Legato NetWorker® 6

Comprehensive Data Protection
Table of Contents

1 INTRODUCTION ............................................................................................................. 4
  1.1 THE DATA PROTECTION CHALLENGE ......................................................................... 4
  1.2 NetWorker 6: THE COMPREHENSIVE SOLUTION .............................................................. 5

2 NETWORKER ARCHITECTURE .................................................................................. 5
  2.1 PLATFORM AND DEVICE SUPPORT ............................................................................ 9
  2.2 NetWorker SERVICES ................................................................................................. 10

3 CORE NETWORKER FEATURES ................................................................................. 10
  3.1 CLIENT FILE INDEX AND MEDIA DATABASE ............................................................... 10
      3.1.1 Client File Index ....................................................................................................... 11
      3.1.2 Media Database ..................................................................................................... 12
  3.2 VOLUME AND DEVICE MANAGEMENT ..................................................................... 13
      3.2.1 Volume Management ............................................................................................... 13
      3.2.2 Devices, Autochangers and Silos ............................................................................... 13
      3.2.3 Auto Media Management .......................................................................................... 14
  3.3 NetWorker BACKUP OPERATIONS ............................................................................ 15
      3.3.1 Manual Backups ...................................................................................................... 15
      3.3.2 Scheduled Group Backups ........................................................................................ 16
      3.3.3 Media Verification .................................................................................................. 17
      3.3.4 Backing Up Open Files ............................................................................................ 17
      3.3.5 Parallelism and Multiplexing .................................................................................... 18
      3.3.6 Save Set Consolidation ............................................................................................ 19
      3.3.7 Special Data Handling .............................................................................................. 19
      3.3.8 Cloning .................................................................................................................. 19
      3.3.9 Save Set Staging ..................................................................................................... 20
      3.3.10 Immediate Save .................................................................................................... 21
  3.4 OPENTAPE ................................................................................................................ 21
  3.5 DATA RECOVERY ...................................................................................................... 23
      3.5.1 Client File Index-Based Recovery ............................................................................ 23
      3.5.2 Save Set Recovery .................................................................................................. 25
      3.5.3 Directed Recovery .................................................................................................. 26
      3.5.4 Scanner .................................................................................................................. 26
      3.5.5 Disaster Recovery .................................................................................................. 27
  3.6 NetWorker IN CLUSTER ENVIRONMENTS .................................................................. 27

4 DATABASE AND APPLICATION BACKUP .................................................................... 28

5 EXTENDING NETWORKER CORE FUNCTIONALITY .................................................. 31
  5.1 NetWorker Dynamic Drive Sharing (DDS) ................................................................. 31
  5.2 NDMP CLIENT CONNECTION ..................................................................................... 33
  5.3 NetWorker Archive ................................................................................................. 36
  5.4 Legato Automated Availability Manager ..................................................................... 36
  5.5 NetWorker SnapImage ............................................................................................. 37
  5.6 Celestra ..................................................................................................................... 39
  5.7 Open File Manager ................................................................................................... 40
  5.8 NetWorker Recovery Manager .................................................................................. 41
  5.9 Alphastor ................................................................................................................ 42
  5.10 Gems ....................................................................................................................... 43
  5.11 NetWorker HSM ..................................................................................................... 44

6 NETWORKER 6 ADMINISTRATION AND MANAGEMENT ......................................... 45
  6.1 Interfacing with NetWorker ....................................................................................... 46
6.2 NETWorker Configuration and Management ................................................................. 47
  6.2.1 Resources and Attributes ....................................................................................... 47
  6.2.2 Notifications and Reports ..................................................................................... 49
  6.2.3 Schedules ............................................................................................................. 49
  6.2.4 Browse and Retention Policies .............................................................................. 50
  6.2.5 Directives .......................................................................................................... 51
  6.2.6 Storage Node Configuration and Management ..................................................... 52
  6.3 SECURITY AND LICENSING.................................................................................. 52

7 CONCLUSION .............................................................................................................. 53
Executive Summary

The combination of rapidly expanding online storage and twenty-four hour operations has made it increasingly difficult to perform regular backups to protect stored data. To meet customer needs, backup software must support a wide variety of system platforms and storage devices, provide online backup for all popular databases, and accommodate network attached storage (NAS) devices, Storage Area Networks (SANs) and cluster configurations.

Legato NetWorker 6 is an industry-leading data protection solution that offers exceptional platform, database and tape device coverage. NetWorker utilizes a client/server architecture with a high degree of parallelism to achieve exceptional performance while centralizing administrative functions so that all backup and recovery operations can be managed from one location. A wide variety of add-on products are available to tailor NetWorker for support of NAS devices, SANs and clusters, and to perform advanced data management functions like archival or hierarchical storage management (HSM).

