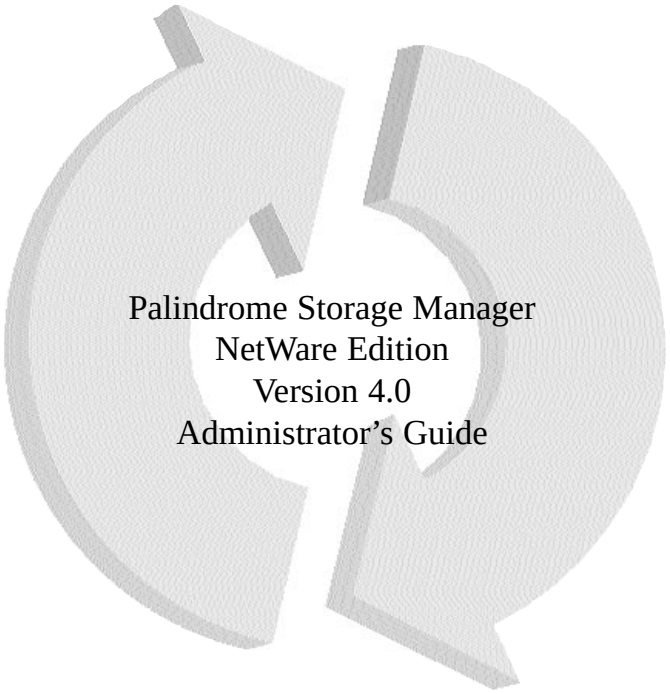


Palindrome Storage Manager
NetWare Edition
Version 4.0
Administrator’s Guide

Palindrome Corporation
Palindrome Storage Manager™ V.4.0 (NetWare Edition)
Administrator's Guide
Manual Number: 0-NWSM-ADMIN-40B
October 1995

Palindrome Corporation
600 East Diehl Road
Naperville, Illinois 60563
(708) 505-3300

Seagate Software, Ltd.
Hayley House
London Road
Bracknell, Berkshire RG12 2US
England
+44 344 360888

Seagate Software, GmbH
Hanns-Martin-Schleyer-Str. 34
47877 Willich
Germany
+49 2154916350

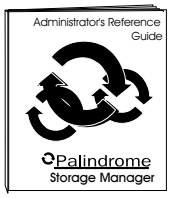
Table of Contents

About This Guide

Use this manual to learn how to back up, archive, migrate, and restore resources, directories, and files on your network and recover from volume or server crashes. This guide gives a brief overview of Storage Manager concepts and terminology in Chapter 2, “Backup Concepts.” A Glossary and “Commonly Asked Questions” appendix are also provided.

To quickly refer to procedures, see the following quick reference cards:

- Installation Quick Reference Card
- Disaster Recovery Quick Reference Card

If you want to....	See....
Register Contact Technical Support Install hardware or software	
Refer to system message recommendations Resolve typical problems	
Learn about the history of LAN backup Understand the theory behind Storage Manager operations Know details about the databases	

Audience

This guide is intended for anyone performing backup and restore operations using Storage Manager. This guide is intended for administrators who are installing and using Storage Manager 4.0 and assumes working knowledge of:

- NetWare 3.x and/or 4.x
- Installing software on Local Area Networks
- Microsoft Windows and MS DOS/PC DOS

This guide assumes you have installed Storage Manager according to the instructions in the *Installation Guide*.

Using the On-Line Help System

Windows Client On-Line Help

You may access the on-line Help system at any time by pressing **<F1>** or opening the Help menu and selecting one of the options.

Current —Displays help on current screen.
Index—Displays list of all topics.
Legend—Displays list of icons used to identify files and directories.
Using Help—Displays instructions for using Help.
Palindrome Support—Displays information about contacting technical support and answers to commonly asked questions.
Palindrome Products—Displays descriptions of the Palindrome family of products.
About—Displays version of Backup Director.

The Windows client provides on-line contextual help to identify the item or action represented by an icon button. Rest your cursor on the lower-right corner of the icon button to display the Tool Tip.

If you select a pop-up menu or highlight a specific field, and then want to know more about that item, press **<F1>** for a detailed explanation of the menu or field. Related topics appear under the "See Also" section.

For more information on using Windows client help, use the Help/*Using Help* menu option.

Server Console On-Line Help

Access on-line help for the current screen by pressing **<F1>**. For additional information about keystrokes used with on-line help, press **<F1>** again.

Chapter 1

Welcome to Storage Manager

Overview

This chapter describes:

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

For a detailed discussion on concepts presented in this chapter, see the *Concepts* guide.

What is Storage Manager?

Storage Manager is much more than a backup system. In addition to copying files to backup media and restoring files easily, Storage Manager provides a comprehensive approach to managing the entire LAN backup and restore process as well as managing the LAN storage capacity. This is why we refer to Storage Manager as a systems solution to LAN data storage management.

Intelligent Storage Management

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

Provides Reliability and Flexibility

Storage Manager provides two methods of backing up your data.

- Automatic jobs—Storage Manager 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

Storage Manager 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. Storage Manager saves time and media by using its unique archiving capabilities and 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 Storage Manager

Storage Manager 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

Key Components

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 the 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 the capacity of resources.
- View the System Messages window.

Resource Manager

- Perform backup, archive, restore, and migration 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.
- Edit migration water marks and monitoring options.

File Manager

- Perform backup, archive, restore, and migration operations on selected directories or files. For example, you can migrate individual files, rather than wait for files become eligible for automatic migration.
- Determine how specific files or those matching a filename pattern are backed up, archived, and migrated.

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.
- Configure HSM 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

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

Job Queue and Job Server

Every job 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). Storage Manager 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. An automatic job is a scheduled job.

Product Features

File Management

Storage Manager tracks time stamp and size changes of each file and records all Storage Manager operations in a relational database.

The program manages each file individually and classifies each as either **stable** or **evolving**. Stable (unchanging) files are permanently copied until you have the number of permanent copies you require for **full protection**. Once the program has made permanent copies of a stable file on three different media sets (the default), the file becomes fully protected. Permanent copies are not overwritten during automatic operations. However, they can still be removed from the media library by erasing and formatting.

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 each time and backs up only those files that changed.

Writing Permanent and Temporary Copies

To handle stable and evolving files, Storage Manager performs two distinct types of operations: **archive** and **backup**. File rules (which are configured by the administrator) and the file's current protection status (tracked in the File History Database) determine when Storage Manager backs up and archives a file. Archive operations occur automatically only on rotation day, the day on which you change media sets and perform database maintenance, in addition to backup operations.

Archive Operations (Archives)

At each media set rotation, Storage Manager makes an **archive** copy on backup media of all the stable files that are not yet considered fully protected. The collection of archive copies written during the same job is an **archive session**, which is never erased. After a file is fully protected, it is not copied to backup media again, unless it has been changed. This archiving process saves significant media space and reduces backup time that traditional backup systems cannot offer. This operation is configurable.

Backup Operations (Backups)

Files that are still changing and are not yet stable enough to be permanently archived are copied to media at each backup operation. Storage Manager 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 Storage Manager unique. Automatic jobs are defined through the Configuration Manager. **Automatic** means Storage Manager automatically determines:

- Which operation to perform—Automatic jobs can include a combination of backup, archive, and database maintenance operations and are performed on the entire Protected Resource List.
- Which managed media to use—Storage Manager 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

Storage Manager’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.

Concurrent Backup Processing

Resource Monitoring and Migration

Storage Manager allows you to manage the amount of disk utilization on each monitored volume resource so that you always have sufficient primary storage. The server-based Resource Monitor (PALRMON.NLM), loaded on the installation server, monitors disk utilization, the amount of disk space used by active and inactive files. When disk utilization exceeds the configured high water mark, Resource Monitor can submit migration job for that resource.

Storage Manager migrates inactive files to ensure that the available disk space remains within the limits you specify. (Migration is the process of deleting inactive files from disk and leaving behind a placeholder for the file called a **phantom file**.) The phantom file is left to remind you that copies of the file are available on media. If you restore the migrated file to its original location, the file on media replaces the phantom file.

The migration feature relies on rules you set in Storage Manager to determine which files are eligible for migration. That is, Storage Manager migrate files only after they are fully protected and eligible according to Storage Manager's migration rules.

Recall Agents

Storage Manager not only monitors resources and migrates inactive data; it allows users to automatically restore migrated files.

That is, when a user tries to access a migrated file, Storage Manager recall agents intercept the request and submit an "Automatic Recall Job" to the job queue.

Storage Manager provides three types of recall agents:

- a NetWare server-based recall agent
- a Windows client recall agent, installed on Windows workstations
- a DOS TSR (terminate-stay resident program) recall agent installed on a DOS workstation

You can install one or more of the above agents.

Restore Operations

Storage Manager'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

Storage Manager 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, Storage Manager 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 Storage Manager restores the file.

Restoring Entire Resources

Storage Manager 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, Storage Manager 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 Storage Manager adds to the label of each media it creates.

Storage Manager'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, Storage Manager always tells you which media you should use.

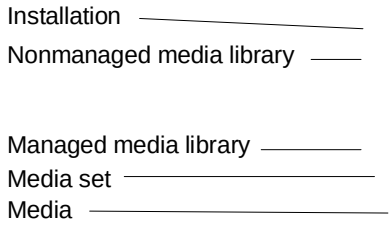
The **non-managed library** contains media that is never used for automatic jobs; only custom jobs can write to media in this library

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
....



Media Manager's main window

"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, Storage Manager labels managed media sets A through L. 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:QUARTER1:1, ADMIN:QUARTER2:1 ...
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 or archive 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. The program never erases an archive session during the course of an automatic job.

Device Management

Storage Manager allows you to configure multiple devices (of the same or different type) and define their use for Storage Manager 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 an optical disk and a tape drive, you might consider using the optical for archive operations and your tape drive for backup operations.

Storage Manager Rules

Storage Manager'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, Storage Manager identifies the rules that apply to an item and then determines the appropriate operation to perform. By doing so, Storage Manager 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

Storage Manager 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. Storage Manager 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—Storage Manager 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. Storage Manager 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.

In the table below you can see the rotation schedule's palindrome as a new media set is added. For example, the sequence on either side of the C media set (Week 4) is the same (A, B, A) until the D set is added. If space allowed, you would see that this pattern would be true for the D set and all others.

Sample comparison of default TOH and GFS rotation schedules

Tower of Hanoi

Week	1	2	3	4	5	6	7	8
	A	B	A	C	A	B	A	D

Grandther-Father-Son

Week	1	2	3	4	5	6	7	8
Daily	M/T/W/Th	M/T/W/Th	M/T/W/Th	M/T/W/Th	M/T/W/Th	M/T/W/Th	M/T/W/Th	M/T/W/Th
Weekly *	WK1	WK2	WK3	WK4		WK1	WK2	WK3
Monthly *					JAN			

***The rotation day is Friday.**

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.

Storage Manager'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 graphics below illustrates how GFS rotation works.

Default GFS Rotation Schedule

Off-Site Media

Storage Manager 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.

Storage Manager Databases

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

Installation Volume and Default Database Locations

System Control Database

The System Control Database always resides in the Storage Manager 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 Storage Manager installation volume and path, but they can be located on any NetWare volume.

File History Databases are stored in subdirectories of the Storage Manager 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—the protection goals for your files, directories, and resources.
- Archive/backup differentiation—which files are recorded as permanent copies and which are recorded as temporary copies.

SMS Architecture

Storage Manager 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 Storage Manager will continue to support future NetWare releases as they ship.

To do this, Storage Manager 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 requires a DOS TSA; to backup a NetWare 3.11 server requires a NetWare 3.11 TSA. The

TSA's basic task is to gather data requested by Storage Manager; Storage Manager then manages the data.

Target Service Agents, Targets, and Resources

TSAs are installed on every server and workstation you want to protect with Storage Manager. 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 Storage Manager 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 Storage Manager writes to backup media. Data written by Storage Manager, 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

Storage Manager 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 Storage Manager from backing up the file and may even cause the program to hang during the backup operation.

DOS Files

- NetWare volumes—Storage Manager backs up all DOS files created on a volume with a DOS name space whether created in DOS, OS/2, or Windows environments.
- DOS workstations—Storage Manager 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 Storage Manager.
- Macintosh workstations—Storage Manager 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 Storage Manager from backing up the file and may even cause the program to hang during the backup operation.

OS/2 Files

- NetWare volumes—Storage Manager protects all OS/2 files created on a volume with the OS/2 name space including HPFS files and extended attributes.
- OS/2 workstations—Storage Manager can protect all files created on OS/2 workstations when the OS/2 Workstation TSA is loaded on the target workstations.

UNIX (NFS) Files

- NetWare volumes—Storage Manager protects UNIX NFS files created on a volume with the NFS name space.
- UNIX workstations—Storage Manager 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—Storage Manager 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.

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 an archive or full backup operation on the resource. Storage Manager 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. Storage Manager protects the Bindery as a separate resource on the Protected Resource List.

NetWare Directory Services

Storage Manager 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.

HCSS Migration Resources

Storage Manager treats resources supporting HCSS as any other resource. It backs up migrated files. When recovering migrated files, however, the files are restored to disk and then migrated by NetWare (files are not restored directly to optical).

File Compression

Volumes with file compression enabled will be protected just like any other volume; Storage Manager backs up files in whichever mode the exist on the volume, compressed or uncompressed.

Protecting Storage Manager Databases

The intelligence of Storage Manager 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

Storage Manager'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, Storage Manager writes the System Control Database to media after each managed backup operation in its own session ("DC" is the session prefix).

File History Databases

Storage Manager's File History Databases contain the backup and archive 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).

Chapter 2

Backup Concepts

Overview

This chapter describes:

- Automatic jobs, including rotation and non-rotation day operations
- Migration jobs
- Custom jobs
- File rules
- Media scheduling
- Retaining backup copies
- Concurrent backup operations and jobs

Introduction

Storage Manager offers data protection and storage management capabilities that can make run-time decisions for you such as:

- Which files are stable.
- Which media should be on-site or off-site.
- Which files can safely be removed to free disk space.
- Which files can be skipped because they are already protected.

Storage Manager submits operations two different ways, as automatic jobs and as custom jobs.

Automatic Jobs

Automatic jobs are the foundation of your data protection strategy and make Storage Manager unique. **Automatic** means that Storage Manager automatically determines:

- Which operation to perform—Automatic jobs include database maintenance, backup, and archive operations and, if configured, migrate operations. Automatic jobs perform different operations on rotation and non-rotation days.
- Which media to use
- When to perform the backup
- When to move media sets on-site and off-site. You must decide whether to implement the recommendations.

The program's decisions are based on the Media Scheduling parameters in Configuration Manager.

See Chapter 4, “Customizing Your Installation,” for information about defining automatic operations, including rotation day and non-rotation day operations.

What Happens On Rotation Day?

Rotation day is the day Storage Manager asks for a different media set to perform the next scheduled automatic job. When you perform your first automatic backup, Storage Manager will perform the operations it normally performs on a rotation day.

Rotation day is the only day Storage Manager will automatically perform archive and/or migrate operations.

On rotation day, Storage Manager:

- Updates media records and verifies the integrity of the databases (referred to as **database maintenance**).
- Copies to media any stable files that are not yet fully protected or archived on the current media set to a permanent portion of media (**archive**).
- Copies to media every eligible file on all protected resources (**full backup)**.

What Happens on Non-Rotation Day

Non-rotation day refers to days on which the automatic job uses the media from the same media set that was used for the previous automatic job. In other words, even if you change media each day, the automatic job performs non-rotation day operations if the media belong to the same set. On a non-rotation day, Storage Manager performs:

- An incremental (or differential or full backup) operation on volume resources.
- A full backup operation on non-volume resources (for example, the Bindery files). The program backs up every file on disk that is not fully protected or that does not have an archive copy on the current media.

Because archive operations do not occur on non-rotation days, automatic jobs on these days can be significantly faster than those on rotation days.

Single Server/25-User Version

If during a backup operation, Storage Manager discovers that the Novell 25-user license has been upgraded on the protected server, Storage Manager notifies you of the license violation. If you do not upgrade your installation to the Single Server or MultiServer version within 45 days, Storage Manager performs only restore operations at this installation. Contact your reseller or Palindrome Customer Service Representative for details about this upgrade.

Migration Jobs

You can manage the storage capacity of your protected volume resources by monitoring their current utilization and migrating inactive files. Migration allows you to maintain optimal disk utilization and access to files. High and low water marks define the upper and lower limit of the optimal range of disk utilization defined for a particular resource.

By migrating inactive files, Storage Manager ensures that sufficient disk space is available for new files. For more information on migration and disk management, see Chapter 9 of the *Concepts Guide.*

Files that are migrated can easily be restored through restore or recall operations. See Chapter 6, "Restoring Files," for details about restoring files. See Appendix E, “Recalling Files,” for details about configuring recall agents.

Automatic Migration

There are three types of migration operations.

Automatic Migration

Automatic migration starts as a result of disk utilization meeting or exceeding the high water mark (default high water mark is 90% utilization) of a monitored volume. Automatic migration is independent from automatic backup operations. Storage Manager migrates only those eligible files sufficient to reduce the disk's utilization to the low water mark. If the level of the disk utilization still exceeds the low water mark after the first migration pass, Storage Manager updates the prestage list and resumes the migration operation. By default, Storage Manager leaves a zero-byte phantom file in place of the migrated file. Phantom files are used to recall files.

This operation applies to all active volume resources as needed. However, you can edit the high and low water marks of individual resources and prevent Storage Manager from monitoring and/or performing automatic migration operations on these resources.

Custom Resource-Level Migration

When you select a resource for migration operations through Resource Manager, Storage Manager only migrates files to the low water mark. This type of migration operation uses the same resource monitoring and water marks that are defined for automatic migration unless you choose to edit these parameters for the individual resource.

Custom File-Level Migration

When you migrate an individual file from File Manager, Storage Manager does not create a prestage list. In File Manager, you can migrate any file that **does not have** a migrate rule of **Exclude** and that has at least on archived copy on managed media.

Configuring Migration Rules

If you are not familiar with migration operations, you may prefer to increase the stability period to delay migrating files from the disk. As you observe how frequently users access certain types of files, you can reduce this time period for specific filenames or types until you reach a balance between a minimum number of restore jobs and a maximum amount of disk space.

If the time period is too short, files are migrated too frequently, resulting in excessive restore and recall requests by end users.

If the time period is too long, your disk space may be consumed by unused files.

NOTE: Other backup programs and some anti-virus software will alter the Last Access Date of your files. Be sure to configure anti-virus software to retain the Last Access Date. Otherwise you may have to manually select certain files to be migrated, since Storage Manager cannot determine which files are eligible based on the access date.

Prestage List

When Storage Manager performs a resource-level migration, it uses the volume resource's prestage list. The *prestage list* contains a list of all files that are eligible for migration based on the defined parameters:

- Archive rule definition—Indicates when Storage Manager can archive the file to managed media.
- Migrate rule definition—Indicates when Storage Manager can migrate the file.
- **Archive Copies Required for Full Protection** option—Indicates the number of archive copies that must be on managed media in order for Storage Manager to migrate the file.
- **Create a Near Line Set** option—An option that requires that Storage Manager to archive a copy of the file to the most frequently used media set, if an archive copy does not already exist on it.

If a file meets all of these eligibility requirements, you are assured that a sufficient number of archive copies exist on managed media. If there is a near line set, then the file will also always be available for restore and recall operations from on-site media. A near line set is especially convenient if users perform many restore and recall operations.

When the migration occurs, Storage Manager may not migrate every eligible file on this list. Since the purpose of maintaining an optimal disk utilization is to ensure sufficient space to accommodate new files, it is not necessary to migrate every eligible file. For migrations, the objective of Storage Manager is to reduce the resource's disk utilization to the low water mark. When the low water mark is reached, Storage Manager stops migrating files regardless of how many other eligible files remain on the prestage list.

At the next migration, Storage Manager begins migrating files remaining from the previous operation. If these files are not sufficient to reduce the disk utilization to the low water mark, Storage Manager updates this list. Storage Manager then resumes migrating the files added to the updated list.

NOTE: If any of the above-mentioned parameters have changed since Storage Manager added files to the prestage list, the affected files will remain on the prestage list until they meet the new requirements.

For example, if the stability period of the migrate rule was increased from four weeks to eight weeks, Storage Manager cannot migrate the files until these files remain unaccessed an additional four weeks.

Custom Jobs

Custom jobs are requests to perform a single operation on selected items (servers, resources, directories, files, etc.). Custom jobs can supplement file protection in special circumstances, or they can provide an alternate backup schedule. Unlike automatic jobs, custom jobs are not required to record session information in the database. These jobs can write to managed or non-managed media (media labeled by the user). Usually, you create a custom job for a special purpose such as:

- Taking snapshots of your system (possibly to store at an off-site location) at regular intervals (for example, weekly or monthly)

- Transferring data to another office (for example, you have to send a snapshot of a resource or directory each week to another location)
- Backing up an entire machine or resource prior to replacing it

The table below summarizes the differences between automatic and custom jobs.

Automatic Jobs…	Custom Jobs…
Automatically label and use managed media.	Use managed or non-managed media.
Include all active resources on the Protected Resource List.	Can include the entire Protected Resource List or specific resources or files.
Can perform multiple operations automatically, specifically, database maintenance, backup and/or archive operations.	Can perform a single operation (backup, archive, migrate, restore, or utility operation).
Automatically perform the required operation at each scheduled interval.	Perform the operation once, periodically, or following another scheduled job.

Operations

Backup, archive, and migration operations roughly correspond to a file's life cycle. When a file is first created, the program backs up the file at the first backup operation and continues to back it up as long as the file continues to change. As you will see, the backup and archive operations not only protect files on disk, they lead to effective storage management.

Backup Operations (Backups)

There are three types of backup operations.

- **Full backup**—Makes a backup copy of all eligible files on all resources and is the default backup operation that occurs on a rotation day. Files eligible for a backup operation are those files that are not already fully protected or not excluded by file rules. Full backup operations always occur on rotation day.
- **Incremental backup**—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.
- **Differential backup**—Makes a backup copy of every file that has changed since the previous full backup. Because this operation does not clear the archive bit, this can result in the same version of files being copied even if they haven't changed since the last full backup.

Incremental backup operations tend to complete more quickly than differential backups. However if the program uses differential backups, Storage Manager can restore an entire resource more quickly because a greater number of the most recently changed files are located on the same media. The program only needs to open one session on each required media set.

If users do not make changes to the file, the file becomes stable and after a specific time period becomes eligible for archive operations. When the program has written a certain number of archive copies, the file is fully protected. By default, the program no longer copies the file to media.

Archive Operations

All archive sessions are permanent and can only be written to managed media. Archive operations occur automatically on rotation day. You can perform archive operations on selected resources or files at any time using managed media.

How Rules Affect Backups

While everyone would prefer to have all of their data backed up continuously, this strategy is rarely feasible given the burden to the network and inconvenience to end users. Most data rarely warrants this type of protection. As an administrator you need to find the best balance of data protection, convenience, and media usage. Storage Manager's file rules can help you define the best protection for the different kinds of data on your network.

File rules are applied to each resource that Storage Manager protects. Because network requirements vary depending on the environment, corporate policy, government specifications, etc., users may find it necessary to customize their system to meet defined requirements.

Storage Manager's system rules are shown in the table below. These rules are set in the root directory of each protected resource for the "*" wild card pattern. See page 9-34 for information about other system rules.

System Rules for Volume Resources ("*" Files)	
Operation	**Rule Parameter**
Backup	**Include** This backup rule ensures that every file (unless covered by a more specific rule) will be backed up whenever it changes.
Archive	**After 6 Weeks** The archive rule ensures that permanent copies of files are written to media if they are stable and have not been modified after six weeks.
Migrate	**After 12 Weeks** The migrate rule ensures that a file will be eligible if it hasn't been accessed for at least 12 weeks (reading the file, as well as updating it, is considered accessing), and it is fully protected.

These rules affect all files in the resource, unless the files are covered by rules for more specific file name patterns.

Common Applications of Rules

This section describes various uses for Storage Manager's rules. See page 9-30 for examples that show you how to specify rules for specific types of files.

Upon installing Storage Manager, it is common to modify or add a number of rules. The system rule, * in the root directory, is sufficient for most files. Rules can affect not only the protection status of a file but also disk and media space.

Consider the effect of decreasing the time period for archive operations. A much shorter time period could result in additional file versions becoming fully protected rather than being overwritten during rotation. The rule for archiving after six weeks could be modified to a much longer or shorter time period, but six weeks is a reasonable time period. The time periods for the system rules can be safely modified, but the rule parameter itself should almost never be changed. Compare the two following examples.

- Changing from **Migrate/After 12 Weeks** to **Migrate/After 24 Weeks**.

  This change in the time period of the rule results in slightly fewer files being migrated. A longer stability period ensures that the files are not needed any longer by users and would reduce the number of custom restore jobs.

- Changing **Migrate/After 12 Weeks** to **Migrate/Exclude**

  This change can dramatically increase the amount of disk space in use since the affected files always remain on the disk.

To expedite backups and conserve media space

➤ Add a rule in the root directory for *.BAK or other extensions, and set the rules to **Backup/On Demand**, **Archive/On Demand**, **Migrate/On Demand**. This prevents BAK files from being backed up during automatic operations.

Media Rotation

The purpose of media rotation is to protect media set copies at an off-site location when they are not in use. If a disaster should occur, you can recover data from media stored at the off-site location. By using several media sets that correspond to different time periods, you achieve two data protection goals:

- Copies on different media sets help you to safeguard at least one copy at any time. Extra media sets can be stored off-site.
- Copies corresponding to different dates exist on different media sets. This provides users with the flexibility of restoring from any of several file versions.

Storage Manager provides two configurable rotation patterns: Tower of Hanoi (TOH) and Grandfather-Father-Son (GFS). Of the two, TOH is considered to offer the greatest depth of file versions. However, GFS uses calendar-based time periods and is more readily understood.

Tower of Hanoi

The Tower of Hanoi (TOH) rotation pattern is based on a sophisticated algorithm that guarantees an organized, systematic approach for scheduling media. One distinctive feature of this pattern is the number of unique file versions that are kept across multiple media sets.

Each time a media set is introduced, the rotation interval doubles for the new media set. For example, using weekly rotation, the program rotates the A set every two weeks, the B set every four weeks, the C set every eight weeks, etc. The frequently used media sets have the most recent copies of files, while the infrequently used sets have older versions available. Therefore a rich assortment of file versions are available across different media sets.

TOH rotation also allows you to use a dedicated near line device, which reduces involvement by the operator during automatic recall jobs.

With a weekly rotation schedule, five media sets maintain various file versions spanning a two- to four-month period. This provides a variety of file versions—equal to or better than that provided by a 12-media set Grandfather-Father-Son system.

Weekly versus Daily Rotation

If you implement TOH rotation with weekly rotation, the program requires a different media set each week. If you implement TOH rotation with daily rotation, rotation day operations occur every day because the program requires a different media set every day. Which rotation schedule is better? It depends on your individual needs.

Tower of Hanoi Weekly Rotation Example

Weekly rotation has several advantages:

- Daily backups take less time.
- More recent backup versions of evolving files.

- Fewer backup media and media changes are required.
- A greater variety of file versions spanning a longer time period.

The diagram above, Tower of Hanoi Weekly Rotation Example, illustrates the number of backup sessions that may be available on managed media during a three-month window.

Daily rotation also has advantages:

- Media will not reach capacity as quickly since only one day's worth of backups are copied between rotation.
- If the media becomes damaged, only copies of that day's data are lost.
- Stable files reach full protection more quickly, since archive operations are performed daily.

If you have data that is volatile (users add, modify, and delete data often) and/or your resources are near capacity, you should use a daily rotation scheme. If your data is generally stable (users do not add and delete a lot of data every day), a weekly rotation schedule is sufficient.

Grandfather-Father-Son

Grandfather-Father-Son (GFS) is the traditional rotation scheme in the PC LAN environment. Storage Manager's implementation includes five pre-defined media set time periods: daily, weekly, monthly, quarterly, and yearly. GFS allows up to 32 media sets, seven of which are automatically designated for your daily media. You can change the number of weekly and monthly media sets to follow a round-robin sequence rather than the calendar. For example, you can set the number of monthly sets to eight rather than twelve media sets.

When using the GFS rotation pattern, the program performs a full backup operation at every automatic job.

The diagram below illustrates the number of backup sessions that may be available on managed media during a three-month window.

Note that the program may not actually build the number of media sets you have configured. For example, if Friday is the rotation day used for weekly media sets, the program will never create a FRIDAY daily media set.

Grandfather-Father-Son Rotation Example

NOTE: Although automatic migration and recall operations are available for GFS installations, Storage Manager does not support a near line set or device for this rotation pattern.

Other Backup Issues

Retaining Backup Copies

For automatic jobs, backup sessions generally exist on a media set until the next time the media is used for the rotation day operations. The program overwrites the previous backup sessions and begins writing a new cycle of backup sessions. For custom jobs, the program does not automatically overwrite previous backup sessions; you have the choice of overwriting the previous session or appending to it.

You can ensure that data located on the session is available for a limited period of time or indefinitely by:

- Preserving backup sessions—Increase the value of the **Preserve Backups** parameter to set the minimum number of days the file version remains on the media. For example, if your installation uses the GFS rotation pattern, the program automatically "preserves" backup copies written to a "MONDAY" media set until the media is rotated the following Monday. If you need to extend this time period, you can set the **Preserve Backups** parameter to seven days or more. Once all of the sessions on a media are older than the value you set for the parameter, the program is able to overwrite the backup sessions.

- Writing to non-managed media—Since, by definition, the program does not rotate non-managed media, the program will not automatically overwrite session on this media. Take this media off-site to prevent other users from overwriting or appending to this media.

- Retiring managed media—You can de-activate, or "retire," managed media so that the program no longer schedules it for rotation. As a result, the sessions on that media all become permanent. You can still restore data from retired media.

Preserving Backup Sessions

When You Use an Unexpected Media Set

Despite the automation of Storage Manager's media rotation schedule, the media itself (or the person implementing the schedule) can still fail. Whether you need to substitute the current set for a damaged set or forgot to retrieve the required media set in time for rotation, the program can adapt to whatever managed or blank media you load. Storage Manager performs the automatic backup on any managed media set that is loaded when the program begins servicing the job.

Early Rotation

If you change media sets prior to rotation day, you are performing an **early rotation**. The program performs the usual rotation and non-rotation day operations using the current media set. At the next rotation day, the program rotates to the media set that normally follows the substitute media set.

In GFS rotation, the program attempts to resume the schedule at the next rotation by asking for the expected media set. For example, if you load PAL:WEEK3:1 instead of the scheduled PAL:WEEK1:1 media, the program will request PAL:WEEK2:1 at the next rotation.

Deferred Rotation

Similarly, you may decide to continue using the current media set rather than rotate to the required media on rotation day. The program continues to append backup sessions to the current media.

In TOH rotation, the program will again attempt to rotate to the media set that normally follows the current set. In GFS rotation, the program will again refer to the original schedule and attempt to resume that schedule.

Moving Daily Backups Off-Site

If you are required to move your backup media off-site on a daily basis, Storage Manager provides two options to assist you: copying media and the **Daily Media Change Within Set** option. Both options require extra backup media that Storage Manager would normally not demand.

The *Copy* operation in Media Manager allows you to duplicate media. You can store the duplicate set of media off-site for security, while keeping the original media set on-site for convenience.

To use Media Manager's *Copy* operation, you must have two backup devices configured. These do not have to be the same media type, nor do they have to be on the same SCSI bus. For example, you could have 4mm and 8mm tape drives or a tape drive and optical drive.

After running your normal backups, keep the media in the drive and perform the media copy operation as described on page 10-17.

When **Daily Media Change within Set** option is turned on, the program requests a different media for each day. This option is only available if you use the TOH rotation pattern. You must determine when to remove and retrieve individual media. Because the Off-Site Media Advisor window displays storage recommendations for media sets only, you must determine the appropriate schedule for moving daily media off-site.

See page 4-25 for more information about this option.

Creating Separate Backup and Archive Media Sets

The **Put Archives on Separate Media from Backups** option allows you to create archive-only and backup-only media within media sets. With this option turned on, Storage Manager writes permanent copies of stable files to one media and temporary copies of evolving files to another media in the same media set. There are a number of reasons for using this option:

- You are using a tape drive, for example, a DC 6000, that requires you to place archive and backup sessions on separate media.

  This type of drive does not allow selective overwrites. Because Storage Manager always appends to the end of the previous session, backup copies would be “trapped” by archive copies if this option weren’t available. Backups could, therefore, never be erased.

- You have multiple devices and you want archive copies on one media type and backup copies on another.

- You routinely write custom archive operations to tape.

  The program appends backup sessions to archive sessions on rotation day. If you write an archive session between rotation days, the previous backup are “trapped.” Any backup sessions sandwiched between archive sessions become, in effect, permanent sessions. Trapped backups only occur when using sequential media; they do not occur on optical disks or other random access storage.

NOTE: Because of Storage Manager’s intelligent storage management features, custom archive and migrate operations are not necessary in most environments since the default settings provide adequate protection.

Concurrency in Storage Manager

Concurrency refers to Storage Manager's ability to simultaneously:

- Perform backup operations on multiple resources simultaneously
- Perform backup jobs and restore and/or utility jobs simultaneously

To take advantage of concurrency, your installation must have at least two devices configured.

However, not all operations that run concurrently require access to a device; these are:

- Migration
- Database maintenance
- Retiring and forgetting media (utility engine)

If you are going to use concurrent operations, be sure:

- You have eligible media loaded in each device.
- You have at least 2 MB RAM available on your server for each concurrent process (for example, if you have two backup devices you need at least 4 MB of RAM).

Workstations with Single Connections

Concurrency does not apply to multiple local drives on DOS (or OS/2) workstations. TSASMS.COM and TSAOS2.EXE (on the workstation) can only communicate with one drive volume at a time. However, if the drives of several workstations follow one another, this is not an issue since Storage Manager automatically begins processing the next available resource. The program continues to check if processing can begin on a workstation's other resource(s). The graphic below illustrates how Storage Manager processes these resources. See "*Re-arranging Resources*" section in Chapter 8, "Managing Resources."

Optimizing Concurrency for Workstation Resources

Running Concurrent Backup Operations

Storage Manager allows you to simultaneously back up multiple volumes to multiple devices during a single backup job or automatic job. The backup engine is the only engine that can simultaneously process resources using multiple devices from a single job request.

Concurrent backup operations are limited by the number of backup devices. For example, if you have two backup devices and submit an archive job for three volumes, the program cannot process the third volume until one of the first volume operations has completed. However, users with a single device can benefit from concurrent database operations.

Depending on the number of backup devices you are using, concurrent backup operations may be affected if another job is using a device.

For example, you have two backup devices and are performing a restore operation, only one device is available for backup operations. If the restore job completes while the backup job is running, you can run the remainder of the backup operations concurrently by loading the second device with the appropriate media.

Concurrency in Backup Operations

Running Concurrent Jobs

Running jobs concurrently allows your installation to run up to eight jobs simultaneously. For example, you could run eight migration jobs or run one backup, one restore, and one utility job in addition to five migration jobs. Each module can perform only one job at a time. While a backup job may run multiple backup operations simultaneously, Storage Manager can process only one backup job in the queue at a time.

If each of the three engines are loaded at the same time and there are three backup jobs in the job queue, the program can only process the first backup job submitted to the queue. The remaining backup jobs must wait until the previous backup job has completed.

Three Jobs Running Concurrently

Chapter 3

Getting Started

Overview

This chapter describes how to:

- Start Storage Manager
- Perform an automatic backup job
- Monitor a job in progress
- View the results of the automatic job
- Manage the job queue
- View system messages
- View tree structures and select items
- Add users
- Customize the user interface

Introduction

If you've installed Storage Manager correctly, you are ready to begin using this comprehensive data protection and storage management tool!

To start Storage Manager

1. Log in as the user you defined during installation.
2. From Windows Program Manager, click the Storage Manager icon from the appropriate group window.

Storage Manager group window

3. Click the Storage Manager icon. The Control Console window appears.

Control Console

The Control Console is the nerve center of your installation. From this manager, you can understand basic information about your entire installation.

The tabs on the Control Console's Control Panel window provide brief descriptions of the managers and menu options that you can choose from Control Console. The four tabs are:

- Basics
- Status
- Reports
- Managers

Basics Tab

When you select an icon representing a basic operation or feature, a Palindrome Cue Card window briefly describes the various options and prompts you to access the appropriate manager or window. Additional cue cards further desc e the operation or feature. You can choose **Close** to return to the Control Console.

rib

Backup

The program describes different types of backup operations. At the cue card prompt, indicate whether you want to proceed with an operation. The program takes you to the appropriate manager and window. A cue card tells you how to complete the operation. For more information about specific types of backup operations:

- To back up a resource, see page 5-5.
- To back up a directory or file, see page 5-12.

- To back up all protected resources using configured automatic operations, see page 3-10. Also, Chapter 2, “Backup Concepts,” contains background information about automatic operations.

Basics tab

Restore

The program describes different types of restore operations. At the cue card prompt, indicate whether you want to proceed with an operation. The program takes you to the appropriate manager and window. A cue card tells you how to complete the operation. For more information about specific types of restore operations:

- To restore a file or directory, see page 6-5.
- To restore an entire resource, see page 6-16.

Media and Devices

The Palindrome Cue Card briefly describes the devices that can be added, supported firmware, and AutoLoader Software. The cue card also describes the types of media it uses. At the prompt, indicate whether you want to proceed with an operation.

A cue card tells you how to complete the operation. For more information about the media and device operations:

- To format media, see page 10-15
- To add a device, see page 11-5.
- To change the configuration of a device, see page 11-6 for devices and page 11-10 for autoloaders.

Automatic Operation

The Palindrome Cue Card briefly describes the configurable parameters for automatic operations. Indicate which feature you want to configure. A cue card tells you how to configure the feature. For more information about the automatic operations parameters:

- To specify the servers and resources the program backs up, see page 8-6.
- To specify at what time and how frequently the program performs the automatic operations, see 5-20.
- To specify which operations to perform, see page 4-23 for parameter descriptions. See page 2-3 for background information about automatic operations.

SmartAlerts

SmartAlerts are icons that represent types of problems that can occur at your installation. It is important to understand what they mean so that you can respond to them appropriately. See page 7-26 for information about alerts.

Migration

Migration is a process of deleting protected files from a resource's disk. Storage Manager allows you to migrate automatically or on an as-needed basis at the resource or file level. For more information about migration:

- To perform migration operations, see page 5-9 for a custom resource-level operation and page 5-15 for a custom file-level operation.
- To configure automatic migration, see page 4-19.
- To configure rules determining eligibility for migration, see page 9-29.

Status Tab

Items on this tab display changing conditions on your installation.

Status tab

Reports Tab

Items on this tab display configuration and rotation information for your installation.

Reports tab

Managers Tab

Items on this tab access other Storage Manager managers.

Managers tab

Performing Your First Backup

Storage Manager comes with default parameters already set for the system, operations, and the rotation schedule of managed media.

Automatic means that Storage Manager automatically determines:

- Which operation to perform—Automatic jobs include database maintenance, archive, and backup operations. Automatic jobs perform different operations on rotation and non-rotation days.
- Which media to use
- When to perform the backup
- When to move media sets on-site and off-site

See page 4-23 for information about media scheduling (automatic job) parameters.

To submit an automatic job

1. Load media in the backup device.
2. From the Control Panel window, open the Operations menu and select the *Automatic* option (this option is also in Resource Manager). A prompt asks if you want the program to prompt you with questions. These questions are typically related to the media or device.
3. If you choose **No**, you are allowing the program to determine how to proceed with a job if it encounters a problem (unattended mode). If you choose **Yes**, the program may prompt you to respond to media or hardware messages (attended mode) and waits for a response.

   Regardless of the mode you choose, an Establishing Communications window appears displaying the job ID assigned to the automatic job and its status in the job queue. The program begins processing this job as soon as possible.

To change the schedule of the automatic job

➤ From the Status tab select the Job Queue icon. If the "Default Automatic" job is in the "ready" state, highlight it and select the **View** button. By default, automatic jobs are scheduled to begin processing at 6 p.m. Monday through Sunday. If you would like to change this schedule, see page 5-20 for information about editing the schedule parameters.

Monitoring Jobs

You can monitor jobs from any manager at the time you submitted the job or, at any time, from the Control Console. Once the program begins processing a job, you can view its progress.

The Backup Job Status window, displays general information about the resources selected for the current job and which resources the program has completed processing so far. The Backup Operation Status displays additional detail. Your first few automatic jobs will take a relatively long time to complete. The program will be archiving stable files until these files become fully protected. By default, stable files become fully protected after the program writes an archive copy to three media sets.

To view a backup job in progress

➤ From the Job Queue window, highlight a backup job that the program is currently servicing and choose the **View** button. The Backup Job Status window appears.

—To view details of the current backup job, choose the **View** button. The Backup Operation Status window appears. This window displays information about the operation(s), the device being used, the activity the device is performing, etc.
—To view details of all processes the program is running concurrently, choose the **View All** button.

Backup Job Status window

Backup Operation Status window

✓ ***TIP:*** While you can continue monitoring the entire job, you will improve performance by closing this window when you are satisfied that the job is running smoothly. If you want to monitor the job later, you can view the job only through Control Console's Job Queue window.

Alert Button

The active **Alert** button reminds you that this job cannot proceed until you correct a problem. When this button is active (the button appears in job status windows only when an alert condition exists), choose the button to display the system message again. See page 7-26 for more information about alerts.

Abort Button

The **Abort** button on the job status windows can be used to stop the processing of a job.

To abort a job

1. From the job status windows, choose **Abort**. A prompt appears.
2. Confirm that you want to abort the job.

After the Job Completes

There are several ways that you can confirm the results of an automatic job:

- **Last Automatic window**—Displays the status of the operation for each resource and automatically filters system messages for that specific automatic job.
- **System Messages window**—Displays all of the messages available for completed jobs.

- **Alerts palette**—Indicates whether a condition exists that requires corrective action.
- **File Manager**—The File History window indicates the latest version recorded by the database.
- **Media Manager**—The session information includes the time the session was written and the label of the media it is located on.

Last Automatic Window

Last Automatic window

To view system messages for a recent automatic job

1. From the Status tab, choose the Last Automatic icon. The Last Automatic window appears. This window displays the results of the most recent automatic job.
2. From the Last Automatic window, choose the **Messages** button. The System Messages window automatically filters system messages based on the job ID of the most recent automatic job.

System Messages

Storage Manager records messages generated by jobs directly in the System Messages window.

The default view of the System Messages window displays all of the system messages, including linked messages, for the most recent jobs. The most recent system messages appear at the top of the list. **Linked messages** provide detailed information and appear indented below the primary message.

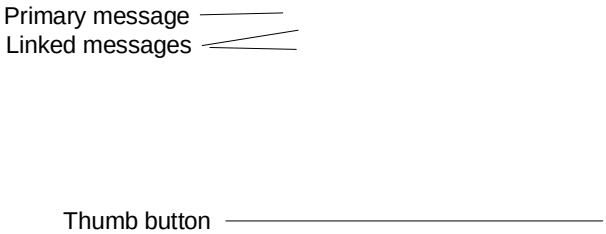
To view a system message

1. Highlight a system message in the System Messages window. The full description of the system message and any recommended action appear below the system messages.
2. Use the thumb button or arrow key to view additional available messages in the window

➤ If the **More** button is active, you can view more messages. Choose this button and continue to scroll through the list of available messages. Continue to choose the **More** button and scroll through the list until the **More** button is no longer active.

To view details about the message

1. Highlight the system message.
2. Choose the **Details** button. The System Message window appears. Use the **Next** button to view any linked messages.



System Messages window

Alerts Palette

Alerts palette

The icons in the alerts palette represent types of problems that need corrective action. The alerts identify general problems relating to jobs, the job server, media, and devices. If an alert is active (appears in color), warning or error messages exist. Click the active alert to view details about the problem. Tool Tips describe the meaning of each alert.

See page 7-26 for more information about alerts.

File Manager

The File History Database automatically records files that have been backed up or archived during automatic operations. To view the media locations of file versions, you can view the Extended History window

in File Manager. This window displays the label of the media that the file version was written to and the time and date the operation occurred.

Media Manager

You can view the latest session written to a media by viewing your installation's media tree. Session information includes the time and date of the most recently written session. If Media Manager was open when you submitted the job, you must select *Refresh Media Tree* to display the latest backup job.

Custom Jobs

By using managers, you can select specific items for backup, archive, migrate, or restore operations. Jobs defined in this way are called **custom jobs**. Custom jobs provide greater flexibility than automatic jobs. They allow you to:

- Use managed or non-managed media.
- Include the entire Protected Resource List or specific resources or files.
- Perform any single operation (backup, archive, migrate, restore or utility operation).
- Perform the operation once, periodically, or following another scheduled job.

Selecting Items

Custom jobs require the user to select the items for an operation. The Resource, File, Media, and Device managers present items in a tree structure to illustrate a hierarchy of items.

