QTR1:1, ADMIN:QTR2:1 ... ADMIN:YEAR1:1, ADMIN:YEAR2:1 ...

"ADMIN" is the media library name.
The time period ("TUESDAY," "JANUARY," etc.) is the media set name.
"1" is the number of the backup media in the particular media set. The quarterly and yearly media sets must be configured; they are not active by default.

## Sessions

Each backup operation produces a session, a group of files that are copied to media as part of a single job request. Backup sessions are eventually overwritten.

## Device Management

Backup Director allows you to configure multiple devices (of the same or different type) and define their use for Backup Director operations. The program supports multiple controller cards and host adapters through ASPI interfaces.

You can daisy-chain multiple devices of the same type (tape drives) or different types (tape and optical). For example, if you have older data on tape and currently back up data using an optical drive, you might consider using the optical drive for backup and restore operations and your tape drive for restoring only from old media.

## Backup Director Rules

Backup Director's protection rules determine when operations are performed on files, directories, or resources. You can use the default rules already configured in the system or customize them.

For each operation, Backup Director identifies the rules that apply to an item and then determines the appropriate operation to perform. By doing so, Backup Director can intelligently react to changes in the protection criteria (known as "rules") and eliminate the need for generating and maintaining complicated backup scripts.

## Scheduling Media

Backup Director automatically schedules media for your automatic jobs. Based on the rotation pattern in use, the program determines when to change (rotate) the media sets.

## Rotation Patterns

Using the rotation pattern and the number of media sets you configure, the program calculates when managed media sets are rotated. The program prompts you to load the required media set and indicates when you should move media sets between on-site and off-site storage.  Backup Director offers two rotation patterns: Tower of Hanoi (the default) and Grandfather-Father-Son (GFS).

## Media Set Rotation

At every media set change (rotation), the program performs a full backup of your system automatically. By default, the program backs up those files that have changed during subsequent backup operations. This feature saves time and media−Backup Director will not make redundant copies of files already on the media set.

#### Tower of Hanoi

Tower of Hanoi is the default media rotation pattern used for automatic jobs. Backup Director adopted this media rotation model, which was created in the mainframe and minicomputer world. This rotation model, actually a palindrome itself, is based on a sophisticated algorithm that guarantees an organized, systematic approach for media scheduling.

Additionally, this rotation scheme ensures a rich assortment of interim versions of evolving files. Palindrome recommends doing backups every day regardless of what rotation method you choose. The default is weekly rotation (media sets are rotated once per week on Friday). Weekly rotation means you change media sets once per week. During the week the program appends daily backups to the same media set.

#### Grandfather-Father-Son

Grandfather-Father-Son (GFS) is a traditional rotation scheme in the PC LAN environment. This rotation pattern uses calendar-based time periods to take a “snapshot” of the data at that moment.

Backup Director's implementation includes three pre-defined media set periods:

**Daily** (Son)−has seven pre-defined media sets
**Weekly** (Father)−has five pre-defined sets
**Monthly** (Grandfather)−has 12 pre-defined sets

You can configure the number of media sets in weekly, monthly, quarterly, and yearly media set periods. For example, you can use six weekly media sets in your rotation schedule. The graphic below illustrates how GFS rotation works.

### Off-Site Media

Backup Director suggests when to move managed media sets off-site, when to retrieve them, and which sets should be on hand at any given time in the  Off-Site Media Advisor window. The Future Media Rotations report displays the media sets you will need in the future and the exact day they should be rotated.

## Backup Director Databases

Backup Director relies on two unique databases to control its storage management features. Every installation of Backup Director includes a single System Control Database and a File History Database for each resource it protects.

### System Control Database

The System Control Database always resides in the Backup Director installation directory and consists of a group of AS*.PAC files. This database keeps track of:

- Rotation schedule including the rotation date and determining which media should be used.

- System configuration information.

- Date, time, and status of the last operation.

- Resources protected.

- General contents of media including backup media names, sessions, and sizes.

- Status (active or retired) of all the backup media.

- Session mapping−Identifies where sessions are located on media.

### File History Database

A File History Database is created for each resource when it is added to the Protected Resource List. The default location for File History Databases is the Backup Director installation volume and path, but they can be located on any NetWare volume.

File History Databases are stored in subdirectories of the Backup Director installation directory path name (default=\PAL) regardless of the volume they reside on.

The File History Database consists of a group of AV*.PAC files.

This database keeps track of:

- File history−versions of files that are on backup media.

- Rules definition−determines which files or filename patterns are included in backup operations.

## SMS Architecture

Backup Director incorporates Novell's Storage Management Services (SMS) architecture enabling protection of heterogeneous workstation clients and NetWare servers (including multiple name spaces). Palindrome's complete support of the SMS architecture ensures that Backup Director will continue to support future NetWare releases as they ship.

To do this, Backup Director uses a unique Target Service Agent (TSA) for each specific platform it supports. TSAs can be loaded on both servers and workstations.

For example, to back up a DOS workstation, you must load a DOS TSA; to back up a NetWare 3.11 server, you must load a NetWare 3.11 TSA. The TSA's basic task is to gather data requested by Backup Director; Backup Director then manages the data.

### Target Service Agents, Targets, and Resources

TSAs are installed on every server and workstation you want to protect with Backup Director. In addition, some workstations require a TSA loaded on a server; therefore you must load a portion of the TSA in both places. The TSA on the server manages communication between the server and the workstation and keeps configuration information about each workstation connected to it.