This white paper explores core NetWorker technologies including architecture, indexing and media management, parallelism and multiplexing, disaster recovery, archive, cloning, staging and tape storage format. The technology used in NetWorker add-on products including database support modules, Open File Manager, GEMS, AlphaStor, NetWorker Recovery Manager, NetWorker SnapImage, and Celestra are covered. Additionally, important administrative features are discussed.

1 Introduction

1.1 The Data Protection Challenge

The past few years have witnessed remarkable growth in online data storage, fueled by increased storage density, reduced storage prices, and new applications. Many large enterprises are doubling online storage capacity every year. Because they have made many of their services Internet-accessible, traditional businesses have been strongly impacted by the Internet. To meet the demands of customer accessible websites and expanding global operations, many data centers are now in full operation twenty-four hours a day, seven days a week.

The rise of the Internet has also resulted in new types of businesses with voracious appetites for storage. These businesses—providing Internet access, applications, web hosting, infrastructure and a variety of other services—are projected to grow at rates in excess of 150% over the next several years. Storage requirements will grow in excess of that rate, and—by their very nature—most of these businesses are 24x7.

The combination of rapidly expanding online storage and twenty-four hour operations has made it increasingly difficult to perform regular backups to protect stored data. Traditional enterprise businesses and Internet businesses have similar requirements for data protection. They need a single, centralized product capable of backing up their entire operation in the minimum time possible, with little or no disruption of ongoing operations. A successful backup product must support all the customer's system platforms and storage devices (including a wide variety of tape media, optical media, and autochangers) and be able to provide online backup for installed databases.

A backup product must also be able to accommodate technological innovations such as Network Attached Storage (NAS) devices, storage area networks (SANs), and clusters. NAS devices are single-purpose systems that provide rapid data access to networked computers. NAS devices often use the Network Data Management Protocol (NDMP) for backups since they typically don't have the open programming interfaces of general-purpose systems. Consequently, NDMP support is therefore increasingly crucial.

Storage Area Networks (SANs) are being deployed in many data centers to facilitate the sharing of tape libraries and other mass storage devices and provide high-speed data sharing. Protecting data in a SAN
environment by leveraging the SAN's unique capabilities presents another challenge. Given the right software to do the job, data can be streamed directly from SAN-attached online storage to SAN-attached backup devices, achieving the highest possible backup speeds with minimum disruption to data access.

Clusters of computers are used to tackle a wide variety of compute and high availability problems. In a cluster, two or more computers typically work together to ensure uninterrupted data access in the face of a system or component failure. It is common for the systems that make up a cluster to have some local data and some data that is shared between some or all members of the cluster. To successfully backup cluster data, the backup application must understand the cluster software and be able to backup all local and shared data. Because backup is itself a mission critical application, backup software should be designed to run in a high availability cluster environment.

1.2 NetWorker 6: The Comprehensive Solution

Legato Systems has been a leading vendor of data protection solutions for many years. NetWorker 6—Legato's flagship product—is in use in more than 90 percent of Global 1000 companies. NetWorker provides a comprehensive feature set to meet a broad variety of needs. This paper explores the technology and features of NetWorker 6 in significant technical detail, illustrating how NetWorker 6 meets the challenges created by exploding data storage, round the clock operations, and technologies such as NAS devices, SANs and clusters.

Sections 2 and 3 of this paper cover core features of NetWorker and provide details of NetWorker technology. Common NetWorker terminology is introduced and defined. Core technologies including index and media database architecture and management, parallelism and multiplexing, Open Tape Format (OTF), backup, recovery and disaster recovery are discussed.

The technology behind NetWorker database modules and other optional features and add-on products such as archive, HSM, Open File Manager, Celestra, NDMP, AlphaStor and SmartMedia are covered in sections 4 and 5.

Section 6 provides a detailed introduction to NetWorker Administration and Management, covering issues of user interface, security and licensing. Common server-side and client-side management functions are presented.

2 NetWorker Architecture

Legato NetWorker is based on a client/server architecture. A NetWorker datazone consists of a single NetWorker server, NetWorker clients and storage nodes. A central server is at the heart of all NetWorker operations. The NetWorker server controls and directs all NetWorker operations. All information is stored or managed by the NetWorker server, including all configuration information, all parameters for client systems to be backed up, the index of files backed up from those clients, and a database of all media volumes where backed up data is stored.

Typically, a NetWorker server hosts one or more backup devices (tape or other media). When a backup occurs, a NetWorker client sends data across the network to the server, which directs the data to appropriate storage. The server receives metadata—information about the files being backed up—separately and makes appropriate entries in the client file index and media database.