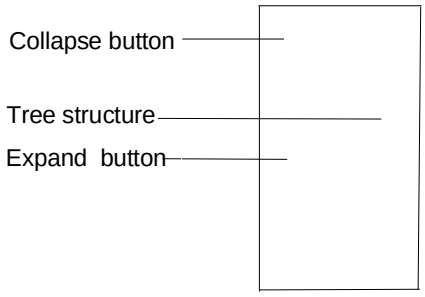
To select a manager

➤ Select the Managers tab and click a manager icon. The main window appears.

✓

TIP:	You can also click a manager icon from the managers palette.

Tree structures let you view how items are organized and let you hide or display details. **Expanding** displays additional detail; **collapsing** hides detail.



Sample Tree Structure

To collapse or expand a tree

1. Highlight an item.
2. Select the appropriate Tree menu option. Next to each item is a collapse/expand button. The plus sign (+) indicates that the highlighted item can be expanded at least one level. The minus (-) sign indicates that all of the levels have been displayed so that the only action available is collapsing.

Tagging Items

Select an item on the device and media trees (in Device Manager and Media Manager) by highlighting the icon. These managers process a single item during each operation. Tree structures with check boxes allow you to tag multiple items before choosing the operation. Tree structures with check boxes appear in Resource Manager, File Manager, and the session windows within Media Manager. See page 9-16 for information about finding, sorting, and filtering the files.

To tag an item

➤ Highlight the item you want to tag and click the item's check box or open the Select menu and select *Current Item*. A red "x" appears next to the tagged item.

or

➤ Click the item's check box.

To tag an item and all items beneath it

➤ Highlight the item and choose *SubTree* from the Select menu. You can also highlight the item and type "/." If you expand the item, you will see that lower-level items had red "x"s. For example, if you tag a server, all of the protected resources residing on the server are immediately tagged. If you tag a directory, its files are tagged as well.

✓ ***TIP:*** To untag items after submitting a job or to select different items for the current job, open the Select menu and select the *Clear Tags* option.

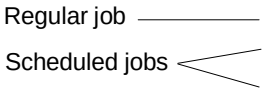
Attended and Unattended Modes

When you submit a job, you can run it in attended or unattended mode. In unattended mode, the program determines how to complete the operation based on parameters that have been configured and information from the configured devices.

In attended mode, the program prompts you to provide instructions in order for the program to continue. Usually the program prompts the user to load the correct media for the current job.

Excluding automatic jobs, the program processes jobs in attended mode by default. When you submit a job, you have the option of choosing unattended mode by turning off the **Prompt With Questions** option. If you submit an automatic job ahead of schedule, you have the opportunity to submit the job in attended mode.

Managing the Job Queue



Job Queue window

To view the Job Queue window

➤ From the Control Console, select the Status tab and click the Job Queue icon.

✓

TIP: If you are submitting several jobs, you may want to note their job IDs. Later, you can filter the System Messages window to display only the messages of a specific job.

The Job Queue window displays all jobs in the queue. Scheduled jobs are indicated by an “alarm clock” icon. All other jobs are indicated by a “document” icon. In the normal state, these icons are yellow, if there is a problem, the icons turn red.

When a job has completed successfully, the program sends a system message indicating that the job completed successfully to the System Messages window. Unless the job repeats, the job disappears from the Job Queue window. If a jobs fails (its status is “server hold”), the program assigns the job a new job ID. The system messages describing the failure appear under the original job ID.

De-activating a Job

Administrators and operators can de-activate (or put on operator hold) jobs. You might do this to allow a more urgent job to process, to repair a device, or retrieve the required media.

To de-activate a job

➤ From the Job Queue window, highlight the job you want to de-activate and select the **Hold** button. The **Status** field changes to **Operator Hold**.

TIP: To put all of the remaining jobs on hold after the program completes processing the current jobs, select the **Halt queue** option. The displayed status of the jobs does not change while the queue is halted.

Activating a Job

Storage Manager puts jobs on server hold if they fail. Whether the jobs are on server or operator hold, they require a user to resubmit them. The job server processes all jobs in the order in which they were submitted or resubmitted.

To activate a job

1. If the job is on server hold, be sure to investigate and resolve the problems that caused the job to fail. You must refer to the System Message window to discover why a job failed. Refer to the *Administrator's Reference Guide*, if necessary.
2. From the Job Queue window, highlight the job on hold and choose the **Submit** button.

➤ If a scheduled job has not been assigned a job ID, you can also submit for processing. If the scheduled job has been assigned a job ID, then it is already due for processing.

3. A prompt asks if you want the program to prompt you with questions (select the **Prompt With Questions** option to run in attended mode). Choose your preference. The job's state changes to "Resubmitted."

Deleting a Job

To delete a job from the queue

1. From the Job Queue window, highlight the job you want to delete. You can delete jobs with the status of "Ready," "Operator Hold" and "Server Hold." Note that deleting an automatic recall job will cause Storage Manager to send notification that the job has failed.
2. Choose the **Delete** button. Storage Manager asks you to confirm that you want to delete the job from the queue.
3. Choose **Yes**.

➤ If this is a repeating scheduled job that has been assigned a job ID, only this repetition of the job is deleted. The job server will process the job at the next scheduled time. To permanently delete the scheduled job, highlight the scheduled job again and choose the **Delete** button. The scheduled job no longer appears in the window.

NOTE: Storage Manager does not allow you to delete your "Default Automatic" job from the database. You can put this job on operator hold, however.

Adding Users

During the installation process, the program adds the auto login user to the Admin List and the group EVERYONE to the User List. Users are divided into three types: administrators, operators, and end users. Each has different rights and are configured in the Configuration Manager.

NOTE: In 4.x installations, any user who needs to submit file-level jobs (in other words, accessing File Manager) must be logged in to the tree where Storage Manager is installed.

Administrators are users with full access to all six managers within Storage Manager. Only administrators have access to the program's most powerful functions:

- Configuring access to users
- Configuring operations and automatic job parameters
- Defining file rules
- Migrating files
- Labeling media
- Configuring access to other Storage Manager installations

Operators have full access to Control Console and limited access to File Manager. Within Control Console, operators have the same rights as administrators and are able to manage the jobs in the queue. You can delegate job monitoring tasks to operators; in most cases they can respond to device and media messages.

End users can access File Manager only. Operators and end users are able to back up and restore directories and files for which they have rights. The Configuration Manager contains the lists of users with access to Storage Manager. End users can recall migrated files automatically where this function is enabled and there is access to a recall agent. See Appendix E, "Recalling Files," for more information.

See page 9-36 for information about end user access to File Manager.

Adding Operators and Administrators

To add operators and administrators

1. From the Control Console window, select the Managers tab.
2. Click the Configuration Manager icon on the Managers tab. The Configuration Manager window appears.
3. Open the Configure menu and select *Systems*.
4. Select the Admin List tab.

Operator user icon
Auto login user icon
Administrator user icon

Admin List tab

5. Choose the **Insert User** button and the list of servers on the network appears.

6. Click the server that the user has access to. The list of users defined on that server appears.

7. Click the user's name. The user appears on the list as an administrator.

8. Choose a user type (**Administrator** or **Operator**).

9. Specify which type(s) of notification the user will receive. By default, administrators are configured to receive NetWare SEND messages on warnings and errors.

➤ If you specify MHS e-mail notification, also enter the user's e-mail address and the volume path of the MHS Mail server.

Adding End Users

The User List tab allows you to configure users and groups of users for access to Storage Manager's File Manager. If you are adding end users or end user groups, you need to allow end users access the File History Database of their resources. See page 9-36 for information about configuring File Manager for end users.

To add a user (or group)

1. From the Configuration Manager window, open the Configure menu and select *Systems*.

2. Select the User List tab.

3. Click the **Insert User** (or **Insert Group**) button. The Pick a User to Add (or Pick a Group to Add) dialog box appears.

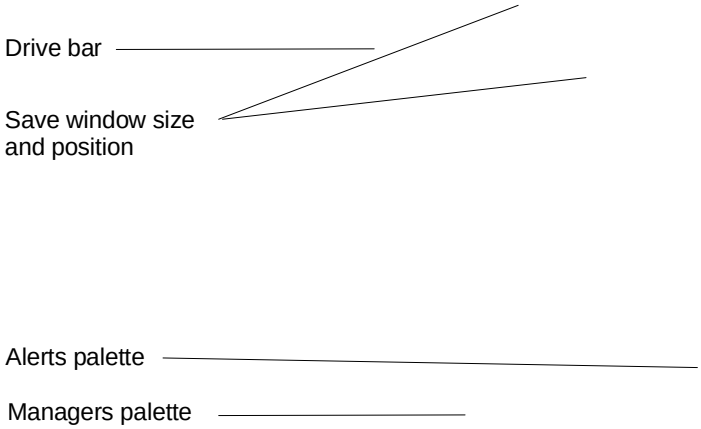
Pick a User to Add dialog box

4. Select a user from the Pick a User to Add (or Pick a Group to Add) dialog box. The user (or group) appears in the **User** list.

See page 4-12 for information about configuring these parameters.

Customizing the User Interface

Storage Manager allows you to set parameters to determine the appearance of your user interface. You can customize the display of each manager individually.



Some of the User Interface Options

The Preferences option, available in every manager, allows you to:

- Display or hide the status bar, which provides information about activities currently being performed through the user interface, such as building a directory.
- Display or hide Tool Tips, which provides a brief description of the tool bar icon's function.
- Change on-screen fonts (This option does not apply to Configuration Manager and Control Console although you can configure this option to apply to other managers).
- Display the horizontal scroll bars.

- Save the size and position of the all windows. When you next open the specific manager, the program displays the windows in the same size and in the same position as they were when you exited.

Some options can only be configured in specific managers.

- Display alerts and managers palettes throughout program (available only in Control Console).
- Configure end user notification (available only in File Manager)
- Display the drive bar (available only in File Manager).
- Configure the end user's workstation names (available only in File Manager).
- Configure notification for end users (available only in File Manager).

To configure display preferences

1. From any manager, open the File menu and select *Preferences*. The Preferences dialog box appears.
2. Set your preferences.
3. Choose **OK** to save your preferences.

At a Glance: Available Menu Options

The tables below display menu options for each of the managers.

Control Console

File	Operations	Status	Reports
Open Installation…	Automatic	Job Queue	Future Media Rotations
Close Installation		Last Automatic	Resource Summary
Print Report…		Next Required Media	Device Summary
Print Preview		Off-Site Media Advisor	Media Summary
Print Setup…		System Messages	Configuration Summary
Preferences…		Resource Monitor	
Exit			

Configuration Manager

File	Configure	Install
Open Installation…	System	Multi Server Software…
Close Installation	Operations	Auto Loader Software…
Save	Media Scheduling	
Preferences…	Enterprise Setup	
Exit		

Resource Manager

File	Operation	Select	View	Tree
Open Installation…	Automatic…	Current Item	Sort by Target Service	Expand One Level
Close Installation	Restore…	SubTree	Sort by Type	Expand SubTree
Preferences…	Backup…	Next Tagged Item	Sort by Location	Expand All
Exit	Archive...	Clear Tags		Collapse One Level
	Migrate...			Collapse All
	History Database Maintenance…			
	Translate History Database			
	Add Resource…			
	Remove Resource…			
	Edit Resource Info…			
	Edit Migration Parameters...			
	Refresh the Tree			
	Change Sequence…			
	History Database Location…			

File Manager

File	Operations	Select	View	Tree	Rules
Open Resource…	File Finder…	Current Item	Enable Filter…	Expand One Level	Rule List
Close Resource	Refresh Directory Tree	SubTree	Define Filter…	Expand SubTree	Edit Rule…
Print To File...	Restore…	Next Tagged Item	Sort…	Expand All	Insert Rule…
Preferences…	Backup…	Clear Tags	File Attributes	Collapse One Level	Delete Rule…
Enterprise Setup…	Archive		File Path	Collapse All	Rule Origin
Exit	Migrate		File Rules	Change Directory…	
	Remove History Record		Tagged Items Window		
			Extended History		

Media Manager

File	Operations	View	Tree	(Mounted Media Only) Operations
Open Installation…	Retire…	Mounted Media	Expand One Level	Journal…
Close Installation	Forget…	Session Window	Expand SubTree	Verify…
Preferences…	Refresh Media Tree		Expand All	Copy…
Exit			CollapseOne Level	Tension…
			Collapse All	Format…
				Secure Erase…
				Robotics …

Device Manager

File	Operations	Tree
Open Installation…	Scan for Devices	Expand One Level
Close Installation	Add Device	Expand Subtree
Preferences…	Edit Device…	Expand All
Exit	Remove Device	Collapse One Level
	Test Device…	Collapse All
	Import Media…	

Basic Menus

The following menus and options are available in all Storage Manager managers.

Managers Menu

Within each manager, the Managers menu lists the five other Storage Manager managers.

Window Menu

Storage Manager allows you to display multiple views of the open dialog boxes and windows. These options help you to organize these multiple views.

- *Cascade*—Arranges windows so they overlap, leaving each title visible.
- *Tile*—Arrange windows so they display side-by-side.
- *Arrange Icons*—Arranges icons at the bottom of the window.

Help Menu

To find out more on how to use help, choose Help/*Using Help* on the Help screen.

- *Current (F1)*—View help for the current menu, procedure, screen, etc.
- *Index*—View a list of available Help topics. From the contents, you can choose topics to explore further.
- *Using Help*—Learn how to use the Help system.
- *Legend*—View the legend of screen symbols.
- *Palindrome Support*—Learn how to contact Technical Support and answers to commonly asked questions.

- *Palindrome Products*—Learn about other Palindrome products.
- *About ...*—View the version, copyright, and serial number of your Storage Manager installation (Control Console only).

Chapter 4

Customizing Your Installation

Overview

This chapter describes:

- Installation parameters
- How to add and delete users
- How to configure Palindrome SNMP messages
- How to add and delete other Storage Manager installations
- How to access other installations

Introduction

The default configuration settings for Storage Manager general operations, user notification, and automatic operations are appropriate for most situations. However, Storage Manager can accommodate the needs and preferences of a various environments. To customize your settings or to familiarize yourself with the parameters, refer to the tables in this chapter.

Before You Customize Your Installation

Storage Manager is ready to run your automatic and custom backup jobs immediately after installation.

If you want to review these settings (or later review changes you have already made), you can print the Configuration Summary report. See page 7-36 for instructions on viewing and printing this report.

NOTE: You cannot access Configuration Manager while Storage Manager is performing an operation. To access Configuration Manager while jobs are processing, select the **Halt queue** option. As soon as it finishes servicing jobs, it puts the remaining jobs in the queue on hold.

To configure ...	See Page
Administrators and operators	4-10
Auto login user and password	4-6
Automatic backup and archive operations	4-24
Automatic recall	4-19
Backup parameters	4-16
Concurrency	4-14
End users	4-12
Full protection of files	4-17
Migration parameters	4-19
Multiple installations	4-37
Notification	4-10
Number of managed media sets	Tower of Hanoi 4-27 Grandfather-Father-Son 4-28
System Messages database size	4-13
Rotation pattern	4-23
Rotation time	Tower of Hanoi 4-26 Grandfather-Father-Son 4-28
SNMP messages	4-7

Configuration Manager Tool Bar

The Configuration Manager tool bar provides a short cut to commonly used operations:

Save Installation Changes—Save your changes immediately. The program also prompts you to save changes upon exiting the manager or closing an installation if any changes have been made.

System Configuration—Configure users, notification, concurrency and other system parameters.

Operations Configuration—Configure how the program performs backup, archive, and migrate operations.

Media Scheduling Configuration—Configure how the program performs automatic jobs.

Help—View on-line help for Configuration Manager.

System Configuration

General tab (default values)

The parameters in the General tab determine how the program accesses NetWare 3.x and 4.x servers in your Protected Resource List.

Parameter	Description	Default
Bindery Auto Login		
Name	The name of the auto login user defined on all of the 3.x servers on your Protected Resource List (and 4.x servers that are not a part of your installation's NDS tree) including the MHS mail server.	Configured at installation
Password	The (optional) password for the auto login user. This parameter is optional.	Configured at installation
Retype Password	Confirm the password by entering it in this field.	Configured at installation

Parameter	Description	Default
NDS Auto Login		
Name	The auto login user defined on the NDS tree on your Protected Resource List. An auto login user is required if you are installing Storage Manager on a NetWare 4.x server.	Configured at installation
Password	The (optional) password for the NDS auto login user.	Configured at installation
Retype Password	Confirm the password by entering it in this field.	Configured at installation
SNMP Alert On		
The following three fields indicate which type of message Storage Manager sends to configured SNMP (Simple Network Management Protocol) management consoles. SNMP messages **do not** include every note, warning, or error message.		
Notes	Provides status information which may be helpful to the user.	Off
Warnings	Indicates that a potential problem requiring the user's attention exists.	Off
Errors	Indicates that Storage Manager requires the user to correct a problem.	Off
Installation Name	The name of the Storage Manager installation. By default, this is the server/volume location and directory path of the System Control Database.	Installation directory

Configuring Palindrome SNMP Notification

If you have not already configured your servers to send SNMP messages to the appropriate SNMP management console, follow the procedure below. Refer to your message system's documentation for configuring SNMP workstations.

To configure SNMP management consoles

1. Copy the file PALINDRO.MIB from the installation directory (by default, this is the \PAL directory) to the appropriate directory on the management console. For example, when using Novell's NMS, copy the file to the NMS\SNMPMIBS\CURRENT directory on the SNMP management console.

2. Compile the PALINDRO.MIB using the SNMP management console's MIB compiler.

3. Edit the TRAPTARG.CFG file located on the \ETC directory of the SYS: volume of your Storage Manager installation server using any text editor.

4. Type the IPX addresses of the SNMP management consoles that will receive the SNMP messages in the "Protocol IPX" section.

➤ If you are targeting a UNIX client, type the IP address in the "Protocol UDP" section and load TCP/IP on the server.

NOTE: If your SNMP management console receives SNMP only through IP protocol, you must also load TCP/IP on your Storage Manager installation server. In the TRAPTARG.CFG file, type the IP address and load TCP/IP.

5. Run the system message software from at least one of SNMP management consoles.

6. At the server console prompt, type:

   LOAD SNMP

   The SNMP management consoles receive a message that SNMP.NLM has been loaded.

7. On the General tab in Configuration Manager, select the levels of message severity the program should send to the SNMP broadcast server.

NOTE: Palindrome SNMP messages appear in one of two forms. If you are using Novell's NMS (NetWare Management System), SNMP will display full message descriptions. If you are using another system, such as HP OpenView, the SNMP message indicates only that a message with a certain level of severity (such as a "Note," "Warning," or "Error") has been recorded.

Admin List tab (default values)

Use this tab to define administrators and operators and the type of notification Storage Manager will send them.

Parameter	Description	Default
User/Server	Displays the user configured on a particular server.	Auto login username and installation server
<User/Server>	Indicates the status of the highlighted user. **Administrator**—User has full access to all Storage Manager applications. **Operator**—User has access to File Manager and to Control Console.	Administrator
Netware SEND Message On		
SEND messages are NetWare SEND messages that appear as pop-up windows to the user. Select the types of message, notes, warnings, or errors, that Storage Manager will send to the highlighted user.		
Notes	Provides status information.	Off

Parameter	Description	Default
Warnings	Indicates that a potential problem exists.	On
Errors	Indicates that Storage Manager requires the user to correct a problem.	On
MHS Email Message On		
The Email notification feature requires that you have Novell's MHS, or Message-Handling System, installed and properly configured. MHS is a software program that transfers electronic messages from one place to another. The user receives a general message concerning the status of a particular job.		
EMail Address	The address required to receive e-mail messages. The user's e-mail address should appear in this format: "USER@WORKGROUP" Example: JSMITH@PALINDRO	None
MHS Mail Path	To send e-mail notification to users, specify the host volume of an MHS Mail Server.	None

To add a user

1. Select the **Insert User** button and the list of servers on the network appears.
2. Click the server that the user logs in to. The list of users appears.
3. Click the user's name.
4. Choose a user type (**Administrator** or **Operator**).

To delete a user

1. Highlight the User/Server name.
2. Select the **Delete User** button. A prompt appears asking you to confirm the delete operation.
3. Choose **Yes**. The user is no longer on the list.

User List tab (default values)

The User List tab allows you to configure users and groups of users for access to Storage Manager's File Manager.

Parameter	Description	Default
User	Individual end users	None
Group	Group of end users, such as EVERYONE.	EVERYONE

To add a user (or group)

1. Click the **Insert User** (or **Group**) button.
2. Select a user from the Pick a User (or Group) dialog box. The user appears in the User List.

To delete a user (or group)

1. Highlight the user (or group) name.
2. Click the **Delete User** (or **Group**) button. Choose **OK** to confirm.

Advanced tab (default values)

The System Advanced tab provides parameters of interest to advanced users such as configuring the size of the System Messages database and the concurrency parameters.

Parameter	Description	Default
System Message Settings		
Storage Manager automatically truncates the System Messages window based on the parameter (days or database size) that is most restrictive. For example, you configure the program to retain messages for 30 days. If the size of the System Messages reaches the maximum value set in the **Maximum size of the Database** parameter before the oldest message is 30 days old, the program begins removing the oldest messages in order to make room for new messages.		
Maximum Size of the Database	Retains the messages totaling up to the byte size you specify (the maximum is 100 megabytes), unless the database size exceeds the maximum age.	**2**(MB)
Estimated Number of Messages	Displays the estimated number of messages the System Messages will retain, based on the maximum byte size you specify.	**1000**

Parameter	Description	Default
Number of Days to Retain Messages	Retains messages for the number of days you indicate (up to 91 days) unless the System Messages exceeds the maximum size (in megabytes).	**30**
Enable Text Error Log	This option creates a separate text file for current system messages. This file (PAL_LOG) is overwritten at every rotation.	On
	NOTE: After you have used the product for a few weeks, you can turn off this unless you are troubleshooting.	
Process Control		
Concurrency refers to Storage Manager's ability to simultaneously use multiple devices to: —Perform backup operations on multiple resources simultaneously —Perform backup, restore , migration,and/or utility jobs simultaneously		
To take advantage of concurrency, your must have: —At least two devices configured. —Eligible media loaded in each device. —At least 2 MB RAM available on your server for each concurrent process (for example, if you have two backup devices you need at least 4 MB of RAM). Concurrency does not apply to DOS and OS/2 workstation volumes. The TSA prevents the program from backing up a workstation's C: and D: drives, but the program can concurrently back up the C: drives of multiple workstations. See page 2- for details		
Maximum Concurrent Backup Operations	The number of backup (including archive and database maintenance) operations Storage Manager can perform simultaneously within a single job.	**3**
	NOTES: To implement concurrency, you must have at least two backup devices. The value of the parameter does not affect installations with one backup device. These installation s will obtain the benefit of performing concurrent database maintenance operations. Be aware that concurrent processing is dependent on environmental factors such as bandwidth, memory, and operations performed by other applications.	
Maximum Concurrent Jobs	The number of different engines that can be loaded simultaneously. The maximum value is **8**.	**4**

Parameter	Description	Default
	NOTES: By default, the program can load one each of the following engines: backup (PALBACK.NLM), restore (PALREST.NLM), and utility (PALUTIL.NLM), in addition to three migration engines (PALMIG.NLM) simultaneously, unless there is a conflict. For example, if one of the jobs is a concurrent backup operation that is using all of the available devices, the program does not have a device available for another job such as restore, which also requires a device. You can run up to six migration jobs (PALMIG.NLM engine) if no other engines are loaded. Some utility operations (such as retire and forget) in addition to database maintenance and migration operations do not require a device. However, jobs representing these operations are limited by the value of this parameter.	

✓ ***TIP:*** To keep records of system messages, you can print the System Messages database periodically rather than maintain an excessively large System Messages database. See page 7-25 for printing instructions.

Operations Configuration

Backup tab (default values)

The Backup tab provides parameters that determine how the program implements backup operations.

Parameter	Description	Default
Backup Parameters		
Preserve Backups	The Preserve Backups parameter allows you to extend the life of a backup session on media beyond the day when the program next rotates to that media set. Increasing this value usually requires additional media.	0
	NOTE: Because archive sessions are written to a permanent portion of the media, Preserve Backups does not affect archive copies of files. To preserve backup sessions, enter the minimum number of days that you want evolving files to exist on the backup media. For example, if you want to preserve a backup session for a minimum of four weeks, set Preserve Backups to **28** (days).	

Parameter	Description	Default
Clear Archive Bits After Backup	This command indicates that Storage Manager should clear a file's archive bit after it has been backed up. When this parameter is turned on, both full and incremental backups clear the archive bit after backing up a file (a differential backup does not clear the archive bit).	On
	NOTE: Do not change this setting unless you have other applications that rely on the status of the archive bit.	

Archive/Migrate tab (default values)

The Archive/Migrate tab provides parameters to determine how Storage Manager archives, fully protects, and migrates files.

Parameter	Description	Default
Archive Parameters		
Archive Copies Required for Full Protection	The number of archive copies that must exist in the current library for a file to be considered "fully protected."	**3**

Parameter	Description	Default
	Palindrome does not advise decreasing this to a value less than three. Decreasing this value could expose your data to increased risk in an on-site disaster.	
Put an Archive Copy on All Media Sets	With this option turned on, Storage Manager writes copies of eligible stable files to every media set. By default, the program writes archives copies to as many managed media sets as necessary in order to fully protect the file.	Off
	NOTE: This option increases the time required for automatic jobs on rotation day but **may** result in quicker restore operations. When this option is turned on, you may also require additional media to accommodate additional archive copies.	
Put Archives on Separate Media from Backups	By default, Storage Manager writes both archive and backup sessions to the same media to minimize the number of media needed in a media set.	Off
	NOTES: There are several reasons why you might want to select this command: —You have at least one device that requires separate media (for example, a DC 6000 tape drive does not allow for selective overwrites and would allow Storage Manager to trap backup sessions). —Your backup sessions typically require over 50% of the media during an automatic operation. —You intend to write archive sessions to optical disk and backup session sessions to tape, a less expensive media. —You perform frequent custom backup and archive operations on managed media (and want to avoid trapped backups). A **trapped backup** session is a backup session to which a custom archive session has been appended. Since the program does not overwrite the archive sessions, the backup written between archive session becomes permanent.	
Create a Near Line Media Set	When turned on, this optional feature designates the most frequently used set (the A set) as the near line set. As a result, the program ensures that an archive copy of a file is on this set before migrating it during a resource-level migration. When these files are later migrated, you will always have an on-site copy to expedite restore/recall operations. Only the Tower-of-Hanoi rotation schedule allows you to designate a near line set.	Off

Parameter	Description	Default
	NOTE: This option is especially useful if you have an autoloader that keeps the near line set available at all times.	
System Migration Parameters		
Resource Monitoring		
Monitor Resource Capacity	Indicates whether Resource Monitor monitors the disk utilization of protected resources. This option must be turned on in order to enable the **Enable Automatic Migration** option.	On
Enable Automatic Migration	Indicates whether Storage Manager automatically migrates eligible files when disks reach their high water marks. Storage Manager migrates as many eligible files as necessary to reduce each disk's utilization to the low water mark. Storage Manager may build or update the list of eligible files (prestage list) and migrate these files if necessary. **NOTE:** The prestage list consists of the TMPEDBDT.PAC and TMPEDBNX.PAC files. These files each grow approximately 3 Mb for every 10,000 files that are prestaged. Be sure that you have adequate disk space available before running your first migration job. These files are located in the directory where each resource has its history records. By default, these files are located in the PAL\DB\1, PAL\DB\2, etc., directories where \PAL is your installation directory and \1, etc., correspond to protected resources.	Off
Enable Automatic Recall	Allows Storage Manager to process a recall job when a user or application attempts to open a phantom file located on this resource. The appropriate recall agent(s) must also be loaded.	On
Migration Thresholds		
High Water Mark	Indicates how full a volume must be before Storage Manager automatically migrates eligible files. Eligible files must be fully protected and meet the dormancy requirement for the applicable migrate rule. **NOTES:** You can select a percentage from 0-100. If you set the level above 95%, the hard disk may not be able to save critical files because the disk reaches full capacity before Storage Manager has the chance to migrate inactive files.	**90%**

Parameter	Description	Default
Low Water Mark	Indicates the level to which Storage Manager attempts to reduce the actual level of disk utilization through resource-level migration.	**80%**
Leave Phantom File(s) after Migration	Selecting this option places a zero-byte file placeholder on the disk when a file is migrated. This option is required to recall files automatically.	On
Files to Migrate	Indicates the order in which Storage Manager migrates files on the prestage list of each resource. **Largest Size**—Migrate eligible files with the largest size first. **Least Recently Used**—Migrate eligible files that are the oldest first. **Most Eligible**—Migrate the eligible files that have been eligible for the longest time relative to the stability period of their respective migrate rules. For example, in the following scenario, File B is most eligible. File A: 1 week (eligibility)/10 weeks (stability period)= 0.1 File B: 3 weeks (eligibility)/2 weeks (stability period)= 1.5	**Least Recently Used**
Tuning Parameters		
Restore Time Out	Indicates the length of time (minutes) that the restore engine remains loaded without a restore (or recall) job in the queue. If there is still no job for the engine to process at the end of this period, the restore engine automatically unloads.	0 (minutes)
Resource Scanning Interval	Indicates how frequently (in seconds) the Resource Monitor scans the disk utilization status of monitored volume resources.	**5** (seconds)

WARNING: If a user attempts to restore a phantom file that was copied from another directory, moved, or renamed (or whose directory was renamed), only a zero-byte file will be restored. The phantom file no longer references the file's current location. Therefore, be sure to warn users not to copy, move, or rename phantom files or rename directories containing phantom files.

Advanced tab (default values)

The Operations Advanced tab provides parameters to determine how Storage Manager verifies that operations are written to media correctly, and whether the program ejects media following automatic operations.

Parameter	Description	Default
CRC Data Verification Level for Backups	If you specify **Calculate** or **Verify**, Storage Manager calculates the 32-bit CRC (Cyclical Redundancy Code) values for each file written to media and stores those values on media. Storage Manager uses these values when restoring (if the **User CRC Data Verification** parameter is turned on) and verifying media to confirm the integrity of the data. Using the **Calculate** and **Verify** options increases backup time. The impact varies with the number of files, file size, processor type in the server, and the type of backup device you are using. For example, the **Calculate** option adds five seconds to the time required by a 386SX-based system to back up a 1MB file. Allow slightly more time to perform the **Verify** option.	**None**

Parameter	Description	Default
	NOTES: Descriptions of the available options follow: **None**—Do not calculate or verify CRCs. **Calculate**—Calculate and store CRC data. The program uses the calculations for verifying media which you can perform through Media Manager (Operation/*Verify*). **Verify**—Calculate media CRC values and compare these with the media's CRC values during backup. If the values do not match the program, it writes the file to media but does not track the file in the database. To ensure proper hardware setup, Palindrome strongly recommends that you verify the CRC values on media during the first week after installation. After the first week, set it back to **None**. Thereafter, verify CRC data periodically.	
Use CRC Data Verification on Restore Jobs	When restoring files to disk, Storage Manager verifies that CRC values match what was written to backup media. To use this option, CRCs must have been calculated when written to media.	Off
Eject Media after Automatic Job	Ejects media after the day's automatic job is complete.	Off
Retain File System Compression	On NetWare volumes supporting compression, Storage Manager backs up and restores data in compressed format if they are compressed.	On
	NOTE: The only time you may want to change the default is to redirect data from a compressed volume to an uncompressed volume. If you turn off this option, Storage Manager de-compresses compressed files when writing the data to backup media which affects performance.	

WARNING: If you turn off the **Retain File System Compression** option and restore uncompressed data to a NetWare compressed volume, be sure the volume has ample space to accommodate the uncompressed data.

Media Scheduling Configuration

General tab (default values)

The General tab provides parameters that determine how the program schedules the automatic jobs and vault storage as well as the label of the managed media sets.

Parameter	Description	Default
Media Rotation Pattern	Storage Manager determines the rotation schedule and the off-site media schedule based on the rotation pattern you select. See page 2-14 for a comparison of Tower of Hanoi and Grandfather-Father-Son rotation patterns.	**Tower of Hanoi (TOH)**
Media Library Name	This parameter indicates the media library name, which becomes part of the media label of all managed media and is defined during installation. If you change the name, Storage Manager retires the managed media library. You have then created a new active media library based on the new name. The formerly active media becomes available for restore operations only.	Name specified at installation
	NOTE: Palindrome recommends that you create a new managed media library name at least yearly.	

Operation tab (default values)

The Operation tab provides parameters to determine which operations occur during automatic jobs. Except for the **Daily Media Change within Set** parameter, which it does not need, the GFS rotation pattern has the same operation parameters as the TOH rotation pattern.

Parameter	Description	Default
Non-Rotation Options		
Operation	The type of automatic backup operation the program performs on a given day when media sets are not rotated. Parameter choices are: —**Diff** (Differential) —**Incr** (Incremental) —**Full** (Full)	**Incr**

Parameter	Description	Default
Check for Deleted Files	With this option, on non-rotation jobs, Storage Manager updates the File History Database to reflect files that were recently deleted from disk. If you select this option, the time required to process non-rotation jobs increases. **NOTE**: If you are using weekly rotation and frequently delete files, you may want to turn on this option. This option prevents the program from restoring files that you recently deleted during a full resource restore operation.	Off
Back Up Fully Protected Files	Writes backup copies of files that are already fully protected (unless already on this media set). To guarantee every media set contains a copy of every file, use this command.	Off
Daily Media Change within Media Set	This parameter applies to TOH rotation only". A different media in the same set is used each day. For example, the program requests a different media each day to perform the non-rotation operations. To change media every day within the current media set, turn on this option. For example, if you are sending your backup media offsite every day. If you are using daily rotation (each day has its own media set), **do not turn on** this option.	Off
Back Up if Archived in Same Media Set	Writes a backup copy on every media set, even if an archive copy already exists.Use this option to prepare for a server shutdown and ensure that a copy of every file exists on a single backup media.	Off
Rotation Options		
Archive Eligible Files	Writes stable files to a permanent portion of media.	On
Back Up Fully Protected Files	See the description under *Non-Rotation Options*.	Off
Back Up if Archived in Same Media Set	See the description under *Non-Rotation Options*.	Off

TOH Scheduling tab (default values)

The Scheduling tab provides parameters that determine when the program requests you to change managed media sets and the number of media sets in your managed media library. This schedule is based on the Tower of Hanoi rotation pattern.

Parameter	Description	Default
Rotation Configuration		
Rotation Day	The day(s) on which you want to rotate media sets. Storage Manager automatically prompts you to change media sets each day that you select for rotation to occur.	**Friday**
Rotation Time	The time at which Storage Manager requests the next scheduled media set. If you turned on the **Daily Media Change within Media Set** option, the program requests the next scheduled media.	**12:00 AM**

Parameter	Description	Default
Number of Media Sets	The number of media sets rotated for automatic jobs. You can designate from two to 12 media sets in a single library. If you reduce the number of media sets in this parameter after the sets have been created, the program no longer schedules the least frequently used set(s). Archive copies on the unscheduled media sets still count toward full protection.	**5**

GFS Scheduling tab (default values)

The Scheduling tab provides parameters that determine when the program requests you to change managed media sets and the number of media sets in your managed media library. This schedule is based on the Grandfather-Father-Son rotation pattern. Because GFS automatically assigns seven of 32 possible media sets to daily media sets, you have 25 media sets to configure for weekly, monthly, quarterly, and/or yearly time periods.

NOTE: The program automatically rotates only one media set. If rotation days for multiple media sets coincide, the program requests the media set covering the broadest time frame.

For example, if the rotation day for weekly media sets is Friday, the program rotates to the weekly media on Friday and does not write to a "FRIDAY" media.

Parameter	Description	Default
Number of Daily Sets	The number of media sets permanently configured for automatic jobs. You cannot configure this parameter.	**7**
Rotation Time	See the **Rotation Time** parameter in the above Scheduling tab.	**12:00 AM**
Weekly Backup		
Rotation Day	See the **Rotation Day** parameter in the above Scheduling tab.	**Friday**
Weekly Media Sets	The number of media sets that the program rotates on a weekly basis. Using the default value, each weekly media set corresponds to a week in the month. The program may request sets WEEK1 through WEEK5 or WEEK1 through WEEK4, depending on the month.	**5**
	NOTES: If you set this parameter to a value other than **5**, the program schedules the weekly sets in a round-robin cycle. In general, the program overwrites backup sessions more frequently with fewer sets and less frequently with more sets.	
Retire Weekly Media Set	Removes the media set from rotation and preserves the backup sessions from being overwritten. The retired media sets are still available for restore operations.	Off
	NOTE: Because media is used only once, your library will require more media when this option is turned on.	
Monthly Backup		

Parameter	Description	Default
Day	Storage Manager requests a new media set to rotate on the last day of the "monthly" interval. The program writes the sessions to the appropriate media set.	**Last**
	NOTES: The options available at this list box are: **Last**—Indicates the last day of any month as the day for monthly media set. **1-31**—Indicates the numerical day of each month that you want the program to rotate to the scheduled monthly media set for an automatic job. For example, to rotate to the monthly media set on the 15th day of the month, set **Day** to **15**. Storage Manager rotates to your monthly media set for an automatic job on the 15th.	
Monthly Media Sets	The number of media sets that the program rotates on a monthly basis. Using the default value, each monthly media set corresponds to a month on a calendar month.	**12**
	NOTE: If you set this parameter to a value other than **12**, the program schedules the monthly sets in a round-robin cycle. For example, under the default, you would use the DECEMBER media set for rotation in December. If you set **Monthly Media Sets** to **4**, you would rotate media set MONTH4 in December. In this last example, the backup session does not remain on the media as long as it would with the default value. The session remains on media only three months compared with 12 months in the default example.	
Retire Monthly Media Set	See the **Retire Weekly Media Set** parameter.	Off
Quarterly Backup		
Month	The month in which the first quarterly backup operation occurs. The remaining quarters are calculated from this value. Quarters are based on calendar months and not the monthly periods you have defined for monthly media set rotation.	**March**
Quarterly Media Sets	The number of media sets that the program rotates on a quarterly basis. If you set this parameter to a value other than **4**, the quarterly rotations will still be performed every three months, but will not correspond to a 12-month period.	**0**

Parameter	Description	Default
Day	See the **Monthly Backup/Day** parameter.	**Last**
Retire Quarterly Media Set	See the **Retire Weekly Media Set** parameter.	Off
Yearly		
Month	The month in which the yearly automatic job occurs.	**December**
Yearly Media Sets	The number of media sets that the program rotates on a yearly basis. The program schedules the yearly sets in a round-robin cycle.	**0**
Retire Yearly Media Set	See the **Retire Weekly Media Set** parameter.	Off
Day	See the **Monthly Backup/Day** parameter.	**31**

NOTE: In GFS rotation, once the program has created all of the configured media sets, you can only add a media set group that covers a larger time period than currently exists in your library.

For example, if you have created daily, weekly and quarterly media sets and attempt to add monthly media sets, the program prompts you for a new library name. However, you could add the yearly media set without changing the library name.

TOH Off-Site Media tab (default values)

The TOH Off-Site Media tab provides parameters used to determine the schedule for storing managed media sets off-site. Palindrome recommends that you follow the off-site storage schedule displayed in the Off-Site Media Advisor window in Control Console. The Off-Site Media Advisor window reflects where your managed media sets **should be located** if you actually implemented the schedule. The program has no mechanism for actually tracking the current location of your media sets.

Parameter	Description	Default
Number of Media Sets On-Site	The number of media sets kept on-site at any given time. Storage Manager automatically excludes the most frequently rotated sets from being rotated off-site.	**2**

Parameter	Description	Default
	NOTE: **Do not** make this parameter greater than or equal to the **Archive Copies Required for Full Protection** parameter. This is to ensure that at least one archive copy of data exists in the vault.	
Notice Required for Retrieving Off-Site Media	The number of days' notice prior to the rotation day that the program recommends that you take media from the off-site storage to the work site.	**14**
	NOTES: Based on the number of days' notice you require, Storage Manager displays the media set in the **Retrieve from off-site storage** field on the Off-Site Media window in Control Console. If you are following the recommended off-site media schedule, be sure to view the Off-Site Media Advisor window regularly. A description of the Off-Site Media Advisor window appears on page 7-18.	

✓ ***TIP:*** To eliminate the risk of any data loss due to on-site disasters, you can copy the managed media to non-managed media. Use the *Copy* menu option in Media Manager and move the duplicate media to the vault. For more information on this feature, see page 10-17.

GFS Off-Site Media dialog box (default values)

The GFS Off-Site Media tab provides parameters used to determine the schedule for storing managed media sets off-site. Palindrome recommends that you follow the off-site storage schedule displayed in the Off-Site Media Advisor window in Control Console. The Off-Site Media Advisor window reflects where your managed media sets **should be located** if you actually implemented the schedule. The program has no mechanism for actually tracking the current location of your media sets.

Parameter	Description	Default
Media Sets to Remain On-Site	Indicates which media set groups are kept on-site at any given time. Storage Manager automatically specifies that daily media sets remain on site. Select one or more media set levels whose number of media sets is less than the number archive copies required for full protection.	**Daily**

Parameter	Description	Default
	NOTE: Since the objective of off-site storage is to prevent data loss, the number of media sets that remains on site must be less than the number of archive copies required for full protection. A prompt appears if the number is too great. This ensures that fully protected files will have at least one archive copy safely off site.	
Notice Required for Retrieving Off-Site Media	See the description in the above Off-Site Media tab (TOH).	**7**

Installing Other Palindrome Products

You can add value to your Palindrome Storage Manager installation with additional software options on the *Install* menu:

- AutoLoader Software
- Multi Server Software

To install additional Palindrome software products

1. Load the product diskette in a drive and select the appropriate *Install* option in Configuration Manager.
2. Enter the location of the install disk.

AutoLoader Software

Palindrome AutoLoader Software provides support for the ultimate in automated storage management: the autoloader (also referred to as a stacker, autochanger, or jukebox).

AutoLoader Software completely integrates the autoloader with Storage Manager operations to provide unparalleled automation for all backup and restoration tasks.

AutoLoader Software enables the program to perform the following functions:

AutoLoader Software allows you to control the autoloader through the Storage Manager's Windows interface. This product allows you to:

- Control the robotic arm of the autoloader
- Retain information about the contents and status of the autoloader
- Provide Storage Manager with automatic access to all media in the autoloader.

AutoLoader Software is available in a single- or multiple-drive license.

MultiServer Software

MultiServer Software allows you to upgrade your installation from the base Storage Manager license, which supports only one server, to an installation that supports multiple servers. If you originally purchased Storage Manager as a MultiServer version, this license was automatically activated during the Storage Manager 4.0 installation process.

Enterprise Setup

If you have multiple Storage Manager installations, you can provide access to the other installations. You can only configure other installations through the *Enterprise Setup* menu option. This feature is also available in File Manager for configuring end users. For information on configuring end users, see page 9-36.

NOTE: In 4.x installations, any user who needs access to File Manager must be logged in to the NDS tree where Storage Manager is installed.

To access other installations

1. From Configuration Manager, open the Configure menu and select *Enterprise Setup*. The Installation Configuration dialog box appears. If you have just installed the program, this dialog box should display only the installation server.
2. Select the **Insert** button. The New Installation dialog box appears.
3. Click the list box arrow in the **Installation Server** list box to display the list of all Storage Manager installations on your network.
4. Highlight an installation you want to add. The dialog box automatically displays the description and installation description of the selected installation.

➤ Your installation's administrators and operators can access another installation that you add to the Enterprise Setup if they are defined as administrators or operators by that installation. If administrators are not logged in to that server, when they select the installation, the program prompts them to enter a login name and password defined on that installation. See page 4-39 for procedures on accessing another installation.

5. Choose **OK** to save the installation change.

At a later time you may need to deny users access to other Storage Manager installations.

To remove an installation

1. Open the Configure menu and select *Enterprise Setup*.
2. Highlight the installation you want to remove.
3. Select the **Delete** button. The Installation Delete dialog box appears. The dialog box automatically displays the job queue and installation path of the selected installation.

WARNING: The **Delete physical queue** option will also remove servicing jobs as well as those waiting in the queue.

4. Choose **OK** to save this change. The installation no longer appears in the Installation Selection dialog box.

To select another installation

1. From any manager, open the File menu and select *Open Installation* (Select *Open Resource* in File Manager). The Installation Selection dialog box appears.
2. Highlight the installation you want to view and choose **OK**.

Installation Configuration dialog box

➤ If you are not logged in to the selected installation server as an administrator or operator, the Login Information dialog box appears. Enter a name and password defined on the selected installation's Admin List. This username must be supervisor-equivalent in order to perform operations.

3. Choose **OK**. The title bar indicates the selected installation.

Chapter 5

Backup, Archive, and Migrate Options

Overview

This chapter describes how to:

- Back up and archive files on selected resources
- Migrate files from resources
- Back up and archive selected directories and files
- Migrate selected files
- Specify custom job parameters
- Configure concurrent backup operations and jobs

Introduction

This chapter addresses the custom data protection and disk grooming operations that you can define independently from automatic operations. Although using automatic operations provides the most complete and secure protection for your data, you may at times want to perform these operations at your discretion.