Some agents are responsible for a single target such as the agent responsible for NetWare

3.11. Other agents, such as the DOS Workstation TSA on the server, handle multiple targets (for example, the workstations advertised to the server).

Server and workstation resources protected by Backup Director are referred to as **resources**. Usually resources are volumes on servers and workstations but protected resources also include items such as the NetWare Bindery, NetWare Directory Services (NDS), or an SQL database.

## Data Interchange

Inherent in SMS is the capability to provide interchange of data among heterogeneous clients. This capability is provided through SMS's System Independent Data Format (SIDF). TSAs generate data in SIDF which Backup Director writes to backup media. Data written by Backup Director, and by other applications supporting SIDF, can be exchanged. Prior to SIDF, data was written in a proprietary format, PALDF.

## File Protection

## Supported File Systems

Backup Director protects the following file systems with the proper name space loaded.

**WARNING:** Do not use the ALT-255 ASCII character in a filename. This character prevents Backup Director from backing up the file and may even cause the program to hang during the backup operation.

### DOS Files

- NetWare volumes−Backup Director backs up all DOS files created on a volume with a DOS name space whether created in DOS, OS/2, or Windows environments. files

- DOS workstations−Backup Director can protect all files created on DOS workstations when the DOS Workstation TSA is loaded on the target workstations.

### Macintosh Files

- NetWare volumes−Apple File Protocol (AFP) files, including Volume and Data Forks are backed up by Backup Director.

- Macintosh workstations−Backup Director can protect all files created on Macintosh workstations when the Macintosh Workstation TSA is loaded on the target workstations.

**WARNING:** Macintosh filenames have additional illegal filenames. Do not include the following character strings:

CON
CLS
LPT1
PRN

These characters prevent Backup Director from backing up the file and may even cause the program to hang during the backup operation.

### OS/2 Files

- NetWare volumes−Backup Director protects all OS/2 files created on a volume with the OS/2 name space including HPFS files and extended attributes.

- OS/2 workstations−Backup Director can protect all files created on Macintosh workstations when the OS/2 Workstation TSA is loaded on the target workstations.

### UNIX (NFS) Files

- NetWare volumes−Backup Director protects UNIX NFS files created on a volume with the NFS name space.

- UNIX workstations−Backup Director can protect all UNIX NFS files created on UNIX workstations when the NFS TSA option is loaded on the NetWare server.

### FTAM (File Transfer Access Method) Files

- NetWare volumes−Backup Director protects FTAM files created on a volume with the FTAM name space.

### ORACLE Database Files

- Palindrome's ORACLE TSA option automates the backup process by putting each tablespace in backup mode so the tablespace can safely be backed up yet remain active and on-line. When the backup of the tablespace is complete, backup mode is turned off.

### Open Files

Backup Director can back up open files. But there are some issues you should be aware of when backing up open files:

- If a file is open for reading only by another user, it will be backed up as usual.

- If a file is open shareably for writing by another user, that file may have changed as it was being backed up and is therefore backed up and flagged as having “suspect” protection. Suspect files are notes in the System Messages window with a message similar to the following:

**File open - suspect file protection.**

Note that the file itself is not suspect, only its protection is, since the file was open for writing during the backup operation. The following summarizes Backup Director actions on open files.

| **If a file is…** | **Backup Director…** |
|---|---|

| | |
|---|---|
| Not open by others | Backs it up. |
| Open by others for reading | Backs it up. |
| *Open by others for writing: | |
| If “deny none” | Backs it up as “suspect.” |
| If “deny write” | Backs it up as “suspect.” |
| If “deny write” or “deny none” and any record is locked. | Backs it up as “suspect.” |
| If “deny all” | Backs it up as “suspect.” |

*NetWare file modes

## Protecting NetWare

NetWare refers to rights granted to users or groups as trustee information, which can be thought of as part of the directory structure. The program protects trustee information for resources and files by performing a full backup operation on the resource. Backup Director protects all NetWare 3.x and NetWare 4.x trustees and attributes.

In order to restore trustee information, the appropriate users or groups must exist in the Bindery or NDS. For this reason, it is important to restore the SYS: resource (with the Bindery [for 3.x servers]) and NDS (for 4.x servers) first in a complete server restoration, so that trustee information in the other resources can be properly recovered.

### The NetWare Bindery

NetWare (pre-4.0 versions) stores its user and group definitions (and related information) in a specialized database known as the Bindery. Physically, the Bindery is implemented as a group of hidden files in the \SYSTEM directory of the server's SYS: resource. Backup Director protects the Bindery as a separate resource on the Protected Resource List.

### NetWare Directory Services

Backup Director protects NetWare Directory Services on 4.x servers using TSANDS.NLM. If you have more than one server, you should use the Replication feature of NetWare Directory Services for additional protection.

### File Compression

Volumes with file compression enabled will be protected just like any other volume, but files are decompressed during backup.

## Protecting Backup Director Databases

The intelligence of Backup Director resides in its two databases. On the rotation day, the program updates and verifies the integrity of these databases to ensure that they are usable.

### System Control Database

Backup Director's System Control Database is dynamic and changing as it manages several key functions including: scheduling media, tracking sessions, and maintaining the automatic operations parameters. Since this information is critical to ensure proper operation, Backup Director writes the System Control Database to media after each managed backup operation in its own session (“DC” is the session prefix).

### File History Databases

Backup Director's File History Databases contain the backup history for all files on a resource. The File History Databases are also dynamic and changing almost by definition; and therefore, they are copied to backup media after backup operations (except selective backups) in their own session (“DH” is the session prefix).