NetWorker manages client data in increments called save sets. A save set originates from a single client and may consist of a single file, a directory, a file system, or a partition. The NetWorker client file index on the server contains detailed information about each save set such as the filename of each file stored, time of back up, size, permissions, ownership, etc. An entry for each save set is also written in the server's media database which maps the save sets to the volumes where they are stored, stores the browse and retention policies for each save set, and maintains tracking information for all storage volumes. The client file index and media databases are essential to NetWorker's ability to locate and recover data rapidly. They are discussed in more detail in a later section.
A *NetWorker client* is any system with data to be backed up, no matter whether the system is a modest desktop system or a large database server. A client runs client software tailored to the operating system it uses. Normally, a client operates under the control of the NetWorker server in accordance with guidelines and schedules established by an administrator. However, users on the client system can initiate backup and recover actions as necessary. For instance, if an important file needs to be recovered from backup, that action can be initiated from the client without administrator intervention. Likewise, important files can be backed up manually without waiting for regularly scheduled backups to occur.

*Storage Nodes* substantially increase the parallelism and resiliency of a NetWorker configuration, and have proven highly useful in many NetWorker installations. A storage node is connected to one or more storage devices. The NetWorker server may direct a client to send its data to a storage node for backup. While client data is sent to the storage node, client metadata is always directed to the NetWorker server. The server maintains the file index and media database information for all data on the storage node. Thus, the storage node acts as a slave to the NetWorker server, and lacks the server’s bookkeeping functions.
Figure 2. Data versus metadata flow in a NetWorker datazone.
All metadata flows to the NetWorker server.

Storage nodes can streamline NetWorker operations in a variety of ways. In large, distributed NetWorker configurations, storage nodes can be used to compartmentalize data. For instance, a company consisting of multiple departments such as Engineering, Marketing, Sales, Accounting might configure one or more storage nodes for each department under the control of a single centralized server. Such a configuration can substantially reduce traffic on backbone networks since the amount of metadata sent to the NetWorker server is usually modest in comparison to the amount of data backed up.

Sometimes, a large file server or database server may be configured as a storage node primarily for the backup of local data. Because such a configuration prevents data from traversing the network, it reduces network congestion and maximizes backup and recovery performance. SAN Storage Nodes provide this capability for storage area network (SAN) environments. A SAN storage node does not provide service to network clients. Instead, a SAN storage node is configured to backup its data directly to a SAN-attached storage device such as a tape library. Multiple SAN storage nodes can share a single storage device.
Some configurations may require more than one NetWorker server (multiple data zones). Reasons for using multiple NetWorker datazones may include:

- **Geography:** A separate datazone may make logical sense when resources are spread across multiple locations (different buildings, different sites, etc.)
- **Administration:** Depending on company organization, it may make sense to partition datazones based on department, the type of systems being backed up, or areas of administrative responsibility.
- **Security:** Separate datazones may be preferable to configurations that would require spanning firewalls. Separate datazones may also be used to limit the amount of company data that any single administrator can access.
- **Performance:** While NetWorker is tremendously scalable, very large configurations may reach the performance limits of NetWorker's internal operations and databases, requiring the addition of more servers to handle the load.

In summary, a typical NetWorker installation may consist of one or more servers, one or more storage nodes and numerous clients. NetWorker servers keep all configuration information and initiate regular backup operations in parallel. When backups are in progress, backup data flows from the clients to storage devices attached to either the server or storage nodes. All file metadata is sent to the server where it is stored (and also backed up regularly.)
2.1 Platform and Device Support

NetWorker Server software is available in three editions targeted to meet specific needs. The Workgroup Edition is intended for workgroups with relatively modest backup needs. The Network Edition provides much greater scalability and flexibility to meet a wide variety of Enterprise needs. The Power Edition offers even greater scalability, and can act as a cluster server.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Included Client Connections</td>
<td>10</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>Parallel Data Streams</td>
<td>64 for server &amp; 32 per storage node</td>
<td>32 for server &amp; 32 per storage node</td>
<td>12</td>
</tr>
<tr>
<td>Number of Devices</td>
<td>32 for server &amp; 32 per storage node</td>
<td>16 for server &amp; 16 per storage node</td>
<td>4</td>
</tr>
<tr>
<td>Cluster Support</td>
<td>Server or Client</td>
<td>Client</td>
<td>No</td>
</tr>
<tr>
<td>Storage Nodes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Options Supported</td>
<td>All</td>
<td>All</td>
<td>Legato Application Modules</td>
</tr>
</tbody>
</table>


Broad platform coverage and device support are standard with NetWorker, which supports all of the common tape standards, as well as a broad variety of optical media, autochangers and silos. The following table illustrates NetWorker’s platform support:

<table>
<thead>
<tr>
<th>Platform</th>
<th>NetWorker Server</th>
<th>NetWorker Storage Node</th>
<th>NetWorker Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compaq Tru64 Unix</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HP-UX</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IBM AIX</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IBM Dynix</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SGI IRIX</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sun OS</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sun Solaris</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Caldera Linux</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat Linux</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SuSE Linux</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Turbolinux Linux</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Novell NetWare</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Microsoft Windows 95/98</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows NT/2000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Appliance</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Table 2. NetWorker Platform support.