Resource Manager and File Manager allow you to choose which items to back up, archive, and migrate. For example, to migrate eligible files for an automatic migration job, the volume's capacity must be at or above the high water mark. Eligible files on that resource can be migrated at any time through Resource Manager. Greater control of the operations through custom jobs lets you accelerate the full protection status of files and migrate them when you want.

See Chapter 4, "Customizing Your Installation," for information about backup, archive, and migration parameters.

Backing Up Machines and Resources

Through Resource Manager, you select entire machines or resources for an operation. The program refers to the applicable file rules and parameters to determine whether a file residing on the resource is eligible for the operation. See page 9-18 for information about file rules.

NOTE: If you are prompted with a Session Information dialog box, be sure to enter a supervisor-equivalent user. If you do not, the program cannot make the appropriate connections with servers and your jobs will not run.

- Backup: There are three types of backup operations.
  Full Backup—Copies every file on the tagged resource and clears the archive bits.

Incremental Backup—Copies every file that has changed since the previous full or incremental backup performed on the tagged resource. This type of backup operation clears the archive bit (by default).

Differential Backup—Copies every file that has changed since the previous full backup of the tagged resource and does not clear the archive bit. Note that an incremental backup using managed media will clear the archive bit. Any subsequent differential backup written to managed media will be based on changes that occurred after the incremental operation.

NOTE: If you turn off the **Clear Archive Bits after Backup** option, an incremental backup operation behaves the same as a differential backup for non-managed backup operations.

- **Archive**—Copies every stable file to a permanent portion of the managed media.
- **Migrate**—Removes fully protected files from disk. In addition, eligible files must be dormant for the time period defined by their respective migrate rules. Storage Manager removes only as many files are necessary to restore the disk utilization to the low water mark level. By default, a zero-byte phantom file indicates that the file is on media.

NOTE: When you are backing up DOS workstations, Palindrome recommends disabling any broadcast message functions on those workstations. These messages can interfere with the workstation TSA and interrupt the backup operation.

To back up or archive resources

1. From Resource Manager, tag the resources you want to perform the operation on. You can use the View menu's *Sort* options to quickly tag an entire group of resources. For example, to back up only workstations (such as DOS, OS/2, and Macintosh), select the *Sort by Type* option and tag the Workstation class.

Tagged Resources

✓ ***TIP:*** To tag all associated items of a highlighted object, press the "/" key. For example, if you highlight a server and press the "/" key, all resources on that server are tagged.

2. From the Operations menu, select *Backup* or *Archive*.

➤ If you choose *Backup*, specify which type of backup (**Full, Differential**, or **Incremental**) operation you want performed.

3. Select any other parameters for this job. The most common job parameter, **Prompt With Questions**, indicates that the job is performed in attended mode when selected.

Establishing Communications window

4. Choose **OK** to submit the job to the job queue. The Establishing Communications window appears as the job attempts to contact the job server.

TIP: To update the operation information displayed in the Resource tab, choose *Refresh the Tree* from the Resource Manager Operations menu.

WARNING: For installations using the Single/25-User version of Storage Manager, Storage Manager will eventually stop backing up your Protected Resource List if you upgrade your Novell license to include more users without upgrading to the Single Server (any NetWare user) version of Storage Manager. You have 45 days to implement the upgrade.

Preparing for Server Shutdown

When preparing for a scheduled shutdown of a volume or server, it is a good idea to copy every file on the volume(s) to a single backup media or media set. This will allow you to restore all of the files from that one media set and possibly a single media. Ideally, you should move this media or a duplicate of this media off-site.

Storage Manager provides two methods of performing full backup operations for this task:

- Full backup job to non-managed media. Select all of the protected resources in Resource Manager for full backup operations. This method writes a copy to media that is not requested by the program for rotation.
- Automatic job with parameter changes. This method creates a "snapshot" of all active resources. Verify that all protected resources are included for automatic operations before submitting the job. Make a duplicate of this media to avoid having the program overwrite the session.

Migrating Eligible Files

Migration is the process of deleting files, for which at least one permanent copy exists on secondary media, from a volume resource. At the resource level, Storage Manager selects files for migration (also called *prestaging*) on the based on the following criteria:

- The files must fully protected. The default is three archive copies.
  - If you use a near line set, and additional archive copy is also required for eligibility if an archive copy does not already exist on the most frequently used media set.
- The applicable migration rule has been satisfied. Frequently, this rule is defined a time period during which no one attempts to access the file. The default is 12 weeks.

Storage Manager provides several methods of migration, from the most manual to the most automatic:

- Select specific files or types of files for migration. See page 5-13 for details about determining which files you want to select for migration.
- Select specific resources and the migration option and manually submit the migration job or schedule the migration job on an on-going basis. See page 5-9 for details about this method.
- Enable automatic migration and let Storage Manager automatically submit the migration job whenever disk utilization exceeds the high water mark. See page 2-6 and page 5-10 for details about this method.

To migrate files on the resource(s)

1. Open Resource Manager.
2. Tag the resource(s) on which you want to migrate files. If you want to migrate files on all resources, tagging is not necessary.
3. Open the Operations menu and select the *Migrate* option. The Migrate Options dialog box appears.
4. Select the type of migration operation, you want to perform.
   - **Build Prestage List Only**—Selects the files eligible for migration and sorts this list in the order specified in Configuration Manager. This operation updates the percentage of files eligible for migration that is listed under the Prestage column in the Resource Monitor window.
   - **Perform Migration Only**—Migrates files on the existing prestage list of the selected volume resource. If these files are insufficient to reduce the disk utilization to the low water mark, Storage Manager updates the resource's prestage list and resumes migration. Because the prestage list is updated only if necessary, this option usually results in faster operations than the **Build Prestage List and Migrate** option.
   - **Build Prestage List and Migrate**—Updates the list of files eligible for migration. Afterwards, Storage Manager migrates files until the low water mark is reached.
5. Specify which resource should be included in this job; select either **Only Tagged Resources** or **All Resources**.
6. Specify any other job parameters, for example, those on the Scheduling Options dialog box (see page 5-20 details about these parameters).

TIP: If you prefer to maintain an up-to-date record of the percentage of disk space used by files eligible for migration, schedule a job to "build a prestage list only". This job should follow the Default Automatic job.

An added benefit for those installations using automatic migration is that Storage Manager will require less time, if any, to update this list prior to migration. This is important since a high water mark can initiate automatic migrations at any time.

7. Choose **OK** to submit this job to the job queue.

Customizing Migration

You enable automatic migration and related migration parameters through the Archive/Migrate tab in Configuration Manager. These parameters define migration for all protected volume resources. You can customize the resource monitoring options and migration thresholds that apply to a selected resource through Resource Manager. See page 4-17 for details about configuring migration parameters for your system.

To customize migration parameters

1. In Resource Manager, highlight the resource for which you want to customize migration parameters.
2. Open the Operations menu and select the *Edit Migration Parameters* menu option. The Edit Migration Parameters dialog box appears.
3. To customize Resource Monitoring and Migration threshold parameters, turn off **Use System Migration Parameters**.

   Even if an option may not change from the system settings, you may have to duplicate the selection. To replace customized migration parameters with the system settings, select **Use System Migration Parameters**.

4. You can only enable or disable Resource Monitoring options that are currently enabled as a system setting in Configuration Manager. For example, if **Enable Automatic Recall** option is disabled in the Archive/Migrate tab, you cannot enable this option for specific resource. The options are:

   Monitor Resource Capacity—Indicates whether Resource Monitor scans the disk of this resource. This option must be turned on in order to enable the **Enable Automatic Migration** option.

   Enable Automatic Migration—Indicates whether Storage Manager automatically migrates eligible files when the disk reaches its high water mark. Storage Manager automatically selects the eligible files (also referred to as *building the prestage list*) and migrates as many eligible files as necessary to reduce each disk's utilization level to the low water mark.

   Enable Automatic Recall—Allows Storage Manager to process an end user's recall job. A recall job is a type of restore job that invisibly submits a single-file restore job when a user or application attempts to access a migrated file.

5. Set the migration thresholds. Enter the high and low water marks that correspond to percentage of disk utilization that corresponds to the optimal usage range.

TIP: Storage Manager/Network Archivist upgraders: To migrate all eligible files during migration (the operation performance in prior versions), set the low water mark to **0**. You will get system messages because the active files prevent Storage Manager from reaching this level.

6. Choose **OK** to save your changes.

   When you migrate files on a resource, Storage Manager migrates only as many files as are necessary to reach the low water mark defind for the resource. For example, if all of your Resource Monitoring options are turned off, a manual migration will reduce the resource's disk utilization to the low water mark.

NOTE: The prestage list consists of two files (TMPEDBDT.PAC and TMPEDBNX.PAC) that each grow approximately 3 Mb for every 10,000 files that are prestaged. Verify that you have adequate disk space available before running your first migration job. These files are located on the File History Database directory of each protected resource. For example, PAL\DB\1 corresponds to the location of a specific resource's File History Database (where \PAL is your installation directory and \1 corresponds to a resource).

Backing Up Directories and Files

Because you are selecting individual files and directories, rather than entire resources, the operation options and the behavior is different. The program logic assumes that you wish to override file rules and operation parameters when you are selecting individual directories and files for an operation. However, the Exclude rule parameter also prevents you from performing an operation even through File Manager.

In 4.x installations, any user who needs to submit file-level jobs (in other words, accessing File Manager) must be logged in to the tree where Storage Manager is installed.

To back up or archive specific directories and files

1. Open File Manager.
2. Open the File menu and select the *Open Resource* menu option. The Open Resource dialog box appears.
3. Choose the **Resources** button.
4. Double-click the resource in which the files or directories reside.

TIP: Use the icons on the drive bar as an alternative to selecting the **Open Resource** menu option. It displays the resources that you are mapped or connected to.

5. Open the Tree menu and select the *Change Directory* option to enter the directory/path you want to view.
6. Tag the directory containing the files you want to back up or archive.

➤ If you want to tag only individual files located in the directory, do not tag the directory. Tag these files in the file window.

7. After tagging the necessary directories and files, select the appropriate operation from the Operation menu.
8. Choose **OK** to submit the custom job. The Job Status window appears.

NOTE: Tagging all of the files on a resource in File Manager is not equivalent to tagging that same resource in Resource Manager. To ensure that you are backing up or restoring a resource's File History Database, tag the resource through Resource Manager rather than tagging all files at the resource's root directory in File Manager.

Migrating Specific Files

Through File Manager you can migrate files with at least one archive copy. Storage Manager does not have any resource-level objectives so you migrate as many eligible files as you want. Migration thresholds do not apply to migration jobs created through File Manager.

Migration for Beginners

If you are not familiar with migrating, you may prefer to extend the time period for the migrate rule of "*" files to **After 20 Weeks**. As you become more familiar with how frequently users access certain types of files, you can adjust the time period or create new rules that provide the best balance of minimizing restore jobs and optimizing disk capacity.

To display only those files eligible for migration, see page 9-15.

Before you migrate files for the first time, you may want to check with users before migrating these.

To identify and print files eligible for migration

1. In File Manager, access a volume resource for which you want to migrate files.
2. Highlight the resource's root directory.
3. Open the View menu and select the *Define Filter* menu option.
4. Choose the **Advanced** button. The Filter Parameters dialog box appears.
5. Select the **Eligible for Migration** option. This option refers to number of archive copies required for full protection (and the near line set, if configured) as well as the applicable migration rules.
6. Choose **OK** to save your selection.
7. Tag the root directory; this automatically tags all file eligible for migration on this resource.
8. Open the View menu and select the *Tagged Items Window* menu option. The Tagged Items window appears displaying all eligible files across all subdirectories in one window.
9. Open the File menu and select the *Print To File* menu option. The Save As dialog box appears.
10. Enter a file name and a file path to which Storage Manager should write this file. This file is an ASCII file in a comma delimited format.
11. Import this file into another application such as a database or spreadsheet application. You may want to open this file first to see whether the list should be printed in portrait or landscape mode.

NOTE: You may want to distribute copies of this list to the appropriate users for their approval. Keep a copy for yourself; you will probably refer to it later. In most cases, users will open the file to reacquaint themselves with the contents of the files. Since this alters the Last Access Date, you can no longer replicate the list by filtering on files eligible for migration.

12. Tag or untag files as necessary and select the *Migrate* option from the Operation menu.

To migrate specific files

1. Open File Manager and tag the files you want to migrate. Storage Manager will notify you during or after migration if the file is not eligible for a file-level migration. File-level migrations requires at least one archive copy (migration rules are ignored unless the applicable rule is **Exclude**).

➤ To migrate all eligible files based on their full protection status and the applicable file rules, define a filter for the resource's root directory using the **Eligible for Migration** option. Tag the filtered files for the migration job.

➤ The Extended History window displays the media location and type of session that contains the file version. Highlight the file version in the Default History window. Open the View menu and select *Extended History* to display the Extended History window.

2. Tag the files and/or directories you want migrated from the disk.

3. Select the *Migrate* option from the Operation menu. A Migrate Options dialog box appears.

4. Select any other job parameters for this job.

5. Choose **OK** to submit the migration job to the job queue.

➤ If any files on the resource are not eligible, based on their respective migrate rules, the program notes these in the System Messages window.

Extended History window

Custom Job Options

Unlike automatic jobs, custom jobs allow greater flexibility in determining the type of media and device used for an individual job. Some of the options are not available for all operations.

- Whether to prompt you with questions during the job
- Which media to use
- Which device to use
- When to submit the job

Media Options

Custom jobs allow you to specify media for the backup or archive operation. For archive operations, you can specify any managed media set. For backup operations, you can also specify an existing non-managed media set or create new non-managed media set.

WARNING: When creating new media labels, be sure to specify unique labels that do not duplicate media labels of media that are active or retired. Many operations are based on the media label. Duplicate labels can lead to inconsistencies on the media and in the database.

Storage Manager writes or appends sessions only to blank media or media formatted by the current installation.

Which media library should you use? It depends on how you intend to use the session.

- Specify non-managed media for your custom backup if you are sending media off site and do not need the media returned.
- Specify a managed media set if you are scheduling a custom job to supplement your automatic jobs.

Media Options dialog box

✓ ***NOTE:*** Be aware that writing custom archive jobs, which can only be written to managed media, may trap backup sessions. If your managed media sets have archive-only and backup-only media, Storage Manager automatically selects the appropriate media.

Managed Media

To specify managed media

1. Tag the items you want to perform the operation on.
2. Select the operation.
3. From the operation dialog box, select the operation type, if necessary, and then the **Media** button.
4. Select the **Managed** option. This option is the default.
5. Choose the media.

➤ To use the best eligible media for the operation, select **Current Set**.

➤ To specify which managed media, select **User Selected** and highlight that media.

6. Determine whether or not you want the program to prompt you with questions when it processes the job (by default, **Prompt With Questions** option is turned on).
7. Choose **OK** to submit the custom backup job.

Non-Managed Media

Using non-managed media allows you to:

- Dedicate the entire capacity of the media to a single session. Because the media is never requested for rotation, you can preserve backup sessions for as long as you want.

- Exclude sessions from being recorded in the File History Database. Since Storage Manager will never call the untracked media for rotation or restore operations, you can send the media permanently off site. By comparison, the program tracks all sessions written to managed media.

To specify non-managed media

1. Tag the items you want to perform the operation on.
2. Open the Operations menu and select *Backup*.
3. From the Backup Options dialog box, select type of backup operation, and then the **Media** button.
4. Select the **Non-managed Media** radio button.
5. Choose the media.

➤ To use new media, choose the **Label New Media** option. Type the label of this new media.

➤ To select one of the existing non-managed media, choose **Existing Media**. Select the non-managed media you want to use from the list. Be sure to load the media that you specified for the backup job, otherwise the job will fail.

➤ To track session information in the File History Database, select **Track in database**.

If you turn off the **Track in database** option, you will not be able to restore data on the untracked sessions through Resource or File Manager. You can only restore data on these sessions in Media Manager following a journal operation.

By tracking a session, you incorporate the file version in the File History Databases. Reasons for not tracking sessions are:

- You are sending the media off-site.

- You are concerned about the size of your File History Databases. Scheduled jobs that periodically write to non-managed media will create new file records for every file on disk.

6. If you are using existing media, indicate whether you want to overwrite data.

➤ If you do not want sessions on the specified media to be overwritten, use **Append to existing media**. If you do not select **Append to existing media**, Storage Manager will overwrite any existing sessions.

7. Select any other parameters for this job.

8. Choose **OK** to submit that custom backup job.

NOTE: You can only append sessions to non-managed media from the current installation.

Schedule Options

Storage Manager provides advanced scheduling features that allow you to schedule automatic and custom jobs to run once or many times from hourly to yearly intervals. Also, you can link a job to run after another scheduled job.

You may want to schedule jobs to run once a week (for example, to back up a certain volume at the end of every week) or every quarter (to get a quarterly snapshot of your entire system, for example).

The scheduling feature is available for all custom jobs, except journal operations. You can edit a job's schedule only through the Job Queue window.

To schedule a job

1. Tag the items you want to perform the operation on.

2. Select the operation.

3. From the operation's dialog box, select the operation type, if necessary, and then the **Schedule** button.

4. Select the **Schedule** button. The Scheduling Options dialog box appears.

Scheduling Options dialog box

5. Type the name of the job in the **Description** field. For example, you might describe a job as "**Monthly Backup**".

6. Specify when Storage Manager processes the job.

➤ To schedule a job to be processed once, select **Once**. After Storage Manager processes the job, it deletes the job's specifications. Enter the time and date to process the job.

➤ To schedule an on-going job, select **Periodically**. Enter the time and date for the job to begin. In the **Repeat Every** field, specify the interval or time period that passes between each repetition of the job. Specify any days on which you do not want the operation repeated.

For example, you want to run a job every 24 hours except on Saturdays and Sundays. Select the **Saturday** and **Sunday** buttons from the **Do not run on these days** parameter.

➤ To schedule a job to follow another scheduled job, select **Start Job After**. From the **Start Job After** list box, select the job to precede the current job. The Scheduling Options dialog box displays the schedule of the preceding job so that you know approximately when the current job will be processed. Specify any days on which you do not want the operation repeated in the **Do not run on these days** parameter.

7. Choose **OK** to confirm your selections. The operation dialog box appears.

8. Choose **OK** to save the parameters for the scheduled job.

To view or edit a job's schedule

1. From Control Console, select the **Job Queue**. The Job Queue window appears.

2. Highlight the scheduled job you want to re-schedule. The status of the job must be "ready." If the job has been assigned a job ID, you cannot edit the schedule.

3. Select the **View** button. The Scheduling Options dialog box appears with the same parameters described in the procedures for scheduling a custom job.

4. Select the new parameters to re-schedule the job.

5. Choose **OK** to save the new parameters.

To clear the schedule parameters

➤ If you no longer want the schedule a job, choose the **Default** button to clear any parameters you have set. This resets the **Time** and **Date** parameters to the present and the job will be performed once.

Device Options

You can choose a device used by the program for the custom job. Selecting a specific device prevents the program from performing concurrent backup operations. If you have received system messages concerning your hardware, you may want to record the SCSI instructions transmitted to the device during the operation.

To specify a device

1. After selecting your operation, define any other parameters for this job. Due to the quantity of instructions generated by the **Device Trace** option, select only **one** volume for each job that records device instructions.
2. Choose the **Devices** button. The Device Options dialog box appears. You may choose one or both options.

Device Options dialog box

- ➤ To use a specific device, select the **User Selected** option. Select a device from the list. If you have selected a specific media that is not on the selected device, this job will fail or prompt
- ➤ To record all SCSI instructions which occurred during the course of the job, select **Device Trace**.

3. Select any other parameters for this job.

4. Choose **OK** to submit the custom job.

NOTE: You cannot specify a specific device for automatic jobs. However, you can indirectly specify a device by restricting other devices from performing an operation before the job server submits the job to the queue.

Concurrency in Storage Manager

Concurrency refers to Storage Manager's ability to simultaneously use multiple devices to perform:

- Multiple backup operations within a single job
- Backup jobs and restore and/or utility jobs

To take advantage of concurrency, your installation must have at least two devices configured.

If you are going to use concurrent operations, be sure:

➤ You have eligible media loaded in each device.

➤ You have at least 2 MB RAM available on your server for each concurrent process (for example, if you have two backup devices you need at least 4 MB of RAM).

To configure concurrent backup operations

1. In Configuration Manager, open the Configure menu and select *System Configuration.*
2. Select the Systems/Advanced tab.
3. Specify a number for the **Maximum Concurrent Backup Operations** parameter that is equal to the number of backup devices configured for backup operations.
4. Open the File menu and select *Save* to save your changes.

When you submit a backup job, Storage Manager begins simultaneously processing the number of volumes equal to your **Maximum Concurrent Backup Operations** parameter. Remaining volumes wait until a backup process becomes available.

During an automatic job, the program must perform more than one operation. The program must process all of the resources for the first operation before it can begin process the next operation. For example, the program cannot begin processing the backup operations, even if devices are available, until it has completed archiving all of the resources.

Optimizing Concurrent Backup Operations

If you are using concurrent operations, you may want to reposition your items in the Protected Resources List so that the program processes resources optimally. Move larger resources to the top of the list so that these resources complete at approximately the same time.

Also, you should separate workstation drives in the Protected Resource List. For example, if the last two resources are a C: and D: drive for the same workstation, the program cannot process these concurrently. See page 8-11 for information about re-arranging resources.

To configure concurrent jobs

1. In Configuration Manager, open the Configure menu and select *System Configuration.*
2. Select the Systems/Advanced tab.
3. Set **Maximum Concurrent Jobs** to **2** or greater. To be able process backup, migrate, utility, and restore jobs simultaneously, set the parameter to **4** or greater.

   Enabling concurrent jobs allows your installation to process one job for each type of engine that is loaded. If there are only three backup jobs in the job queue, the program can only process the first backup job submitted to the queue. If a restore job is submitted to the queue, the program processes the restore job concurrently with the backup job.

Usually, installations that run concurrent jobs also run backup operations concurrently. If the backup job is performed on multiple resources, there may not be any available devices for performing the other job(s). Similarly, if the program is already processing restore and utility jobs, the backup job cannot run concurrently until at least one other device and the appropriate media are available.

Chapter 6

Restoring Data

Overview

This chapter describes how to:

- Restore selected files and directories
- Restore sessions from media
- Restore an entire resource
- Restore an older version of a database
- Restore data to another location
- Restore a server
- Recover the installation volume
- Clone a server

Introduction

Recovering data with Storage Manager is easy because of its File History and System Control Databases. Using the databases, the program automatically prompts you for the backup media that will result in the most efficient restore process.

You can restore an entire volume, including the directory structure, data, and history database of a selected resource in Resource Manager, and selected directories and files on a resource in File Manager. Additionally, you can search for files on mounted media and restore them to disk using Media Manager.

Monitoring Restore Jobs

Restore Job Status window

If you view the progress of a restore job through the Restore Job Status window, you will be able to see how many of the items remain to be restored.

The window displays information about the number of items specified for the restore operation (**Scheduled Items** parameter) and the number files that have yet to be restored (**Remaining Items** parameter)

Redirecting a Resource's Data

In some recovery situations, a volume may be off-line, requiring you to redirect data from that volume to an on-line volume.

The **Redirect to** option in the Restore Options dialog box allows you to redirect data (or an entire volume) to another volume.

To redirect data from one volume to another, select Restore/*Data* and choose **Redirect to**. All data (including directories) is redirected from the current volume to the target volume you choose. Use this procedure when a volume is going to be down temporarily, but you want access to the data on that volume.

To redirect an entire volume, including the volume's File History Database, to another volume, select Restore/*Full Resource* and choose **Redirect to**. When redirecting a full volume, you are basically "cloning" the source volume.

Generally, you would only use this procedure if you were replacing one volume with another volume and removing the original volume from the Protected Resource List.

NOTE: If you plan on a full or partial restore of a volume to a **different server** (for example, from NetWare 3.11 or 3.12), you must recreate directory and file trustees for users not on the target server.

Restoring Directories and Files

This section details procedures for restoring the most current version of files to their original or new location. If you want to restore an older version, proceed to "*Restoring an Older Version of a File*" section beginning on page 6-10.

To automatically restore a file to its original location, see also Appendix E, "Recalling Files."

NOTE: If you want to restore directories and files from one server to another, you must first create the trustees and Object IDs on the target server for users that are not already defined there.

To restore directories or files

1. In File Manager, select the volume containing the files you want to restore.

TIP: If you are unsure where the file is located, you can use the View menu's *Define File Filter* option or the Operations menu's *File Finder* option to locate the file.

2. Tag the directories and files you want to restore.
3. Open the Operations menu and select *Restore*.
4. Select the type of restore you want to perform. The Restore Options dialog box appears.

Restore Options dialog box

- To restore the tagged file(s) to their original location, select *Restore/Original*.
- To restore only the tagged file(s) to a different location, select *Restore/Redirected*. The SMS Target dialog box appears. Choose the **Resources** button to select the server, TSA, target service, and resource associated with the new location. Choose the **Path** button to specify the target directory path and its name space.
  —To also redirect the directories of the files, turn on the **Retain Directory Structure** option.

5. Sometimes the files scheduled for a restore operation already exist on the disk. Set the **Overwrite** parameter to specify when the program should overwrite the disk copy with the media copy.

- To overwrite the disk file with the media version, select **Always**.
- To preserve the file on disk, select **Never.**
- To overwrite the disk copy only if it is older than the copy on media, select **Older**.

➤ To receive a prompt when the program finds a file already on disk, select **Prompt**. If you submit a restore job in unattended mode with this parameter set to **Prompt**, the program will not restore any file that already exists on disk. Storage Manager records a message in the System Message database.

6. Select any other job parameters.

7. Choose **OK** to submit the restore job to the job queue.

8. You may have to load media. If Storage Manager cannot find any media or it needs additional media to complete the restore operation, it will prompt you for media. This provides the most automated restore behavior.

9. If Backup Director finds that no eligible media are mounted, a System Message dialog box appears. This dialog box provides a choice of options.

System Message dialog box

10. Select the **Display list of suggested media** option (choose **Defer** if you want to deal with the restore job at a later time). The Media Pick List dialog box appears.

Media Pick List dialog box

Parameter	Description
Media	Displays the media label.
Status	Displays the media that Storage Manager determines is best for the operation (resource-level restore operations only). Preferred media is the media with the greatest number of unique files scheduled for the restore operation. There can be multiple preferred media. Eligible media are all other media that have at least one of the scheduled files.
Files	Number of the scheduled files that are on a specific media (file-level restore operations only).
Unique	Number of scheduled files which exist only on one media (file-level restore operations only).
Type	The type of media (optical disk, 8 mm tape, etc.) the data is located on.
Location	The device or slot the media is located in (if any).

11. Load the media. Highlight the media and choose **OK**. If you turned on a device after the Media Pick List dialog box appeared, select the **Scan** button to refresh the list of media and devices.

➤ If you are using an autoloader with an import/export door, you may need to choose the **Import** button to load the media in the door. When you close the door, the device loads the media into the first available slot. Choose **Scan** to refresh the choices on the Media Pick List. Highlight the media and choose **OK**. When the program has restored all of the files from a media, the media no longer appears in the Media Pick List.

As media are used, subsequent pop-up windows indicate the correct number of files that still need to be restored.

In addition, the program automatically deletes a media from the list if it contains only those files which have already been restored from a previous media. As a result, the Media Pick List shows only those media containing files which have not yet been restored.

12. Continue to insert media until all of the files have been restored.

Restoring an Older Version of a File

Restoring an older version of a file is a common request in most LAN environments. Storage Manager's use of the File History Database allows administrators, operators, and end users to restore an older version of a file from that file's history quickly and easily. The database maintains the history of every object that exists in the File History Database.

In order to restore an older version of a file, you must tag the desired version of the file in the history window.

✓ ***TIP:*** To quickly restore a single file version, you can select the file version from the Extended History window and choose the **Restore** button. The program restores the file to the original location.

To restore older versions

1. Highlight the file that you want to restore. The history window displays any available file versions for that file.
2. Tag the file version you want to restore. You cannot restore multiple file versions of the same file to the same location because each subsequent version will overwrite the previous one.
3. Open the Operations menu and select *Restore*. The Restore Options dialog box appears.
4. Select the location where you want to restore the file.
5. Specify the **Overwrite** parameter you want Storage Manager to apply if it finds any files already on disk.
6. Specify any other job parameters.
7. Choose **OK** to submit the restore job to the job queue.

8. Insert the media requested by Storage Manager until all of the files have been restored.

Restoring Files in Media Manager

Restoring from Mounted Media

If a file copy is not tracked in the File History Database, you must use Media Manager to select the file copy directly from mounted media and perform the restore operation. Some reasons why file versions are not recorded in the File History Database:

- The user did not choose to track this session in the File History Database when creating the job.
- The file was written to a non-managed media by a pre-4.0 Palindrome product and could not be tracked in the File History Database.
- The media has been forgotten.
- The file was written by another SMS-compliant application and therefore, Storage Manager has no knowledge of these files.

  In each of these cases, the only way to restore (or copy) a file from media to disk is to display the contents of the media (also called "journaling"). Then, search for the sessions containing the files you want.

To restore a file using the session journal

1. Mount the media in the device.
2. From Media Manager, open the View menu and select *Mounted Media*. The Mounted Media window appears.
3. Highlight the mounted media you want to journal.

Mounted Media window

4. Choose the **Journal** button. Do not close the job window or Media manager while the journal job is running; you will abort the job. The Session List window appears.

5. Select the appropriate button depending on the kind of restore job you want to create.

➤ To restore an entire session, highlight a session and choose the **Restore** button. The Restore Options dialog box appears.

➤ To restore selected directories or files, highlight a session and choose the **View** button. The media session window appears. The file window lists files located under the highlighted directory.

6. If you choose the **View** button, the program begins building the directory and file windows. This can take some time, depending on the size and complexity of the directory structure. The program allows you to pause from building after it completes a directory. You can view the file window or perform an activity elsewhere while the program is building the directory structure.

➤ To interrupt the building process, choose the **Pause** button after the program builds the directory you want to see. Choose the **Resume** button to let the program resume building directories.

In this window, the volume appears at the top of the tree, followed by a list of directories. The file information includes the date and time stamp, attributes, and byte size of each file.

You can collapse and expand directories. When you highlight a directory, the files residing on the directory appear in the file window on the right.

7. Tag the directories or files you want to restore.
8. Open the Operations menu and select *Restore*.
9. Select the type of restore operation. The Restore Options dialog box appears.
10. Specify the location where you want to restore the file(s).
11. Specify the type of **Overwrite** parameter.
12. Select any other job parameters.
13. Choose **OK** to submit the restore job to the job queue.
14. You can continue to journal the session and tag items for additional restore operations. Periodically, the program prompts you to indicate whether you are finished journaling the media. Choose **Yes** to end journaling and exit the mounted media's session window. The program will not attempt to process the restore jobs until you have completed journaling.

Restoring Tracked Files in Media Manager

Occasionally you may want to identify the files copies that reside on a particular tracked session. Media Manager provides a database session window which provides the same restore features as File Manager's directory and file windows.

While the database sessions appear similar, they are created in very different ways. If you know which tracked directories and files you want to restore, you can restore them more quickly through File Manager. If you want to view the files and directories located on a particular session, it is quicker to view the contents of the session through the Mounted Media window than through the database session window. If the media is not available and the session is tracked, you can still restore from the database session window.

To restore tracked file copies in Media Manager

1. From Media Manager, highlight a session.
2. Open the View menu and select *Session Window*. The program begins building the session window.
3. Tag the directories and files you want to restore.

➤ If you must search for specific files, open the Operations menu and select *File Finder*.

4. Open the Operations menu and select *Restore*.
5. Select the type of restore operation. The Restore Options dialog box appears.
6. Specify the location where you want to restore the file(s).
7. Specify the type of **Overwrite** parameter.
8. Specify any other job parameters.
9. Choose **OK** to submit the restore job to the job queue.

10. Choose **Yes** to end journaling and exit the mounted media's session window. The program will not attempt to process the restore jobs until you have completed journaling.

Data from non-SMS versions

To restore a File History Database from non-SMS media, you must restore the appropriate *.PAC files through the Session List window. When restoring data from media written with non-SMS versions of Storage Manager, all file data and attributes, and directories and their attributes are restored. CRCs (Cyclical Redundancy Codes) are also valid.

The following objects cannot be restored, however: trustees, volume restrictions, directory restrictions, owners, Bindery files, System Control Databases, and File History Databases.

Restoring Machines and/or Resources

To restore a machine and/or resource

1. From Resource Manager, tag the machine or resource you want to restore.
2. Open the Operations menu, and select *Restore*. The Restore menu appears.
3. Select *Full Resource*. For more information on this option, see the "*Restore Options*" section below.
4. Specify the location where you want to restore the resource.
5. Select any other job parameters.
6. Choose **OK** to submit the restore job to the job queue.
7. Load the media as requested to restore all directory, file, and trustee information that existed on the volume the last time you backed up.

   A complete volume recovery may take some time depending on the amount of data to be restored. See page 6-20 for information about restoring a volume's data to another volume.

Restoring an Older Version of a Database

If you need to restore a version that is older than the most current version on media, you must select the version from the physical journal rather than through the database.

To restore an older version of the File History Database

1. Load the media you want to journal.

2. From Media Manager, open the View menu and select *Mounted Media*. The Mounted Media window appears.
3. Highlight the media you want to journal.
4. Choose the **Journal** button. Do not close the job window or Media manager while the journal job is running; you will abort the job. The Session List window appears. This window displays the date, size, and number of files contained on each session.
5. Highlight the File History Database session you want to restore. File History Database sessions are labeled “DH”.
6. Choose the **Restore** button. The Restore Options dialog box appears.
7. Specify the restore parameters.
8. Choose **OK**.
9. Choose **Yes** to end journaling and exit the mounted media’s session window. The program will not attempt to process the restore jobs until you have completed journaling.

Restore Options

This section details the options available through Resource Manager for restoring entire resources or resource information. The *Restore* operation has four available options:

Full Resource(s)

The *Full Resource(s)* option recovers all of the information for the tagged resource(s), including the File History Database(s), directories, trustees, volume/disk and directory restrictions, and files. Selecting this operation overwrites any existing information.

Typical use: This operation should be used if a complete server or volume was lost since it will restore all of the information for a selected volume.

File History Database(s)

The *File History Database(s)* option restores a resource's File History Database from media, overwriting the existing database.

The program restores the most recent copy of the database on media to its configured location.

Typical use: Use this operation if a volume's File History Database has been deleted or damaged and, therefore, must be restored from media (for example, the File History Database files are corrupt).

Directory Structure(s)

The *Directory Structure(s)* option allows you to recover the directory tree for the selected volume(s). NetWare trustee rights and volume/disk and directory restrictions on NetWare server volumes are also recovered. This option also restores empty directories. Depending on the version of directory structure you are restoring, this type of restore operation overwrites trustees for existing users and may recreate user trustees that were not currently configured prior to the restore. This operation does not restore user data.

Typical use: This operation can be a used to duplicate a directory structure on a new volume. After you restore the directory structure, you typically use the Restore/*Data* option to restore files. This operation can also be used to restore the most recent version of trustee rights from media and is the only option available to restore empty directories.

Data

The *Data* option recovers all user data for the selected volume(s), the directory structure, and associated trustee rights. This option does not restore empty directories.

This does not include the NetWare Bindery files on SYS: volumes. Selecting this operation overwrites existing files only if the file on media has a newer time stamp (i.e., if the disk file is older than the file on media). NetWare Bindery files and NetWare Directory Services can only be recovered by tagging the Bindery resource and then selecting *Full Resource(s)*.

Typical use: This option should be preceded by the *Directory Structure(s)* operation (unless the volume's directory structure already exists).

Redirecting Volume Data

The following provides instructions for redirecting data from one volume to another volume on the Protected Resource List. This procedure is especially useful if a volume is down and you want immediate access to its data.

Assumptions

- The volume you are redirecting data to is on the Protected Resource List
- Your installation directory is not on a failed volume.

To redirect a volume to a new or existing volume

1. If the volume you are redirecting to is not one that is currently protected, add the resource using Resource Manager.
2. In Resource Manager, highlight your original source volume (the volume you want to redirect data from) and tag it.
3. Select Operations/*Restore*.

- Select *Data* to redirect data without moving the source volume's File History Database.
- Select *Full Resource* if you want to clone the volume (redirect data and the source volume's File History Database to the target volume). The File History Database is copied to the target volume's File History Database location.

4. On the restore options dialog box, select **Redirect to**.
5. Choose the Server, TSA, Target Service, and Resource to redirect data to and choose **OK**.

   If the server does not appear in the window, be sure you have loaded the correct TSA for that server.

   All information (including all directory, file, and trustee information) is restored from your original volume to the target volume you have selected.

   If you selected *Full Resource* as your restore option, the File History Database from your original volume now belongs to the target volume.

Recovering an Installation Volume

Storage Manager relies on its databases, the Windows executables, and the engine NLM files to run properly. If any of these components is missing, you will have to perform some type of recovery operation either at the Windows workstation or at the server.

Recovering Databases and Executables

If a volume fails that contains the System Control Database (and/or the executables), you can restore that volume using the Server Control Console on the installation server or from a workstation (using SETUP.EXE on the installation diskettes).

Assumptions

- The failed volume is not a SYS: volume
- Your Storage Manager NLMs are available.

NOTE: If you need to recover a SYS: volume and/or Storage Manager NLMs, proceed to "*Recovering a SYS: Volumes and NLMs*" below.

To recover an installation volume using the server console

1. Insert the most recently used media in your backup device (the System Control Database is written to the media with every backup operation).
2. At the server console of your installation server, type:

   LOAD PAL

   The following screen appears.

3. At the Server Control Console, select *Recover System Control Database.*
4. Select the server volume and path of your System Control Database (AS*.PAC) files.
5. Type in your auto login user name and password in the appropriate fields. This must be a valid user.

If the Bindery or NDS doesn't exist on your installation server at this point, type SUPERVISOR in the auto login name field for NetWare 3.x servers; type **ADMIN** in the auto login name field for NetWare 4.x servers.

6. Select **Start Recovery**.

   When the System Control Database is found on media, you are notified of the date of the System Control Database on media. Be sure the date indicated represents the last backup operation performed; if it does not insert the media with the latest backup session and retry the operation.

   Once the System Control Database has been restored from media, the program will have access to the Protected Resource List so you can begin restore operations.

NOTE: If you typed in a name different than your auto login user, the program asks if you want to use the name you typed in or the original auto login user to continue the recovery. If you need to restore NDS or the Bindery, use the current name (for example, ADMIN or SUPERVISOR). If not, use the original auto login user name.

After the bindery (or NDS) is restored, update the System Control Database with the original auto login user name using the *Update Auto Login Information* option on the Palindrome Server Console.

7. After the System Control Database is restored, at the Server Control Console, select *Backup or Restore Resources*.

8. Tag the installation volume and select *Restore*.

   If you need to restore NDS or the Bindery, restore the SYS: volume first. When the SYS: volume is restored, restore the NDS or Bindery resource. After the Bindery or NDS is restored, restore the installation volume.

9. Insert the requested media as prompted. This will restore to the new volume all directory, file, and trustee information that existed on the failed volume at the last backup.

To recover an installation volume using the workstation

1. Insert Storage Manager installation diskette #1 into your disk drive.
2. At a Windows workstation, access Windows.
3. Open the File menu and select *Run*. Type:

   A:SETUP
   (where A: is the drive your diskette is in)

4. Specify your current installation directories for the Windows executables and the database files. Be sure to specify the same directory as you originally installed them. Choose **OK**. Files are copied to the directory(s) that you specified.
5. After the files are copied, you are asked if you are performing an installation (including an upgrade) or a recovery. Select **Recovery**.
6. If the System Control Database needs to be recovered, Storage Manager will prompt you to configure a device to use for the recovery.

   After the device is configured, Storage Manager automatically submits a job to restore the System Control Database and launches Control Console.

   If for some reason, the job is not submitted to the job queue, load **PAL** at the server console and select *Recover System Control Database.* Specify the path of the installation directory and the auto login user name and select *Start Recovery*.
7. Monitor the job using Control Console at the workstation and respond to prompts.
8. After the System Control Database is restored, open Resource Manager. Tag the installation volume. Open the Operations menu and select *Restore/Full Resource*.

9. Insert the requested media as prompted. This will restore to the new volume all directory, file, and trustee information that existed on the failed volume at the last backup.

Recovering a SYS: Volume and NLMs

The procedure below outlines steps to recover a SYS: volume and Storage Manager NLMs. NLMs must be recovered using the installation diskettes.

Storage Manager requires the following NLMs and resource files to perform restore operations at the server:

PALREST.NLM	PALLIB.NLM
PALMEDIA.NLM	PALJSRVR.NLM
PAL.NLM	ARNADAT.RSF
PALALDRV.NLM	ARNANDX.RSF
PALSDRV.NLM	

These files are copied during installation to the SYS:\SYSTEM directory.

Depending on the type of recovery you need to perform, you may not need to perform all of the steps listed below.

To recover a SYS: volume and Storage Manager NLMs

1. Reinstall NetWare and mount the volume. If recovering a 4.x server volume, be sure to add the server into the NDS tree into the same container where it previously resided. Also, prior to adding a server back into the tree, delete all of the server volume objects from the tree.
2. Be sure to load the proper device driver for your backup device if it is not already loaded.
3. To ensure you have the most recent NetWare modules, run SETUP.NLM on the server (SETUP.NLM is found on the Storage Manager server preparation diskette #1). See the *Installation Guide* for more information on running SETUP.NLM.
4. If you ran SETUP.NLM, PALLOADR.NLM was copied to the SYS:\SYSTEM directory on your server.

At the server console prompt, type:

LOAD PALLOADR

5. At a workstation, insert the Storage Manager installation diskette #1 into a workstation drive.

6. Access Windows.

7. Open the File menu and select *Run*. Type:

   A:SETUP
   (where A: is the drive your diskette is in)

8. Specify your current installation directories for the Windows executables and the database files. Be sure to specify the same directory as you originally installed them. Choose **OK**. Files are copied to the directory(s) that you specified.

9. After the files are copied, you are asked if you are performing an installation (including an upgrade) or a recovery.

➤ If your System Control Database exists (i.e., it is not on the SYS: volume you are recovering) select **Abort** and continue to the section "*Load NLMs*" below.

➤ If you need to recover the System Control Database, Select **Recovery**.

10. If the System Control Database needs to be recovered, Storage Manager will prompt you to configure a device to use for the recovery.

    After the device is configured, Storage Manager automatically submits a job to restore the System Control Database and launches Control Console.

    If for some reason, the job is not submitted to the job queue, load **PAL** at the server console and select *Recover System Control Database.* Specify the path of the installation directory and the auto login user name and select *Start Recovery*.

11. Monitor the job using Control Console at the workstation and respond to prompts.

12. After the System Control Database is restored, at the workstation, open Resource Manager.

13. Tag the SYS: volume. Open the Operations menu and select *Restore/Full Resource*. The SYS: volume will be restored to its most recent state.

NOTE: On 3.x servers, restore the Bindery resource prior to recovering the SYS: volume.

On 4.x servers, you do not need to restore NDS unless your installation server is the only server in your NDS tree.

Load NLMs

If you didn't need to recover the System Control Database when recovering the SYS: volume, perform the following. The job server (PALJSRVR) and PALMEDIA must be loaded on your installation server if they are not already loaded.

1. To load the job server, at the server console prompt, type:

   LOAD PALJSRVR /I<*installation path*>

   where <*installation path*> is the volume and directory of your installation directory (for example, VOL1:\PAL).

2. After the job server is loaded, at the server console prompt, type:

   LOAD PALMEDIA

3. At a workstation, open Resource Manager. Tag the SYS: volume in Resource Manager. Open the Operations menu and select *Restore/Full Resource*. The SYS: volume will be restored to its most recent state.

Restoring a Server

The following provides steps for replacing a server that has crashed.

NOTE: To prepare for disaster recovery such as a complete server crash, follow the instructions in Appendix C, "Disaster Recovery."

If the server you are recovering contains the Storage Manager installation volume, see the instructions for recovering an installation volume beginning on page 6-22 before beginning your server restore.

Assumptions

- Your new server has the same name, NetWare version, and volume names as the original server.
- You are replacing your original server on the Protected Resource List.
- The File History Databases for your original server are accessible.

1. Remove the original server from your network by downing it.
2. Generate a replacement server by installing the same version of NetWare as your original server and giving it the same name. Add volumes with the same name as the volumes on your original server. Bring the server on-line and install the appropriate TSAs (see the *Installation Guide*).
3. Recreate your auto login user assigning the user the same name and password as on your original installation server.
4. In Resource Manager, tag the volumes on your failed server.

TIP: In Resource Manager, to tag all of resources on the same target, highlight one of the resources from that machine and press the "/" key to tag all of the resources for that machine.

5. Open the Operations menu and select *Restore/Full Resource*.
6. Insert the media as requested. This will restore the data on all tagged volumes on your original server to the new server.

Moving a Storage Manager Installation

This section details procedures for moving a Storage Manager installation from one server/volume to another.

Assumptions

- The Storage Manager installation directory name has been created on the target server and is identical to the directory name on the source server.
- The auto login user exists on the target server with the same password and appropriate rights as the auto login user on the source server.
- The target server/volume supports the same name spaces as the source server/volume.

Procedures

Reconfigure the Installation

Before copying the installation files, you need to update the System Control Database and Enterprise Setup so it will represent the new installation.

✓ ***TIP:*** To save your original database files prior to updating them, copy or rename the *.PAC files in your installation directory.

1. Open Configuration Manager.
2. Open Configure/*Enterprise Setup*. Delete the current installation and the job queue (select **Delete Physical Queue**).

3. If appropriate, type in a installation description name in the installation name field.

Installing On a New Server

If you are not moving your Storage Manager installation to a new server, proceed to "*Copy Software*" below. If you are moving your Storage Manager installation to a new server, follow the steps below.

1. Open Configuration Manager. If using a new auto login user, add the user in the auto login name and password fields. If moving from a 3.x server to a 4.x server, use the NDS auto login name and password fields.
2. In the Admin list tab, remove any obsolete administrators/operators..
3. Add any new administrators/operators from the new installation server.
4. In the User list tab, remove any obsolete users and groups.

To install hardware on a new server

1. Install the SCSI Host Adapter and backup device on your target server.
2. Load the appropriate SCSI drivers on your server.
3. Copy SCSISCAN.NLM from the \TOOLS directory on the last Storage Manager installation diskette to the SYS:\SYSTEM directory on your target server.
4. After the hardware is set up and the proper drivers loaded, type the following command at the server console:

   LOAD SCSISCAN

   SCSISCAN scans the SCSI bus and displays all SCSI devices. If the backup device is not displayed, this indicates that there is a hardware issue that needs to be resolved. See the *Installation Guide* for more details on installing the backup device and SCSI host adapter.

Copying Software

1. Create the Storage Manager directory on the target volume using the DOS MKDIR command.

2. Copy the Storage Manager installation and its subdirectories from the source server/volume to the target machine/volume using a command similar to the following:

   XCOPY FS1\VOL1:\PAL*.* FS2\VOL1:\PAL /S

   (where FS1 is your source server, FS2 is your target server, and PAL is your installation directory. The /S parameter copies all subdirectories.)

NOTE: You must keep the same path for your System Control Database. For example, if your original installation directory was \PAL you must move it to a \PAL directory.

3. Copy all Storage Manager NLMs and appropriate TSAs to the target server's SYS:\SYSTEM directory. If you are not moving your Storage Manager installation to a different server, you probably do not have to perform this step (by default the NLMs are copied to the SYS:\SYSTEM directory).

   From the source server's SYS:\SYSTEM directory, copy the following files to the target server:

AR*.RSF	TSAxxx.NLM[+]
PAL*.NLM	SMDR.NLM
PALSTART.NCF	WSMAN.NLM

   [+]substitute the appropriate TSA for your server.

Unload NLMs

If you moved your Storage Manager installation to a new server, skip to "*Preparing the New Server*" below.

If you moved your Storage Manager installation to a different volume on the same server you must:

- Unload the job server (PALJSRVR.NLM) and PALMEDIA.NLM
- Delete the job queue
- Reload the job server and specify the proper path.

To unload PALJSRVR and PALMEDIA

➤ At the server console prompt, type:

UNLOAD PALJSRVR
UNLOAD PALMEDIA

If you haven't already, delete the job queue on the installation server.

➤ Open Configuration Manager and select Configure/*Enterprise Setup*.

➤ Delete the current installation and the job queue (select **Delete Physical Queue**).

To reload the job server and PALMEDIA

1. At the server console prompt, type:

   LOAD PALJSRVR /I<*installation path*>
   where <installation path> is the volume and directory that you copied your installation directory to (for example, VOL1:\PAL).

2. At the server console prompt, type:

   LOAD PALMEDIA

   Continue to *Installation Configuration* below.

Preparing the New Server

1. If you have configured a new auto login user for the new installation, create the user on the server or in the NDS tree.

2. Load the appropriate TSA's on the target server. Refer to the *Installation Guide* if you are unsure of which TSA's need to be loaded.

3. At the server console prompt of your target server, type:

   LOAD PALJSRVR /I<*installation path*>

   where <*installation path*> is the volume and directory that you copied your installation directory to (for example, VOL1:\PAL).

4. At the server console prompt, type:

   LOAD PALMEDIA

Installation Configuration

Be sure to login as an administrator prior to running Storage Manager.

To configure the installation

After successfully loading the job server and PALMEDIA:

1. Change the properties of your Storage Manager icon so that the command line specifies the new installation location. If end users use File Manager, be sure to inform them of the new location of PALFILER.EXE.

2. Open Configuration manager. Open Configure/*Enterprise Setup*.

3. Choose **Insert**.

4. Select the installation server and the installation. (The path for your new installation should display in the installation text box.) Choose **OK**.

5. If necessary, add any administrators/operators to the Admin List and users to the User List.

Configuring File History Database Location

NOTE: This section should be completed only if the Storage Manager's databases are centralized.

Each resource on the protected resource list must have the File History Database location updated to reflect their new location.

1. Access Resource Manager. Highlight a resource that your original installation was protecting.
2. Open the Operations menu and select *Edit Resource Info*.
3. Select **Change File History Database Location**.
4. A pick list appears listing the target servers. Choose the target server, then select the target volume that you moved your Storage Manager installation to.

   You should receive a message indicating that the File History Database already exists for the resource. Choose **Use Existing Histories**.
5. Repeat steps 1 through 4 for the rest of the resources on the Protected Resource List. The History path for each resource should identify the new target server.
6. After updating your resource's history database location, update the default location for your centralized databases. Choose Operations/*File History Database*. Select *Configure* and select the default server volume on which to store your history database(s).

Configuring a Backup Device

If the host adapter number or SCSI ID on the backup device has changed from the original setup, then the backup device may need to be re-configured. To do so, access Device Manager, choose Operations/*Scan for Devices*, then choose the *Add Device* menu option. You may need to delete the current device and re-scan the bus to find the new host adapter number and/or SCSI ID.

Consolidating Volumes

Consolidating volumes is the process of combining two or more volumes. It is usually the result of adding a new, larger volume to replace existing volumes.

To consolidate volumes using Storage Manager, you should

- Perform a Full Backup operation on the source volume(s).
- Tag the source volume in Resource Manager, open the Operations menu and select *Restore/Full Resource*. Select the **Redirect to** option.
- Select the target volume.

To perform a full backup

Prior to consolidating volumes, be sure have a snapshot of the volume(s) as it exists prior to redirecting its data to a new volume.

➤ In Resource Manager, tag the volumes being consolidated.

➤ Open the Operations menu. Select *Backup/Full*.

To copy data from one volume to another

1. In Resource Manager, tag one volume that you want to consolidate.
2. Open the Operations menu and select *Restore/Data*.
3. In the restore dialog box, select **Redirect to**.
4. Choose the Server, Target Service, TSA, and Resource to restore the data to and choose **OK**.

   This operation will restore all directories, files, and trustees from your source volume to the target volume.
5. Perform the steps above for each volume you want to consolidate.
6. When you have successfully consolidated the volumes to a single volume, perform a full backup on the volume so that all data is copied to backup media and so that the File History Database reflects the new volume configuration.
7. If you no longer will be using the volumes you are consolidating (VOL1 and VOL2 in the above example), delete them from the Protected Resource List or make them inactive (see page 8-9 for more information).

File History Databases

When consolidating volumes, you must decide which File History Database you want to use for the new volume or create a new File History Database for the new volume.

Your original File History Databases will not be redirected when performing the procedures above.

If there is a specific File History Database you want to use for your new volume, you should restore it to the new volume (note that you cannot merge File History Databases and a volume can have only one File History Database).

To redirect a File History Database

1. In Resource Manager, tag the source volume.
2. Open the Operations menu and select *Restore/File History Database*.
3. On the restore dialog box, select **Redirect to**.
4. Choose the Server, Target Service, TSA, and Resource to redirect the File History Database to and choose **OK**.

   Note that, unless distributing File History Databases, the File History Database is not actually moved to the target volume but it moves to the target volume's File History Database location.

File Server/Volume Cloning

Cloning is the process of making an exact duplicate of an existing volume or an entire server. When cloning a volume, the new volume includes the directory/file structure of the original volume and retains the original volume's File History Database.

Why Clone?

Why would you use Storage Manager to clone a volume and/or file server? Why not just place the file server on the network and copy the directory/files to the new volume?

Cloning a volume involves more than just reconstructing the directory/file structure. In the case of a NetWare volume, there may be user privilege restrictions attached to directories that are just as important to duplicate as the directory/file structure.

For a NetWare 3.x file server to be cloned, the Bindery must also be duplicated. Without the help of Storage Manager, this process involves multiple steps and can be very complicated.

When performing a cloning operation, if the file server and all the volume names are identical, you can run the same operation as you would for a full server restore.

Full Backup

Before cloning a volume or server you will want to be sure all files are copied to a single media set. The best method is to perform a full backup on each volume you are cloning.

Cloning a Server

The following is a summary of the steps required to perform a cloning operation.

- ➤ Perform a full backup on the source volume(s) to be cloned.
- ➤ In Resource Manager, tag the volume to be cloned.
- ➤ Open the Operations menu. Select *Restore/Full Resource*.
- ➤ On the restore options dialog box, select **Redirect to**.
- ➤ Choose the Server, Target Service, TSA, and Resource to redirect data to and choose **OK**.

Assumptions

The following procedure assumes the following for your new server:

- The target volumes have identical names to the source volumes
- You have installed and loaded the appropriate TSAs on the target server and added that server to the Protected Resource List

NOTE: If cloning volumes on a 3.x server to another server, you must also redirect the Bindery resource so the trustees and Object IDs for users not defined on the target server will not have to be recreated.

Procedure

1. If your new server is a NetWare 3.x server, recreate your auto login user with the same name and password.
2. In Resource Manager, tag the volume(s) you are cloning. Open the Operations menu and select *Full Backup*. This ensures you have a snapshot of your volumes on a single media or media set.

3. After the backup is complete, tag one of the volumes you are cloning. If you are cloning a 3.x server, you should tag the Bindery resource as your first resource to clone and then the SYS: volume.

4. Open the Operations menu and select *Restore/Full Resource*.

5. On the restore options dialog box, select **Redirect to**.

6. Choose the Server, Target Service, TSA, and Resource to redirect data to and choose **OK**.

7. Repeat the above procedures for each volume you are cloning.

NOTE: If you are cloning a Storage Manager installation server, follow the instructions in *Moving a Storage Manager Installation* for instructions on loading the appropriate NLMs and other setup information.

Chapter 7

Managing Jobs

Overview

This chapter describes how to:

- Re-schedule, delete, and de-activate jobs
- View:
  - The results of the last automatic job
  - The media required for the next automatic job
  - The media that may be off-site (if you followed the schedule)
- View and print reports, system messages, and attached files
- Respond to alerts

Control Console

You enter Control Console whenever you start the program. From the Control Console, you can access information from the various managers that comprise Storage Manager. In Storage Manager, various managers provide different views of your installation. For example, protected resources are featured in Resource Manager; managed and non-managed media are featured in Media Manager, etc.

In fact, Control Console is so comprehensive, you could use it without ever having to use the other managers, aside from updating your resources and your configured devices.

But then you would not be taking advantage Storage Manager's flexibility!

Control Console provides a high-level view of your entire installation:

- Which media are required for the next automatic job
- Which jobs are waiting for processing
- The status of the last automatic job
- Any conditions that are interfering with jobs, such unavailable devices
- System messages
- The disk utilization of monitored volume resources

Control Console Tabs

To help orient you to Storage Manager, the Control Console is organized by tabs which briefly describe each icon option.

- **Basics**—Displays a list of basic operations and guides you through the basic steps to perform each operation.
- **Status**—Provides a list of windows that display different information about current and upcoming jobs.
- **Reports**—Provides a list of reports that display different information about the installation.
- **Managers**—Provides an alternate means of accessing the different managers.

Basics Tab

Basics tab

The Basics tab provides “tutors” to guide you through basic Storage Manager operations. Refer to this tab the first time you are performing one of the listed operations. After you are familiar with operations, you can turn off the display of this tab through the Control Console’s Preferences dialog box. See page 3-4 for a description of Basics options.

Status Tab

Status tab

This tab lists features that display various types of information about your installation's jobs and managed media.

- **Job Queue**—View, edit, delete jobs in the job queue.
- **Last Automatic**—View all system messages generated by the last automatic backup job.
- **Next Required Media**—View the status of managed media required for the next media rotation.
- **Off-Site Media Advisor**—View the location (on- or off-site) and vault rotation status of your managed media.
- **System Messages**—View system messages generated by jobs.

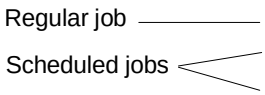
- **Resource Monitor**—View the disk utilization status of monitored resources.

Job Queue

The queue is where all backup, restore, and utility jobs are placed for processing. If your installation is configured for concurrent jobs, Storage Manager can process multiple jobs simultaneously. For example, a backup job can run on one device, while a restore job runs on another device.

To view the Job Queue window

➤ From the Control Panel window, select the Status tab and click the Job Queue icon.



Job Queue window

Parameter	Description
Submitter	The name of the user who created the job.
Operation	The type of operation the program requested by the job or the description of a scheduled job. For example, this parameter displays **Media Journal** or **Default Automatic**.
Status	Describes the job's state relative to the job server. The possible states are: **Ready**—The job is waiting for the job server to call the appropriate operation engine. **Selected**—The job server has selected the job for servicing. This should appear very briefly. **Servicing**—The operation engine is processing the job. **Server Hold**—The job has failed during processing. **Operator Hold**—An operator or administrator has deliberately de-activated the job. **Resubmitted**—The job has been on server or operator hold and is being returned to the queue.
Job ID	The identification number Storage Manager assigns a job.

NOTE: Due to NetWare's QMS behavior, one user can hold, delete, disable, or submit a job while another user is viewing the job's status or editing its schedule. NetWare performs the most recent action, unless the job has already been deleted.

Processing a Job

Storage Manager processes jobs in the order in which they are submitted to the job queue. The order in which jobs appear or are listed in the queue window is not always the order in which the program processes the jobs. For example, a scheduled job may appear at the top of the list but it will not be processed until after its start time or after you choose to submit it. Another example is that of a restore job that is processed ahead of a backup job while another backup job is running.

Unless a job is scheduled to run again, it disappears from the job queue after completing successfully. The program also sends a system message indicating that the job completed successfully to the System Messages window. Jobs that fail go on server hold and are assigned a new job ID.

✓

TIP: If you are submitting several jobs, you may want to note their job IDs. Later, you can filter the System Messages window to display only the messages of a specific job.

To view job activity

➤ From the Job Queue window, highlight the job that the program is currently servicing and choose the **View** button.

—If the job is a backup job, the Backup Summary Status window appears. Remember that the archive, database maintenance, and migrate operations use the backup engine.

—If the job is a restore, migrate, or utility job, the Job Status window appears.

Backup Job Status window

Parameter	Description
Operation	The operation Storage Manager is performing during the job.
Phase	The activity of the user interface. Usually, the phase will be **Monitoring operations**.
State	The state of the device being used for the operation being performed on the highlighted resource. The program report one of eight states: completed, volume error, media or hardware error, session error, unknown failure (**FAILED**), in progress, not performed, or unknown status. **Unknown status** means the program does not know what happened.
Job ID	The identification number Storage Manager assigns a job.
Elapsed Time	Records the time that has passed since the program began processing the job.

TIP: If you are enabling concurrent backup operations, choose the **View All** button. You can simultaneously view Backup Operation Status windows for all of the resources that the program is currently processing.

Backup Operation Status window

Parameter	Description
Operation	The operation performed during the job.
Phase	The current activity.
Job ID	The identification number Storage Manager assigns a job.
Elapsed Time	Records the time that has passed since the program began processing the job.
Resource	The resource currently being accessed.
Path	The path currently being operated on.
File	The file currently being operated on.

Parameter	Description
Media	The label of the media in use during the current operation.
Session	The name of current session written for or accessed by the current job.
Device	The device in use during the job.
State	The activity performed by the device.
Scheduled	
Items	The total number of items submitted for the current operation. This parameter is used for restore operations only.
Bytes	The total number of bytes submitted for the current operation. This parameter is used for restore operations only.
Remaining	
Items	The remaining number of items submitted for the current operation. This parameter is used for restore operations only.
Bytes	The remaining number of bytes submitted for the current operation. This parameter is used for restore operations only.

To view a restore, migrate, or utility job being processed

➤ From the Job Queue window, highlight a restore or utility job that the program is currently servicing and choose the **View** button. The Restore, Migrate, or Utility Job Status window appears. If you are doing a restore, this window also displays the number of items scheduled to be restored and how many remain to be restored. A sample of the Restore Job Status window appears on page 6-3.

Aborting a Jobs and Operations

To abort a job

1. From the Backup, Restore, Migrate, or Utility Job Status windows, choose **Abort**. A prompt appears.
2. Confirm that you want to abort the job.

Changing a Job's Schedule

Through the Job Queue window you can change the schedule of existing scheduled jobs.

To view or edit a job's schedule

1. From the Status tab, select the **Job Queue**. The Job Queue window appears.
2. Highlight the job you want to re-schedule. The status of the job must be "Ready" in order for you to edit it. An alarm clock icon indicates a scheduled job.
3. Select the **View** button. The Scheduling Options dialog box appears.
4. Select the new parameters to re-schedule the job.
5. Select **OK** to save the new parameters.

See page 5-20 for information about editing the schedule parameters.

Last Automatic

This window lists the type of process the program performed on each resource and the outcome of the process during the automatic operation.

To view system messages for the last automatic job

➤ From the Last Automatic window, choose the **Messages** button. The System Messages window automatically filters systems messages based on the jobs ID of the most recent automatic job.

Last Automatic window

Parameter	Description
Status	Indicates whether the program successfully completed (**Completed**) on a particular resource or, if an error occurred, the type of error such as **Media/HW Error**.

Next Required Media

The Next Required Media window displays the name of the media required for the next automatic job or, more specifically, next rotation day operation.

To view media required for the next automatic job

1. From the Control Panel window, select the Status tab and select **Next Required Media**. The Next Required Media window appears.

Next Required Media window

Parameter	Description
Media	The media that Storage Manager requires to complete the next automatic job. The program will use any of the listed media.

Parameter	Description
Device	Indicates whether the media required for the next type of automatic job you selected is mounted (**Yes** or **No**). If the device is an autoloader, the program considers media in the magazine to be mounted.

2. Select the type of operation, **Next Automatic Backup** (the default option) or **Next Scheduled Rotation**. When you view this window the day before rotation day, the next automatic job and rotation day job are identical. The window displays the media label and indicates whether it is mounted on a configured device. The **Scheduled** parameter displays the date and time the program will initiate the selected job.

➤ If it is after the rotation time and you have not rotated media sets, a prompt appears.

For more information about configuring the rotation time, see page 4-26 for Tower of Hanoi and 4-28 for Grandfather-Father-Son rotation.

Off-Site Media Advisor

Palindrome recommends that you follow the off-site storage schedule displayed in the Off-Site Media Advisor window. The Off-Site Media Advisor window indicates where your managed media sets **would be located** if you actually followed the schedule.

To view the status of the on- and off-site media

➤ From the Control Panel window, select the Status tab and select **Off-Site Media Advisor**.

Off-Site Media Advisor window

Parameter	Description
Retrieve from off-site storage	The managed media set(s) that you should retrieve from off-site storage for the next rotation day. The program schedules media set for retrieval based on the number of days notice specified in Configuration Manager.
Take to off-site storage	The managed media set(s) that you should deliver to the off-site storage facility.
Should be off-site	A summary of managed media sets that should currently be at the off-site storage facility.
Should be on-site	A summary of managed media sets that should currently be on-site.

System Messages

Storage Manager records messages generated by jobs directly in the System Messages window. If you are monitoring jobs that are processing in attended mode (**Prompt With Questions** option is turned on), some messages may prompt you to take action. You should check the System Messages window frequently for important system messages pertaining to your automatic operations.

You can limit the number of system messages available at any one time by restricting how many days a message can remain in the window or by limiting the size of the System Messages window.

See page 4-13 for information parameters for the System Message database.

To view a system message

1. From the Control Panel, select the Status tab and choose **System Messages**. The System Messages window appears.
2. Highlight a system message in the System Messages window. The full description of the system message and any recommended action appear below the system messages.
3. Choose the **Close** button to leave this window.

System Messages window

Parameter	Description
Severity	The message's level of importance. The choices are: **All**—Displays all of the message severity levels. **Note**—Displays status information which may be useful. **Warning**—Alerts you to a potential problem which may require action. **Error**—Requires prompt action. **Internal**—Usually indicates that an internal software error occurred. You should report these to your reseller or Palindrome Technical Support.
Module	The module that is used to a perform an operation. For example, PALREST.NLM is used to restore items.

Parameter	Description
Code	The subject category of a system message. For example, MUM refers to media usage. The subject code precedes a number assigned to a specific message in that category. You can find the subject categories and specific messages described in the *Administrator's Reference Guide.*
Date	The date and time the program recorded the system message.
Job ID	The identification number Storage Manager assigns a job.
Description	The full description of the system message corresponding to the code and number.
Recommendations	When available, text in this parameter describes the significance of the message and often indicates what action you should take.

The default view of the System Messages window displays both primary and linked messages, for the most recent jobs. The most recent system messages appear at the top of the list. **Primary messages** indicate general information. **Linked messages** provide detailed information about issues addressed in primary messages. Linked messages appear indented below the primary message they describe.

To enlarge the message description

1. Highlight the system message.
2. Choose the **Details** button. The System Message appears.

System Message window

In addition to providing a description and recommendation, the window indicates any linked messages associated with this message in the upper-right corner. Choose the **Next** and **Previous** buttons to review these messages.

➤ If the **Attached** button is active, there is a file with additional information that is linked to the System Message window.

3. Choose **OK** to close the System Message dialog box.

To view additional available system messages.

1. Browse through the currently available messages by sliding the thumb button or clicking the down arrow.

2. If the **More** button is active, the program has additional messages to generate for the current filter parameters. Choose the **More** button to generate additional messages. The program appends these messages to the bottom of the window. Continue to browse.

Filtering the System Messages

Filtering messages can help you focus on a manageable number of system messages. You can select one value for each of the following parameters:

To filter system messages

1. From the System Messages window, select the **Define Filter** button. The Filter dialog box appears. You can select only one value for each parameter.

➤ To view only primary messages, select the **Show Primary Messages Only** option. You can still view any linked messages through the System Message window.

2. In the **Severity** parameter, select the message severity you want to view.
3. In the **Module** parameter, select the module you are interested in.
4. In the **Code** parameter, select the subject category you are interested in.
5. In the **Job ID** parameter, type the Job ID for which you want to view messages.
6. Choose **OK** to save your filter parameters.
7. From the System Messages window, choose the **Enable** button to display the System Messages window based on the criteria you chose.

NOTE: When looking for system messages associated with a failed job, you must filter on the job's original job ID, not the new job ID assigned by the program.

To return to the default view,

➤ Choose the **Disable** button. The **Enable** button retains the filter parameters you saved.

Printing the System Messages

Since the System Messages window does not retain system messages indefinitely, you may want to have a record of system messages. Also, this record may be helpful for troubleshooting problems.

To print the system messages

1. Select the File/*Print Report* option. To see the format of the report before you print it, select *Print Preview*. The Print Report dialog box appears.
2. Select your printing parameters.
3. Choose **OK** to print the messages currently in the system messages database.

TIP: You can use the **Print** button to print an individual system mesage from the System Message window).

Administrator/Operator Notification

Storage Manager provides a variety of tools to notify you and other authorized staff of important events as they occur. These notification features signal that operations have completed or that a problem exists which interferes with the processing of a job. These notification messages are very general. You can investigate the cause of these messages by viewing the System Messages window.

- Alert icons
- Notification messages
  —E-mail messages
  —SEND messages
  —SNMP messages

Alerts

Alerts palette

Alerts inform you of situations which require attention. These buttons can help you monitor your installation and address problems in a timely manner. Storage Manager checks your installation for system messages and conditions that require your attention. If there are any conditions or new messages that require attention, the program activates the appropriate alert. When active, the alert icons appear in color; when inactive, the alert icons are gray.

The alerts palette notifies you of up to seven installation conditions.

Job Server Inactive—Indicates that the job server is not loaded.

Job(s) Require Attention—Indicates that an attended job requires a response to a system message.

Job(s) On Hold—Indicates that a fatal error occurred while processing an unattended job. In the Job Queue window, red document and alarm clock icons indicate jobs on hold. The status of the job is "Server Hold."

Check Last Automatic—Indicates that the last automatic operation failed. For example, a fatal media or device error occurred.

Check Next Media—Indicates that the media set for the next automatic operation has not been mounted.

Check Device—Indicates that the device is not available for scanning.

Check Resource Monitor—Indicates that either the Resource Monitor (PALRMON.NLM) is not loaded or that one or more resources cannot be migrated below their respective high water marks.

To respond to an active alert

1. Click the active alert.

➤ If the Job Server Inactive alert is on, a system message appears with a description and recommendations.

If you need to load the job server, at the server console prompt type:

LOAD PALJSRVR /I<*installation path*>

where <*installation path*> is the volume and directory of your installation directory (for example, VOL1:\PAL).

➤ If the Check Next Media alert is on, the Next Required Media window appears indicating the media that should be mounted.

- If the Check Last Automatic alert is on, the Last Automatic window appears from which you can view messages specific to this job.
- If the Check Resource Monitor alert is on, the Resource Monitor window appears indicating which resources are on hold or a system message appears regarding the status of the Resource Monitor.
- If either the Job(s) on Hold or Job(s) Require Attention button is on, the Job Queue window appears. A red phone icon indicates one or more attended jobs need attention. The server hold status indicates that one or more jobs failed. Highlight this job and choose **View** to display the system message(s).

Job(s) Require Attention alert

Job Queue window with Job(s) Require Attention alert

2. Correct the condition. Refer to the *Administrator's Reference Guide*, if necessary.

Notification on the Windows Desktop

Control Console can notify you of any problem, even if you are working in another Windows application.

You can receive notification from Storage Manager while working in other applications by minimizing Control Console. If an alert condition exists, the Storage Manager icon will flash.

Message Notification

Through Configuration Manager you can configure:

- NetWare SEND messages
- E-Mail messages
- SNMP messages

The program sends the messages or e-mail based on the outcome of an operation to administrators and operators. Only a subset of all system messages are significant enough to generate notification messages.

Through File Manager, end users can configure notification of completed restore jobs; administrators are notified of unsuccessful backup and restore jobs and certain error conditions resulting from end user jobs.

The e-mail notification feature requires that you have Novell's MHS, or Message-Handling Service, installed and properly configured. MHS is a software program that permits reliable transfer of electronic messages from one place to another.

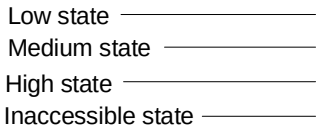
SNMP Messages

SNMP (Simple Network Management Protocol) sends messages to specially configured workstations. Palindrome SNMP messages appear in one of two forms. If you are using NMS (NetWare Management System), configured workstations receive full message descriptions. If you are using another system, such as HP Open View, the SNMP message indicates only that a message with a certain level of severity (such as a "Warning") has been recorded.

See page 4-7 for information about configuring Palindrome SNMP messages.

Resource Monitor

This window displays the utilization and the status of the volume resources by Storage Manager. Only resources configured for monitoring options either under system or customized resource settings appear in this window.



Resource Monitor window

Parameter	Description
(Icon state)	Icons represent the status of disk utilization. Green—Indicates that the disk utilization of the resource is below the low water mark. Yellow—Indicates that the disk utilization of the resource is below the high water mark. Red—Indicates that the disk utilization of the resource is above the high water mark. Grey—Indicates that the status of this monitored resource is unknown because it is not accessible be Resource Monitor.
Resource	The name of the monitored resource.
Actual (%)	The current level of disk utilization expressed as a percentage of the disk's total storage capacity.
Prestaged (%)	The portion of the disk's capacity that consists of files eligible for migration. Since this column displays a value as of the most recent migration or build of the prestage list, it's possible that more files may be eligible than are indicated.

Parameter	Description
State	The state of the resource's disk utilization relative to the high and low water marks. The possible states are: **Low**—The current disk utilization is below the low water mark. **Medium** —The current disk utilization is between the low and high water marks. **High**—The current disk utilization is above the high water mark. If this resource is included in automatic migration operations, Storage Manager submits a migration job for this resource. If not, you should perform a manual migration operation on this resource to ensure that new files can be stored on the disk. **On Hold**—The current disk utilization remains above the high water mark following a migration job. **??**—The value is unknown because the resource is inaccessible.

The Resource Monitor window provides buttons for performing operations:

Edit—Customize the resource monitoring settings for a particular resource.

Print—Print the Resource Monitor report, which contains status information for all monitored resources.

Retry—Resubmit a migration job for a resource in the on hold state. For the resubmitted job to be successful, you usually must change parameters that affect migration eligibility.

To resubmit migration jobs for an "on hold" resource

1. "On hold" indicates that there are no more files eligible for migration. Your must accelerate the eligibility of files by changing one or more of the following parameters:

   - **Archive Copies Required for Full Protection** (Configuration Manager)
   - Applicable archive and/or migrate rules (File Manager)
   - **Create a Near Line Set** (Configuration Manager)

2. After you change the parameter(s) access File Manager. View the eligible files by filtering the file window using the **Eligible for Migration** option. Modify the parameters further if necessary.

3. In the Resource Monitor window, highlight the resource and choose the **Retry** button. The job is submitted. Open the Job Queue window to view the status of this job. Note that the **Retry** button is available only to resources in the "on hold" state. You cannot submit jobs for any other type of resource state.

To customize migration parameters

1. Choose the **Edit** button. The Edit Migration Parameters dialog box appears. See the page 5-10 for details about customizing these migration parameters.

2. After you change the parameter(s), access File Manager and filter the file window using the **Eligible for Migration** option. If there are not enough files to migrate, you may have to modify the parameters again.

To view applicable migration parameters

➤ Choose the **Edit** button. The Edit Migration Parameters dialog box appears. To view the system migration parameters if the highlighted resource uses custom parameters, choose the **Use System Migration Parameters** button and choose **OK** and close the window. After you return to the Resource Monitor window, choose **Edit** again. The dialog box displays the system migration settings in gray text.

To print the Resource Monitor report

➤ Choose the **Print** button. See page 7-31 for details about printing reports.

Reports Tab

Reports tab

Reports provide a means of quickly summarizing the current status of various aspects of your Storage Manager installation. Device, Resource, and Media summary reports use parameters from the information tabs. See Appendix D, “Viewing Installation Information,” for further descriptions.

- **Future Media Rotations**—Displays the managed media sets and the dates on which they are required for rotation. The program calculates the rotation dates based on the media scheduling parameters and takes into account changes such as deferred or early rotations that impact future dates.
- **Resource Summary**—Displays the resources that are currently protected by your installation. This is the same list of resources that appears when you open the Operations menu and select *Change Sequence* in Resource Manager.

- **Device Summary**—Displays all devices that are connected to the Storage Manager installation server and indicates which devices are configured for Storage Manager operations.
- **Media Summary**—Displays information about the installation's media.
- **Configuration Summary**—Displays the current settings of the system, operations, and media scheduling parameters.

Summary Reports

To view a report from the Reports tab

1. Choose the report icon you want printed.

➤ A prompt asks if you want to preview the report. Choose **Yes**. Choose **No** to select printing parameters and print the report.

➤ If you selected the Media Summary icon, the prompt first asks if you want session-level detail.

➤ If you selected the Future Media Rotations icon, a window appears. Use the **More** button and the thumb button to display additional dates. The program appends these rotation dates to the bottom of the window. Select the **Print Preview** button to display the report format.

2. The Print Preview window appears.

➤ To view all pages in the report, choose the **Next Page** and **Prev Page** buttons.
—To view two consecutive report pages on your screen, choose the **Two Page** button.
—To view report line items, choose the **Zoom In** button.

To print a report

1. From the Print Preview screen, choose the **Print** button. The Print dialog box appears.

   Change the parameters if necessary.

   ➤ Set the **Print Range**, **Print Quality**, **Copies**, and **Printer** parameters.

   ➤ To change the default printer and the page layout, choose the **Setup** button.

   ✓ ***TIP:*** Palindrome recommends that you print the reports in landscape (horizontal) mode in order to print the reports in the largest font size possible.

2. Choose **OK** to submit the print job.

Sample Summary Reports

The Resource, Device, and Media Summary reports contain some of the parameters described in Appendix D, “Viewing Installation Information.” The parameters in the Configuration Summary report are described in Chapter 4,“Customizing Your Installation.”

Future Media Rotations Report

Resource Summary

Device Summary

Media Summary

Configuration Summary

Managers Tab

Managers tab

This tab lists the other Storage Manager managers and the functions you can perform:

- **Resource Manager**—Manage your Protected Resource List and perform operations on selected resources.
- **File Manager**—Perform operations on selected directories and files on a single resource. This manager is also available for end users to back up and restore their own files.
- **Media Manager**—View the contents of media in your library, de-activate damaged media, and perform other utility operations on physical media.
- **Device Manager**—Configure devices for Storage Manager operations and perform read/write and autoloader tests.

- **Configuration Manager**—Configure access to other Storage Manager installations, manage users, customize operations, or install other Palindrome products.

To select a manager

➤ From any manager, open the Managers menu and select a menu option. The manager window appears.

or

➤ Click a manager icon from the Managers tab or managers palette.

Managers palette

Chapter 8

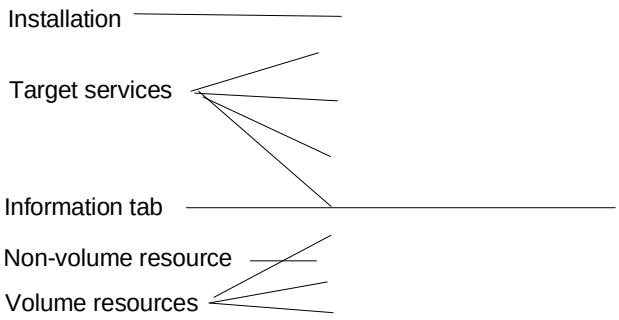
Managing Resources

Overview

This chapter describes how to:

- Manage your Protected Resource List
- Add and delete resources
- Upgrade TSAs by renaming them
- Manage databases
- Re-arrange the Protected Resource List
- Customize migration parameters

Introduction



Resource Manager window

The Resource Manager's protected resource tree displays items currently protected by your Storage Manager installation. The protected resource tree provides three different views of your protected resources based on different criteria.

To select a view of the Protected Resource List

➤ From Resource Manager, open the *View* menu and select one of the three tree views:

Sort by Target Service—The default view of the protected resource tree
Sort by Type—The resources are organized by the type of resource they are. For example, workstations are grouped together, NetWare servers and their resources are grouped together.
Sort by Location—The resources are organized by the SMDR they communicate with.

From any of these views, you can perform archive, backup, migrate or restore operations on any protected resource.

To update the tree view and information tabs

➤ Open the Operations menu and select *Refresh the Tree*. The program will update any changes that have been made to the protected resources and/or information on the latest operation performed on the resources. Storage Manager does not automatically reflect the most recent operations completed on the various resources.

See Appendix D, "Viewing Installation Information," for descriptions of each parameter in the information tabs.

Resource Manager Tool Bar

The Resource Manager tool bar provides a short cut to commonly used operations:

Automatic job—Submit an automatic job for processing as soon as possible.

Backup—Perform a custom backup operation on the selected resource(s).

Restore—Perform a complete restore operation on selected resource. A complete restore consists of the resource's history database, directory structure, and data.

Add Resource—Add a resource located on the server or installation to the Protected Resource List.

Remove Resource—Remove the selected resource(s) from the Protected Resource List.

Help—View on-line help for Resource Manager.

Managing Your Protected Resources

Your storage management strategy is based on automatic operations which back up all active protected resources. Therefore, it is important to add, delete, and reposition your protected resources as your current data protection requirements change.

Resource Summary Report

The Resource Summary includes selected parameters from the information tabs. You may want to print this report if you:

- Have an extensive Protected Resource List that does not fit on the screen.
- Want to compare information for different resources.
- Want to fax a copy of your Protected Resource List to a Palindrome Technical Support representative who is helping you with a problem.

The Resource Summary report displays all of the maintain your protected resources is available in Console Manager on the Reports tab.

See page 7-36 for instructions on viewing and printing the Resource Summary report.

Adding Resources

Whether you are adding a server volume, workstation volume, NetWare Directory Services, etc., you must load the appropriate TSAs and related communications software before you add the resource to Resource Manager. Use the server preparation diskette to copy the appropriate TSAs to each server. When you installed Storage Manager, the program automatically loaded the appropriate TSAs for your installation server. See the *Installation Guide* for detailed information about TSAs.

During an automatic job, Storage Manager processes the protected resources in the order in which the resources appear in the Protected Resource List (see the Resource Sequence for Automatic Operations dialog box).

The resource at the top of the list is backed up first, the second resource is backed up next, etc. If you are backing up resources concurrently, this is the order in which the program assigns resources to available engines or devices.

Once you add a resource to the list, the Resource Manager displays the capacity of the resource and its File History Database location. The File History Database is created in your installation directory (the default) or the location you specify using Operations/*History Database Location.* If you are upgrading an existing installation, you should have already added protected resources and translated File History Databases during the installation process. See the *Installation Guide* for details regarding the *Translate History Database* menu option.

Use the following procedure to add one or more resources on an unprotected server.

To add a server

1. Highlight the installation icon on the protected resources tree.
2. Open the Operations menu and select *Add Resource*. The Choose a Server/SMDR dialog box appears with a list of servers that have TSAs loaded. The server and SMDR are almost always the same entity.

3. Click the server with the resource you want to add. The Choose a Target Service Agent dialog box appears. This dialog box displays a list of all the TSAs loaded on the server.

Choose a TSA dialog box

4. Select a TSA that is appropriate for the resource you want to add and choose **OK**. The Choose a Target Service dialog box appears. It displays a list of target services on the selected server.

5. Select the target service and choose **OK**. The Choose a Resource dialog box appears. It displays all of the resources on the selected server that are not already on the protected resource tree.

Choose a Resource dialog box

6. Select the resources you want to add.

TIP: Use <**Ctrl**> key-click to tag or select multiple items in a list or eligible tree. Use <**Shift**> key-click to define a range of items in a list or eligible tree.

7. Choose **OK**. The resource appears on the protected resource tree.

Use the following procedure to add one or more resources on a protected server.

To add a volume resource

1. Highlight the protected target service.
2. Open the Operations menu and select *Add Resource*. If there are multiple TSAs loaded on the target service, you must choose a TSA.
3. Choose one or more available resources from the Choose a Resource dialog box.

Use the following procedure to add a local drive to a protected workstation.

To add a local drive

1. Highlight the workstation target service icon.
2. Open the Operations menu and select *Add Resource*.
3. Choose the local drive from the Choose a Resource dialog box.
4. Choose **OK**.

De-activating a Resource

When you de-activate a resource, Storage Manager excludes this resource from automatic jobs. However, the resource is still available for custom jobs because the File History Database has only been excluded from automatic jobs.

There are a two main reasons for de-activating a resource:

- You want to perform maintenance on a downed resource.
- You are experiencing problems with a resource during backups and you want to troubleshoot the problem.

De-activated resources are not listed in the Last Automatic window.

To temporarily exclude a resource from automatic jobs

1. On the protected resource tree, highlight the resource you want to de-activate.
2. Open the Operations menu and select *Edit Resource Info*. The Edit Protected Resource Attributes dialog box appears.
3. Turn off the **Included for Automatic Operations** option.
4. Choose **OK** to save your change. The Configure tab displays the change you made. The Resource Sequence for Automatic Operations dialog box also indicates which resources have been included in automatic operations.

Removing a Resource

Removing the resource automatically excludes the resource from future operations. Usually, you'll remove a resource only when you no longer wish to protect it. If you think you may add the resource later, you have the option of keeping the File History Database.

WARNING: Do not remove a resource and its File History Database if you intend to add it to Resource Manager at a later time. You will delete records of previous file versions and other session information that you may need for a restore operation.

To remove a resource

1. Highlight a resource.
2. Open the Operations menu and select *Remove Resource*. A prompt appears.

Removing a Resource prompt

3. Choose **Yes** to confirm the removal of the resource and its database, if applicable. The resource no longer appears on the protected resource tree.

To remove a server

➤ Highlight each of the server's resources and delete these one by one. When all resources are deleted, the server is removed from the tree.

Re-arranging Resources

When you re-arrange resources, you are changing the order in which Storage Manager performs automatic operations on the protected resources. There are a few reasons why you may want to re-arrange resources after you have installed or added resources:

- You suspect that a certain resource causes your operation to fail. By moving this resource to the last position, the program will have already protected the data of the other resources prior to failing on the last resource.
- You want to improve the efficiency of concurrent backup operations.

To re-arrange the sequence of resources for automatic jobs

1. Open the Operations menu and choose the *Change Sequence* menu option. The Resource Sequence for Automatic Operations dialog box appears; it displays the Protected Resource List.
2. Highlight the resource and choose the appropriate button. The **Up** and **Down** buttons move the highlighted resource one position from the resource's original position. The **Top** button moves the resource to the first position and the **Bottom** button moves the resource to the last position on the Resource Sequence for Automatic Operations dialog box.

➤ Move the larger resources to the top of the list so that these resources complete at approximately the same time. When processing automatic operations concurrently, the program completes an operation on all active resources before beginning the next operation. For example, the program completes archive operations on all resources before beginning backup operations.

Resource Sequence for Automatic Operations dialog box

- ➤ Separate workstation resources from the same workstation on the list. For example, if the last two resources are a C: and D: drive for the same workstation, the program cannot process these concurrently.

3. Choose **OK** to save the new sequence.

Configuring Tracking Name Space

Storage Manager allows you to configure the name space that it will use to track each resource. This is the name space that appears when viewing files within the user interface and the name space stored in the File History Database. Storage Manager determines a default name space for volumes with multiple name spaces loaded. When Storage Manager encounters multiple name spaces, it prioritizes them in the following order:

1. OS/2
2. MAC
3. NFS
4. FTAM
5. DOS

For example, if you have the OS/2 and DOS name spaces loaded on this resource, Storage Manager defaults to OS/2. Storage Manager tries to take advantage of name spaces that allow longer names first. Files with longer names will most likely have their real names displayed as opposed to displaying them in a DOS name space which limits the file to eight characters (excluding the extension).

If you have only one name space loaded on a resource, Storage Manager will use the loaded name space. Generally, you will not want to change the tracking name space unless you've removed the current tracking name space from the volume.

If you have multiple name spaces loaded, you can specify which name space you want Storage Manager to use for this resource before running your first backup.

Changing Name Spaces

Once you have backed up a resource, Palindrome recommends that you do NOT change the tracked name space. Modifying the name space after a resource has been backed up can change the resource's history information.

Also, if you change the default name space, be sure the file rules in effect for the resource apply to your new tracked name space. If you remove a name space from a resource, you may want to change the name space tracking to a parameter other than the default.

If you select a case-sensitive name space to track a resource in (such as NFS), Storage Manager will not allow you to change it to a name space that does not support case-sensitivity (such as DOS). Changing name spaces in this manner would cause duplicate directory and file entries in the File History Database. If you must change from a case-sensitive name space, contact Palindrome Technical Support.

To change the tracking name space

1. From the Protected Resource tree, highlight the resource you want to configure.

2. Open the Operations menu and choose *Edit Resource Info*. The Edit Protected Resource Attributes dialog box appears.

Edit Protected Resource Attributes dialog box

3. Click the **Change Tracking Name Space** button. The list of name spaces available on the highlighted resource appears.
4. Click the name space you want to use from the list of available name spaces.
5. Choose **OK**. The selected name space now appears in the **Tracking Name Space** field.
6. Choose **OK** to close the dialog box.

Renaming a Resource

There are two reasons why you may need to rename a resource:

- The resource's Protected Resource Name, which includes the loaded TSA, has changed.

For example, if you upgraded from an installation using Novell's pre-1994 TSAs, you would have observed the following system message:

PLSM-53 There are no Target Service Agents that match the <ServerName> pattern.

The problem occurs because the System Control Database still refers to the name of the former version of the Novell TSA (for example, "NetWare 3.11 File System"), which was in use when you last added the resource. Now it does not recognize the name of the new TSA ("NetWare File System").

- You recover a downed volume by redirecting it to a target volume and renaming it with the source volume name. By renaming the volume, you ensure continuity between the pre- and post-recovery File History Databases for the redirected data.

To rename a resource

1. In NetWare, change the name of the resource.

➤ If the resource you are renaming is a workstation, you must change the name of the workstation in the configuration file first. See the "*Editing the Workstation's Configuration Files*" section below.

1. Highlight the resource you want to rename.
2. Open the Operations menu and select *Edit Resource Info*. The Edit Protected Resource Attributes dialog box appears.
3. Choose the **Change Protected Resource Name** button. The SMS Target dialog box appears.