For the most up-to-date platform and device support information check the Legato website: www.legato.com.
Legato takes great care to maintain product consistency across platforms. However, because of software differences and/or limitations, interfaces may not be identical on different platforms. While the look and feel of NetWorker differ between Unix/Linux and Windows, the feature set is the same for all platforms. Some features and add-on products may only be available on a subset of platforms.

2.2 NetWorker Services

To understand the inner workings of NetWorker, it is necessary to know the functions of the key services \(^1\) in operation on the server, storage node and client. The NetWorker server has three main services that run continuously: `nsrd`, `nsrindexd`, and `nsrmmdbd`. In addition, the `nsrmmd` service runs continuously on the server and on storage nodes (if any).

The `nsrd` service is the master service responsible for such functions as:

- Starting other services and programs
- Maintaining configuration information
- Authorizing client backup and recover
- Initiating and monitoring scheduled backups
- Maintaining statistics and message logs

The `nsrindexd` service controls the client file index. As saves occur, `nsrindexd` receives file information from the client and creates entries in the client file index. The `nsrmmdbd` service controls the media management database. It records the state of each storage volume available to NetWorker and maintains entries for every save set backed up.

The `nsrmmd` service runs on either the NetWorker server or storage node. At startup, `nsrd` starts one instance of `nsrmmd` for each device used by NetWorker. For remote devices, `nsrmmd` is started on the storage node to which the device is attached. When a client performs a save, it sends its data directly to the `nsrmmd` service associated with the target device; `nsrmmd` is responsible for writing data to the device and also handles multiplexing, volume labeling, and mount and unmount requests. As data is written to storage, `nsrmmd` communicates with the `nsrmmdbd` service to update the media database.

A single service, `nsrexecd`, runs on the NetWorker client. This service authenticates requests from the NetWorker server and then initiates `save` and `recover` as directed. This service also runs on the NetWorker server and storage nodes to initiate save and recover operations for local data.

3 Core NetWorker Features

This section discusses the core technologies that contribute to NetWorker performance, scalability, reliability and usability. These technologies are available in all NetWorker editions. Optional features and add-on products are discussed in later sections.

3.1 Client File Index and Media Database

NetWorker’s client file index and media database entries record what files NetWorker has stored and on what media. They serve as the foundation for all data recovery operations and data lifecycle policies. Because of their great importance, care has been taken to ensure that both are highly efficient and safe from corruption. NetWorker provides built in mechanisms to regularly backup these databases. They can be rebuilt from scratch if necessary using the `scanner` utility.

\(^1\) The term service is used throughout this paper. In UNIX environments these would more typically be referred to as daemons, while in the NT environment they correspond to NT services.
The relationship of the client file index to the media database is conceptually child-to-parent. The client file index entries map to specific entries in the media database which in turn map to locations on the storage media.

### 3.1.1 Client File Index

The client file index stores a file record for each file backed up in a save set. The information in the client file index can be browsed by end users, allowing them to recover a single file, a set of files, or entire directories without administrator intervention (subject to proper NetWorker authorization). In NetWorker 6, the architecture of the client file index has been completely re-designed to improve performance, parallelism, scalability and robustness.

NetWorker 6 maintains a separate database directory for each client. The name takes the form:

```
/nsr/index/client_name/db6
```

or

```
%SystemDrive%\Program Files\nsr\index\client_name\db6 (for Windows platforms)
```

For every save set backed up, a separate index file is created in this database directory. (Previous versions of NetWorker used a single database structure for every client.) Adding a set of records for a save set, backing up recently added save set records and purging timed-out save sets are simple operations on individual files. Two key files are generated per index file. These are organized by filename and fileID and are used to accelerate access to individual records.

![Figure 4. Client File Index organization in NetWorker 6.](image)

A separate index file is created each time a save set is backed. The file v6hdr keeps track of all the index files stored in the directory. Two key files are also created to accelerate access to file records (not shown).