SMS Target dialog box

4. Specify the resource's server, the current TSA, the target service, and the resource.

5. Choose **OK** to save the name change.

Editing the Workstation's Configuration Files

To change the name of a DOS workstation

1. Unload TSADOS.NLM and WSMAN.NLM from the server that TSASMS.COM connects to.

2. Unload TSASMS.COM from the workstation.

3. Edit the workstation's NET.CFG file to reflect the new workstation name.

NOTE: Be sure that the workstation is logged on when you name the resource in Resource Manager.

NET.CFG Example	
Parameter	**Example**
TSA server name	PMTEST
Workstation	Alane
Password	t
Disk Buffers	30
Stack Size	2048
Drives	C

4. Load TSASMS.COM on the workstation.

To change the name of a protected OS/2 workstation

1. Edit the TSAOS2.CFG file on the workstation. Below is an example of what your TSAOS2.CFG may look like and an example of each parameter. Note that the TSAOS2.CFG file is not case-sensitive.

TSAOS2.CFG Example	
Parameter	**Example**
WSName	JSMITH
ServerName	FS1
UserName	STORAGE [PASSWORD]
AutoRegister	ON
TempFilesDir	c:\temp

2. Save this file to the directory where TSAOS2.EXE is located (usually \NETWARE).

   For more information on Target Service Agents, see the *Installation Guide.*

Changing Passwords

If you change a workstation's password, be sure to define the new password in Resource Manager so that the program can automatically open the workstation during operations.

To change a password

1. Highlight the workstation (target service).
2. Open the Operations menu and select *Edit Resource Info* . The Edit Protected Resource Attributes dialog box appears.
3. Choose the **Edit Login User** button.
4. Enter the password. Choose **OK** to save the new password and choose **OK** to close the dialog box.

Customizing Migration Parameters

System migration parameters are set in Configuration Manager; however, you can override resource monitoring options and water marks for individual resources in Resource Manager. See page 4-19 for details about these parameters.

To edit migration parameters

1. Highlight the volume resource.
2. Open the Operations menu and select the *Edit Migration Paramerers* menu option. The Edit Migration Parameters dialog box appears.
3. Change the resource monitoring options and/or the water mark values. You can disable resource monitoring options that are enabled for the entire system, but you cannot enable options that are disabled for the system.

Maintaining Databases

Storage Manager automatically performs complete database maintenance operations at every rotation operation. Between rotation days, you may want to perform certain maintenance operations.

NOTE: If you notice poor performance during database maintenance, check the minimum directory cache buffers on the server (see "Tuning Your Servers" in chapter 2 of the *Installation Guide* for more information).

The **Check for Deleted Files** option ensures that deleted directories and files are not automatically restored if the volume needs to be recovered. Since the program performs this operation automatically on every rotation day, you do not have to initiate this operation.

The **Verify** option compares the File History Database against the System Control Database and corrects any minor discrepancies between the databases. The database verification also includes updating the status of media, such as recording retired and forgotten media. As a result, this option updates the file versions displayed in the History and Extended History windows.

Checking for Deleted Files

Perform this operation to avoid restoring files that have been deleted since the previous rotation day.

To update deleted file records in the File History Database

1. Tag the resource with the File History Database you want to check. You can tag multiple resources.

2. Open the Operations menu and select *History Database Maintenance*. The Database Maintenance Options dialog box appears.

Database Maintenance Options dialog box

3. Select **Check for Deleted Files** to update media records in the File History Database.
4. Select any other job parameters.
5. Choose **OK** to submit the job to the job queue.

WARNING: Do not check for deleted files when you are in the process of recovering a resource. If you run this operation after you have restored the File History Database, but before you have recovered the data, the database will not be able to restore the data because the files have been marked as deleted.

Verifying the File History Database

There are two reasons for performing this operation:

- You suspect a resource's File History Database is corrupt. In most cases, the program prompts you to perform a database verification through a system message. You can select this option to recover a copy of the File History Database following a recovery error.
- You have performed a retire or forget operation and want to update the status records immediately.

To verify the File History Database

1. Tag the resource(s) whose database(s) you want to verify.
2. Open the Operations menu and select *History Database Maintenance*. The Database Maintenance dialog box appears.
3. Select **Verify**.
4. Select any other job parameters
5. Choose **OK** to submit the job to the job queue.
6. View the database verification report. Every database verification job generates this report. This report is a file which is attached to a system message in the System Messages window.

➤ If the program determines that the File History Database is corrupt, you will be prompted to restore it. See page 6-16 for information about restoring an entire resource.

Configuring File History Database Locations

By default, Storage Manager places a File History Database in the Storage Manager installation directory for each resource you add to Resource Manager. This is known as the central location.

File History Database Locations

An alternative is to distribute the databases. Instead of placing all File History Databases on one resource, you can specify multiple resources as locations for one or more File History Database. One resource at a time can be identified as a default database location. File History Databases for non-volume resources are always stored in the central location.

The benefits of centralizing databases on a single location are:

- You can easily locate File History Databases.
- If a volume is down, you can redirect restored data to another volume.
- Storage Manager can access the File History Databases more quickly if the databases are on the installation server/volume.

The benefits of distributed databases are:

- You can minimize the amount of disk space required to maintain File History Databases on your installation server.

- The risk of simultaneously losing access to all File History Databases is reduced. If one volume goes down, the other protected volumes still have their File History Databases available.

NOTE: Changing the default File History Database location only affects resources that you add in the future. Existing File History Databases are not affected. If you want existing File History Databases at the new default location, you must move the databases individually.

To change the default File History Database location

1. From Resource Manager, open the Operations menu and select *History Database Location*. The History Database Location dialog box appears.

History Database Location dialog box

2. Select the new database location for new resources.

➤ To centralize the databases of new resources on a single volume, select **Always on the default Server/Volume**. Choose the **Configure** button to choose a the new server/volume location.

- To place each File History Database on its volume resource, select **On the Protected Resource when Possible**. Storage Manager automatically places the File History Databases of non-volume resources on the default server/volume. The original default location still appears because this is the location where new non-volume resources will go.

Moving File History Databases

You may want to relocate a File History Database(s) if you have them centralized on a server and you know the server is going to be off-line or if a volume's disk space is decreasing and you want to store its File History Database elsewhere. If relocating File History Databases, you must relocate them to a server that has the required TSAs loaded, otherwise Storage Manager will not be able to access the File History Database.

To move a File History Database

1. Highlight the resource whose File History Database you want to move.
2. Open the Operations menu and select the *Edit Resource Info* option. The Edit Protected Resource Attributes dialog box appears.
3. Choose the **Change History Database Location** button. The Choose a Server dialog box appears.
4. Select a server. The Choose a Resource dialog box appears.
5. Select the resource that you want to move the database to (the target resource).
6. If the target resource has a File History Database, you can abort the procedure or overwrite the existing File History Database.
7. If the target resource already has a File History Database for the source resource, you have the additional option of using the existing version on the target resource.

Chapter 9

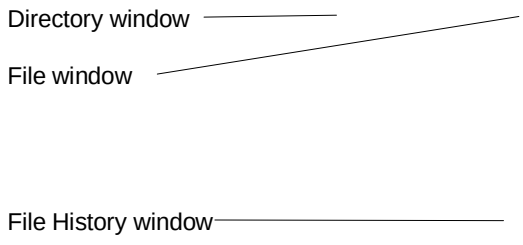
Managing Files

Overview

This chapter describes:

- Types of file windows
- Types of history windows
- How to sort and filter file windows
- How to add, change, and delete file rules
- Common applications of files rules

Viewing Directories and Files



File Manager's main window

File Manager displays directory and file information for the current resource based on the File History Database and the resource's disk. Files that are currently on disk are represented by yellow document icons. Files that have been deleted from disk but have file history recorded are represented by gray document icons.

NOTE: In 4.x installations, any user who needs access to File Manager must be logged in to the tree where Storage Manager is installed.

The drive bar displays all of the resources and/or drives that you are currently mapped or connected to.

File Manager Tool Bar

The File Manager tool bar provides a short cut to commonly used operations:

Define Filter—Specify the filename pattern and/or other criteria.

Enable Filter—Apply the defined filter and display only those files that match the filename pattern and/or criteria during the session.

Sort—Sort files by specified criteria.

File Finder—Find files that match the specified criteria.

Backup—Back up tagged directories and/or files.

Restore—Restore the selected item(s).

Help—Open the Help menu.

Viewing Directories and Files

To view directories and files

➤ To view a resource that you are currently mapped to or connected to, select the corresponding button from the drive bar. Tool Tips identify a workstation drive or other network resource.

or

1. To specify a resource that you are not currently mapped to, open the File menu and select the *Open Resource* option. The Open Resource dialog box appears. Choose the **Resource** button to display the installation's protected installation.

Open Resource dialog box

NOTE: End users do not have the *Open Resource* menu option. The drive bar displays resources that the end users are mapped to. By selecting a drive icon, end users can view the directories and files for which they have read rights residing on the selected resource.

➤ If you are selecting a resource on another installations, you must first select an installation and then choose the **Resources** button.

2. In the **Available Resources** list box, click the resource.

3. Choose **OK**. The directory and file windows appear.

➤ If the program cannot find the physical resource you selected, a prompt informs you that the resource is off-line. You can continue with the operation and view the database records for the resource; you cannot view files on the disk. You can also view the specific system message.

Viewing the File Window

The file window lists the files residing in the highlighted directory. The *View* menu lists three options that provide different information about the files currently listed:

- File Attributes
- File Path
- File Rules

To view a different file window display

➤ Open the View menu and choose *File Attributes*, *File Path*, or *File Rules*.

Occasionally you may want to print filename information, such as files eligible for migration, which you can access as a text file.

To print filenames to a text file

1. Highlight files in a file or Tagged Items window.

2. Open the File menu and select the *Print To File* menu option.

3. Specify the filename and directory path for this list of files and choose **OK**.

Viewing File Attributes

File Attributes, the default display of the file window, includes the file attribute, Create/Modify date, and size information. Gray icons represent indicate that the item is deleted from the disk. Because Storage Manager does not know the level of security defined for a deleted directory, it cannot display any deleted directories to end users. A file may have one or more of the following attributes:

Attribute	Indicates ...
a	The archive bit has been set for this file on disk.
r	This file is read only.
h	This file is a hidden file.
s	This file is a system file.

Viewing File Path

The *File Path* option displays the directory path in which a file is located. This view can be useful to list files that have similar name patterns or tagged files from different directories.

File Path window

Viewing File Rules

The *File Rules* option displays the file rules that apply to files in the highlighted directory or root. To access menu options under the Rules menu, you must be viewing the File Rules window.

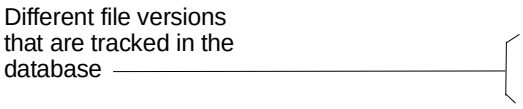
See page 9-17 for detailed information about file rules.

Updating the File Window

If you or another user performs an operation on a file while you are in File Manager, you will not see the effect of the operation (such as a restore) unless you select Operations/*Refresh Directory Tree*.

Viewing the File Versions

File History Window



File History window

The File History window displays all of the versions of the highlighted file that exist on backup media. Each file version displays the Create/Modify date and byte size.

Extended History Window

The Extended History window displays the number of backup and archive copies on media for a specific file. The Extended History window also has a **Restore** button to restore a selected version on a specific session.

To view the media location of a file version

1. Highlight a file version in the File History window.
2. Open the View menu and select *Extended History*. The Extended History window appears.

Extended History window

Parameter	Description
File	The selected filename.
Path	The directory path of the selected file version.
Media	The label of the media containing a copy of the selected file version.
Session	The session number that contains the selected file version. “CP” indicates a backup session. “SV” indicates an archive session.
Size	The size of the file version as written to the session.
Create/Modify	The time and date the file version was last modified.

Tagging Files and Directories

Tagging indicates which directories and files have been selected for an operation. See page 3-19 for instructions on how to tag and untag items.

To tag a file or directory

➤ Click the check box to the left of the filename or directory. The red "x" next to the filename indicates that the file is tagged for an operation. The gray "x" in the directory check box indicates that one or more files in a collapsed subdirectory are tagged.

To view the next tagged item

➤ From either the directory or file window, open the Select menu and choose *Next Tagged Item*. The cursor moves to the next tagged item in that window. In the directory window, the cursor also moves to the next directory on which only some of the files have been tagged.

Before you perform an operation on tagged files, you may want to review the files that will be included in the operation. This can be difficult if the files are located in many directories.

To view all tagged files

➤ After tagging files, open the View menu and select *Tagged Items Window*.

Changing Directories

To view specific directories on the current resource

1. Open the Tree menu and choose *Change Directory*. The Path Selection dialog box appears.
2. Type the path that you want to view. For example, to move from the root of the SYS: volume to SYS:\SYSTEM, type **SYSTEM** in the dialog box.
3. To move to a directory on the same level, type the entire path or the relative path. For example, to move from SYS:\SYSTEM to SYS:\LOGIN, you must type **\LOGIN** or **..\LOGIN** in the dialog box.
4. After typing in the path, choose **OK**.

Removing History Records

Directories that have been deleted from disk are represented by gray folder icons. The File History Database maintains these records so that you can restore these directories. If you no longer want to be able to restore these directories, you can remove these records. Removing the records does **not** reduce the size of the database or make additional space available on the disk.

WARNING: Remove history records from the database only if you are certain that you will not need to restore these directories.

To remove a directory's history records

1. Tag the deleted directory. The deleted directory has a gray folder icon.
2. Open the Operations menu and select *Remove History Record*. The directory disappears from the directory tree.

NOTE: End users cannot view deleted directories.

Sorting Files

The sorting features can help you arrange files residing on a particular directory.

To sort files

➤ Open the View menu and select the *Sort* option. The Sort Options dialog box appears. Select the feature on which you want to sort: name, extension, date, size, attribute type or no order. Then indicate whether you want to rank the items in ascending or descending order by feature.

Filtering Files

Filtering files allows you to view only those files that are currently relevant to the operation you want to perform. The filter you define applies to any resource you open during the current session. This option allows you to narrow your search, even if you know only a few details about the file.

Before you filter the file window, you should understand how the display is defined by default. The file window is based on records in the File History Database and those files currently on the resource's disk. The file records can include files and directories that been deleted from the disk. So by default, a file (or directory) may be in one of three states in the file window:

- The file is on both the disk and the database.
- The file is deleted from the disk and marked for deletion from the database.
- The file is deleted from both the disk and the database. When a file is deleted from the history database, the program no longer records history for the file.

To filter files

Open the View menu and select the *Define Filter* menu option. The File Finder Parameters dialog box appears.

1. In the **File Name Pattern(s)** parameter, type the name of the file or part of the name and wild cards. When entering more than one pattern (you can enter up to 10 patterns), separate each with a comma (",") to find several different patterns during one search. For example, you can type ***.EXE,*.BAT** in the **File Name Pattern(s)** text box to find files matching those patterns.
2. Select the option combination that selects the source of the files that you want to view. For example, select the **Display Files on Disk** and the **No Deleted Files** options to view files only on the disk. Descriptions of other combinations appear in the table.

Option Combination	Result
Display Files on Disk and All Deleted Files	Displays all files for which there are records in the File History Database and files currently on the disk. This is the default display of the file window.
Display Files on Disk and Files Deleted as of __	Displays files that are on disk and files deleted from disk between the present and specified number of days.
Display Files on Disk and No Deleted Files	Displays only the files that are on disk.
All Deleted Files	When **Display Files on Disk** is turned off, the program displays all files deleted from the disk that have also been recorded in the File History Database.
Files Deleted as of __	When **Display Files on Disk** is turned off, the program displays files that have been deleted from the disk between the present and specified number of days. This option combination is useful for identifying files deleted recently. You may be able to restore them from a backup session and preserve the continuity of the file's history if you have updated file records on the database (or the rotation has not yet occurred).

3. Select the **Advanced** button if you want to define additional criteria on which to filter the file window.

   Date Range—Finds file versions that have a modification date within the date range you specify. The program displays file versions that exist on the resource or on media which have a version in the specified date range.

   Start—Specify the earliest date and time for the date range you are filtering.

   End—Specify the latest date and time for the date range you are filtering.

   File Size—Search for files that are greater than, equal to, or less than the specified size (in bytes).

Migrated Files—Displays files that have been migrated from the resource in addition to the database and disk option selected above. For example, to view only the migrated files, use the default disk and database settings (Display Files on Disk and All Deleted Files) and select **Migrated Files**.

Files Eligible for Migration—Displays files that are eligible for resource-level migration in addition to the other options selected. To view only files eligible for migration, use the default disk and database settings (**Display Files on Disk** and **All Deleted Files**) and select **Files Eligible for Migration**.

4. Choose **OK** to save the filter parameters.

5. Open the View menu and select *Enable Filter* to apply the filter to the window. To toggle between a filtered and an unfiltered file window by selecting *Enable Filter*.

TIP: You can use *SubTree* in conjunction with the *Enable Filter* options to tag items that match criteria you specify.

After choosing your filter, move your cursor to the root directory and select *SubTree*. This will tag all of the items on the resource that match your filter criteria.

Viewing Files Eligible for Migration

You can use the filter parameters to display only files that are eligible for migration. The resulting list displays files that are eligible for resource-level restore operations. The program identifies files as eligible for migration if they meet the following requirements:

- The migration rule's stability period is met
- The file is fully protected.
- If there is a near line set, the program has copied an additional archive copy to it.

To view only the files eligible for migration

1. Highlight the root directory.
2. Open the View menu and select *Define Filter*.
3. Be sure that **Display Files on Disk** and **All Deleted Files** options are selected (these are defaults).
4. Choose the **Advanced** button. Additional parameters appear in the dialog box.
5. Select the **Eligible for Migration** option.
6. Choose **OK**.
7. Open the Select menu and select *SubTree*.
8. Open the View menu and select *Tagged Items Window*.

Finding Files

Use *File Finder* to quickly find files on your resource that match parameters you define.

To find a file

1. Open the Operations menu and choose *File Finder*. The File Finder Parameters dialog box appears.
2. In the **Starting Search Path** parameter, enter the directory path that you want the search to begin on the current resource. By default the currently highlighted directory appears in the **Starting Search Path** parameter of the File Finder Parameters dialog box and the program searches for any file (the wild card pattern) in that directory.
3. To search a different directory path on the current resource, type a directory name to start searching from that directory. If you type a "\" as the search path, the program searches the entire resource from the root directory.

4. In the **File Name Pattern(s)** parameter, type the name of the file or part of the name and wild cards. When entering more than one pattern (you can enter up to 10 patterns), separate each with a comma (“,”) to find several different patterns during one search. For example, you can type ***.EXE,*.BAT** in the **File Name Pattern(s)** text box to find files matching those patterns.

➤ To specify more specific parameters for the search, choose the **Advanced** button. Additional parameters are available specify the file’s size, status, modify date, etc.

5. Choose **OK** start searching for the file. All matching files are found and displayed in a separate window with a history window. From either window you can tag and restore files.

✓

TIP: *File Finder* can be a useful way of doing a “WhereIs” or “NDir” operation for an item that is no longer on disk.

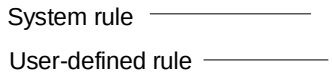
See page 9-13 to review descriptions of these parameters.

Customizing File Rules

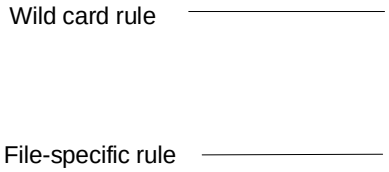
The File Rules window displays file rules in effect for files in the current directory. From any directory you view all of the rules that apply to the current resource.

To view the file rules of the current resource

➤ Once you have selected View/*File Rules*, open the *Rules* menu and select the *File Rules* option. The Rules List window displays all rules that have been created for current resource. The Palindrome logo identifies a system rule.



Rule List window



File Rules window

The File Rules window shows rules created for the current directory. If no rules have been created in the current directory, you can view the origin of a particular file's rule using Rules/*Rule Origin* or view all of the rules for the resource on the Rule List window.

To view the source of a file's rule

➤ Highlight the filename and select Rules/*Rule Origin*. The Rule Origin window appears.

Storage Manager comes with a defined set of rules that ensures the appropriate protection of files on most LANs. Most likely you will not need to change your file rules. Some resources, however, may have files (or groups of files) that could benefit from special protection. In these cases, administrators can customize the file rules of these files. For example, to save time and media, you may want Storage Manager to exclude unwanted files such as *.BAK files from backup operations.

System Resource Rules

Because network requirements vary depending on the environment, corporate policy, government specifications, etc., users may find it necessary to customize their system to meet defined requirements.

Storage Manager defines a number of rules on protected resources. Storage Manager's default rules are shown in the table below. These rules are set in the root directory of each protected resource for the * filename pattern.

System Rules for Volume Resources ("*" Files)	
Operation	**Rule**
Backup	**Include** The Include rule ensures that every file will be backed up whenever it changes.
Archive	**After 6 Weeks** The archive rule for volume resources ensures that permanent copies of files are written to media if they have not been modified for six weeks.
Migrate	**After 12 Weeks** The migrate rule for volume resources ensures that a file will be eligible if it hasn't been accessed for at least 12 weeks and it is fully protected.

System Rules for Non-Volume Resources	
Operation	**Rule**
Backup	**Include** Include ensures that every file (unless covered by a more specific rule) will be backed up whenever it changes.
Archive	**On Demand** The archive rule ensures that these files will be archived if specifically requested.
Migrate	**Exclude** The migrate rule ensures that files are never deleted from disk.

NOTE: Non-volume resources are not eligible for automatic archive operations or migration because they do not support Modify or Last Access Date attributes which Storage Manager uses to determine eligibility.

Time-relative rules (such as **After 6 Weeks**) use the current system date and the DOS file date/time stamp. The exception to this is migration. Migration uses the Last Accessed Date date information instead of the DOS file date, since migration eligibility is determined by a file's usage (both reading and writing), and not simply by how often it is modified.

See page 9-30 for other system file rules.

How Rules Affect Resources, Directories, and Files

Rules may be defined for an entire resource (although not for an entire server), a directory, a group of files, or an individual file. By default, when you create a rule, all files that match a filename pattern in the current directory are affected. The filename pattern can include wild card characters or a specific filename.

- A rule is more specific if it occurs farther down in a directory tree.
- A rule is more specific if it is defined with a more restrictive (less generic) filename pattern.

Any rule in a subdirectory takes precedence over rules in the directories above. If two rules are defined in the same directory, the more specific one takes precedence for the files it covers.

For example, "*" is the least specific filename possible, and an individual filename (ABC.WK1) is the most specific possible. The following list of filename patterns is arranged from least specific to most specific.

* (Least specific)
.W
*.WK?
*.WK1
A*.WK1
ABC.WK1 (Most specific)

If rules were defined for all six filename patterns in a single directory in the above example:

- The ABC.WK1 rules would be the effective rules for the file ABC.WK1.
- Any WK1 file that started with an A (except ABC.WK1) would be covered by the A*.WK1 rules. All other WK1 files would be covered by the *.WK1 rules.
- Any files with an extension of WKS would be covered by the *.WK? rules. The *.W* rules would cover any files that have an

extension beginning with "W," unless they were covered by a more specific rule.

- All other files would be covered by the * rules.

Enhancing the Effect of a Rule

By default, the program applies a new rule only to matching files within the current directory. You can determine whether the program will apply the file rule to like-named files in subdirectories. The **Apply to Subtree** option allows you to control the impact of a rule. You can turn on the **Apply to Subtree** option and apply the new rule to matching files along the subtree. For example, if you select this option when creating a rule for the filename pattern "*.WK*" at the root of the resource (the "\" directory), all files on the entire resource matching that pattern are affected.

The procedure for adding file-specific rules is detailed below in the "*Adding Rules*" section.

NOTE: To be protected, all files must be governed by a set of file rules. To ensure that all files on your protected resources are covered by file rules, you cannot turn off the **Apply to Subtree** option for system rules. System rules are identified by the Palindrome logo on the Rule List window.

Changing, Adding, and Deleting Rules

This section describes how to change, add and delete rules to customize Storage Manager to your environment. Rules allow you to refine your operations by expediting, delaying, or preventing the protection of certain files. You can add, delete, and edit file rules.

Changing Rules

To change a rule

1. From the File Rule window, highlight the rule you want to edit. Rules for a filename pattern defined for the current directory appear at the top of the File Rules window. File-specific icons appear next to the filename.
2. Open the Rules menu and select *Edit Rule*. The Rule Definition dialog box appears with the backup, archive, and migrate rules applicable to the currently highlighted file rule.

Rule Definition dialog box

3. For each operation you want to change, select the rule parameter from the list. See the descriptions of rule parameters available for backup, archive, and migration operations beginning on page 9-27.
4. By default, the changes to the updated rule apply only to matching files in the current directory. To apply the updated file rule to a matching filenames throughout the subtree, select the **Apply to Subtree** option.
5. Choose **OK** to save the changes. The File Rules window displays the result of your change.

Adding Rules

Most of your changes to file rules will be due to adding specifically defined rules to supersede system rules.

To add a rule

1. Select the resource on which you want to create a rule.
2. With your cursor at the appropriate directory, open the *View* menu and choose *File Rules*. The File Rules window appears.
3. From the File Rules window, highlight any item whose rule you want to make more specific.
4. Open the Rule menu and select *Insert Rule*. The Rules Definition dialog box appears.
5. In the **Name** parameter, type the file pattern (or specific file) that you want to add a rule for. For example, to add a rule for all files on the resource with the file pattern *.BAK, type ***.BAK**.
6. Specify rules for backup, archive, and migration that apply to this file pattern. Descriptions of parameters specific to each operation a begin on page 9-27.
7. Indicate whether this rule will become effective for subdirectory files.

➤ To apply this rule to subdirectory files, select **Apply to Subtree**.

8. Choose **OK**. The new rule appears in the file window.

Deleting Rules

You can delete a filename pattern rule for a specific file by deleting the rule using the steps below.

NOTE: You cannot delete system rules or edit the **Apply to Subtree** option of system rules. If there are no specific file pattern rules, every file is automatically covered by a set of system rules.

To delete a rule

1. With your cursor at the root of the appropriate directory, open the *View* menu and choose *File Rules*. The File Rules window appears.
2. Highlight the rule you want to delete.
3. Open the Rules menu select *Delete Rule*. The Rule Definition dialog box appears.
4. Confirm that this is the rule you want to delete and choose **OK**. The File Rules window appears. On the directory where the rule originated, you will see that the deleted rule no longer appears at the top of the File Rules window.

   If it is a filename, the rule will be deleted, and files that were covered by that rule will now be controlled by the next most specific rule.

Options for Customizing Rules

The six rule parameters (**Include**, **On Demand**, **Always**, **Exclude**, **After Stability**, **Every Period**) have different uses for backup, archive, and migrate operations. The following section discusses special uses for each and provides a table with a description of the functions for each rule parameter.

Backup Rules

Backups provide a rich selection of interim versions of an evolving file, without permanently dedicating media for all these versions.

The following table summarizes how rules affect backup operations.

Rules for Backing Up Files	
If the Rule is...	**Storage Manager writes the file to media...**
Include	If the file has changed (the archive bit is on).
	NOTE: There are no restrictions to writing files with this rule to non-managed media. The **Back Up Fully Protected Files** and **Back Up if Archived in Same Media Set** parameters override restrictions to backing up files to managed media only.
On Demand	Only if you manually select the file in File Manager or perform a full backup operation through Resource Manager.
	NOTES: Use this rule carefully because this parameter does not protect files through automatic operations. Use this rule for files that do not normally need backups (for example,. *.BAK or *.TMP files).
Always	Even if the current version is on the media set.
	NOTE: Do not use this rule unless you need to make multiple copies on the same media set.
Exclude	Never.
	NOTES: Use this rule for files that are generated from other files that are backed up (for example, *.BAK or *.OBJ files). This rule conserves media and reduces processing time.

Archive Rules

Archives are used to create permanent copies of files. Permanent file copies are important because they:

- Expedite backup operations once files have been archived to three different media sets—no need to back it up over and over again.
- Make safe migration possible, since the program never erases the archive copy from media.

Rules for Archiving Files	
If the rule is...	**Storage Manager writes the file to media...**
After Stability	Once stable for the time period specified.
	NOTE: This is the default parameter. Default=6 Weeks.
On Demand	Only if you manually select the file through File Manager.
	NOTES: The program does not write files with this rule during rotation day operations. This is for files that do not normally need permanent copies (for example, *.BAK or *.TMP files).
Every Period	Once each specified time period during custom (Resource Manager) or automatic jobs.
	NOTES: You can archive a file with this at any time through File Manager. This rule ensures that regularly edited or updated files have permanent copies.
Exclude	Never.
	NOTE: This rule is for files that are generated from other files that are backed up (e.g., *.BAK or *.OBJ files).

Migration Rules

Migration is performed as a custom or automatic migration job. In addition to meeting the migration rule, files are only eligible for automatic migration if they are fully protected. To initiate an automatic migration, the resource must meet or exceed the high water mark.

The following table summarizes how rules affect files when using Migrate operations.

Rules for Migrating Files	
If the rule is...	**Storage Manager removes the file from disk...**
After Stability	During a resource- or file-level operation, if it has not been **accessed** for the specified time period.
	NOTES: This is usually the best choice for the Migrate rule, and will cause files to be included in a migration list if they are completely protected, and have not been accessed for the defined time period. This is the default parameter (Default=12 Weeks). For automatic migration to occur, the resource must also be at or above the configured high water mark. If you select the file through File Manager and the file has at least once archive copy, the program migrates the file regardless of the After Stability rule.
On Demand	Only when you select it through File Manager.
	NOTE: May be useful for SYS:SYSTEM and SYS:PUBLIC directories and possibly *.COM and *.EXE files.
Exclude	Never.
	NOTE: This rule is appropriate for files you want to keep on disk.

NOTE: Other backup programs and some anti-virus software will alter the Last Access Date of your files. If using anti-virus software, be sure to configure it so it retains the Last Access Date, otherwise you may have to manually select certain files to be migrated.

Other System Rules

Storage Manager automatically assigns file-specific rules for its own databases, workstation volumes, and NetWare servers. Note that although the *.PAC file rules are set to **Exclude**, the program protects these files by writing them to their own DH and DC sessions at every full backup, incremental, or differential operation.

Examples of Rules

This section provides you with some typical rules you might set up in your own system for particular types of files.

To expedite backups and conserve media space

➤ Add a rule in the root directory for *.BAK or other extensions, and set the rules to **Backup/On Demand**, **Archive/On Demand**, **Migrate/On Demand**. This prevents BAK files from being backed up during resource-level operations. You can still select the file for an operation through File Manager.

Network Management Tools

This will prevent your network management tools from being migrated, even if they are infrequently used.

SYS:NETTOOLS directory: (*)

The following rules are recommended:

- Backup—**Include**
- Archive—**After 1 Week**
- Migrate—**On Demand**

Applications

This will limit migration of applications and their associated files (drivers, overlays, etc.) to those that have not been used in over two years. In most networks, application directories tend not to develop large numbers of abandoned files, the prime candidates for migration.

SYS:APPS directory (where application files are stored): (*)

The following rules are recommended:

- Backup—**Include**
- Archive—**After 6 Weeks**
- Migrate—**After 100 Weeks**

Users' Directories

These recommendations will quickly archive files to speed up the backup operation (limiting the number of files to be backed up), and will make dormant files the first candidates for migration.

SYS:USERS directory (or the directory under which your users have their home directories): (*)

The following rules are recommended:

- Backup—**Include**
- Archive—**After 1 Week**
- Migrate—**After 12 Weeks**

Database and Spreadsheet Files

Some database and worksheet files are very important, and should be archived whenever possible, but not migrated too quickly. (The archive rule should be reset to a longer period if the evolving databases or spreadsheets are very large. Frequently archiving these files will increase the amount of media used.)

SYS:\ (*.DBF and *.WK?)

The following rules are recommended:

- Backup—Include
- Archive—After 1 week
- Migrate—**After 53 weeks**

Temporary Files or Backup Copy Files

This concept has been referred to repeatedly in this chapter and is included here for completeness. Use these rules for files that do not need to be written to media.

SYS:\ (*.BAK) or (*.TMP)

The following rules are recommended:

- Backup—**On Demand**
- Archive—**On Demand**
- Migrate—**On Demand**

If this rule is used, make sure that your users understand that important files must not be given BAK or TMP extensions.

Files that Change Every Day

It may be important to periodically archive a file like an accounts payable file or a database file, even if these files never become stable.

SYS:\ACCOUNTING DIRECTORY: (*.DBF)

The following rules are recommended:

- Backup—**Include**
- Archive—**Every 4 weeks**
- Migrate—**On Demand**

✓ ***NOTE:*** You can accomplish the same results by retiring monthly media sets in a GFS rotation pattern or scheduling custom archive or backup jobs to non-managed media every four weeks.

Word Processing Files

SYS:USERNAME (directory for word processing documents): (*.WP)

The following rules are recommended:

- Backup—**Include**
- Archive—**After 1 week**
- Migrate—**After 6 weeks**

The word processing files would be fully protected quickly, allowing for quick migration. You can lengthen the migration time frame if you find that users often need access to these files.

Other Storage Manager System Rules	Backup	Archive	Migrate
Resources with File History Database			
\PAL (Installation Directory)			
ENTR???.PAC	On Demand	On Demand	On Demand
AS??.PAC	Exclude	Exclude	Exclude
ST??.PAC	Exclude	Exclude	Exclude
AV*.PAC	Exclude	Exclude	Exclude
TMP*	Exclude	Exclude	Exclude
COMMANDS	Exclude	Exclude	Exclude
Resources with System Control Database			
\PNA (Installation Directory)			
***.HLP**	Exclude	Exclude	Exclude
***.EXE**	Include	After 6 Weeks	Exclude
***.RSF**	Exclude	Exclude	Exclude
AS*.PAC	Exclude	Exclude	Exclude
TMPDB*	Exclude	Exclude	Exclude
DOS Workstation Volumes			
\CONFIG.SYS	Include	After 6 Weeks	Exclude
\COMMAND.COM	Include	After 6 Weeks	Exclude
\AUTOEXEC.BAT	Include	After 6 Weeks	Exclude
***.SYS**	Include	After 6 Weeks	Exclude
\IBM*.COM	Include	After 6 Weeks	Exclude
OS/2 Workstation Volumes			
\CONFIG.SYS	Include	After 6 Weeks	Exclude
\EA DATA. SF	Exclude	Exclude	Exclude
\WP ROOT. SF	Include	After 6 Weeks	Exclude
\STARTUP.CMD	Include	After 6 Weeks	Exclude
\OS2LDR	Include	After 6 Weeks	Exclude
\OS2LDR.MSG	Include	After 6 Weeks	Exclude

Other Storage Manager System Rules	Backup	Archive	Migrate
\OS2KRNL	Include	After 6 Weeks	Exclude
\OS2BOOT	Include	After 6 Weeks	Exclude
\NET.CFG	Include	After 6 Weeks	Exclude
\SWAPPER.DAT	Exclude	Exclude	Exclude
\OS2			
CMD.EXE	Include	After 6 Weeks	Exclude
***.INI**	Include	After 6 Weeks	Exclude

Rules for NetWare Volumes	Backup	Archive	Migrate
***.Q**	Exclude	Exclude	Exclude
\Trash Can Usage Map	Exclude	Exclude	Exclude
Q_*	Exclude	Exclude	Exclude
Q$*	Exclude	Exclude	Exclude
\DIRSTAMP.SYS	Exclude	Exclude	Exclude
SYS:			
\BACKOUT.TTS	Exclude	Exclude	Exclude
\SYSTEM			
*****	Include	After 1 Week	On Demand
SYS$LOG.ERR	Include	After 1 Weeks	On Demand
TSA*.DER	Exclude	Exclude	Exclude
\PUBLIC			
*****	Include	After 1 Week	On Demand
\LOGIN			
*****	Include	After 6 Weeks	On Demand
\MAIL			
*****	Include	After 6 Weeks	On Demand

End User File Manager

The end user version of File Manager provides the essential backup and restore operations. To perform operations, end users must have access to File Manager (PALFILER.EXE) and be given rights to the File History Databases of their files.

To give end users access to File Manager

1. During installation, File Manager is copied to the installation directory. You can allow users to access the installation directory or copy PALFILER.EXE to one or more public directories.

➤ If you copy PALFILER.EXE to a public directory, be sure to also copy the resource (*.RSF), help (*.HLP), and *.DLL files from the installation directory to the public directory.

2. Grant users Read and File Scan rights to the Storage Manager installation directory (or public directory) so they can access PALFILER.EXE.

➤ If you have distributed File History Databases, grant rights to the installation directory of each of those servers.

➤ If you have a group EVERYONE, grant that group Read and File Scan rights to the same the directories.

➤ If you have multiple installations or PALFILER.EXE exists on servers other than your installation server, create a File Manager rights user with Read and File Scan rights to the installation directory. The File Manager rights user allows end users who are not attached to the installation server to access the File History Database. You will specify this user later ("*Configuring Access to an Installation*" section).

To create the File Manager icon

1. From the Windows desktop of each end user's workstation, open the File menu and select *New*. Create the program group.

2. Open the File menu and select *New*. Create a new program item.
3. Type **File Manager** in the **Description** parameter.
4. Use the **Browse** button to complete the command line. Select the public directory path and PALFILER.EXE.
5. Choose **OK** to confirm the properties. At the Network Path Specified prompt, choose **Yes** to continue .

Configuring Access to an Installation

If you copy PALFILER.EXE to a public directory or if you have multiple installations, you must configure the Storage Manager installation(s) that users can access when using File Manager.

If you have multiple copies of PALFILER.EXE

1. Access File Manager.
2. Open the File menu and select *Enterprise Setup*. The Installation Configuration dialog box appears.

Installation Configuration dialog box

3. Choose **Insert**.

4. From the Select Installation dialog box, select the installation you want end users to have access to and choose **OK**.

5. Choose the **User** button to configure the name and password of the File Manager rights user. This is the user that you created above ("To give end users access to File Manager" steps).

Default Login dialog box

6. Choose **OK**.

7. Choose **Close** to exit.

   Only administrators (defined on the Admin List in Configuration Manager) can configure rules, add installations, etc. within File Manager. Whenever users access a resource (using the drive bar or the File/*Open Resource* option), they will be prompted for a login name and password. While users access the Installation Configuration dialog box, they cannot make any changes since they do not have the appropriate NetWare rights to the installation.

   To submit jobs, end users must be defined in the User List in Configuration Manager or the jobs will fail. The group EVERYONE is actually added to the User List during the install.

Configuring End User Workstations

If you are protecting workstations and you want end users to be able to submit backup and restore jobs for their workstation files, each workstation must be configured. Although end users' local drives are on the Protected Resource List, they cannot access database records for their own workstations by default. Use the Preferences option to configure end users to view the files and database records of their local drive.

See also Appendix E, "Recalling Files," for information about automatic recall and workstation recall agents.

To configure an end user's protected workstation

1. In File Manager, open the File menu and select *Preferences*.

Preferences dialog box

2. Specify the workstation name as it appears in the Protected Resource List.

- To configure workstation names using an environment variable in a system login script, select **Environment**. This is the default selection. Use "WSNAME" (or a another name you specify) in the login script to configure workstations automatically.
- If you are not using an environment variable for the names of the protected workstations, select **Specific**. You must type the workstation name as it appears in the Protected Resource List. With this option you must configure the name at each workstation.

3. Choose **OK**.

Notification

End users configure notification through *Preferences*. Storage Manager can notify end users about the status of restore requests. Each user can choose how they want to be notified prior to submitting the request.

To receive notification through e-mail

1. Open the File menu and select *Preferences*. The Preferences dialog box appears. File Manager's Preferences dialog box is similar to those of the other managers. The drive bar is an additional option.
2. Specify the notification you want to receive. You can specify one or both types.

- Select **Novell Send**. This operation notifies end users if a restore job failed or succeeded.
- Select **E-Mail**. Choose a method for specifying e-mail addresses: **Specific**—Select this option to specify the e-mail address for each individual workstation. Enter your e-mail account name and address in the **E-mail Address** text box. The correct format is "USER@WORKGROUP" (for example, "JSMITH@PALINDRO").

  Environment—Select this option to automatically use an e-mail environment variable to configure all e-mail reports. Use "FMUSER" (or another name you specify).

3. Choose **OK** to save the notification parameters.

Chapter 10

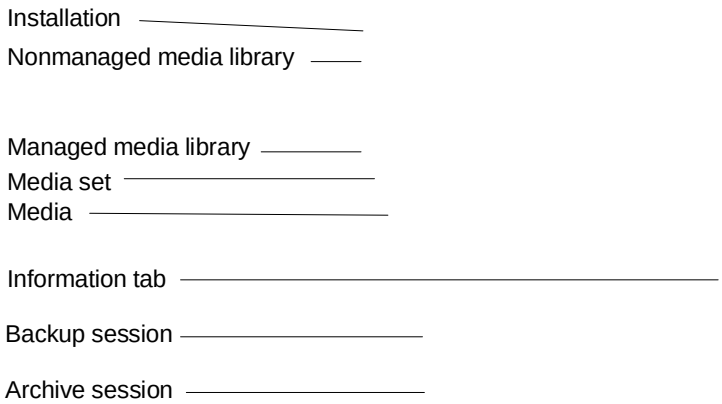
Managing Media

Overview

This chapter describes how to:

- View the contents of media
- De-activate and remove media in your managed media set
- Perform physical media operations

Viewing the Media Tree



Media Manager's main window

Media Manager provides detailed information on media created by the current installation, including:

- Number of media within each media set
- Percentage of capacity utilized on the media
- Detailed session information

Managed media are located in the managed media library. Within the managed media library, media sets appear in order from the least frequently used media set through the most frequently used.

The program does not create a non-managed library until you create a custom job that specifies non-managed media.

Since non-managed media are not required for rotation, they may be moved permanently off-site. Non-managed media are labeled by the user. When creating jobs written to non-managed media, you can also prevent the program from recording the contents of the session in the File History Database.

In all media sets, the most recently written sessions appear at the top of the list. While all media created for the current library appear in the tree, any sessions that were not tracked in the File History Database, do not appear. The prefix "CP" indicates a backup session; the prefix "SV" indicates an archive session.

NOTE: An optical disk is considered a single media, although each side is labeled separately. For example, media A:1 and A:2 may refer to different sides of the same disk.

Refreshing the Media Tree

Occasionally, you may want to refresh the media tree to display the most recent operations, such as a *Forget* or backup operation, performed by you or other users.

To view the most current media tree

➤ Open the Operations menu and select *Refresh Media Tree*. The media tree displays the most current information about your media library.

Media Manager Tool Bar

The Media Manager tool bar provides a short cut to commonly used operations:

Display Mounted Media—Show the Mounted Media window.

Restore—Restore the selected item(s).

Define Filter—Specify the filename pattern and/or other criteria that the program should search the session for.

Enable Filter—Apply the defined filter and display only those files that match the filename pattern and/or criteria for the current session.

Help—Open the Help menu.

Media Summary Report

Storage Manager can print a list of media currently configured for Storage Manager operations. See page 7-36 for information about viewing and printing reports including the Media Summary report.

Viewing Directories and Files

The session window displays the directories and files from a single volume that were written to a particular session. All sessions written by automatic jobs are tracked in the File History Database. By tagging directories and files, you can restore the tagged items to the disk. See page 9-12 for information about finding files and filtering the files. Media Manager provides a subset of the parameters described in File Manager.

To view the session window

1. Highlight the session for which you want to display directories and files.
2. Open the View menu and select *Session Window*.

➤ You can also double-click the highlighted session to view the session window.

3. The program begins building the first directory and file windows. This can take some time, depending on the size and complexity of the directory structure. The program allows you to pause from building after it completes a directory. You can view the file window or perform an activity elsewhere while the program is building the directory structure.

➤ To interrupt the building process, choose the **Pause** button after the program builds the directory you want to see. Choose the **Resume** button to let the program continue building directories.

Database Session window

In this window, the volume appears at the top of the tree, followed by a list of directories. The file information includes the date and time stamp, and byte size of each file. The session window also displays "suspect" file information.

4. View the desired directories and files. To view files and directories contained in untracked sessions, you must journal the media. See page 10-9 for information about journaling.

Viewing Mounted Media

While the session window generated by the View/*Session Window* option displays the media records in the File History Database, the session information displayed in the Mounted Media window is read directly from the media.

Through the Mounted Media window, you can read media containing untracked sessions written by the current installation and PALDF- or SIDF-formatted media. Storage Manager also provides information about the type of media mounted and any bar code label.

Mounted Media window

Parameter	Description
Location	The name of the device the media is loaded on. If the device is an autoloader, this parameter also indicates the slot position of the media.
Media	The label of the media. If the media has no label, the program identifies the media as a **Clean** (cleaning tape), **Blank**, **Unformatted** (new optical disks), or **Unknown** media (the program does not recognized the file system).

Parameter	Description
Format	The data format of the media: **SIDF**, **PALDF**, or **Unknown**. SIDF refers to System Independent Data Format. PALDF is a Palindrome proprietary format used in earlier versions. Unknown indicates a format not recognized by the program.
Type	The type of media loaded, for example, 4mm DAT.
Bar Code	The numbers corresponding to the media's bar code label, if applicable.