This re-organization plus additional changes to the indexing mechanism in NetWorker 6 result in substantial performance benefits:

- Reduction in the size of file indexes, typically by 20% to 40% compared with previous NetWorker versions
- Better scaling for concurrent index operations
- More rapid backup and recovery of file indexes
- Faster browsing
- Index performance scales linearly with the number of save sets

Legato Systems, Inc. 11
NetWorker 6 provides substantial improvements for index management including:

- Better scaling/support for very large client file indexes
- Nearly instantaneous crosschecks
- Simplified relocation of client indexes to new file systems

When disaster occurs, getting the NetWorker server up and running so that other systems can be recovered is the first priority. Enhancements in NetWorker 6 allow more rapid creation of bootstraps, and bootstraps are now completely self-contained. (A bootstrap contains the site-specific information that a server needs to get up and running after a disaster.) File recovery or regular backups can commence in minutes.

In addition, several new client file index features were added to NetWorker 6, including index roll-in—the ability to restore old versions of a client file index without overwriting newer ones.

A complete discussion of the client file index can be found in the Legato white paper entitled, *File Indexing Enhancements in NetWorker 6: Improved Performance, Scalability and Robustness*.

### 3.1.2 Media Database

The media database records which data is available for recovery and the storage location of that data. An entry is made each time a save set is backed up and each time a storage volume is added to the NetWorker system. The media database stores all the information necessary to allow an administrator to recover complete save sets without reference to the client file index.

When a save occurs, a NetWorker client directs its data to the appropriate `nsrmmd`. As `nsrmmd` writes the data to a storage volume, it passes information to the `nsrmmdbd` service, which makes entries in the media database.

- One entry is made for each save set, describing the starting location of the save set on the storage volume and the status of the save set.
- One entry is made for each storage volume. Each volume entry contains a unique volume id, a unique name and the mode (status) of the volume.

The media database also tracks browse and retention policies for each save set\(^2\). These policies are used to manage the life cycle of data and control the size of the client file index. The browse policy determines how long file entries are maintained in the client file index. The retention policy determines how long save sets are stored on backup media.

The sizes of the client file index and media database vary, depending upon the number of files saved, the frequency of backups, and the periods of the browse and retention policies. The size of the client file index is directly proportional to the total number of individual files that are backed up and the frequency with which backups occur. A change in the length of the browse policy generates a directly proportional change in the size of the client file index. Double the length of the browse policy and, in most cases, the size of the client file index doubles because file entries are retained twice as long.

Media database growth is slower and less responsive to policy changes. Entries are added only on a one-per-save-set basis, and are retained until they are manually deleted or the volume is recycled. In general, the media database is significantly smaller than the client file index.

---

\(^2\) In NetWorker 6, different browse and retention policies can be specified for each save set, and policies can be changed as necessary. This flexibility simplifies the creation of daily, weekly, monthly and yearly backups.
3.2 Volume and Device Management

3.2.1 Volume Management

One of the strengths of NetWorker is its ability to integrate and manage a large number of storage volumes and devices. NetWorker supports three classes of storage media: tape, optical, and disk, including a wide variety of specific storage devices including all popular tape formats and a broad array of autochangers and silos.

To simplify volume management, storage volumes are grouped into volume pools. NetWorker operations are directed to pools rather than specific volumes. A pool is a specific collection of volumes to which the NetWorker server writes data. The server uses pools of volumes to sort and store data. The configuration settings for each pool act as filters that tell the server which volumes should receive specific data. The NetWorker server uses pools in conjunction with label templates to keep track of what data is on which specific volume.

Pools provide a simple and flexible means of directing data to specific types of devices. For example, by choosing criteria correctly, data from important servers can be directed to the fastest and most reliable devices, while less important data can be sent to lower performance—and probably more economical—devices.

When a scheduled backup occurs, the NetWorker server tries to match the save stream to a pool configuration. If the save stream matches the criteria of a pool configuration, it is directed to a labeled volume in that pool. The server then checks if a correctly labeled volume is mounted on a storage device:

- If a correctly labeled volume is mounted on a storage device, the NetWorker server writes data to the volume.
- If there is no correctly labeled volume mounted on a storage device, the NetWorker server requests that such a volume be mounted and waits until an operator or an autochanger mounts an appropriate volume.

NetWorker always maintains a default pool in addition to any user-configured volume pools. Save streams that don't match the storage criteria of specific pools are directed to the default pool. NetWorker maintains separate default pools for different types of data. For instance, backup data, clone data and archive data are always directed to separate pools.

3.2.2 Devices, Autochangers and Silos

NetWorker servers running Windows can automatically detect and configure SCSI devices attached to the NetWorker server or storage nodes. Devices must be manually configured on NetWorker servers running Unix. Manual configuration can be accomplished using a graphical interface.

The term autochanger is used to describe a device that contains multiple storage volumes with the ability to access and change volumes automatically. This encompasses a variety of storage device terminology, including the following: jukebox, carousel, library, near-line storage, datawheel, and autoloader. Note that tape stackers are not considered autochangers by NetWorker. Stackers access tapes sequentially, while autochangers can access media in any order. An autochanger may itself contain multiple individual devices that have to be configured one by one. Autochanger configuration is accomplished using the jbconfig utility.

NetWorker can use bar codes on autochangers that support them. Bar codes dramatically speed up the process of inventorying the contents of the autochanger and can simplify media management. However, NetWorker can also inventory the contents of an autochanger that does not have bar code support. This process is slower since NetWorker must load each volume and read its volume label. Inventory must be
taken any time the contents of an autochanger are manually changed. NetWorker also supports automatic cleaning of autochanger devices according to a defined schedule.

Autochangers can be shared between a NetWorker server and its storage nodes. With library sharing (optional in NetWorker 6 and standard in NetWorker 6.1) one NetWorker host controls the autochanger’s robotic capabilities for the benefit of all attached systems. Individual drives are dedicated to single systems. Dynamic Drive Sharing (DDS)—an optional product for NetWorker 6.1, allows pools of drives to be dynamically shared between a NetWorker server and its storage nodes in a single datazone. More information on DDS is provided in a later section. A complete discussion of DDS can be found in the Legato White Paper entitled, Dynamic Drive Sharing in NetWorker 6.1: Maximizing the Benefits of SAN for Data Protection.

Broader sharing of autochangers—including sharing an autochanger between different applications, spanning datazones, and dynamic drive sharing—can be accomplished using either GEMS SmartMedia or AlphaStor. (See the later sections entitled GEMS and AlphaStor for more information.)

NetWorker software manages silos and silo media similarly to autochangers. A silo tape library (STL) is a peripheral that usually contains many storage devices. Silos are controlled by silo management software, which is provided by the silo vendor and installed on a silo server. The silo server cannot be the same computer as the NetWorker server.

A silo can be shared among many applications, systems, and platforms. Like autochangers, silos make data and media operations more automatic. Silos can load, change, and manage volumes, and clean devices automatically.

A NetWorker server acts as a client of the silo management software, which resides on the silo server. NetWorker communicates with the silo through the Silo Tape Library Interface (STLI), which must be installed on the NetWorker server that uses the silo.

To access the volumes and devices in a silo, NetWorker sends a request to the silo management software, in the form of an STLI call. For example, to mount a volume in a silo device, the NetWorker media service sends a request to the silo management software to mount the volume into a particular device in the silo. The silo server responds to the request and mounts the volume in the requested device.

An Autochanger or Silo Software Module must be installed for each autochanger or silo managed by the NetWorker server.

### 3.2.3 Auto Media Management

Auto media management gives the NetWorker server automatic control over media loaded in a storage device. With auto media management enabled, the server automatically:

- Labels volumes
- Mounts or unmounts volumes loaded in standalone devices
- Overwrites a volume it considers unlabeled
- Recycles volumes eligible for reuse that are loaded into a device

The NetWorker server considers a volume unlabeled under the following conditions:

- The volume has no internal label.
- The volume is labeled with information other than a recognizable NetWorker label.
- The volume is labeled with a NetWorker label, but the density indicated on the internal label differs from the density of the device where the volume is mounted. (Because of this, some care must be taken when using Auto Media Management. See the NetWorker Administrator’s Guide for details.)
When auto media management is enabled for an autochanger device, NetWorker assumes that it has control of all volumes within the device and may overwrite volumes written by other applications if they are present. Auto media management should not be enabled on an autochanger that is being used for multiple applications.

NetWorker tries to mimic the behavior of autochanger devices as much as possible when auto media management is enabled on standalone devices. The following processes occur when a volume becomes full during a backup:

1. A notification is sent indicating the server or storage node is waiting for a writable volume. At the same time, the NetWorker server waits for the full, verified volume to be unmounted.
2. NetWorker monitors the device, waiting for another volume to be inserted into the device.
3. After a volume is detected, NetWorker checks that the volume is labeled.
4. If the volume is labeled, NetWorker mounts the volume. NetWorker checks to see if the volume is a candidate for writing. If so, the write continues. If not, NetWorker continues to wait for a writable volume to continue the backup.
5. If a newly inserted volume is recyclable and is a member of the required pool, NetWorker recycles the volume and continues.
6. If a newly inserted volume is unlabeled, NetWorker labels it and continues with the backup.