From the Mounted Media window you can access physical media operations listed in the Operations menu. *Journal*, *Verify*, and *Format* options are also available as control buttons on the window. Your autoloader may require additional instruction to perform operations. See the *AutoLoader Software Guide* for information about performing operations using the Robotics menu.

Restoring Directories and Files

You can restore directories and files from tracked or untracked sessions. To restore tracked files, File Manager provides the most convenient method of restoring. To restore from untracked sessions or files, you must use Media Manager. First, journal the mounted media with the untracked session. From that point you can choose to restore an entire session or select a session to view its directories and files.

See page 6-11 for details on restoring files and directories through Media Manager.

Journaling Media

The *Journal* option displays the contents on a physical media. While the program performs this operation, you can access another program or manager, but do not exit this manager. You will abort the journal operation.

To journal a media

1. Load the media you want to journal, if it is not currently loaded.
2. Open the View menu and select *Mounted Media*. The Mounted Media window appears.
3. Highlight one of the media on the Mounted Media window.
4. Open the Operations menu and select *Journal*. The program always performs the *Journal* operation in attended mode (**Prompt With Questions** option is turned off). The Session List window appears. The media label also appears in the title bar.

Session List window

Parameter	Description
Name	The type of session and session number.
Elapsed Time	Displays the time that passes between initiating the journal operation and ending the journal operation.
Archives	The number bytes used for archive files. This is also expressed as a percentage of the media's total capacity.
Backups	The number of bytes used for backup files. This is also expressed as a percentage of the media's total capacity.
Available	The number of bytes available for writing additional sessions. This is also expressed as a percentage of the media's total capacity.
Capacity	The number of bytes in the media's total storage capacity. This is also expressed as a percentage of the media's total capacity.
Resource	The resource on which the session was written.There are four types of sessions: **SV** —Archive sessions, never erased **CP** —Backup sessions, eventually erased **DC** —System Control Database **DH** —File History Database
Session	The name of the session.
Items	The number of items contained in the session.
Size	The size of the session in megabytes.
Date	The date on which the session was written.
Time	The time at which the session was written.
Phase	The activity of the user interface. Usually, the phase will be **Opening the media**.
State	The state of the device being used for the operation being performed on the mounted media.

The backup and archive sessions are always visible on the media tree. The database sessions are only visible through the *Journal* operation.

➤ To view the directories and files residing on a session, highlight a session and choose the **View** button. The media session window appears. The file window lists files located under the highlighted directory. Locate, sort, and build directories just as you would for the database's session window.

5. The program prompts you to indicate whether you are finished journaling the media. Choose **Yes** to end journaling and exit the mounted media's session window

6. You can end the operation at any time by choosing the **Close** button in the media session and the Session List windows.

De-activating and Removing Media

A significant number of soft errors indicates that you may need to de-activate, or, in more severe cases, remove the media records from your database. The *Retire* and *Forget* options allow you to prevent data from being written to damaged media by removing the media from your rotation. Or, in the case of non-managed media, removing the media from the list of existing media. You should consider these options when:

- The System Messages window contains messages indicating that a media's integrity is questionable.
- A *Verify* operation results in excessive soft errors. If the errors exceed the recommended threshold for the type of media you are using, the media is probably damaged.

Before you retire (de-activate) or forget (remove) media, you may want to verify that the device is not causing the soft errors. To ensure that the errors are not due to hardware failures, perform the media troubleshooting tests beginning on page 11-18.

Retiring Media

If only certain sessions on the tape are damaged, use the *Retire* option. Retiring a media maintains the media in the media set, but removes it from your active rotation. The next time the program rotates to this media set, it will require a blank media and continue the media number sequence. For example, if you retire media MONDAY:1 and MONDAY:2, the new media added to the set will be MONDAY:3 and MONDAY:4, if necessary. You can still restore files using retired media.

When you retire the media, the program updates the File History Database to reflect the change in the protection status of the files.

TIP: After you perform a full backup operation, the *Retire* option is useful for a snapshot of your installation and moving the media off site permanently.

To retire media

1. Highlight the appropriate icon. To retire all of the media in a media set, select the media set icon. You cannot select media from multiple media sets for a single operation.
2. Open the Operations menu and select *Retire*. The program prompts you to confirm the operation. The media continues to be represented in the tree since you can still perform restore operations with it. During the next automatic job, the program updates the status records in the File History Database to reflect the change in the media's status.

TIP: After performing a *Retire* operation, you may want to update the media's status in the database immediately. This operation will immediately remove the media from the rotation sequence. Through Resource Manager, perform a database verification (Operations/*History Database Maintenance*/**Verify**). This operation updates your File History Database so that the protection status of your files is updated immediately.

Forgetting Media

When you do not want or cannot use the media or session for future restore operations, use the *Forget* option. The *Forget* option should be reserved for media or sessions that are virtually unreadable. You should use your *Forget* option if you receive a fatal tape error and an Operations/*Verify* operation also produces unacceptable errors.

The *Forget* option clears all references to those file copies from the File History Databases. Forgotten media or sessions disappear from the media tree. *Forget* should be used only when you have located damaged or lost sessions on a media. If necessary, you can restore data from a forgotten media or session by using the Mounted Media window.

NOTE: The program does not erase forgotten sessions and media. While they no longer appear in the database, the program can still display forgotten sessions through the Mounted Media window.

Because archive copies written to forgotten sessions no longer count toward full protection, some files may no longer be fully protected. If any files still exist on disk, Storage Manager writes files on forgotten sessions to another media set on rotation day. The program counts these new copies toward each file's protection status.

To forget a session or media

1. Highlight the media icon. You can only select one item for each operation.

2. Open the Operations menu and select *Forget.* The program prompts you to confirm the operation. The item disappears from the media tree. During the next automatic job, the program updates the media records in the File History Database to reflect the change in the file version's status.

✓

TIP: After performing a *Forget* operation, you may want to update the media's rotation status in the database immediately. Through Resource Manager, perform a database verification (Operations/*History Database Maintenance*/**Verify**).

Other Utility Operations

You must perform the following operations from the Mounted Media window.

Secure Erase

Only 8mm and QIC drives support the *Secure Erase* option. Use *Secure Erase* to erase the entire length of a tape to prevent any data on the media from being recovered. To simply re-use media, use the *Format* option.

For some drives this process may take several hours. A bulk eraser might erase the media more quickly than this operation.

To erase data from media

➤ Select the media you want to erase. Open the Operations menu and select *Secure Erase*. If you try to erase a media that is in active rotation, the program warns you. Storage Manager prompts you to confirm the operation.

If the media already has sessions written by Storage Manager, the program warns you that sessions will be destroyed when it erases the media.

Format

Use the *Format* option to format new media or to re-use media. *Format* is required on non-SMS formatted media before using with Storage Manager and on Random Access Devices such as optical devices. The formatting time varies with the media's length and capacity. You **do not** need to format new, blank tapes "out of the box." You should use Operations/*Format* only when you are recycling used media.

To format a media

➤ Select the media you want to format. Open the Operations menu and select *Format*.

If the media already has sessions written by Storage Manager, the program warns you that sessions will be destroyed when it formats the media.

WARNING: Formatting active media in your current media library is not recommended; you risk losing specific file versions. Storage Manager re-writes files that are still on disk to another media at the next rotation.

Tension

The *Tension* option simply spins forward and backward through the current tape. This is useful for tensioning infrequently used tapes, to minimize potential damage to the tape caused by magnetic print-through. Storage Manager performs frequent start and stop operations on the tape. When using older backup devices such as DC 6000 and 8mm (2.2GB) tape drives, you should tension the tape. It is a good idea to tension your tapes after every other use of the tape, regardless of the operation you perform.

This feature is not supported on DDS DAT or 8mm (5.0GB) drives.

To tension a tape

➤ Select the media you want to tension. Open the Operations menu and select *Tension.* Storage Manager prompts you to confirm the operation.

Verify

Use *Verify* to verify that the contents of a media are readable using ECC (Error Correcting Code) and CRC (Cyclical Redundancy Code) checking. Any errors found will be reported to the screen and to the System Messages window. The program can only perform this operation if the **CRC Data Verification Level for Backups** parameter was set to **Calculate** or **Verify** at the time the sessions were written.

To perform a *Verify* operation

➤ Select the media you want to perform the operation on. Open the Operations menu and select *Verify*. Storage Manager prompts you to confirm the operation.

Copy

Copy allows you to copy the contents of one backup media to another. Two backup devices are required. The two backup media do not have to be the same type. For example, you can copy from a DC 6000 drive to a DDS-DAT drive.

Examples of Media Types Used in Copy Operations

Duplicate media are considered non-managed; the program does not request duplicate media for automatic jobs. For restore operations, Storage Manager treats the duplicate exactly as it would the original so you can restore from it at anytime.

Benefits

The benefits of the utility can be seen in a number of situations:

- Moving backups offsite—Copy your daily backup sessions to duplicate media to move the duplicate offsite. Duplicate media do not appear in the media library.
- Restoring when original media is forgotten or retired—If your original media has unrecoverable physical errors, you can retire or forget it, and, if necessary, restore data from the duplicate media.
- Upgrading backup media—you can copy an older library on to new media in case you need to restore from it in the future.

Once a duplicate media is created, Storage Manager can only copy the source media to the duplicate media.

To copy media

1. Load blank media in the target device and the source media in the source device.
2. Highlight the mounted media you want to copy (the source media).
3. Open the Operations menu and select *Copy*. The Copy dialog box appears listing the configured devices.
4. Specify the source device and target device.
5. Choose **OK** to submit the job. If media is not mounted in either device, a pop-up window appears. The media will be assigned “COPY” as its type with the source media’s label as its internal label name.

- If the source media has more data than can fit on the target media, the program notifies you that it did not copy the session. You must then insert a new target media. Next, submit another copy operation beginning with the session which was interrupted.

Using Duplicate Media

Restore Operations

When performing restore operations, Storage Manager will treat the duplicate media as an original. You would most likely want to use a duplicate media if your original was damaged or lost.

If during a restore operation, Storage Manager requests a specific media, you may substitute the duplicate. However, you must ensure that your duplicate has been kept up-to-date, otherwise, the files on the original may not exist on the duplicate.

Appending to Duplicate Media

You can append to the duplicate media, but only if you are copying from the same source media used for the original copy operation. This allows you to copy data from a media numerous times without having to erase it first. Sessions that already exist on the duplicate will not be copied again.

For example, if you copied managed media MEDIA:A:1 and then later updated MEDIA:A:1 and copied it again, only the changed data on MEDIA:A:1 would get copied to your duplicate media.

Copying Media after Backup Operations

If you want to immediately copy a media after a backup is complete, link the copy operation to follow a backup operation. You need at least two devices, the device on which the backup is written and the device with blank media (or existing duplicate media if you are appending) to which the copy will be written.

Writing Backup Sessions

Storage Manager **cannot** perform backup operations on duplicate media and will reject all requested operations, even in unattended mode (When **Prompt With Questions** option is turned off).

Maintaining Your Media

Tape Handling

Tapes are very sensitive to environmental conditions. Exercise great care in storing and using them. Physical damage to the tape is often the root cause of unsuccessful recovery from backup media. This damage can be caused by equipment, environment, or mishandling.

The second most probable cause of tape failure is contamination. Contamination can pre-exist, originate, or be created during every phase of the storage process.

If you take care of your tape drive and store the tapes according to recommended procedures below, you can successfully recover data from media that is over 10 years old!

Palindrome recommends the following procedures to enhance the shelf life of your company's precious data.

For information on maintaining your backup device, see Appendix B, "Maintaining Your Tape Drive."

Use Only Data-certified Tapes

Palindrome recommends using high-quality tapes and cleaning the tape drive after the initial pass of a new tape cartridge.

NOTE: Use only data grade tape cartridges! **Do not** use video or analog grade tapes, no matter how economically appealing they may be. They are generally of a lesser quality, and are not approved for use with tape drives.

Palindrome customers have experienced a greater number of tape errors using unapproved tapes than with approved tapes. Additionally, use of contaminated tapes may transfer contaminates to the tape drive heads which can lead to contamination of quality tapes.

TIP: Contact Palindrome's BBS and download the APRVMED.ASC to obtain a list of approved media.

Keep Your Tapes Clean

Dirty tape drive heads and media account for one of the most probable reasons for recovery failure. Keep the tapes clean in both the operation and storage areas. Do not permit smoking, eating, or drinking in the area where you perform backups. Keep everything clean.

The tape drive you use for recording backup data must also be exceptionally clean. Also, be sure to operate the tape drive using the manufacturer's electrical and mechanical specifications.

NOTE: Storage Manager performs frequent start and stop operations on the tape. When using older backup devices such as DC 6000 and 8mm (2.2GB) tape drives, you should tension the tape. Tension your tapes after every other use of the tape, regardless of the operation you perform. DDS DAT and 8mm, 5GB tapes cannot be tensioned.

Store Your Tapes Properly

Store the tapes on edge. Do not stack them horizontally.

Store your cartridges in their protective box, away from heat sources and electromagnetic fields when they are not mounted in the tape drive. Do not place cartridges on the computer, monitor, or any other peripheral device.

✓ ***TIP:*** Do not locate a tape drive unit near a printer, a copier, or any other source of magnetic fields or paper dust.

Chapter 11

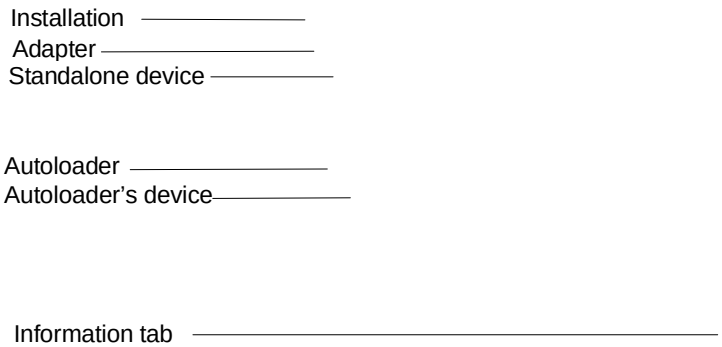
Managing Devices

Overview

This chapter describes how to:

- Add and remove configured devices
- Test devices
- Troubleshoot soft errors
- Prioritize devices for specific operations

Introduction



Device Manager's main window

The device tree displays the connected devices that were turned on at installation or when you most recently scanned the SCSI bus. To display any devices that may have been turned on since you accessed Device Manager, open the Operations menu and select *Scan for Devices*. Any devices that were recently turned on appear in the window.

The device tree includes all devices on the SCSI bus of your Storage Manager installation server, whether or not you have added them as configured devices. Configured devices appear with logical names beside the device drive icons.

Non-configured devices appear with the label "Not Configured." SCSI hard drives appear on the device tree, and the tree indicates their type, such as a CD-ROM or Direct Access Storage Device. However, SCSI hard drives are not available for Storage Manager operations.

✓

TIP: You may want to collapse the adapter icon of any SCSI hard drive on the device tree. Collapsing the adapter icon will hide the non-configurable device and may help to avoid confusion later. Use the Tree/*Collapse* option.

Storage Manager allows you to use different types of devices (optical and tape drives, for example) for your backup operations. These devices can be daisy-chained or attached to separate SCSI host adapters. Once you have installed the devices, you can then configure them for different operations, if necessary.

See the *Installation Guide* for more information about installing devices.

Device Manager Tool Bar

The Device Manager tool bar provides a short cut to commonly used operations:

Add Device—Add an unconfigured device

Remove Device—Remove a configured device

Scan for Devices—Search for any new devices on the bus.

Help—Open the Help menu.

Adding a Device

When you first install Storage Manager, the program scans the SCSI bus to identify all connected devices. You can configure one or more devices during installation. At installation, you can only configure the drive of an autoloader. You must first install AutoLoader Software before configuring the autoloader (specifically, the robotic arm—also known as a "media changer"). The remaining backup devices appear as "Not Configured" in the devices window.

To add a device

1. Be sure that the device you want to configure is turned on.

➤ If the device was turned off, you must turn it on and scan the SCSI bus again. Open the Operations menu in Device Manager and choose the *Scan for Devices* option.

2. Highlight the device icon, open the Operations menu, and select *Add Device*. The "Not Configured" status disappears from the tree.

➤ To add an autoloader, highlight the device icon, open the Operations menu and select *Add Device*. If there are multiple devices, add these first before adding the autoloader. Highlight the autoloader icon. Select *Add Device*. Notice that the device icon appears connected to the autoloader icon and no longer appears as an independent item on the tree.

Once you have added the device, its logical name is stored in the System Control Database. For more information about using an autoloader to perform operations, see the *AutoLoader Software Guide*.

✓ ***TIP:*** If you have multiple backup devices, see page 5-25 for information on enabling concurrency. See page 2-23 for a description of concurrent backup operations and concurrent jobs.

Assigning a Logical Name to a Device

Storage Manager automatically assigns configured devices a logical name such as “DEFAULT_0_1”. The first number refers to its adapter number and the second number refers to the device’s SCSI ID. You may want to give a device a more descriptive logical name.

To change the logical name of a device

1. From the device window, highlight a device.
2. Open the Operations menu and select the *Edit Device* option. The Configure Device dialog box appears.

Configure Device dialog box

3. In the **Logical Name** parameter, type the name you want to call the device.
4. Choose **OK** to save the name.

Near Line Device

The **Near Line Device** option allows you to reserve a device exclusively for your near line set. That is, the device contains only your near line set and therefore will only be used when the near line set is the preferred or eligible media for a backup or restore operation.

A near line set is not required for managing storage capacity; it simply ensures that copies of migrated files are always on site. The near line set is the most frequently rotated set (that is the A media set.

In order to take advantage of the near line device, you must have at least two backup devices. You must also have configured a near line set in Configuration Manager.

See page 4-18 for configuring the near line media set.

To configure a near line device

1. Highlight the device icon.
2. Open the Operations menu and select *Edit Device*. The Configure Device dialog box appears.
3. Turn on the **Near Line Device** parameter.
4. Choose **OK**.

Changing the SCSI Address

If you are moving a device to another SCSI card or if you changed the SCSI ID, Device Manager can no longer identify the device (it appears dimmed on the device tree). You can add the device again to the device tree by deleting the device from the device tree and selecting *Operations/Scan for Devices*.

Upgrading Devices

Upgrading your backup device can enhance the flexibility and performance of your Storage Manager installation. If your new device uses a different media type, you can continue using the current media library. Storage Manager simply adds the new media to the managed media sets.

NOTE: If you are upgrading firmware, you must unload PALMEDIA.NLM from the server before adding the new firmware. If you do not, the SCSI bus "locks up." At the server console prompt, type **UNLOAD PALMEDIA**. After you have upgraded the firmware, return to the server console and type **LOAD PALMEDIA**. NetWare adds the PALMEDIA module.

To upgrade a device

1. Open the File menu and select *Scan for Devices*. The new device appears in the device tree.
2. Highlight the new device.
3. Open the File menu and select *Add Device*.
4. Edit the parameters for the new device if appropriate. For example, if you are adding an autoloader, edit the new device's slot configuration.

Upgrading to a Different Media Type

If the new device also entails a media type change (e.g., upgrading from 4mm to 8mm), you may want to configure the original device for restore operations only. Set the operational priorities using the Operations/*Edit Device* option. At the next rotation the program will continue to request the original media.

To use only the new media type for write operations, retire the original media from the managed media sets. The program will automatically request these media for restore operations if necessary.

Removing a Device

To remove a device from the configured device list

➤ If you are removing a single tape drive, highlight the device icon, open the Operations menu, and select *Remove Device.*

➤ If you are removing an autoloader and its device from the configured device list, highlight the autoloader icon, open the Operations menu and select *Remove Device*. Highlight the device icon and select *Remove Device*. If there are multiple drives in the autoloader, repeat this task for each device.

Once you have removed the device, its logical name is removed from the System Control Database. The device now appears in the device window as "Not Configured."

NOTE: If a device on your device window appears dimmed, the device has been disabled. It may have been turned off or unplugged since you most recently scanned the SCSI Bus. Check the status of the device and scan the bus for devices.

Device Summary Report

Storage Manager can print a list of devices currently configured for Storage Manager operations. See page 7-36 for information about viewing and printing the Device Summary report.

Editing the Autoloader's Slot Configuration

There are two reasons for editing the slot configuration:

- You are reserving some of the slots, possibly for use by another drive.

- You are changing the location of the cleaning cartridge. By default, Storage Manager uses the total number of slots designed for the device and does not assign a location to the cleaning cartridge.

To edit the slot configuration

1. Highlight the device icon of the autoloader you want to reconfigure.
2. Open the *Operation* menu and select *Edit Device*. The Configure Autoloader dialog box appears.

Configure Autoloader dialog box

3. Enter the appropriate slots.

➤ To specify the range of slots you want Storage Manager to use, indicate the beginning and end of the range in the **First** and **Last** parameters.

➤ To specify the cleaning cartridge's location, enter the slot number in the **Cleaning** parameter.

4. Choose **OK** to save your changes.

Loading Media in Autoloaders

If you are using an autoloader with an import/export door, you may need to perform an additional step when loading different media into the device.

To load media into the autoloader's door

1. Open the Operations menu and select *Import.*
2. Load the media into the autoloader. When you close the door, the device loads the media into the first available slot.
3. Open the Operations menu and select **Scan for Devices**. To confirm that the correct media is now mounted, highlight the device and select the Status tab. The tab displays the label of the media currently mounted in the device.

Updating the List of Media in Autoloaders

Some autoloaders (both tape and optical devices) cannot update the list of media loaded in the device and their respective slot locations after the device door has been opened. The *Learn Media* operation verifies the status of media by reading the media label in each slot of the drive.

To update the autoloader's list of media

1. In Device Manager, highlight the autoloader.
2. Open the Operations menu and select *Learn Media.*
3. Choose **OK** at the start prompt. There is no prompt that tells you the operation is complete.

➤ If you wish to see the updated media list, access Media Manager and view the Mounted Media window. Choose the **Rescan** button to refresh this window.

Testing Your Device

If you receive system messages indicating a media or hardware problem such as a failed write operation or excessive soft errors, you should perform a read/write test on your device. A read/write test identifies read, write, compare, and positioning failures. The short version takes approximately 15 to 20 minutes; the long version takes approximately 45 to 60 minutes. In most cases, the short test is sufficient. If you continue to have problems, run the long test.

TIP: Dirty backup devices are responsible for most soft errors. Avoid soft errors by periodically reviewing the Statistics tab in Device Manager. The **Cleaning Required** check box on the Devices tab indicates that the device needs to be cleaned immediately.

WARNING: To avoid losing data, never perform the read/write test with a tape that contains data.

Read/Write Test

To test the read/write tape heads

1. Insert blank media into the drive.
2. Highlight the device icon.
3. Open the Operations menu and choose *Test Device*. The Test Device dialog box appears.
4. Indicate which test (**Long** or **Short**) you want to perform.

Submit Job to Test Device dialog box

5. Indicate whether you want to record the SCSI instructions that occur during the test. Selecting the **Device Trace** option creates an attached file that can be viewed through the System Messages window. When this option is turned off, the program simply reports the percentage of read and write errors that occurred as system messages.

6. Specify any other parameters for this job.

7. Choose **OK** to submit the test job to the job queue. The results of the test are written as an attachment in the System Messages window. If the test indicates a relatively high percentage of soft errors, see page 11-18 for the troubleshooting recommendations.

Autoloader Test

In addition to being able to read and write data correctly, autoloaders must also retrieve media from the correct slot and load media into the device. The autoloader test determines whether the robotic arm performs correctly by checking the robotic arm's ability to locate, retrieve, and load media.

To test the autoloader

1. Highlight the autoloader icon.

2. Open the Operations menu and choose *Test Device*.
3. Indicate whether you want to perform the short or long autoloader test. The length of the test depends on the type of autoloader you have and the number of media the autoloader must retrieve and load. The short test loads each media once and the long test loads each media five times. The longer test is more likely to identify errors that occur sporadically.
4. Indicate whether you want to record the SCSI instructions that occur during the read/write test.
5. Specify any other parameters for this job.
6. Choose **OK** to submit the test job to the job queue.

Reviewing Test Results

The results of a SCSI device trace or a hardware test are written to files attached to the System Messages database.

To view test results

1. From the Control Panel in Control Console, select the Status tab and choose **System Messages**. The System Messages window appears.
2. Highlight the system message that corresponds to the module (PALUTIL.NLM) and the job ID of the test. The full description of the system message appears below the system messages.
3. Choose the **Details** button. The System Messages dialog box appears.
4. Choose the **Attached** button. A window displaying the attached file appears. This displays the contents of a separate file such as a SCSI device trace report.

➤ To print the attached file, open the Operations menu and select the *Print* option. The Print dialog box appears. Select printing parameters and choose **OK**.

5. Open the Attached File Windows system menu and select *Close* to close this window.

Cleaning Your Tape Drive

Storage Manager automatically cleans your backup device if the following conditions are true:

- You have an autoloader that supports cleaning detection.
- You have installed AutoLoader Software.

If you have a standalone device, Storage Manager can help you keep track of the cleanings you perform.

To record that the device has been cleaned

1. Clean the device according to the manufacturer's instructions. See Appendix B, "Maintaining Your Tape Drive," for recommendations and cleaning schedules for various devices.
2. Highlight the device icon representing the device you cleaned.
3. From the device's Statistics tab, choose the **Record a Cleaning** button. The new date appears in the **Time of Last Cleaning** parameter and the **Bytes Read since Last Cleaning** is set to zero.

Media and Device Errors

This section helps you identify types of media errors that can occur.

There are four basic types of media messages:

- Tape positioning
- Soft errors
- Unrecoverable write error
- Unrecoverable read error

When any of these types of media errors are reported, follow the troubleshooting procedures outlined below.

NOTE: The first read operation on a blank tape (rotation day) may result in a higher than normal soft error count. This is due to the debris that remains from the manufacturing process. Ignore the initial errors since subsequent reads should result in a significantly lower value.

Soft Errors Reported by Tape Drive

A soft error is an error that was corrected through some form of recovery action. If the tape heads encounter debris or a defect, they attempt to write the data on another location on the media. Soft errors are a normal part of writing and reading magnetic tape and are a drive's way of compensating for defects in the tape and debris that momentarily clog a read/write head.

Storage Manager monitors the number of soft errors reported by tape drives. The program writes a "note" in the System Messages window to notify the users that an unusually high percentage of errors has occurred.

Occasional soft errors are common and do not necessarily indicate a problem. In fact, many drives will report a soft error on new or infrequently used tapes that may have collected dust or become untensioned while idle. However, a consistently high percentage of soft errors may indicate a problem with the tape or tape drive.

When the amount of data read or written is small, Storage Manager allows a higher percentage of soft errors. This helps prevent false alarms, since a small number of soft errors would have a large effect on the percentage reported.

The note placed in the System Messages window has the following format:

Excessive soft errors reported, percentage = % writing session *xx* on *yy*

"xx" is the session, such as "CP57".
"yy" shows the label of the tape, such as "ADMIN:F:1".

The table below describes the read/write error thresholds used by Storage Manager for different devices.

Read/Write Errors Threshold		
Tape Drive	**Read**	**Write**
DC 600	2.00%	2.00%
4mm DDS DAT	0.55%	5.00%
DLT	3.00%	3.00%
8mm, 2.2GB	3.00%	4.00%
8mm, 5.0GB	6.00%	8.00%

Troubleshooting Media and Device Errors

Tape positioning, soft error, unrecoverable write error, and/or unrecoverable read error messages are typical errors caused by either media or the device. To determine the source of the problem, you must perform a series of up to three tests in order to identify the source of the errors. To verify your results, run the tests a second time using a second blank tape. Occasionally a new blank media (or even an entire box) will be defective and provide false results.

✓ ***NOTE:*** If you are unable to perform operations with a device, you may want to verify that Storage Manager supports your firmware as well as the device. For the latest version of the Certified Device List, download CDL40.ASC from the Palindrome BBS.

Tests 1 and 2 use the *Verify* operation in Media Manager. When troubleshooting, use this operation to eliminate the possibility of any media errors, not to diagnose hardware errors. Refer to the Read/Write Error Thresholds Table earlier in this chapter.

Does the Device Need Cleaning? (Test 1)

To check whether the drive needs cleaning (Test 1)

1. Insert the suspect data tape into the drive.
2. From Media Manager, run the *Verify* operation.
3. Review any system messages for soft errors.

➤ If the soft errors are **below** the acceptable threshold level and **no fatal error** appears, clean the drive with an approved, data-grade cleaning tape.

The cleaning process eliminates any debris which may cause intermittent errors. Before resuming normal operations, you may want to run another *Verify* operation as an added precaution.

➤ If the soft errors are **above** the acceptable threshold level or a **fatal error** appears, go to Test 2.

Does the Media Need to Be Retired or Forgotten? (Test 2)

To determine whether to retire or forget media (Test 2)

1. Insert a new, blank tape into the drive.
2. From Resource Manager, create a custom backup job on approximately 10 to 50 MB of data and write this session to non-managed media. You do not need to track this session in the File History Database.
3. From Media Manager, select the session on non-managed media and run the *Verify* operation.
4. Review any system messages for any soft errors.

➤ If the soft errors are **below** the acceptable threshold level and **no fatal error** appears, go to Step 5 in this test.

➤ If the soft errors are **above** the acceptable threshold level or a **fatal error** appears, go to Test 3 to run a comprehensive test of the tape drive.

5. Clean the drive with an approved, data grade cleaning tape to remove any debris.
6. Insert the suspect data tape into the drive.
7. Run the *Verify* operation.
8. Check the System Messages window for any soft errors.

➤ If the soft errors are **below** the acceptable threshold level and **no fatal error** appears, clean the drive to ensure that the drive functions properly.

➤ If the soft errors are **above** the acceptable threshold level or a **fatal error** appears again, you must either forget or retire this tape (see the "*Forgetting Media*" and "*Retiring Media*" sections in Chapter 10, "Managing Media.").

Are the Tape Heads Working? (Test 3)

To determine whether the drive is not working (Test 3)

1. Remove the data tape and insert a new, blank tape into the drive.
2. From Device Manager, highlight the device you are investigating and run the short read/write test (Operations/*Test Device*). This program runs for approximately 25 minutes.
3. Check the System Messages window.

➤ If the read/write test indicates **drive errors**, such as read or write errors, contact the vendor for information about returning the drive for repair.

➤ If the read/write test indicates **normal drive operation**, investigate possible contamination of data tapes or changes in your system's operating environment.

Setting Device Priorities

This section is for users with more than one backup device and who want to reserve devices for a specific purpose.

Numbered device priorities are not absolute. During a backup operation, the program will use a device with a lower priority if it has eligible media. As long as the device is available for the operation, the program uses that device if it had the preferred or required media is loaded on a device

NOTE: If you have any WORM (Write Once Read Many) devices, Palindrome recommends using those devices for archive sessions only and not for backup sessions. If backup sessions are written to WORM devices, they will become permanent sessions, since you cannot erase data from WORM devices.

For restore operations, if two or more eligible media are loaded on configured devices, Storage Manager uses the device with the highest priority.

The following examples illustrate how to effectively assign priorities to devices.

Example 1

Let's assume you are replacing an older tape drive with a faster drive using different media. You want to gradually eliminate the need for the original drive.

Device	Archive	Backup	Restore
Old Tape Drive	N/A	N/A	2
New Tape Drive	1	1	1

Retire the media used by the original drive. You can then configure your original drive to perform restore operations only (see above table). At the next automatic job, the program prompts you for blank media with which to add to the existing media set. Your new tape drive will be used for all backup and restore operations from the new media. You can use the original tape drive to restore from the original media type without having to create a temporary installation for the old device.

Example 2

This example assumes you have two backup devices—one a tape drive; the other an optical drive.

Device	Archive	Backup	Restore
Optical drive	1	2	1
Tape	N/A	1	2

This priority scheme maximizes the benefit of tape and optical media by using the optical device for archive operations and the tape device for backup operations. Since optical disks generally have a longer shelf life than tape, it makes sense to archive permanent copies on optical disks.

For restore operations you may want to rank the optical drive as your priority **1** device to maximize the benefits of the optical device's random access capabilities for quicker restore operations.

Example 3

This example also assumes you have two backup devices—one, a tape drive; the other, an optical drive.

Device	Archive	Backup	Restore
Optical drive	2	1	1
Tape	1	2	2

This example illustrates how you can reduce storage costs by using tape media and restore backup copies more quickly by using optical disks. If much of your data consists of stable files and you want multiple archive copies, this priority scheme allows you to take advantage of the greater storage capacity of tape relative to optical disk. In this example, the optical drive is the preferred backup device. End users can restore files they accidentally deleted or previous versions more quickly from optical disks with backup versions.

To edit operational priorities

1. Highlight the device icon whose priorities you want to change.
2. Open the Operations menu and select the *Edit Device* menu option. The Configure Device dialog box appears.

Configure Device dialog box

3. In each parameter, **Archive**, **Backup**, and **Restore**, set the value to a specific priority. The value **1** is the highest priority; **99** is the lowest.

➤ To de-activate a device for an operation, you can select **N/A**. The device is no longer available for the selected operation.

4. Choose **OK** to save your changes.

Chapter 12

Server Control Console

Overview

This chapter briefly describes the troubleshooting features available through the Server Control Console.

Introduction

The Server Control Console is designed to provide a way for you to perform critical activities at the server. For example, if you cannot use your workstation or the installation server has crashed, you would need to use the Server Control Console.

Some of these tasks you have probably performed at the client workstation. These options are intended to help you troubleshoot problems, such as recovering the System Control Database. The Server Control Console provides access to the job queue and perform backup and restore operations on the Protected Resource List.

To access the Server Control Console

➤ At the server prompt, type

LOAD PAL. The list of available options appears.

To select a server console feature

➤ Press the <**Tab**> key to highlight the option and press <**Enter**>. The appropriate screen appears.

To exit any screen

➤ Press <**Esc**>. The previous screen appears. To exit the server Control Console, also press<**Esc**>.

Options

Server Control Console options menu

About This Installation

This option provides an overview of the status of this server's installation and identifies obvious problems such as an inactive job server.

System Messages

This option allows you to investigate problems on your installation. The System Messages screen displays all of the system messages for the most recent jobs at the top of the list. Use this screen to find out why a job failed and the recommended course of action.

Job Queue

Use this option to identify the status of current jobs. For example, you would refer to this screen verify that no jobs were currently servicing before you brought the server down. You can also use the Job Queue screen to monitor operations on problematic resources, delete jobs, or resubmit jobs that have failed, or been on operator hold.

Next Required Media

This option is useful for verifying the correct media that should be loaded or available prior to the start of the next automatic job or rotation day operations.

Resources

Use this option to perform a full backup operation or a restore operation on a resource. The restore operation restores the selected resource's history, directory structure, and data to the original location. Through this screen you submit job on a single resource at a time. The jobs are submitted for individual resources. For example, prior to shutting down a server, you may want to ensure that each resource is backed up.

Update the Auto Login Information

Use this option in a disaster recovery situation when your Auto Login name and password are invalid. If the NDS or Bindery files have been destroyed or corrupted, you will need an Auto Login name to recover the System Control Database.

Verify System Control Database

Use this option if you receive system messages questioning the integrity of the System Control Database. You should attempt to verify the database before recovering a previous version. You can only verify the System Control Database through the Server Control Console. The operation corrects and/or identifies errors which it cannot correct.

Once you select the **Verify System Control Database** option, a job status window appears and describes the operation's activities. Use this option before attempting to recover the System Control Database. The resulting system message will indicate whether you need to recover the System Control Database.

Recover System Control Database

The System Control Database is a critical to running your installation. Without it you cannot locate the File History Database, configure operations, or submit jobs. Once you have restored the System Control Database, you can continue operations such as restoring protected resources from either the server console or the Windows client workstation.

When the installation server cannot locate the job queue or the System Control Database, the program automatically assumes that a critical event has occurred and that you need to restore your installation server. You can restore your installation server only from the server console. You can restore the protected resources from either the server console or the client workstation.

See page Appendix C, "Disaster Recovery," for additional information about disaster recovery. See page 6-16 for information about restoring protected resources.

Appendix A

Commonly Asked Questions

The purpose of this section is to answer frequently asked questions that are not directly addressed in the descriptions of Storage Manager concepts, procedures, and parameters. NetWare 4.x issues are addressed separately.

General

Question: What are TSA*.TMP files?

Answer: TSA*.TMP files are temporary files created by TSAs and are normally deleted by the TSA after Storage Manager disconnects. They remain on disk due to abnormal termination of a TSA operation.

- TSA*.TMP files may be manually deleted.
- Setting the rules at the root of the volume to Backup/Exclude, Archive/Exclude, and Migrate/Exclude for the wild card name TSA*.TMP will prevent Storage Manager from attempting to backup these files.

Question: What are some causes of database corruption?

Answer: Recurring database corruptions are usually a sign of an environmental problem such as a faulty network interface card or cable. If corruptions continually occur, test the network using a network analyzing tool (sometimes referred to as a “sniffer” or “lanalyzer”) to locate the problem.

Whenever there is a loss of the data stream from the backup source location to the backup device during a backup operation, database corruption may occur.

This can be due to lost connections across the system, other NLM’s initiating conflicts with Storage Manager, and intermittent hardware problems. Substituting known working devices for suspect devices can narrow the search for the problem source.

VLM shells prior to version 1.10 and NETX shells prior to 3.31 have been known to cause database corruptions and should be upgraded.

Environmental conditions within the work place (and even strong magnetic and static fields behind walls of adjoining offices) can add to the possibility of corruptions. It is important to properly shield hardware and terminate the SCSI bus at both ends.

Question: How can I optimize Storage Manager performance?

Answer: Operating system settings, hardware on the system, the complexity and depth of directory structures, and Storage Manager configuration settings all affect performance.

Operating system settings: The *Installation Guide* contains a "*Server Tuning*" section with detailed information on settings such as Packet Receive Buffers, Directory Cache, and Total Cache Buffers.

Hardware: Often, adding memory to the server will help improve performance, as the settings for various options can then be given a broader range to handle peak loads on the system. Replacing 16-bit controller cards with 32-bit cards, using compression backup devices, compressing files prior to backup, and using computers with higher speed CPUs can increase performance.

Storage Manager Configuration: Storage Manager default settings are sufficient for most environments, so little customization is needed. However, the rules, rotation schedules, and backup choices can be customized to optimize Storage Manager for specific needs.

Configuring automatic backups to execute at non-peak memory utilization times is important, so that other applications do not compete with Storage Manager demands.

Installation

Question: How do I relocate my Storage Manager installation?

Answer: To relocate the Storage Manager installation:

- At the target location, specify the same directory path as the original installation directory.
- Be sure that the configured auto login user exists on the target server.
- Be sure that the target server/volume supports the same name spaces as the original installation server/volume.

See also: "*Moving a Storage Manager Installation*" in Chapter 6 of this guide.

Question: Why can't I configure my backup device?

Solution: Check for each of the following:

- **Termination**—Ensure that the backup device is properly terminated and/or try a different termination cap.
- **Device Drivers**—Ensure that the correct Palindrome supported device drivers are loaded. Both the SCSI hardware driver and the ASPI module (for example, ASPITRAN or CPQASPI) must be loaded. Download TSTDRVR.ASC from the Palindrome BBS for a list of supported device drivers.
- **SCSI ID conflict—**Use Device Manager to "Scan for Devices". If there is a SCSI conflict, scanning will show the same device multiple times. Be sure that the device has a unique SCSI ID.
- **Supported Devices**—Ensure that the host adapter and backup device are supported and have a proper firmware and associated EE Code (must support SCSI-2 command set). Download CDL40.ASC from the Palindrome BBS for the latest list of supported devices.
- **Servers with more than 16MB of RAM**—If the server has more than 16MB of RAM and the installation is using a host adapter that cannot access more than 16MB of RAM, be sure to use the "LOAD PALSDRV ABOVE16MEG" statement.

Question: Why do I see PLSM-53 errors when adding resources to the Protected Resource list?

Answer: Check the following:

- ➤ Be sure the proper TSA is loaded on the server being added to the list.
- ➤ For 4.x servers in a different tree than the installation server, be sure the configured auto login user has been created within the bindery context for those servers.
- ➤ Ensure that the configured auto login user does not have concurrent connection restrictions.
- ➤ If upgrading from TSA's dated June 1994 or earlier, be sure to re-select each resource on the Protected Resource List so that each resource will be associated with the upgraded TSA.

See also: "*Renaming Resources*" in Chapter 8 of this guide.

Backup

Question What are the requirements for protecting 4.x servers?

Answer: NetWare 4.x server resources are added to the Protected Resource List similarly to any other server's resources.

- ■ Load the appropriate TSA for the server being added to the Protected Resource List (for example, TSA3.1x, TSA410)
- ■ Unique to 4.x servers is a Network Directory Services (NDS). To protect this resource, load TSANDS on one of the servers in the NDS tree. To backup the NDS in full, add "Full_Directory_Backup" to the Protected Resource List.

- If protecting 4.x servers not part of the installation server's NDS tree, create an auto login user on each of these servers. Add this user to the default bindery context for each server and assign the user supervisory object rights to the ".[Root]" object within the NDS tree.

See also: *Installation Guide*

Question: What is the difference between NDS "Full Directory Backup" and ".[Root]"?

Answer: There is no difference currently. It is recommended that the user select "Full Directory Backup" so that as enhancements (such as the ability to backup schema information) are added to TSANDS, this additional data will be protected without the need to modify the Protected Resource List.

Currently TSANDS only backs up NDS objects and associated data. It is anticipated that schema, but not partition information, will be backed up with future TSA releases.

Question: How do I perform full backups on specific days?

Answer: For a complete "snapshot" of the system, custom jobs can be scheduled to run periodically (daily, if desired) and these custom sessions can (optionally) be tracked within the File History Database.

Note that with both the Tower of Hanoi and Grandfather/Father/Son rotations, full backups automatically occur every rotation day. In addition, the system administrator can configure for full backups on non-rotation days.

Question: What causes backups to run slowly?

Answer: The following are some common causes of slow backups:

- Using the job status window to monitor jobs in progress can adversely affect performance. Monitoring is only recommended for specific purposes and for short periods.
- The number of directories on a volume, and the amount of server memory allocated to access those directories, are closely related. The default settings are often too low for good performance. A formula for computing the Minimum Directory Cache Buffers setting is available in the "*Server Tuning*" section of the *Installation Guide*.

Question: Why do scheduled automatic backups not execute?

Answer: There are a number of items that may affect the execution of automatic backup operations. Be sure:

- ➤ There is a job queue.
- ➤ PALJSRVR (the Job Server) is loaded on the server. To load PALJSRVR, at the server console prompt, type:

  LOAD PALJSRVR /I<*installation path***>**

  where <installation path> is the volume and directory of your installation directory (for example, VOL1:\PAL).
- ➤ Eligible media is loaded.
- ➤ The configured auto login user has supervisory rights.
- ➤ There are no NLMs loaded that conflict with Storage Manager NLMs.
- ➤ There is sufficient memory to execute the operation.

Question: Why are some files skipped during a backup operation?

Answer: Depending upon the backup operation running, Storage Manager will not copy files (with the default settings) when:

- They are already archived on the same media set (for example, media set “E” might include media “E:1”, “E:2”, “E:n”...).
- They are fully protected (by default, three archive copies on different media sets).
- Rules are defined that exclude those files from all backups.
- The files have invalid characters within the file name.
- The files have no date or an invalid date.
- The files are opened by another application unshareably. Storage Manager can back up most open files. But there are some issues you should be aware of when backing up open files:
  - If a file is open shareably for reading only by another user, it will be backed up as usual.
  - If the file is not shareable, it will be skipped until the next backup operation.
  - 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 table summarizes Storage Manager actions on open files.

How Storage Manager Handles Open Files	
If a file is…	**Storage Manager…**
Not opened by others	Backs it up.
Opened by others for reading	Backs it up.
*Opened 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.	Shareably—Backs it up as “suspect.” Non-shareably—skips it.
If “deny all”	Skips it.
*NetWare file modes	

Restore

Question: Why do tagged phantom files not restore?

Answer: By default, Storage Manager creates phantom files for migrated files. If tagging a phantom file does not result in a restore of that file, the following are possible causes:

- The file has been moved to a new directory (or if the directory in which it resides has been renamed), the file loses its phantom stamp and Storage Manager sees it as a standard (non-phantom) zero-byte file, and cannot restore it.

  To restore phantom files whose path has changed, the system administrator should tag the file in its original directory location and resubmit the restore request, or tag the file version directly from media and restore redirected to a new target location.

- The forget operation has been performed on all of the media or sessions on which the archive copies are located and backup copies no longer exist. These file can only be restored by reading the physical media.
- The System Control Database and/or File History Database, dated before the creation of these copies, have been restored. As a result records of the archive copies are not available. However, these copies may still exist on media and must be located though the journal operation.

Question: What is the best way to recover from a corrupted or missing System Control Database (files ASDB.PAC and ASNX.PAC)?

Answer: To restore the latest System Control Database, use Palindrome Control Console at the server (PAL.NLM). Select "Recover System Control Database" and specify the location of the System Control Database.

If the latest System Control Database is not available on backup media, then restore the next most recent set. If the latest System Control Database is not restored, File History Databases for the same backup date for **all** resources on the Protected Resource List must also be restored—so that both databases are synchronized. This method is the second choice because some file history information may be lost.