### 3.3 NetWorker Backup Operations

The following sections explore the details of NetWorker backup. Covered topics include manual and scheduled backups, supported backup levels, backup of open files, parallelism during NetWorker operations, save set consolidation, cloning, and staging.

NetWorker 6 supports a wide range of storage devices and media types, including tape, optical, and disk devices. Backups can easily span storage volumes as necessary. Special backup save sets are supported for many client types. For instance, backups of Windows NT 4.0 clients include the special save set REPAIRDISK to ensure that critical system data is regularly preserved.

NetWorker performs two types of backups: user-initiated manual backups and scheduled group backups. Scheduled backups are preferred because they occur automatically, facilitate data recovery and automatically backup the databases on the NetWorker server.

#### 3.3.1 Manual Backups

Users can issue backup requests either through a graphical interface or by executing the `save` command from the command line. Manual backups give users the flexibility to protect an important file or files immediately, without waiting for the next scheduled backup to occur. A user can designate an entire file system, specific directories, or individual files for manual backup. Specific files can also be explicitly excluded from backup.

The following steps occur when a manual backup is initiated:

1. One or more instances of the `save` program running on the NetWorker client creates one or more savestreams of data, one savestream per save set.
2. The `save` program connects to the designated, receiving `nsrmmd` service (either on the NetWorker server or on a storage node) and sends the savestream to `nsrmmd` for writing.
3. The `save` program initiates a connection to the `nsrindexd` service and sends records to `nsrindexd`, one per backed-up file. The `nsrindexd` service makes an entry for each backed-up file in the client file index. These save records contain the time the file was saved, the number of bytes from the beginning of the save set to the beginning of the file, the length of the file in bytes, and other information.
4. The `nsmmd` service sends information to the `nsmmdbd` service on the NetWorker server, which stores entries in the media database for each backed up save set and for each newly labeled or relabeled volume.

![Figure 5. Data and metadata flow during a manual backup.](image)

### 3.3.2 Scheduled Group Backups

Since manual backups are performed on an ad hoc basis, the concept of full versus incremental backup does not apply to them. Scheduled group backups, on the other hand, can be full, incremental, or level backups as indicated in the following table:

<table>
<thead>
<tr>
<th>Backup Level</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Backs up all files, regardless of whether or not they have changed.</td>
</tr>
<tr>
<td>Level [1 – 9]</td>
<td>Backs up files that have changed since the last lowered numbered backup. For example, a level 1 backup backs up all the files that have changed since the last full backup (considered a level zero). A level 3 backup backs up all the files that have changed since the last level 2 backup, level 1 backup, or full backup. A level 9 backs up all the files that have changed since the last level 8, 7, 6, 5, 4, 3, 2, 1, or full (0) backup.</td>
</tr>
<tr>
<td>Incremental</td>
<td>Backs up files that have changed since the last backup, regardless of level.</td>
</tr>
<tr>
<td>Consolidated</td>
<td>Backs up all data that has changed since last full backup and subsequently merges these changes with the last full backup. See the later section entitled <em>Save Set Consolidation</em> for more information.</td>
</tr>
<tr>
<td>Skip</td>
<td>Skips the scheduled backup. For example, holidays may be skipped if no one will be available to change or add media volumes, etc.</td>
</tr>
</tbody>
</table>

Table 3. NetWorker Backup Levels

Scheduled group backups include the core activities described above for manual backups, with additional activities occurring before and after the execution of the `save` program. For convenience, NetWorker allows an administrator to group clients with similar characteristics. The administrator may then designate a schedule that applies to every client in the group. When the scheduled time for a group to be backed up arrives, `nsrd` executes the `savegrp` program to perform the necessary steps to prepare for backup.

The `savegrp` program first creates a work list to identify the save sets to be backed up, their backup level, and any other processing parameters that must be passed to the `save` program. The `savelfs` program may be initiated on each client to perform a probe of the client to obtain much of the necessary information.
Once the work list is created, NetWorker initiates as many backups as possible in parallel. The amount of parallelism is based on resource availability and software configuration. (See the later section entitled Parallelism and Multiplexing for more details.) The order in which clients in the group are selected for backup is based on assigned client priority. Each client is contacted in turn, and the save program is executed for each save set.

Four major tasks remain after the client-side save programs complete all backup work:

1. A save is initiated on the server to backup the now updated client file index.
2. The need for a bootstrap is assessed and one is created if necessary.
3. Cloning is initiated if it is part of the scheduled backup.
4. A savegroup completion report is generated.