Question: Why aren't some files restored during a restore operation?

Answer: The following are some reasons that files are not restored:

- The file is already on disk and the **Overwrite** parameter for replacing existing files is set to **Never** (a file on disk is never replaced) or **Older** (a file on disk is never replaced with an older version from media).
- The file does not exist in the File History Database.
- The System Control Database and the File History Database(s) are not synchronized. This can result from restoring an older System Control Database without restoring File History Databases from the same date or earlier.
- A TZ (Time Zone) variable has been set.

  Use of the TZ variable can cause a date/time mismatch between the file versions in the File History Database and the files on media. Palindrome does not recommend using the TZ variable.

  To restore specific versions of files that were backed up when a TZ variable was set, journal the media containing the file in Media Manager, and tag the version to restore.

Question: How do I restore an object in an NDS tree?

Answer: Single objects can be restored by tagging them using File Manager. Due to NDS limitations, however, linkages with other objects (rights to use printers, file trustee information, etc.) do not get restored with single object restores.

To restore user objects in an NDS tree where users access only services within their own container, **restore the entire container** in which they are defined.

Media Scheduling

Question: How can I predict how many tapes (media) I will need for backups?

Answer: The number of media required varies depending upon combinations of the following:

- The rotation pattern configured.
  The default Tower of Hanoi rotation pattern, which rotates media weekly, requires a minimum of one media in each of five media sets (more if the data to copy to media exceeds one media per backup).

  The GFS (Grandfather/Father/Son) rotation pattern is based upon sets of daily media, weekly media, and monthly media. Seven media sets are required for daily media sets. Using the default settings, a total of 23 media sets will be requested. If copied data will not fit on one media per set, then additional media (but not media sets) will be needed.

- The storage capacity of the media relative to the amount of data to be copied to media.

- The types of backup being performed (full, incremental, or differential operations).

- The setting of the **Put Archive Copies on Separate Media from Backups** option. If selected, the program requires additional media, as archive copies and backup copies will be written to separate media within a media set.

- The setting of the **Preserve Backups** parameter. The longer the time period that you preserve these sessions, the more media the program will require. The program cannot overwrite any backup session on the managed media until the most recent session is eligible for overwriting.

Question: How do I know ahead of time what backup media will be needed?

Answer: View the Next Required Media window to find out which media will be needed to continue an incomplete automatic job, for the next automatic backup operation, or the next rotation day.

Question: What happens when a tape (media) fills during a backup?

Answer: If a media fills during a backup operation, Storage Manager automatically continues writing on the next eligible media. If no other eligible media is available within the backup device, Storage Manager logs or displays message indicating that the backup could not complete and to insert an eligible media.

Migration and Automatic Recall

Question: How does a file become eligible for migration?

Answer: There are two sets of eligibility requirements, one for Resource Manager operations and one for File Manager operations.

Custom resource-level and automatic migration operations require that a file be fully protected (a minimum number of archive copies exist on managed media) and the applicable migrate rule is satisfied. For example, if a file is fully protected, but the migrate rule is **Exclude**, the file can never be eligible. If you have designated a near line set, Storage Manager will ensure that an archive copy exists on this set before migrating the file.

File Manager migration operations require that one archive copy exists in the media library. An additional requirement is that the must not have its migrate rule set to **Exclude** rule. The stability period does not apply to a file-level operation.

Question: If I tag a resource for a migration job, does Storage Manager migrate all files eligible for migration?

Answer: Not necessarily. The low water mark determines to what extent Storage Manager migrates files to reach a configured level of disk utilization. To ensure that **all** eligible files are migrated during each resource-level migration operation, set the low water mark to **0**. This setting generates system messages because the active files prevent Storage Manager from reaching the low water mark of zero.

Question: Is automatic migration a prerequisite for automatic recall?

Answer: No, you can submit migration jobs manually and still recall these files (assuming that Storage Manager has tracked at least one copy of the file).

Question: How can I ensure that the percentage of prestaged files is up-to-date?

Answer: Storage Manager automatically updates the prestage list once during resource-level migration if the existing list was not sufficient to reduce the utilization to the low water mark. The percentage of disk capacity consisting of files eligible for migration appears in the Resource Monitor window.

However, the percentage that appears under the **Prestaged (%)** parameter is based on the list that existed following the previous migration. If you perform custom migration operations infrequently, these values may underestimate the actual percentage that is eligible for migration. You can schedule a prestage job to follow automatic jobs to update the list on an on-going basis or manually submit a job to build the prestage list as you need it. Migration operations often perform more quickly if the prestage list has been updated prior to the migration job.

To update the prestaged list

1. In Resource Manager, select the monitored resources, if necessary.

2. Open the Operations menu and select the *Migrate* option. The Migrate Options dialog box appears.

3. Select the **Build Prestaged List Only** option.

4. Select the appropriate Which Resources? option (**Tagged Resources Only** or **All Active Resources**).

5. To update the prestaged list regularly, choose the **Schedule** button. The Scheduling Options dialog box appears.

➤ Name this job in the **Description** parameter and select the **After Job** option.

➤ Select the Default Automatic job listed in the **Start job after** list box. The job will run after *every* automatic job to determine which files have most recently become eligible for migration.

➤ Choose **OK**.

6. Choose **OK** in the Migrate Options dialog box.

Question: What is the difference between a near line set and a near line device?

Answer: A *near line set* is the A media set in your managed media library. This media set usually remains available in a backup device at all times in order to expedite restore and recall jobs. When you turn on the **Create a Near Line Set** option, you are adding another eligibility requirement for a resource-level migration operation.

Once the file is fully protected and the migration rule is satisfied, Storage Manager also verifies the status of the near line set. Before a file is eligible for a resource-level migration operation, Storage Manager verifies that an archive copy of the file exists on this media set. Storage Manager writes an archive copy if it does not already exist on this set.

A *near line device* refers to the device used exclusively for the near line set. To make the most of a hierarchical storage management, use an optical device to complete restore and recall as fast as possible.

Question: Is a near line set or a near line device required for automatic migration and automatic recall?

Answer: The near line set and near line parameters only tell where to find the files and from which device they can be restored. Recall operations can use any media set on which the tracked file is written.

A near line set does not require a near line device. However, if using a near line set, a near line device helps Storage Manager to quickly find and restore or recall the files.

Neither the near line set or near line device are required for manual or automatic migration or automatic recall operations. However, having a near line set and device can expedite operations if a media set is off site or if another operation is using other devices.

Question: Does the near line media set have to be a particular type of media?

Answer: No. However high quality media reduces the risk of media failure. High-quality media such as an optical disk can survive more read and write operations than many tape formats. Storage Manager accesses the near line set frequently to write the additional archive copy, especially if many users recall files.

Question: Should the operational priorities of a near line device differ from those of other devices?

Answer: By default, the operational priorities of a near line device are the same as those of any other device. This device can perform backup, archive, and restore operations.

However, you may want to configure these priorities differently for your near line device:

To dedicate the device for HSM

➤ Edit the operational priorities in Device Manager. On the Configure Device dialog box, disable the **Backup** parameter so that this type of operation would not interfere with an automatic recall operation.

To ensure that Storage Manager uses the near line set

➤ Edit the operational priorities in Device Manager. On the Configure Device dialog box, Rank the restore operation higher on the near line device than on other devices. For example, set the **Restore** parameter to **1** on the near line device; on other devices set this parameter to **2** or greater. When performing a restore operation, the near line device will be Storage Manager's first choice.

Question: If I change the media library name, my near line set is also retired. How does this affect future migration and recall operations?

Answer: Whether or not you use a near line set, you can still recall files, but the jobs will go on server hold if the retired regular or near line set or a copy of the media is not available. After these files are restored from retired media, they will eventually be archived to the active managed media. Depending on your concern for the integrity of the media, you can use the original or a duplicate of the retired media set(s).

You could also restore files from the retired media and wait for Storage Manager to migrate these to the active near line set. However, this will greatly increase disk utilization and may exceed the high water mark or activate a Check Resource Monitor alert.

NetWare 4.x

Bindery Emulation

For more information on bindery emulation, see chapter 2 of the Installation Guide.

Due to a NetWare limitation, if you are protecting 4.x servers that are not part of your installation server's NDS tree, you must enable bindery emulation on each of those servers and create the auto login user on each of those servers in the proper bindery context for that server.

Storage Manager follows the default methods of NetWare, whereby it uses NDS logins for servers within the same tree and bindery logins for servers outside of the current NDS tree.

HCSS Migration Volumes

Storage Manager treats volumes supporting HCSS as any other volume. It backs up migrated files (files on optical) but does not cause recall requests.

When recovering migrated files, however, the files are restored to disk and then migrated by NetWare (files are not restored directly to optical). This may cause the volume to fill up before all of the files have been restored on versions prior to NetWare 4.1.

As of NetWare 4.1, migration has sufficient priority that disks should not fill during a restore.

Compressed Files

Storage Manager protects NetWare 4.x compressed volumes. You can back up these volumes as compressed or uncompressed by toggling the **Retain File System Compression** option in Configuration Manager (select Configure/*Operation* and then the Advanced tab). When you turn on this option, compressed data cannot be restored to a volume that does not support compression.

If you turn off this option, the compressed data is backed up uncompressed on media (this affects performance). Note that if you choose this option, you **cannot restore** the data in compressed format, only uncompressed.

Generally, the option should only be used if there is a likelihood that you need to restore data to a volume that does not support NetWare 4.x compression (for example, a NetWare 3.11 or a workstation volume).

SYSCON

Avoid using SYSCON to administer NetWare 4.x servers and especially do not use SYSCON to create user objects.

If you use SYSCON to create a user on a 4.x server and have to restore, neither the login script nor directory or file trustees will be restored for the user.

If use NWADMIN to create the user objects, they are restored completely.

Read Fault Emulation

Be sure to set **Read Fault Emulation** to ON on all 4.x servers.

Protecting NetWare Directory Services

Storage Manager uses the NetWare Directory Services Target Service Agent provided by Novell, Inc., to back up the NDS database. You should use TSANDS.NLM that ships with the current version of Storage Manager (or a newer version). Do **not** use the version TSA_NDS.NLM that shipped with NetWare 4.01.

TSANDS backs up the entire NDS database for a Directory tree from a single point, regardless of the number of partitions that exist. A Directory tree need only be added once to the Protected Resource List.

If performance becomes an issue while backing up the NDS database, you may consider storing a replica of each partition on the server where TSANDS is loaded.

NDS Database Replication

Although Palindrome provides comprehensive backup of NDS, Palindrome strongly recommends that you have at least two replicas of each partition of your Directory tree.

Replicating the NDS database among multiple servers has several benefits:

- It provides faster access to NDS information for users across a wide area network data link.
- It eliminates a single point of failure. If a disk crashes or a server goes down, a replica on another server can continue to authenticate users to use the network and to provide information on objects in that partition.
- It allows a partition that becomes corrupted to be recreated from a replica.

Partition Loss

It is important to note that the loss of an NDS partition can have far-reaching consequences. Not only is the NDS data contained in that partition lost, but subsequent partitions are also lost.

For example, if the Root partition is not replicated and is lost, the entire NDS database is destroyed. Furthermore, loss of the NDS database invalidates the file system trustee information on all servers in the Directory tree. It is also not currently possible to back up the NDS database once a portion of it is off line.

Reinstallation

Should you ever need to re-install NetWare Directory Services, you should call the new Directory tree by the same name as the tree it is replacing. You must add servers to the same container objects as before.

Be sure to record the NDS tree name, Organization names, Organizational units, and servers that are located in each container. You will need this information if you ever need to restore the NDS tree.

Extended schema, partition, and replication information should also be recorded as they are not protected.

TSANDS Limitations

Novell releases updates to TSAs periodically. These updates can be obtained from Novell via the NOVLIB forum on Compuserve. Once updates have been certified by Palindrome, they will also be made available on the Palindrome BBS.

Palindrome has seen the following limitations with the current NDS Target Service Agent (TSANDS.NLM [dated 10/21/94]):

Limitations

Partition Information is Not Saved

You must repartition and/or replicate the database manually during a restore operation.

Because of this limitation, when restoring **large** NDS databases:

- First restore containers only
- Secondly, partition and replicate as necessary.
- Thirdly, restore the data.

Schema Information is Not Saved

Applications that modify the NDS schema may need to be re-installed if data is restored into a new NDS database as opposed to an existing NDS database. This is because only the default schema is available whenever NDS is installed.

NOTE: Palindrome recommends that you add "<tree>/Full Directory Backup" to the Protected Resource List, rather than "<tree>/Root". This ensures that schema information will also be backed up once this capability is added to TSANDS by Novell.

Bindery Emulation login scripts are not saved.

Login scripts created via the NetWare 3.x SYSCON utility for users who log in via bindery emulation are stored as files in the appropriate MAIL directory, rather than as a property of the User object (as is the case with the login script for a user who logs into NDS).

While these login files are backed up, the directories in which they reside are based on a user identification number under the SYS:MAIL directory that becomes invalid once NetWare Directory Services is removed from a server.

Single Point Backup

Currently, Palindrome recommends that the entire NDS database be backed up from a single point using a single NetWare Directory Services Target Service Agent (TSANDS.NLM). This presents several problems:

- It may take considerable time for portions of the tree that may exist on the other side of a WAN link. In this case, a local replica of the remote partition might be useful.
- Multiple system administrators may be responsible for different portions of the NDS tree. To avoid this problem you should consider two alternatives:

1. Make one administrator responsible for backups of the NDS database, or

2. Allow each administrator rights to back up the entire NDS database (i.e., backup NDS multiple times from multiple Storage Manager installations).

Future releases of Storage Manager will be enhanced to back up portions of the NDS database.

Off-line Partitions

The NDS database cannot be backed up if any partitions are off-line. If a server that contains a Master replica is off line and there is no other replica of the partition on any other server, TSANDS terminates with the following error:

NWSMTSReadDataSet: -626 All referrals have failed. Directory Object Name <container object> (FFFDFEAE)

where <container object> is the full name of the root object of the partition that is missing. If this partition is needed, you must wait until it is back on line before attempting another back up of the NDS database. Consider replicating the partition once it is again available so as to avoid a reoccurrence of this problem.

Restore Limitations

Rights to Other Objects Not Restored

It is possible to restore a single object once it has been deleted. Note, however, that restoring a single object does not restore that object's rights to other objects, nor are directory and file rights of the deleted object restored.

For example, if a User object is deleted, then later restored, the User object and data associated with that object are restored (i.e., the user's name, location, telephone number, login script and other properties are restored). However, rights to other objects must be restored manually (i.e., the groups to which the user belonged, the printers that the user had rights to use, the files and directories the user could access or owned, etc.).

You can restore directory trustees in Resource Manager using Operations/*Restore Directory Structure*.

Palindrome recommends that when designing your NDS tree, objects that users have rights to are in the same container that the user is defined in. Then when restoring a single object, restore all objects in a single container to ensure all objects associated with that object are restored.

Printer Information

Printers are likely to need re-configuring after restoring an NDS database. Not all of the information relating the Print Servers, Print Queues and Printers is restored properly.

NDS Recovery Techniques

Whenever a problem with NDS is encountered, a multi-step approach should be taken before attempting to re-install NetWare Directory Services.

Palindrome strongly recommends that you familiarize yourself with all of these steps by studying the NetWare 4.x documentation *before* you have a need to restore NDS.

Repairing the NDS Database

DSREPAIR is a server utility that checks and repairs the NDS database similar to the way VREPAIR checks and repairs volumes. It is important to ensure that the NDS database is not corrupted before trying to restore data into it.

You can use DSREPAIR to repair the NDS partitions and replicas that reside on a particular server. If the problem persists after running DSREPAIR, run the utility again on any other servers that contain the same partition replicas. To repair the entire NDS database, you must run the utility on each server that contains a part of the NDS database.

For further information refer to the following Novell Documentation: "Repairing the NetWare Directory Services Database" in Chapter 4 of *Supervising the Network,* and "DSREPAIR" in Chapter 4 of *Utilities Reference.*

Replacing an NDS Replica with a New Copy

If your NDS database is replicated across multiple servers and you find users on only one server tend to experience problems, you may find it beneficial to replace the suspect replica with a fresh copy.

You can do this by deleting replicas that you suspect contain corrupt data and replacing them with a new copies of the Master replica.

If you suspect that the Master replica is corrupt, but that other replicas still contain valid data, you should first make one of the other replicas the new Master replica before proceeding with this operation. This method ensures that all other replicas contain the same data as the Master replica.

Restore the NDS Database into the Existing Directory Tree

When you restore data into an existing database, trustee ID information is maintained, thereby avoiding the need to re-synchronize the file system data with a new NDS database. It is worthwhile attempting to restore into an existing database first before taking more drastic measures (such as removing NDS from a server) since the procedure can be done fairly quickly.

The NDS database can be restored by tagging the NDS resource in Resource Manager and selecting Operations/*Restore*. Be sure to set the overwrite options to ALL in the restore dialog box.

Installing a New Directory Tree

If none of the above procedures is successful, or you need to recover from a situation where a partition has been lost that is not replicated, then you may need to re-install NetWare Directory Services on all of your servers. This procedure has far-reaching consequences.

Once NetWare Directory Services is removed from a server, that server's file system trustees are invalidated, even though the file system data is still valid. Thus, the trustee information on all NetWare volumes that were in the Directory tree must also be restored as part of this procedure.

To restore directory and file trustees, using Storage Manager, you must use the Restore/*Directory Structure* and the Restore/*Data* options.

Re-installing NetWare Directory Services

1. Unload all Palindrome NLMs from the server.
2. Before removing NetWare Directory Services from a server it is recommended that all replicas be removed from the server. Replica management is done via the Partition Manager. Delete Read/Write and Read Only partitions from each server. Merge Master Partitions into parents until only the Root partition remains on a single server.

3. Remove NetWare Directory Services from each server in the Directory tree. This is done using the INSTALL utility at each server containing a part of the NDS database. The order in which this is done can be important. You should remove NetWare Directory Services from the server containing the Root partition last.

4. Down and cold boot each server on which Directory Services was removed before reinstalling. For a cold boot, turn off the machines power, wait at least 30 seconds, then turn on the machines power.

5. Install NetWare Directory Services on one of the servers, specifying the same Directory tree name, Organization, and optional Organizational Unit(s) as before. This is done using the INSTALL utility at the server console.

6. Install NetWare Directory Services on each of the remaining servers that existed in the Directory tree prior to removing the NDS database. Ensure that the same Directory tree, Organization and Organizational Unit(s) are specified as existed prior to removing the NDS database.

7. Install mounted volumes into the NetWare Directory tree on each server using the INSTALL utility. (Newer versions of NetWare 4.x may install the mounted volumes for you as part of the previous step. Do not be alarmed if you receive a message stating that no volumes were found that needed installing into the Directory.

8. Use the TIME command on the server console to verify that the time is synchronized on the network. This is important for proper NDS functioning. Do NOT use the time command to force a server's time to synchronize. Refer to your NetWare documentation if you have problems with synchronizing time.

9. Run the DSREPAIR utility on each server. This operation removes old (obsolete) trustee IDs from the file system. Running the utility once should be sufficient. However, you may want to run it a second time to ensure that no more errors are found.

10. Recreate the Auto Login User object where it existed previously.

11. Repartition and replicate the NDS database as it was before, or at least to the extent necessary.

It should not be necessary to re-install Storage Manager, however, you may have difficulty if some of the Storage Manager files are no longer owned by the Auto Login User object, particularly if these files have no owner. Most important are the log files, database files, and lingering temporary files in and under the directory where Storage Manager is installed.

12. Be sure all Storage Manager files are owned by the auto login user. Use the NetWare 4.x FLAG utility to verify file ownership.

13. In order to create a Palindrome job queue you must extend the NDS schema by either by reinstalling Storage Manager or by restoring the system control database using the Storage Manager control console (PAL.NLM). The following describes how to extend the schema by restoring the system control database.

14. Prior to restoring the database, at a workstation, rename the *.PAC files in your installation directory. For example, from the DOS prompt of the installation directory, type:

    REN *.PAC *.SAV

15. At the server console, type:

    LOAD PAL.NLM

16. Select *Recover System Control Database.* Specify the installation volume and auto login information.

17. When prompted for the correct media, select **ABORT** as you do not have to actually restore the system control database. Exit from the job view screen and from the control console.

18. At a workstation rename the original *.PAC files to their original name. From the DOS prompt of the installation directory, type:

    REN *.SAV *.PAC

19. In Storage Manager, restore the NDS database data by tagging the NDS object in Resource Manager and selecting Operations/*Restore.* Select *Full Resource*. Set the overwrite parameter to **ALL**.

20. Check that the auto login user has sufficient file system rights to restore data. If you have granted the auto login user the Supervisor object right to the server object, these rights will have been restored automatically.

21. Reconstruct the trustee information on each server volume in the NDS tree by accessing Resource Manager and tagging each resource that is in the NDS tree.

22. For each server, select Operations/*Restore*. Choose *Directory Structure*. This restores directory trustees for each directory.

23. To restore file-level trustees, you have to restore all data to the volumes. For each server, select Operations/*Restore*. Choose *Data*. This restores all data on each of your volumes.

Appendix B

Maintaining Your Tape Drive

The purpose of this section is to inform you of external factors which can have a negative effect on drive performance and thus interfere with Storage Manager operations. This section also tells you how to avoid or minimize these factors and how to care for your storage devices.

Factors Affecting Drive Performance

Your tape drive, whether it is from Palindrome or another manufacturer, requires proper care and maintenance to function reliably over the lifetime of the unit.

There are many aspects to tape drive maintenance that go beyond the normal cleaning function. You should familiarize yourself with these issues from the outset to ensure reliable operation.

Several operating conditions exist that affect the reliability of the drive including:

- Operating environment
- Temperature and humidity
- Electromagnetic interference (EMI)
- Electrostatic discharge (ESD)
- Shock and vibration
- Air flow requirements
- Power protection

Operating Environment

Usually common sense is all that's needed to ensure the proper operating environment (for example, keep all liquids away from your drive and media). Nevertheless, Palindrome recommends a quick review of the recommended environmental specifications.

Temperature and Humidity

Maintain a temperature range of +40 to +100 Fahrenheit (+4 to +38 Celsius) and a relative humidity of 20% to 80%. Most offices meet these criteria. Also, the storage device and media should be at the same relative temperature.

✓ ***TIP:*** If a tape remained at a temperature lower than 60 degrees Fahrenheit (15 degrees Celsius) overnight, don't use the tape until it has reached room temperature (60 degrees Fahrenheit or greater).

Electromagnetic Interference (EMI)

Tape drives tolerate moderate levels of EMI. To minimize this interference, keep external drives a safe distance away from equipment that is known to generate excess amounts of EMI (computer monitors for example).

Electrostatic Discharge (ESD)

Most computer equipment is susceptible to ESD, including tape cartridges and tape drives. Be sure that you discharge any static that you may have accumulated prior to contacting a tape unit or its tapes.

Shock and Vibration

Like computer hard disks, tape drives are adversely affected by sudden jolts and excessive vibration. To minimize vibration, mount the drive on a stable surface, free from excessive vibration.

Air Flow Requirements

The tape drive requires adequate air flow through its vents to dissipate excess heat. Dust and debris accumulating on the vent or inside the unit can prevent the unit from cooling properly and result in contaminating the unit and media.

To avoid contaminating the storage device and media

- Be sure to allow sufficient space around the unit to allow air to flow freely.
- Keep the unit away from paper dust generated from office equipment such as printers and photocopiers.
- Always operate the tape drive with its cover on.

➤ If you must operate the storage device in a dirty environment, such as a warehouse, clean the tape drive more thoroughly and more frequently than recommended.

NOTE: Many drives have a replaceable filter that should be replaced regularly. A dirty filter may reduce the flow of air through the drive. Failing follow the manufacturer's replacement instructions may cause erratic drive behavior, void your warranty, and result in costly repairs.

Power Protection

Most computer equipment is susceptible to power fluctuations. Your Storage Manager system is no exception—it can be vulnerable unless it receives clean, uninterrupted power. Palindrome **highly** recommends connecting the tape drive and workstation running Storage Manager to a UPS (uninterruptable power supply). Power disturbances can damage the tape drive and the workstation, and will create problems that are unpredictable and difficult to trace.

While LAN managers usually protect their file servers with UPS, the storage devices often have unprotected or under-protected (with only a simple surge supressor) power supplies.

Studies show that power spikes account for a minority of electrical disturbances. Most often, blackouts, brownouts, voltage sags, or line noise cause the bigger problems. An inexpensive surge suppressor is not the answer. It may not trap power spikes quickly enough, and it does not address the other electrical disturbances mentioned above.

When Do Drives Report a Soft Error?

Different technologies are used when recording on magnetic media. This affects the nature of the soft errors reported. The following paragraphs discuss the meaning of soft errors for the different tape technologies.

8mm Tape Drives

Soft errors are reported on 1024-byte blocks. If a block that was just written fails on a read-after-write test, then the block will be rewritten and a soft error reported. When reading, if the contents of a block must be corrected using its Error Correction Code (ECC), then a soft error is reported.

4mm DDS DAT Tape Drives

DDS DAT drives use a complex three-level error correction scheme. When reading from tape, Storage Manager monitors the lowest level, called C1, to detect the earliest signs of problems. When writing, a DDS DAT drive reports the number of frames that are rewritten. A frame is a physical measure of data being transferred to the media; it's the amount of data transferred by a single rotation of two DAT write heads. The soft error report is based on the percentage of frames that must be rewritten.

DC 6000 Tape Drives

QIC 150

Soft errors are reported on 512-byte blocks. If a block that was just written fails on a read-after-write test, then the block is rewritten and a soft error reported. This type of drive does not use an Error Correction Code. It relies on a Cyclical Redundancy Code check (CRC) to detect an error and rereading to correct the error. If a CRC error is detected during a reading operation, the device reports a soft error.

Other DC 6000 Drives

Soft errors are reported on 1,024-byte blocks. These type of drives use Error Correction Code (ECC) to correct errors. Storage Manager monitors rewrites and ECC usage.

Maintaining Your Tape Device

Tape drives require regular maintenance. If dust or debris collects at one or more of the tape heads or in the tape path, magnetic media may become unreadable or unwriteable.

To reduce the possibility of hardware or media errors, establish a regular cleaning schedule. Failure to maintain your drive properly **will void your warranty**.

In Device Manager, if the **Cleaning Required** check box is turned on, you should clean your drive. If you have an autoloader, this parameter indicates that your cleaning cartridge is either full or defective. If you have a standalone tape drive, this parameter prompts you to perform a cleaning operation.

TIP: For tape drives that support cleaning detection through motion tracking (for example, Exabyte 4mm and 8mm drives), Storage Manager will also record a message in System Messages database if a drive needs to be cleaned.

Storage Manager automatically schedules the cleaning of the device's drive and loads the cleaning cartridge if the following conditions are true for your device:

- You have properly configured an autoloader that supports cleaning detection.
- You have installed AutoLoader Software.

NOTE: For instructions on maintaining optical drives, please refer to the manufacturer's documentation.

Palindrome provides a list of recommended cleaning practices for each tape drive below. Use only manufacturer-approved cleaning cartridges available from Palindrome or your authorized dealer.

Palindrome specifies use of its cleaning cartridges because some cleaning cartridges are very abrasive and may damage the tape heads and void your warranty.

Do not exceed the recommended maximum number of cleaning passes with a single cartridge. Refer to the documentation supplied with the cleaning cartridge for specific instructions on cleaning procedures.

DC 6000 Tape Drives

Palindrome recommends cleaning the recording head after each initial pass with a new tape cartridge, in addition to cleaning after every eight hours of read, write or erase activity.

Clean the sensor openings and tape cartridge cavity whenever you can see dust or debris inside the cartridge cavity.

NOTE: Do not over-clean DC 6000 tape drives. Excessive cleaning will reduce tape head life.

4mm DDS DAT and DDS-DC DAT Tape Drives

Clean the tape head/path of 4mm tape drives after each initial pass with a new tape cartridge, as well as every 25 hours of data transfer, whichever comes first.

Whenever the Cassette In Place Status LED flashes (the green light at the front of the drive), you should clean the drive heads with a data grade cleaning cassette (do not use cleaning cartridges designed for audio DAT machines).

8mm, 2.2GB Tape Drive

8mm, 2.2GB tape drives require cleaning of the tape head/path once a month or after 30 hours of data transfer, whichever comes first.

Cleaning as often as once a week may be necessary. **Do not use** video machine cleaning tapes. They often consist of only plastic tape, which can abrade tape heads. Use only a data grade dry cloth cleaning cartridge.

8mm, 5.0GB Tape Drive

8mm, 5.0GB tape drives require cleaning of the tape head/path once a month or after 30 hours of data transfer, whichever comes first.

Cleaning as often as once a week may be necessary. Do NOT use video machine cleaning tapes. They often consist of only plastic tape, which can abrade tape heads. Use only a data grade dry cloth cleaning cartridge.

NOTE: Run the cleaning tape immediately after a new blank tape is placed into service. New tapes carry debris along their edges due to the manufacturing process.

8mm Tape Drive Replaceable Air Filter

8mm tape drives have a replaceable air filter. This should be inspected (and replaced if necessary) every 30 days or during normal cleaning intervals. If dust or dark and light patterns are visible on the filter, or if the filter is torn, discard it and replace it (contact your Palindrome Authorized Reseller for replacements).

To replace the air filter

1. Power off your tape drive.
2. Grasp the top of the filter retainer and gently pry it from the fan guard.
3. Remove the old filter from the filter retainer.
4. Place the new filter inside the filter retainer.
5. Replace the filter retainer. First, be sure the “hinge” is facing downward. Then put the hinge in place on the fan guard and snap the top of the retainer in place.

Maintenance Summary

The following table summarizes tape drive cleaning procedures discussed in this section.

NOTE: Failure to follow the prescribed cleaning practices, or meet the recommended environmental specifications, may void your warranty.

TAPE DRIVE	CLEANING FREQUENCY	SPECIAL INSTRUCTIONS
DC 6000	Clean the tape head/path every eight hours of read, write, or erase activity.	Clean the sensor openings and tape cartridge cavity whenever you can see dust or debris inside the cartridge cavity.*
DLT	Does not require periodic maintenance.	Use a cleaning tape only if *Use Cleaning Tape* light is on or if drive indicates excessive read/write errors.
4mm DDS DAT— 4mm DDS-DC DAT	Clean the tape head/path every 25 hours of data transfer.	If the Cassette In Place Status LED flashes**(the green light at the front of the drive), you should clean the drive heads with a Palindrome-approved cleaning cassette (do not use cleaning cartridges designed for audio DAT machines).
8mm, 2.2GB	Clean the tape head/path once a month or every 30 hours of data transfer.	Cleaning as often as once a week may be necessary.***
8mm, 5.0GB	Clean the tape head/path once a month or every 30 hours of data transfer.	Cleaning as often as once a week may be necessary.***

CAUTION: *Do not over-clean DC 6000 tape drives. Excessive cleaning will reduce tape head life.

******The slowly flashing green LED may indicate a damaged tape or a tape nearing the end of its life. If cleaning the head does not correct the flashing LED condition, replace the cassette and, if applicable, retire the tape using the Operations/*Retire* option available through Media Manager.

The slowly flashing LED does not indicate a loss of data, nor does it affect operation.

***Do not** use video machine cleaning tapes. They often consist of only plastic tape, which can abrade tape heads. Use only a data grade, dry cloth cleaning cartridge.

Failure to perform these simple preventive maintenance procedures results in excessive wear and tear on the unit. This wear and tear could result in failures during backup or restoration.

Appendix C

Disaster Recovery

Introduction

This section provides instructions for helping you to prepare for disasters (such as complete server failures). It outlines the steps you should perform prior to running recovery procedures. The basic topics are outlined below.

Disaster Recovery

Any organization that has experienced data loss due to a server failure or complete on-site disaster knows that disaster recovery planning involves more than just installing backup devices and reliable software.

You need software that can manage the complete recovery of your data as it existed before the disaster. Storage Manager not only provides backup, archiving, and migration but ensures your data is properly protected both on and offsite using its automated media scheduling and flexible backup schemes.

✓ ***TIP:*** Fires, earthquakes, winter storms, floods, etc. are always in the news. But broken water pipes, theft, long term power and telephone outages, etc. can also make it necessary to temporarily relocate critical business operations.

Palindrome Prepare! software is designed to simplify the creation and maintenance of a reliable Disaster Recovery Plan for all areas of your organization. Contact Palindrome for more information.

Understand Recovery Issues

In today's rapidly expanding networks, three key issues emerge in the disaster recovery category.

File Loss

The most common disaster administrators experience is file loss, not server or volume loss. Depending on the file, this type of disaster may be nearly as significant as a total server failure.

Storage Manager's powerful searching and tagging features and flexible media management options allow you to restore lost data quickly and efficiently by automatically determining the best media to restore the lost files.

Server/Volume Loss

Server/Volume loss is the second most critical disaster in today's LANs. While many products focus on the "backup window" (how long it takes to complete backups), Storage Manager is designed for "restore time objectives" (how long it takes to restore your server volume in case of a disaster).

Using its high levels of automation and intelligence, Storage Manager provides clear directives when recovering a server or volume. Because it tracks what media is on- and off-site, the software knows what media can restore your server or volume to its most recent state with the fewest amount of media changes.

On-site Disaster

Today, many organizations are realizing what impact a disaster can have on their entire business unit. Questions such as: "How can I recover if my server room is flooded?" and "What happens if I lose my entire building?" are being asked frequently.

Storage Manager is flexible so that you can configure it with your corporate objectives in mind. For example, you can automatically schedule snapshots of your accounting data once a month or configure full backups every day to a non-managed media so it can be sent off-site without affecting your media rotation schedule.

The Storage Manager Solution

Once configured, Storage Manager makes recommendations regarding what media should be on-site and offsite. Through automatic adjustments, the software always recommends actions that will insure objectives are met despite issues such as:

- Missed tape changes (due to 3-day weekends, etc.)
- Missed backups (due to drive or media failure or other factors)
- Interruptions to the schedule
- Scheduled media being unavailable (misplaced or offsite)

Preparing for a Server Failure

Introduction

This section details procedures how you can prepare for a server failure by recording server information and creating disaster recovery diskettes.

By following the instructions below, you can recover a NetWare server without having to completely re-install NetWare or Storage Manager.

The recovery procedures outlined in this section can serve as a template for your own server recovery procedure and should be followed for each of your protected servers.

When you are finished recording information and preparing diskettes, you should test the recovery procedures so you have experience with unexpected issues that may arise.

Assumptions

The following procedures assume:

- The person creating recovery diskettes and recovering servers has a good understanding of NetWare and Storage Manager.
- The server has a high-density floppy drive (the A: drive).
- The user has several blank formatted high-density floppy diskettes.
- The servers to be recovered will retain the same name and volume structure.
- DOS partitions on the servers have all DOS utilities including FDISK.EXE, FORMAT.COM, BACKUP.EXE, RESTORE.EXE, etc.

- On 4.1 servers, NDS partitions have been replicated according to Novell recommendations. In other words, either a MASTER or R/W replicas of the partition which contains the server to be recovered exists on other servers within the tree.

Record Server Information

By recording information about your server's environment, you will have the required information to restore the server to its previous state prior to a server crash.

Review Your Server Environment

➤ Review and understand the layout of the server.

Is the SYS: volume physically on a separate hard drive compared to the DOS partition?

➤ Review and understand the network protocols being used by the server.

How do these protocols interact with server related issues such as SAPs and TIMESYNC?

➤ For 4.1 servers, review and understand the structure of your NDS tree and how the server fits into that structure.

Are the NDS partitions replicated according to the Novell recommendation of three replicas per partition? Does the server to be recovered contain a read/write replica or a master? Is the auto login user object properly configured?

Run PALSDUMP

PALSDUMP is a Palindrome utility that provides summary information about your server's environment such as SET parameters, NCF files, and what modules you have loaded on the server. PALSDUMP is located on your last Storage Manager installation diskette in the \TOOLS directory.

To run PALSDUMP from the server console, type:

➤ **LOAD PALSDUMP**

PALSDUMP creates a PALSDUMP.DAT file on the root of your SYS: volume. Print the SYS:\PALSDUMP.DAT output file for later reference.

NLM Modules

Review the PALSDUMP.DAT printout to determine what NLMs are required to restore the server.

NLMs such as Virus or CD Rom drivers do not need to be loaded for a recovery, but special LAN drivers, name space NLMs, or configuration files do need to be loaded.

TIMESYNC

On 4.1 servers, it is necessary to document the type of time server. If preparing a 4.1 server, perform the following; otherwise, skip to *Recording Partition Information*.

At the server console prompt, type:

➤ **SET TIMESYNC TYPE**

If the server is a PRIMARY, REFERENCE, or SECONDARY time server type, then no further action will be needed. If the server is SINGLE time server, then another server in the tree will need to be designated as a new SINGLE time server type during the recovery. This will be covered in the section entitled *Setting TIMESYNC Type*.

Record Partition Information

Run INSTALL.NLM and document ALL information about the NetWare partitions and volumes. Pay close attention to the volume names, volume sizes, block sizes, file compression, sub-allocation, and migration.

At the server console prompt, type:

➤ **LOAD INSTALL**

➤ Choose *Disk Options* and record partition information for each disk on your server. (On 3.x servers, highlight each drive and press <**Enter**> to see detailed partition information.)

➤ Choose *Volume Options*. Select a volume and press <**Enter**>. Record all volume information for each volume.

Make a copy of all the information you recorded in the previous steps and store a copy both on-site and off-site.

Create Recovery Diskettes

By creating recovery diskettes, you can easily rebuild your server in the event of a server crash without having to manually re-install NetWare as a separate step. You will create the following diskettes:

- Diskettes containing DOS boot information and NetWare startup files.
- A diskette containing the necessary network files to perform data recovery.
- A diskette containing the necessary Palindrome files to perform data recovery.

Create "DOS_BOOT" Diskette(s)

NOTE: If the DOS partition does not need protection, skip this section.

The diskette(s) generated in the section will be used as the bootable floppy when necessary to recover DOS partitions. Label the diskettes DOS_BOOT1, DOS_BOOT2, etc.

Before starting the following procedures, be sure to have enough blank, formatted diskettes to copy your entire DOS partition.

To create the DOS_BOOT diskettes:

1. Down your server.
2. Place a blank, high-density floppy in the disk drive of your server.
3. From the DOS prompt, type:

   FORMAT A: /S
   (where A is the drive you are using).

   It is important that the diskette is formatted at the server to ensure the DOS version used to boot off the diskette is identical to the DOS version on the server. Label this diskette DOS_BOOT1.

4. Copy FORMAT.COM, FDISK.EXE, RESTORE.EXE, and any other utilities you feel might be needed to DOS_BOOT1 from the DOS partition on your server. If copying these files from a workstation, be sure the workstation is using the same DOS version as your DOS partition.
5. Remove DOS_BOOT1 diskette and insert another blank, formatted diskette.
6. From the DOS prompt, type:

   BACKUP C:\ A: /S
   (where A: is the drive your diskette is in and C: is your DOS partition)
   This command duplicates your DOS partition onto the floppy diskettes.

   Insert as many floppy disks as needed to backup the DOS partition. Label the diskettes in sequential order (for example, DOS_BOOT2, DOS_BOOT3, etc.).

7. Repeat the previous step as necessary to copy your entire DOS partition.

8. When finished copy the DOS partition to the diskettes, from the DOS prompt, type:

   FDISK
   and document the information about the DOS partition (e.g., size, volume label, DOS version etc). Keep this information with your BOOT diskette(s). If you ever upgrade DOS versions, you must recreate the DOS boot diskettes.

Create Recovery Diskettes

The following procedures use the PKZIP™ compression utility to compress and copy files onto multiple diskettes. If you do not have this utility, you must manually copy the files onto diskettes.

Prior to copying the files, create a directory structure on the network or local drive to copy the files into.

To prepare files for recovery diskettes

1. Create a directory named RECOV on a NetWare or local drive.

2. Create \SYSTEM, \LOGIN\NLS, \PAL subdirectories under the RECOV directory using the DOS MKDIR command. The directory structure should look similar to:

   \RECOV
   \SYSTEM
   \LOGIN\NLS
   \PAL*

   *If your Storage Manager NLMs are located in the SYS:\SYSTEM directory you do not have to create a \PAL directory.

3. Copy the following files from the SYS:\SYSTEM (or equivalent) directory to the \RECOV\SYSTEM directory you just created. Note that not all files apply to all NetWare versions. For example, the DS*.NLM files apply to NetWare 4.x only.

3C5X9.LAN*
ETHERTSM.NLM*
AFTER311.NLM
MSM.NLM
NWSNUT.NLM
INSTALL.NLM
EDIT.NLM
AUTOEXEC.NCF
DS.NLM
DSI.NLM
DSAPI.NLM
DSREPAIR.NLM
CLIB.NLM
MATHLIB.NLM (or MATHLIBC.NLM)
STREAMS.NLM
TLI.NLM
IPXS.NLM
TSAxxx.NLM+
SMDR.NLM
AHA*.DSK (SCSI host adapter driver)
ASPITRAN.DSK (ASPI module)
SPXS.NLM (and related patches [SPXFSFIX, etc.])

*substitute equivalent NIC LAN driver and proper Topology Support modules
+Copy the appropriate TSAs for your server.

If your hard disk drivers are not loaded from your DOS partition via the STARTUP.NCF file, copy these to the \RECOV\SYSTEM directory also (reference the PALSDUMP printout).

NOTE: If this server is NOT the Storage Manager installation server, you do not need to copy the Palindrome files (PAL*.NLM) you can skip the next two steps.

4. Copy the following files from the SYS:\SYSTEM directory to the \RECOV\SYSTEM directory. If your Storage Manager NLMs are located in a different directory than SYS:\SYSTEM copy them from their directory to the \RECOV\PAL directory.

   ARNANDX.RSF
   ARNADAT.RSF
   PALREST.NLM
   PALMEDIA.NLM
   PALSDRV.NLM
   PALLIB.NLM
   PAL.NLM
   PALALDRV.NLM
   PALJSRVR.NLM

5. For 3.12 and 4.1 servers, copy SERVER.MLS from the server's NetWare license diskette (or CD ROM) to the RECOV\SYSTEM\ directory.

   Different versions of NetWare may have different modules. All of the above files may not apply to your particular servers. Copy any additional NLMs or other files (such as namespaces) that might be needed after reviewing the PALSDUMP.DAT file.

6. From the SYS:\LOGIN\\NLS directory on 4.1 servers, copy *.001 files to the \RECOV\LOGIN\\NLS directory.

PALFCOPY.NLM

PALFCOPY.NLM (part of the TOOLS.EXE self-extracting file in the \TOOLS directory on diskette #4) is a Palindrome utility that allows you to copy files directly from your server's floppy drive to a mounted NetWare volume. By using PALFCOPY.NLM, you don't need a workstation to recover a server.

➤ Copy PALFCOPY.NLM from the \TOOLS directory on your last Storage Manager installation diskette to the \SYSTEM directory.

To create the recovery diskettes

To perform the following, you need multiple blank, high-density formatted diskettes. Label them RECOVERY1, RECOVERY2, etc. for each disk you create during the following steps.

NOTE: If you do not have PKZIP.EXE, copy the contents of the \RECOV directory onto the blank diskettes.

1. Insert a blank diskette into the local drive at your workstation.
2. At the \RECOV directory prompt, type the following command:

   PKZIP A:RECOV.ZIP *.* -r -p -&

   (this command compress the directories and files in the \RECOV directory into a compressed file RECOV.ZIP. The RECOV.ZIP file will span multiple diskettes.
3. Copy PKUNZIP.EXE to the last diskette.

   You have completed creating recovery diskettes.

Store the Recovery Diskettes

Make copies of the recovery diskettes and the NetWare environment information (recorded previously) and store in an on-site and off-site location such as in a vault.

Recovery from Server Failure

The following procedures provide instructions for rebuilding DOS and NetWare partitions, recovering the minimum NetWare and Palindrome modules, and then recovering all other data on failed servers.

If you created the recovery diskettes and recorded the server environment information as explained previously, you do not have to re-install NetWare to get your server running.

On a failed server, to...	See page...
Create DOS partitions	C-16
Create NetWare partitions and Volumes	C-17
Restore NetWare Modules	C-20
Restore Storage Manager	C-22

Some of the procedures may have to be adapted to suite your environment. For example, not all server failures will require you to recreate a DOS partition.

Prior to restoring the server, retrieve the recovery diskettes and NetWare environment information created during the server recovery planning steps (see page C-6).

Setting TIMESYNC type (4.1 servers only)

If the server you are recovering is a SINGLE-type time server, then another server in the tree must be designated as the SINGLE time server. Locate another server in the tree and at that server's console, type:

➤ **SET TIMESYNC TYPE = SINGLE**

NOTE: You can have only one "SINGLE"-type time server within the network.

Installing Hardware

If you are recovering a Storage Manager installation server, install the same type of host adapter and backup device on the new server. Be sure the backup device has the same SCSI address as on the original server.

Creating DOS Partitions

This procedure assumes your DOS partition on your server is no longer operational. Prior to restoring the DOS partition, obtain the server information recorded earlier (see page C-7).

If your server failure necessitates recreating DOS partitions, follow the procedures below; otherwise skip to *Creating NetWare Partitions*.

To restore DOS partitions:

1. Insert the DOS_BOOT1 diskette into the floppy disk drive on your server and power on the PC.
2. Enter the date and time when prompted.
3. At the DOS prompt (A:\) type:

   FDISK

4. Choose *Create DOS Partition or Logical DOS Drive*. Choose *Create Primary DOS Partition.*
5. When prompted for the partition size, enter the parameters recorded when you recorded the server environment information for this server.
6. At the main menu, choose *Set Partition Active* and select the primary DOS partition.

7. Press <ESC> to exit FDISK.

8. When the PC is done rebooting, enter the date and time when prompted.

9. At the DOS prompt (A:\), type:

   FORMAT C: /S
   (where C: is the DOS partition you are creating)

10. From the DOS prompt, type:

    RESTORE A: C:*.* /S

    and insert the requested floppy disks as needed to restore the DOS partition.

11. When finished restoring the DOS partition, reboot the machine to ensure system is bootable.

Creating NetWare Partitions and Volumes

Prior to recreating the NetWare partitions, you need to restore the files from the recovery diskettes to the DOS partition so they can be loaded on your server.

Be sure your DOS partition has adequate space to restore the files from the recovery diskette. Remove obsolete files if necessary from the partition.

Copying Recovery Diskettes

Copy the contents of the Recovery diskettes to the DOS partition using the PKUNZIP™ command.

1. Create a \RECOV directory on your DOS partition using the DOS MKDIR command. Change to that directory.

2. Place the last recovery diskette into the local drive at the server and type:

   PKUNZIP A:RECOV.ZIP -d C:\RECOV

   (where A: is the drive your diskette is in and C: is your DOS partition.)

   This step recreates the \RECOV directory structure (that you created when making the recovery diskettes) on your DOS Partition which contains the required NetWare and Palindrome files.

   Prior to rebuilding the NetWare partition, be sure you have the printout from PALSDUMP (PALSDUMP.DAT) available and the partition information recorded as part of the recording server information steps beginning on page C-7.

1. Type **SERVER** from the NetWare directory in DOS.

2. When prompted, type the FILE SERVER name and IPX INTERNAL ADDRESS (refer to the AUTOEXEC.NCF file and the PALSDUMP.DAT printout as necessary).

3. From the server console prompt, type:

   SEARCH ADD C:\RECOV\SYSTEM

4. Type **MODULES** at the server console to verify whether hard disk drivers have been loaded via the STARTUP.NCF file. If not, load them now.

   For example, type **LOAD ISADISK.DSK** (where ISADISK.DSK is the name of your hard disk driver) and choose parameters according to NCF files (review the PALSDUMP printout if necessary). If these drivers are loaded from your STARTUP.NCF file, then this step is not required.

5. Type the following command:

   LOAD INSTALL

For NetWare 4.1 servers

- Choose *Disk Options*. Choose *Modify Disk Partitions and Hot Fix*. Recreate the former NetWare disk partitions according to the server environment information you recorded.
- Choose *Volume Options*. Recreate the former server volumes according to the server environment information you recorded.
- Mount all volumes when prompted.

For NetWare 3.1x servers

- Choose *Disk Options*. Choose *Partition Tables*. Recreate the NetWare partition according to the server environment information you recorded.
- After recreating the partitions, choose *Volume Options* and press <**Insert**> to create the volumes as they existed prior to the disaster according to the server environment information you recorded.

1. If you haven't already, at the server console prompt, type:

   MOUNT ALL
   (to mount all volumes on your server)

2. At the server console prompt, type:

   SEARCH ADD C:\RECOV\SYSTEM

3. Load LAN drivers and bind the proper protocols to them. Reference the AUTOEXEC.NCF file found in the PALSDUMP printout.

4. For NetWare 3.12 and above servers, license the server. From INSTALL.NLM, choose the license option and license the server. Press **<F3>** to specify a different path then type in:

   C:\RECOV\SYSTEM

Restoring NetWare Modules

1. Load any namespace modules (e.g., MAC.NAM) and add name spaces as appropriate using the "ADD NAME SPACE <name> to <volume>" command for all namespaces on all mounted volumes.

2. At the server console prompt, type:

   LOAD CLIB

3. At the server console prompt, type:

   LOAD PALFCOPY C:\RECOV*.* SYS:\ /S
   This command copies all NetWare and Palindrome NLMs to the appropriate directory on the SYS: volume.

4. To load server resources type the following commands depending on your version of NetWare. You may want to review your PALSDUMP.DAT file to determine what modules to load.

   LOAD IPXS
   LOAD MATHLIB (or MATHLIBC)
   LOAD TSA41 (or appropriate TSA for your server)
   LOAD DS.NLM
   LOAD SPXS.NLM
   LOAD DSAPI.NLM
   LOAD TSANDS (if necessary)

NetWare Directory Services (NDS) for 4.x Servers

Because the NDS database is located on the SYS: volume, a hard drive crash involving the SYS: volume is equivalent to removing NetWare 4.1 from the file server. In recovering the server, you will need to re-install NDS. This also requires the server be removed and then re-installed into the tree.

To re-install NDS, it is imperative to understand how the NDS tree is partitioned and which servers in the tree contain the replicas. It is also important to understand which servers contain a master compared to which servers contain read/write replicas.

To re-install NDS

1. At a workstation on the network, use NWADMIN'S Partition Manager and select each partition and record the replicas listed. Be sure to document what type of replica (if any) the server to be recovered contains. If the server contains the master of a partition, go to step 2; otherwise skip to step 4.

2. If the server to be recovered contains a master of a partition, you must designate a new master on a different server within the tree.

   Locate another server in the tree which contains an up-to-date read/write replica of the partition you need to change and run DSREPAIR. (Refer to Novell documentation for proper procedures on how to designate a new master).

3. At this point, the server to be restored should NOT contain a master of a partition.

4. Use NETADMIN to delete the volume objects associated with the server to be recovered.

5. Run INSTALL.NLM to install Directory Services onto the server.

6. From INSTALL.NLM's *Installation Options* menu, choose *Directory Options*. Choose Install Directory Services Onto This Server.

7. Select the tree on which the server resided, and then log in to NDS and re-establish the server into the tree with the same context that it had before. It is imperative that the server is placed into the tree exactly as it was before.

8. Since the server object already exists in the tree, you will receive the following messages from NetWare:

   An NCP server object (or an unknown object) with name <server name> already exists in context "OU=SE.O=PALINDROME". Press <Enter> to continue. Install-4.1-389.

9. Press <**Enter**> to continue. The following message appears: Delete the existing NCP server object and continue?

10. Choose **YES**.

    After Directory Services Installation is complete, Install the mounted volumes into the directory tree.

    From INSTALL.NLM Installation Options menu, choose Directory Options. Choose Install/*Reinstall Mounted Volumes into Directory*. Be sure to install ALL volumes into the tree.

NOTE: The volume objects may have already been installed into Directory Services via the Directory Services install.

Restoring Storage Manager

NOTE: If this is not the Storage Manager installation server, skip this section.

1. Load the SCSI device drivers. For example, type:

   LOAD AHA1740.DSK port=XXX
   reference the PALSDUMP printout to verify the command syntax.

   Be sure to load all SCSI device drivers in the same order as on the original server. If your ASPI module isn't autoloaded, load it now.

2. Ensure the most recent backup tape is inserted in the backup device. If any of the following operations causes a PLSM-53 error, verify the appropriate SMDR and TSA have been properly loaded.

3. If this is the backup server, restore the System Control Database. If necessary, add a search statement to your Storage Manager NLM files first.

4. At the server console prompt, type:

   LOAD PAL

5. Select **Recover System Control Database**.

6. Select the volume and path of your installation (the location of your System Control Database [AS*.PAC] files).

7. Type your auto login user name and password in the appropriate fields. Select *Start Recovery*.

   If you receive a PLSM-110 error, this indicates the auto login user or password defined in the System Control Database (AS*.PAC files) does not have login rights to the server using the TSA.

   If the bindery does not exist, type **Supervisor** with no password in the auto login user name and password fields. If NDS does not exist, type in **ADMIN** with no password.

8. If you typed in an auto login name different than that which is in the restored System Control Database, you will be prompted to use the original user or the new user.

   If the bindery or NDS needs to be recovered, continue to use **Supervisor** or **Admin**. After they are restored, update the System Control Database with the original auto login user name using the *Upgrade Auto Login Information* option on the Palindrome Server Console.

9. After the System Control Database is restored, select *Backup or Restore Resources.*

10. Highlight a resource on the server you are restoring (if recovering a 3.x server, recover the Bindery resource first).

    Select <**Restore**>. Repeat this step for each volume on the server you are restoring.

Final Steps

This section details the final tasks necessary to completely restore your server.

4.1 Servers

- After server restoration is complete, verify your NDS partitions are replicated properly according to Novell's recommendations.
- Verify the time server type is correct on the recovered server.
- Verify the recovered server's time is synchronized on the network by typing **TIME** at the server console.
- If the recovered server contains partition replicas or a master, verify the server's synchronization state. To do this, at the server console, type the following commands:

  SET DSTRACE=ON
  SET DSTRACE=*H

  Toggle to the directory services screen and check it for the message "ALL processed=YES" for each partition on the server.

All Servers

- When the last restore command is complete, at the server console, type the following commands:

  DOWN
  EXIT

- At the DOS prompt, type:

  SERVER

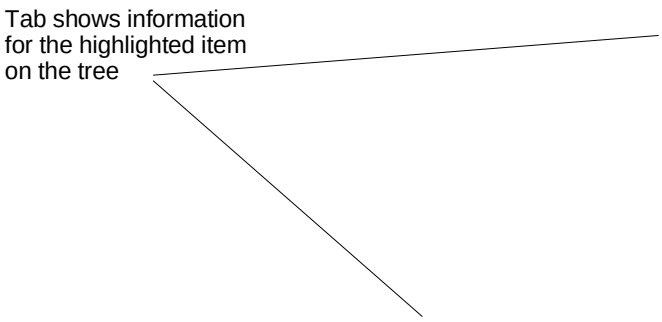
  Your server is now restored to its former operating state.

Appendix D

Viewing Installation Information

For each item represented in the tree window, there is at least one corresponding tab with information about that item.

To view information about an item



Viewing Information for the CP40 (Backup) Session

➤ Highlight the item you are interested in. As you highlight an item on the device tree, one or more tabs appear in the information window.

Resource Manager Information Tabs

Installation Information

Installation tab

Parameter	Description
Name	The installation name defined in Configuration Manager. By default, this name is the server/volume and directory location of the System Control Database.
Type	The name of the Palindrome product.
Database Version	The name version number of the Palindrome product.

Target Service tab

Parameter	Description
Protected Resources	The number of resources configured for protection by this installation.

Target Service Information

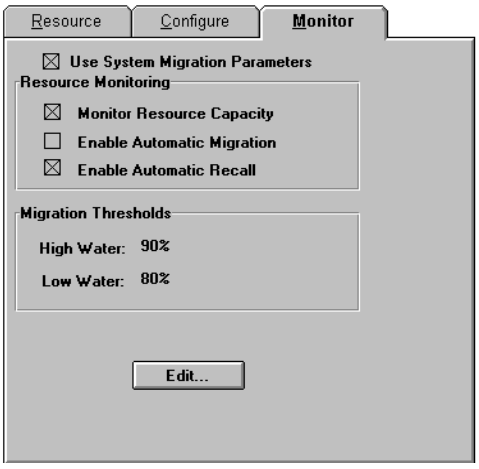
Resource tab

Parameter	Description
Target Service Agent Name	The name of the TSAs associated with this resource.
Target Service Name	The name of the target service (server or workstation).
Login User Name	The name of the auto login user.

Configure tab

Resource Information

Parameter	Description
Information	
Name	The name of the resource such as the volume or drive letter.
Size	The size of a volume resource; the size is not available for non-volume resources.
Type	Indicates the type of resource (**Volume Resource** or **Non-Volume Resource**).



Monitor tab

Parameter	Description
Sequence Number	The order in which Storage Manager processes the resource during automatic operations.
Last Operation	
Type	The operations that Storage Manager most recently performed on the resource.
Time	The date and time that Storage Manager most recently performed any operation on the resource.

Parameter	Description
Resource Name	The name of the current resource.

Parameter	Description
History Database Server/Volume Location	The server and volume where the resource's File History Database resides.
History Database Path	The directory path where the resource's File History Database resides.
Tracking Name Space	The tracking name space Storage Manager uses for files on this resource.
Included for Automatic Operations	Indicates that the resource is included (box is checked) in or excluded (box is empty) from automatic operations.

Parameter	Description
Resource Monitoring	
Monitor Resource Capacity	Indicates whether Resource Monitor monitors disk utilization of the highlighted resource. This option must be turned on in order to enable the Enable Automatic Migration option.
Enable Automatic Migration	Indicates whether Storage Manager automatically migrates eligible files on the highlighted resource when the disk reaches its high water mark. Storage Manager migrates as many eligible files as necessary to reduce each disk's utilization to the low water mark. Storage Manager may build or update the list of eligible files (prestage list) and migrate additional files if necessary.

Class tab

Parameter	Description
Enable Automatic Recall	Allows Storage Manager to process a recall job when a user attempts to open a phantom file located on this resource. The appropriate recall agent(s) must also be loaded.
Migration Thresholds	

SMDR tab

Parameter	Description
High Water Mark	Indicates the upper limit of the disk's utilization as a percentage of the disk's total capacity. When automatic migration is enabled, disk utilization above the high water mark initiates a migration job.
Low Water Mark	Indicates the disk utilization level to which Storage Manager attempts to migrate during resource-level operations.

NOTE:

Installation tab

	You can select a percentage from 0-100. If you set the level above 95%, the hard disk may not be able to save critical files because the volume reaches capacity before Storage Manager has the chance to migrate inactive files.

The *Sort by Type* view includes a Class tab, and the *Sort by Location* view includes a SMDR tab.

Library tab

Class Information

Parameter	Description
Protected Type	Indicates the type of protected resource.

Details tab

SMDR Information

Parameter	Description
SMDR Name	Indicates the name of the SMDR installed on the installation server.

Media Manager Information Tabs

Media Set tab

Installation Information

Parameter	Description
Active Library	The name of the current library.
Managed Media Information	
Libraries	The total number of libraries created by this installation.
Media Sets	The total number of media sets in the managed and non-managed libraries.

Details tab

Parameter	Description
Media	The total number of media in both the managed and non-managed libraries.

Media Library Information

Parameter	Description
Name	The name of the media library.
Rotation Pattern	The type of rotation pattern (**Tower of Hanoi** or **GFS**) that determines which media are used for automatic operations.

Media tab

Parameter	Description
Last Rotation	The most recent date on which a media set was called for rotation. Does not apply to non-managed media.
Active	Indicates whether the media in the library is active (**Yes**) or retired (**No**).

Details tab

Parameter	Description
Media	
Number of Sets in Library	The number of media sets in the media library.
Total Number of Media in All Sets	The number of media in the media library.
Library Usage (bytes)	
Capacity	The number of bytes in the media library's total storage capacity.
Free Space	The number of bytes available for writing additional sessions.

Statistics tab

Parameter	Description
Backup	The number of bytes used for backup files.
Archive	The number bytes used for archive files.

Media Set Information

Parameter	Description
Name	The name of the media set.
Last Rotation	The date the media set was most recently rotated.

Parameter	Description
Rotation Status	Indicates whether the media set is active or retired from rotation.
Near Line Set	Indicates whether the media set is a near line set (**Yes** or **No**).

Session tab

Parameter	Description
Number of Media in Set	The number of media in the media set.
Media Set Usage (bytes)	
Capacity	The media set's total storage capacity.
Free Space	The number of bytes available for writing additional sessions on the media set.
Backup	The number of bytes used for backup files on the media set.

Parameter	Description
Archive	The number of bytes used for archive files on the media set.

Statistics tab

Media Information

Parameter	Description
Name	The media label.
Number of Sessions	The number of sessions located on the media.

Parameter	Description
Active	Indicates whether the media is active (**Yes**) or retired (**No**).
Full	Indicates if the media is full (**Yes**) or has available capacity (**No**).
Type	The type and capacity of the media.
Bar Code	The bar code label assigned to the media.

Parameter	Description
Operation	

Server tab

Parameter	Description
Last Operation	The type of operation that was most recently written to the media.
Last Formatted	The date and time a format operation was most recently performed on the media.
Media Usage (bytes)	
Capacity	The media's total storage capacity.

Adapter tab

Parameter	Description
Free Space	The number of bytes available for writing additional sessions on the media.
Backup	The number of megabytes used for backup files on the media.
Archive	The number of megabytes used for archive files on the media.

Configure tab

Parameter	Description
Read/Write Activity	
Total Bytes Read	The cumulative number of bytes read on this media since the media was labeled for this installation.
Total Bytes Written	The cumulative number of bytes written on this media since the media was labeled for this installation.
Soft Errors	

SCSI tab

Parameter	Description
Percentage of Rereads	The cumulative number of units that have been reread divided by the cumulative number of units that have been read from this media. This will display a value of zero until you restore data from the media.
Percentage of Rewrites	The cumulative number of units that have been re-written divided by the cumulative number of units that have been written to this media. Units are specific to devices. The program does not display this statistic for devices that do not record soft error statistics.

Parameter	Description
Above Reread Threshold	Indicates whether the read soft errors exceed (**Yes**, **No**, or **Unknown**) a fixed percentage of read errors that are acceptable for this particular type of media. Some devices may not be able to calculate this statistic. In these cases the program will report **Unknown**. The program also reports **Unknown** if no data has been restored from the media.
Above Rewrite Threshold	Indicates whether the write soft errors exceed (**Yes**, **No**, or **Unknown**) a fixed percentage of read errors that are acceptable for this particular type of media. Some devices may not be able to calculate this statistic. In these cases the program will report **Unknown**.
Usage	
Number of Opens	The number of times the media's index has been opened.
Number of Passes	For tape media only. The number of times a device head has passed over the media. Opening the media index is considered two passes; writing a session after opening the index is considered one pass; and verifying a session after opening the index is considered one pass.
Number of Overwrites	The number of times the media has been overwritten as a result of automatic operations. This statistic does not apply of non-managed media.

Session Information

Configure tab

Parameter	Description
Name	The session type and number. “CP” indicates a backup session. “SV” indicates an archive session.
Job ID	The job ID corresponding to the session.
Resource	The name of the resource the session data was copied from.
Tracking Name Space	The tracking name space used to write the session.
Number of Files	The number of files in the session.

Status tab

Parameter	Description
Size	The number of bytes required to store the session.
Type	The type of operation that generated the session, for example, **Full Backup**.
Start Time	The time at which Storage Manager began writing the session.
End Time	The time at which Storage Manager completed writing the session.

SCSI tab

Parameter	Description
Read/Write Activity	
Bytes Read	The cumulative number of bytes read from this session.
Bytes Written	The number of bytes written to this session.
Read Accesses	Number of times the session was opened for reads.
Soft Errors	

Parameter	Description
Percentage of Rereads	The cumulative number of units that have been reread divided by the cumulative number of units that have been read from this media. If after you your first restore operation this parameters continues to display **Unknown**, the device may not be able to calculate this statistic.
Percentage of Rewrites	The cumulative number of units that have been rewritten divided by the cumulative number of units that have been written to this media. Units are specific to devices. The program does not display this statistic for devices that do not record soft error statistics. In these cases the program will report **Unknown**.
Above Reread Threshold	Indicates whether the read soft errors exceed (**Yes**, **No**, or **Unknown**) a fixed percentage of read errors that are acceptable for this type of media. Some devices may not be able to calculate this statistic. In these cases the program will report **Unknown**.
Above Rewrite Threshold	Indicates whether the write soft errors exceed (**Yes**, **No**, or **Unknown**) a fixed percentage of write errors that are acceptable for this type of media. Some devices may not be able to calculate this statistic. In these cases the program will report **Unknown**.
% of Rereads in Last Access	The number of units reread divided by the number of units read when the program last opened the session.

Statistics tab

Device Manager Information Tabs

Server Information

Parameter	Description
Name	The name of the installation server to which the devices are connected.
Number of SCSI Host Adapters	The number of SCSI adapters connected on the Storage Manager installation server.
Number of Configured Devices	The number of backup devices configured in the Storage Manager database.

Adapter Information

Parameter	Description
Name	The manufacturer's name and model number of the adapter.
Driver	The manufacturer's name and the version number of the device driver used by the adapter. This information may vary as the parameter displays the information made available through the ASPI interface.
Number	The number of the adapter.
SCSI Bus Target ID	The SCSI Bus address of the adapter.

Autoloader Information

Parameter	Description
Number of Slots	The number of slots in the autoloader.
Number of Drives	The number of drives in the autoloader.
Slot Usage Restrictions	
You can edit the following parameters through the *Edit Device* menu option.	

Parameter	Description
First	The first slot location in a range of slots reserved for Storage Manager.
Last	The last slot location in a range of slots reserved for Storage Manager.
Cleaning Cartridge	The slot location of the cleaning cartridge. While your device may have a fixed cleaning slot, all of the device's slots appear identical to the software.

Parameter	Description
Manufacturer	The name of the manufacturer of the autoloader.
Product	The model name of the autoloader.
Type	The type of backup device.
Firmware	The version number of the firmware that operates the device.
Removable Media	Indicates whether the device writes to removable media (such as tape). The program does not support devices with nonremovable media.
Supported Device	Indicates whether the device is acceptable for use with the current program setup. For example, if you have not installed AutoLoader Software, the program cannot support the autoloader device. The program will use the device as a standalone backup drive. Also, this parameter does not reflect the status of the firmware; the program does not support devices with unacceptable firmware.
SCSI Address	
Target	The device's SCSI address.
Logical Unit	The SCSI logical unit number of the autoloader (media changer).

NOTE: If you are unable to perform operations with a device, you may want to verify that Storage Manager supports your firmware as well as the device. For the latest version of the Certified Device List, download CDL40.ASC from the Palindrome BBS.

Device Information

Parameter	Description
Name	Displays any name you assign to the device. By default, the program labels a device with the SCSI target and logical unit numbers.
Operational Priorities	
The following three options indicate the operations you want the device to perform and the order of preference. For example, priority **1** indicates that the device, if available, is Storage Manager's first choice to perform that operation.	
Backup	Values are **1** - **99**.
Archive	Values are **1** - **99**.
Restore	Values are **1** - **99**.
Near Line Device	Indicates that the drive is reserved for the near line media set. You can only use the near line set in this device.

Parameter	Description
Device State	
If an option appears dimmed, the device does not support the option.	
Cleaning Required	Indicates that the drive needs cleaning.

Parameter	Description
Compression	Indicates whether a device's compression feature is enabled (**Enabled**) or disabled (**Disabled**).
Mounted Media	
Label	The label of the mounted media. If the program cannot read the label, the program determines whether it is one of the following types: —Cleaning media (**Clean**) —New optical disk (**Unformatted**) —Formatted media that is ready for use (**Blank**) —Formatted with an unrecognizable file system (**Unknown**). —Non-managed media (**Export**).
Format	The format of the mounted media: **SIDF**, **PALDF**, or **Unknown**.
Type	The type of media mounted in the device, such as 8mm tape.

Parameter	Description
Manufacturer	The name of the device's manufacturer.
Product	The name and model number of the device, if applicable.
Type	The type of backup device such as a tape drive.
Firmware	The version number of the firmware that operates the device.
Removable Media	Indicates whether the device writes to removable media (such as tape). The program does not support devices with nonremovable media.
Supported Device	Indicates whether the device is acceptable for use with the current program setup. Also, this parameter does not reflect the status of the firmware; the program does not support devices with unacceptable firmware.
SCSI Address	
Target	The device's SCSI address.
Logical Unit	The SCSI logical unit number of the device.

NOTE: If you are unable to perform operations with a device, you may want to verify that Storage Manager supports your firmware as well as the device. For the latest version of the Certified Device List, download CDL40.ASC from the Palindrome BBS.

Parameter	Description
Device Usage	**+**
Bytes Written	The cumulative bytes written by this device since the device was configured for this installation.
Bytes Read	The cumulative bytes read by this device since the device was configured for this installation.
Device Usage Since Last Cleaning	
Bytes Written	The number of bytes written since the device was most recently cleaned or stated to have been cleaned by the administrator.
Bytes Read	The number of bytes read since the device was most recently cleaned or stated to have been cleaned by the administrator.
Last Cleaning	The date and time that the device was most recently cleaned. Some devices do not notify Storage Manager when they need to be cleaned and thus cannot have the program automatically record a cleaning. Administrators should follow their maintenance schedule and manually record that a cleaning has occurred.

Appendix E

Recalling Files

Overview

This chapter describes how to:

- Recall migrated files
- Configure server and workstation recall agents

Recall Operations

Recall Process

A recall operation is an operation in which Storage Manager automatically restores a file migrated from a NetWare server when an end user attempts to open its phantom file placeholder.

Unlike a restore job, the user does not access Palindrome's File Manager to select the phantom file to be restored and any other job parameters. Instead, the recall agent (either the server or workstation recall agent) automatically submits a job to restore the single, migrated file for the end user.

In the Job Queue window, the recall job is described as the “Automatic Recall Job”.

Recall Components

The following components are involved in recalling a file:

- A phantom file on the NetWare server representing a migrated DOS. OS/2, Windows, or Macintosh file.
- _PALRC40 directory is the directory on which recall jobs are placed to prior to being submitted to the job queue by Resource Monitor. A _PALRC40 directory must exist on all monitored volumes. Each end user must have “write” rights to the _PALRC40 directory on each server that is available for automatic recall.
- Resource Monitor (PALRMON.NLM), which retrieves recall jobs from the _PALRC40 directory and submits the recall job to the job queue. PALRMON.NLM must be loaded on the installation server, and the **Enable Automatic Recall** option must be selected from the Archive/Migrate tab. Loading PALRMON.NLM creates a _PALRC40 directory on all monitored resources.
- Job Server (PALJSRVR.NLM) and the restore module (PALREST.NLM), which process the recall job as any other restore job.
- Various recall agents for end user workstations:
  - PALRECAL.NLM, the module that creates the recall job for a file that an end user has attempted to open. This agent resides on a server. You can recall phantom files residing on the server. In OS/2 workstations, users can recall files only through the DOS window.
  - Windows recall agent (PALWINRC.EXE), the recall agent for Windows-based workstations.

- DOS recall agent (PALRECAL.EXE), a DOS recall agent, loaded on the workstation, which provides status messages regarding the recall job. This TSR (terminate-stay resident program) can also recall files on an OS/2 workstation through the DOS window.
- DOS recall agent (PALSMRCL.EXE), a DOS recall agent, loaded on the workstation, which beeps until the recall job has completed. This version of the DOS TSR requires minimal memory and provides minimal status information (beeping) while job is pending. This TSR (terminate-stay resident program) can also recall files on an OS/2 workstation through the DOS window.

WARNING: To ensure proper file restores, warn users not to copy, move, or rename phantom files (or rename the directories phantom files are in). If phantom files are put in a different location, when requested to be restored, only the zero-byte file will be restored, not the original file. The original file still exists on backup media.

Determine the location of the original file and restore it using File Manager.

Installing Recall Agents

If using Storage Manager's migration feature, recall agents provide a quick and easy method to restore migrated files.

When a recall agent detects a "open file" request of a phantom file, the recall agent immediately submits a restore request for the file, eliminating the need for an administrator or user to manually restore files. You are not required to install both workstation and server recall agents.

NOTE: You can load the Windows recall agent and one of the DOS recall agents on any workstation. You cannot run both DOS recall agents on the same workstation.

See sections "*Installing the Server Recall Agent*" and "*Installing the Workstation Recall Agents*" sections in chapter 3 of the *Installation Guide* for detailed instructions.

Recalling a File

A user can initiate a recall job through either the server or workstation recall agent. The migrated file must be represented by a phantom file for this operation to occur.

Using the Server Recall Agent

When a user attempts to open a phantom file on a server, the server recall agent assumes control of the application's interface. The keyboard is locked. The end user cannot return to the original application until the job has completed or the timeout period has expired, whichever occurs first. Deleting or holding the job through the Job Queue window also releases the end user from the server recall agent. To allow a user to resume activity as soon as possible, you should configure a timeout period to release the user from the agent without affecting the job.

If the user does not have rights to the _PALRC40 directory, the job will fail. The server recall agent does not display an error message, but you can configure it to notify users of failed recall requests with a NetWare SEND message.

Using a Workstation Recall Agent

When a user attempts to open a phantom file with a workstation agent loaded, one of the following windows appears (there is no window if using PALSMRCL.EXE):

Windows Recall Agent window

DOS Recall Agent window

To exit the "recall pending" mode

1. If you do not want to wait for the job to complete (or the configured timeout period to expire), you may also continue working in the original application. You cannot resize or move the Windows Recall Agent window.

NOTE: If the _PALRC40 directory does not exist on the resource (or if the end user has no rights to this directory), this pop-up window appears briefly with an error message before disappearing.

➤ To return to the original application while you wait, choose the **Continue** button. If using PALSMRCL.EXE, type "**C**".

Unless running the Windows recall agent in a DOS window, you cannot use another application (move to another window) while a recall is in progress unless you select *Continue*. If an open request is intercepted while in a DOS window, you will be able to switch to other applications.

➤ To delete the current recall job, choose the **Delete** button (or type "**D**"). You return to the original application.

➤ To turn off the beeping (for PALSMRCL.EXE only), type "**S**" (Silence).

2. At the bottom of the pop-up windows, the status line (not available if using PALSMRCL.EXE) displays the current state of the job:

Idle—Resource Monitor has no yet submitted the recall job to the job queue.
Submitted—The recall job has been submitted to the job queue.
Ready—The job is ready for servicing by the job server.
Servicing—The job is being serviced by the job server.
Completed—The recall request completed successfully.
Recall Failed—The job server finished processing the request and attempted to recall the file but the file was not restored
Not Submitted—The recall request could not be placed in the queue

Recall Job Status

Resubmitted—The job has been on server or operator hold and has been returned to the queue.
Operator Hold—An operator or administrator has put the job on hold. It will not be serviced until the hold is removed.
Aborted—The job has been aborted and not yet requeued.

If a job is submitted and the job server is not loaded, the pop-up screen will appear and remain in the "ready" state until PALJSRVR is loaded or the request is deleted or the timeout period has expired.

Deleting an Automatic Recall Job

The workstation recall agents allow you to delete the recall job from their respective windows.

To delete the recall job

➤ Choose the **Delete** button on the Windows Recall Agent window. The end user returns to the original application.

See the "Disabling Automatic Recall" section for additional configuration information.

You can also delete recall jobs initiated by an recall agent through the Job Queue window.

NOTE: You may notice that some Windows applications attempt to open files even after you have deleted recall requests. This is an application-specific function and cannot be controlled by the recall agent. Turn off the **Automatic Recall Enabled** option to halt further recall attempts. Choose the **Delete** button to delete the current recall job.

Server versus Workstation Recall Agents

If you want a majority of your users (or all of them) to have automatic recall available, you should load the server recall agent on all of your servers. If a client accesses a migrated phantom file on a server where the recall agent is installed, the job is submitted to the job queue through the Resource Monitor.

On the other hand, workstation agents are specific to the workstation they are installed on. That is, only the user using a workstation where the workstation agent is loaded can automatically recall migrated phantom files. The table below summarizes differences between the various recall agents.

Server Recall Agent (PALRECAL.NLM)

Users can recall files residing on the server from NetWare, DOS, OS/2, and Macintosh clients.

Recall Options	Timeout Option	Notification Option
To disable the server recall agent, see the /R option and the **Recall Automatic Enabled** option under the workstation agent recall options. You can also prevent recall jobs from being performed on a server by adding it to the PALRECAL.DAT file.	/T option indicates when control is returned to the application. This option does not interfere with the servicing of the recall job. At server console prompt, type: **PALRECAL /T***x* (x=number of minutes) **NOTE:** You should set the timeout period to avoid locking users in the "recall pending" mode.	/N indicate where to sends a NetWare SEND message (only if the recall fails), At server console prompt, type: **PALRECAL /N**(option type) Types are: **S**-Receive notification at a single location (where you initiate the recall) **A**-Receive notification at all logged-in locations **N**-Receive no notification

Windows Recall Agent (PALWINRC.EXE)		
Use this agent if Windows is the predominant operating environment (this agent can recall files through a DOS window).		
Recall Options	**Timeout Option**	**Notification Option**
The **Automatic Recall Enabled** option enables (disables) the automatic recall of files by the workstation recall agent and server recall agent . The **Unload Recall Agent** option (on the Control-box menu) disables only the Windows recall agent.	The **Timeout Threshold** indicates the number of minutes before returning to the application.	The **Email Address** parameter. This user should be defined on each workstation. The correct format is: **USER@WORKGROUP**

DOS Recall Agents (PALRECAL.EXE and "beeping" PALSMRCL.EXE)

Use either agent if DOS or OS/2 is the predominant operating environment (this agent can also recall files through Windows applications). In OS/2 workstations, end users can recall files only through the DOS window.

Recall Options	Timeout Option	Notification Option
/R (Recall) enables or disables the automatic recall function at the agent level. This option can disable or enable the server and workstation recall agents if both are loaded. /M (Monitor) enables or disables the monitoring of "open file" requests. When monitoring is disabled, the end user cannot recall files using the workstation agent. * /U (Unload) unloads the loaded workstation agent from memory. * *The end user may use the server recall agent.	/T (Timeout) option is used to indicate when control is returned to the original application. This option does not interfere with the servicing of the recall job. You should configure a time period to avoid waiting indefinitelyif the file is on off-site media, for example. At the DOS prompt, type: **PALRECAL /T***x* (where *x*=number of minutes the agent returns control to the original application)	/E (E-mail notification) indicates how Storage Manager notifies end users of failed recall jobs. At the DOS prompt, type: **PALRECAL /EUSR** (where **USR** is your predefined e-mail environment variable)

Configuring Recall Agents

Server Recall Agent

By default, the server recall agent controls the application the user is in when recalling a file until the job completes (successfully or unsuccessfully) or is deleted from the job queue. If there is no timeout period configured and Resource Monitor is not accessible, a user receives no notification and has no means of discontinuing the "recall pending" mode. You can configure the server recall agent to return control to the user after a defined time period. In the meantime, Storage Manager continues to complete the recall job.

NOTE: You should set the timeout period to avoid locking users in the recall pending mode. Usually, you should base the timeout period on average amount of time required to restore a migrated file. This estimate is based on whether your installation has a near line set, what type of physical media it uses, network traffic, and the number of job processed by the job server.

End users can receive NetWare SEND message regarding failed recall jobs. The option switch is /N and the types of options are:

N—None. End users receive no notification.

S—Single connection. End users receive notification at the workstation from which the end user recalled the file.

A—All connections. End users receive notification at all workstation to which they are logged in.

The workstation agents provide enhanced notification.

To configure the server recall agent

➤ At the server console prompt, load the PALRECAL module with the appropriate option settings. For example, type:

LOAD PALRECAL /T1 /NS

(where /T is the timeout option switch and **1** the number of minutes after which the agent returns control to the application where **/N** is the notification option and **S** indicates that end users receive notification at a single workstation).

The application will probably have a "file open" error if the recall job has not completed when the timeout expires. The user can try opening the file after the recall job is complete.

Workstation Agents

Normally, if Windows is the predominant operating environment load the Windows recall agent; if DOS is the predominant environment, load the DOS recall agent. The Windows agent works only in the Windows environment; the DOS agents work in both the Windows and DOS environments.

Both agents can intercept file open requests in either environment.

Windows Recall Agent

The Windows Agent Recall window always appears when a recall operation is active and disappears when a recall job completes or is deleted.

The Windows recall agent can intercept open requests from DOS or Windows applications, also.

Workstation agents are installed on individual workstations and intercept file open requests at each workstation. They can also be used to disable the server recall agent at specific workstations.

As with the DOS recall agents, you can identify a user to receive notification on failed restore jobs and configure a timeout threshold.

To open the Windows Recall Agent window

➤ To open the recall agent window, double-click the icon. Note that if the recall agent is already loaded and hidden, this does not load another copy of the recall agent into memory; it just opens the window for the agent that is already loaded.

To close the Windows Recall Agent window

➤ Click the Control-menu box in the upper-left corner to show available options. Choose *Hide Recall Agent* (as alternatives, you can double-click the Control box or use Alt-F4). The agent is still loaded an ready to recall a file.

✓ ***TIP:*** To automatically load the recall agent whenever starting Windows, copy or move the PALWINRC icon to your Windows StartUp Group. Refer to your Windows documentation for more information on loading applications when starting Windows.

You must open the Recall Agent window's Control menu when a recall operation is **not** active in order to modify configuration settings.

To configure the Windows Recall Agents

1. Open the Control menu and select *Configuration*. The Recall Configuration Options dialog box.

➤ To configure notification for a user, enter the username and workgroup in the **Email Address** parameter. The user will receive message notification if a recall job *fails*. This user should be defined on each workstation running the recall agent by his/her MHS-compatible name.

The correct format is: **USER@WORKGROUP** (for example, JSMITH@PALINDROME).

To configure the time period that elapses before control is returned to the application, enter the number of minutes in the **Timeout Threshold** parameter. By default, the recall agent window appears until the job completes.

For example, **Timeout Threshold=2** indicates that the recall agent window remains active for two minutes before returning to the application. As a result, the user can resume activity in the original application while waiting for the recall job to complete. Choose **OK** to save configuration changes.

2. In the Windows Recall Agent window, configure automatic recall for any user of the current workstation. Turn on (off) the **Automatic Recall Enabled** option to enable (disable) the automatic recall of migrated files by the workstation recall agent and server recall agent (if installed). When this option is disabled, "open file" requests fail.

➤ You can also configure the Windows recall agent through the PALWINRC.INI file in your Windows directory. The Windows recall agent loads according to its last configuration of the **Automatic Recall Enabled** option. For example, if you disabled this option and unloaded the agent, the option would be disabled when you next loaded the agent.

In the PALWINRC.INI file, the Recall Agent window parameter (**recallWindow**=*xxxx yyyy*) defines and maintains the position of the dialog box; **do not** modify this parameter.

NOTE: If for some reason a user corrupts the PALWINRC.INI file, you can delete the file and the recall agent will automatically recreate it. You must then re-configure the options for the recall agent.

DOS Recall Agent

PALRECAL.EXE produces a pop-up window when a user attempts to access a phantom file. (If a Windows application accesses a phantom file, the PALRECAL.EXE produces a "beeping" sound pending the completion of the recall job.)

The window provides status messages about the recall job. The user has the option of waiting for the job to complete in a locked state or returning (choose **Continue**) to the original application while waiting for the recall job to complete.

PALSMRCL.EXE is a requires less memory and provides less functionality than PALRECAL.EXE. Instead of displaying a pop-up window, PALSMRCL.EXE "beeps" pending the completion of the recall job or returning to the original application. Because PALSMRCL.EXE does not display a pop-up window, users can interact with the agent through the keyboard:

Press...	To...
C	Continue current task but proceed with the recall request (instead of waiting for the file to be restored).
D	Delete the recall job and return to the original application.
S	Silence (disable) continuous beeping during a recall.

NOTE: You cannot load either agent into memory more than once.

If running a program in a DOS window under Windows, the DOS recall agent works as it would running under DOS (for instance, the pop-up window displays if using PALRECAL.EXE; PALSMRCL.EXE beeps).

To configure DOS recall agents

➤ At the DOS prompt, type PALRECAL (or PALSMRCL) and the option(s).For example, type:

PALRECAL /T0 /EUSR
A message appears confirming the result of the command you entered.

/E Specifies the E-mail environment variable for message notification. This is the variable you may have configured for message notification for File Manager administrators and users. From the DOS prompt, type something similar to the following to enable message notification:
PALRECAL /EUSR
(where USR is your pre-defined E-mail environment variable.)

Note that end users will only receive E-mail notification on **failed** recall jobs. Also, the variable cannot be changed once loaded into memory without first removing the recall agent from memory (unloading the recall agent) and typing the command again.

/M A toggle which enables and disables monitoring of "open file" requests of phantom files . When this option is disabled, users at this workstation cannot access the workstation recall agent.

Note that this option can deactivate only the workstation agent and not the server recall agent. If the server recall agent is loaded on the server where the phantom file resides, it will intercept the "open file" request and submit the recall job, regardless of the status of the workstation recall agent.

/R A toggle that enables or disables recall functionality. When you load the agent the first time, it is enabled by default. If you load the agent with the /R switch (while the agent is already loaded), automatic recall will be disabled. As a result, the user at this workstation cannot access the server or the workstation recall agent.

NOTE: If you load PALRECAL with the /R switch and the server recall agent is also loaded (PALRECAL.NLM), no recalls will take place. When the recall agent is disabled at the workstation, the server based recall agent is also disabled.

The /M switch, however, does not disable the server recall agent's ability to submit restore requests however.

/T A toggle that determines the number of minutes you wait for the recall request to complete before returning to the original application (the default is to continue until the recall request as completed.) Once the timeout period has expired, you are returned to the original application. The recall job is still processed however.

Use this option if you're running recall jobs in unattended mode (for example, in a batch file), and you don't want the program to wait on a recall request that cannot be completed (for example, if the proper media was not available).
Example:
PALRECAL /T10

In this example, the recall agent will wait 10 minutes for the file open request to complete.

/U Unloads the loaded DOS recall agent from memory. As a result, the end user cannot recall files through the DOS agent.

Disabling Automatic Recall

Automatic recall is a very convenient feature, but there may be circumstances which require you to disable this feature. Automatic recall can enabled and disabled through agents, Configuration Manager, or Resource Manager.

Note that configuring the recall parameters in Storage Manager and editing the PALRECAL.DAT files are methods controlled by the administrator. End users can configure the recall options available through the workstation agents.

System

Through Configuration Manager, turn off the **Enable Automatic Recall** option. As a result, Resource Monitor cannot check the status of jobs in the _PALRC40 directory. If the job queue is processing a recall job, Storage Manager will complete the recall job successfully.

If there are jobs awaiting processing, these jobs will not be processed but will remain in the _PALRC40 directory. When the recall feature is later enabled, Storage Manager will submit these jobs to the job queue.

Individual Resource

In Resource Manager you can turn off the **Enable Automatic Recall** option for each volume resource.

By Users or NLMs

The PALRECAL.DAT file contains a list of NLMs and users for which the server agent should disable automatic recall when those NLMs or users attempt to open a migrated file. For example, PALREST.NLM can initiate multiple recall jobs when opening the phantom files on a resource during a restore job. As a result, unnecessary recall jobs could overrun the job queue. When a user or NLM listed in the PALRECAL.DAT file attempts to request a migrated file, the zero-byte phantom is accessed instead. However if these users are at a workstation where a workstation recall agent is loaded, they can continue to recall files.

Note that NLM names are not case sensitive in the PALRECAL.DAT file, but user names are. If you are running a virus-scanning NLM, non-Palindrome backup software, or any other application that scans the entire file system, you may want to exclude that NLM from recalling migrated files.

To disable automatic recall for users and NLMs

➤ Edit each server's PALRECAL.DAT file using the following format:
nlm=PALREST.NLM
(where PALREST is the NLM you do not want to recall files on the current server)
user=JSMITH
(where jsmith is a user whom you do not want to recall files on the current server)

Sample PALRECAL.DAT File:

```
nlm=PALREST.NLM
nlm=SMDR
nlm=TSA
user=supervisor
user=JSMITH
```

NOTE: If you have added an NLM to the PALRECAL.DAT file but it still recalls files, verify that the process name of the NLM matches the name listed in the PALRECAL.DAT file. Type **MONITOR** at the server console to view the process names, for example, PALREST.NLM. If the process name is different, record the process name in the PALRECAL.DAT file.

Server Recall Agent

Although the server recall agent can be disabled for certain users configured in the PALRECAL.DAT file, the workstation recall agents can also be used to disable the server recall agent.

Although you do not need to install both the workstation agent and the server agent, if you choose to install the server agent and wish to disable it for certain workstations, you can use the workstation agents to disable the server recall functionality.

To disable a server recall agent

- If using a Windows recall agent, disable the **Automatic Recall Enable** option on the Recall Agent window.
- If using a DOS recall agent, use the /R option switch to disable automatic recall. For example, the command line is PALSMRCL /R. Remember, this is a toggle so you may be enabling automatic recall if it had previously been disabled.

Workstation Recall Agents

To disable the Windows workstation agent

➤ Open the Control-menu box and select **Unload Recall Agent** option. Choose **Yes** at the prompt. Recall is still possible if the user can access the server recall or DOS workstation recall agent.

To disable a DOS recall agent

➤ At the DOS prompt, type the **PALRECAL** (or **PALSMRCL**) **/U**. A message indicates that you have unloaded automatic recall. The /M option is an alternate to /U, but does not unload the agent from memory. Recall is still possible if the user can access the server recall or Windows workstation recall agent. The /R option can prevent a user at the workstation from accessing both server and recall agents.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

INDEX

T

U

V

W

Y

Z

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

INDEX

T

U

V

W

Y

Z