Protection of the client file index and media database is of paramount importance to the proper functioning of NetWorker. This is why the client file index is backed up immediately after a client's save sets finish. NetWorker next assesses the need to save a bootstrap. The bootstrap contains the media database and all NetWorker configuration information; it can be used to recover the NetWorker server in case of disaster. If the NetWorker server is part of a regularly scheduled backup group, a bootstrap is created only when that backup group runs. If it is not part of a regular backup group, a bootstrap is created at the end of every savegrp.

3.3.3 Media Verification

NetWorker can be configured to automatically verify data written to backup media. Media is verified whenever a volume goes idle because all save sets being written to the volume are complete, or when a volume becomes full while saving and it becomes necessary to continue on another volume.

As nsrmmd writes data to a storage volume, it periodically notes the location of data blocks while retaining that data in memory. To perform verification, the nsrmmd locates the most recent such block on the volume, reads the block, and compares it to the copy of the data previously saved. If the verification is successful, the write operation continues on the next volume. If not, the volume is marked as suspect. Suspect volumes are ineligible for future writes. Previously saved data is still available for access if the volume can still be read.

3.3.4 Backing Up Open Files

NetWorker can back up many open files using the features of the standalone product. The success of backing up open files may depend on the operating system(s) in use, active applications, etc. If an open file changes during a scheduled backup, the NetWorker server notices that it is changing as it backs up the file. The server also checks to see if the size of the file changed. If the file size did change, the server reports the discrepancy. Files that change during backup are flagged by a warning message. An operator can ensure that open files are backed up correctly by restarting the backup group or simply backing up those files manually at a later time.

Legato offers several add-on products that deal specifically with online backups. Legato Open File Manager ensures that open files residing on NetWare, Windows 2000 or Windows NT servers are backed up consistently, even if the file is locked. NetWorker SnapImage Module, Celestra and NetWorker Modules (for databases and applications) also provide support for consistent online backups of regular files and applications. These products are discussed in detail in the sections entitled Database and Application Backup and Extending NetWorker Core Functionality.
3.3.5 Parallelism and Multiplexing

The ability to perform many operations in parallel is fundamental to NetWorker performance. Each NetWorker Edition is configured to support a maximum number of parallel data streams. (See Table 1.) For example, the NetWorker Power Edition supports up to 64 simultaneous data streams to and from the server and up to 64 simultaneous data streams to and from each storage node. The amount of parallelism in a NetWorker environment can be manually tuned to optimize performance. The server parallelism parameter is used to control the number of concurrent data streams that a server will accept. The client parallelism parameter controls the maximum number of concurrent data streams a client will send.

Multiple savestreams can be multiplexed to a single device to ensure that each backup device is kept operating at maximum throughput. Multiplexing interleaves data from more than one save set into each record written to a storage volume.

![Diagram of NetWorker Client, Server, and Storage Medium](image)

**Figure 6. Two savestreams being multiplexed to a single storage volume.**

For each device in a NetWorker environment, the administrator configures a variable called target sessions, which is the optimal number of savestreams to multiplex to the device. By setting higher values for fast devices and lower values for slower devices, all available devices can be utilized to capacity.

The goal of multiplexing is to improve backup performance. By directing multiple streams of data to a device, data flow is kept consistent and device utilization is most efficient. Target sessions is used as a load-balancing value—intended to optimize backup performance—not as a maximum value. If the target number of sessions is reached for all devices, but the value of server parallelism permits additional write operations, then more saves will be started if possible (i.e. if there are more backup operations waiting to be started). Some devices will exceed their target sessions values.

The extent of multiplexing on storage volumes has an impact on recovery performance. De-multiplexing a storage volume or volumes to recover an individual save set takes more time than reading from a non-multiplexed volume. In environments where recovery performance is critical, target sessions should be set to a low value.
3.3.6 Save Set Consolidation

Save set consolidation eliminates the need to perform Full backups at regular intervals. Save set consolidation merges a new level 1 backup with the last Full backup of a save set to create a new Full backup. (If no previous Full backup exists, NetWorker automatically performs one when a level 1 backup for save set consolidation is scheduled. This Full backup is then used in the next scheduled save set consolidation.)

<table>
<thead>
<tr>
<th>Full</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>A₁</td>
<td>B</td>
<td>C₁</td>
<td>D</td>
<td>E₁</td>
<td>F</td>
</tr>
</tbody>
</table>

Figure 7. Save set consolidation combines data recovered from a previous full backup with data from a new level 1 incremental backup to create the equivalent of an up-to-date full backup.

Save set consolidation is particularly useful under the following conditions:

- A client is at a remote location and data transfer over the network to the server is a performance issue for either the network or the client.
- Network bandwidth is limited, or large backups over the network are cost-prohibitive.
- File systems are large, and little data changes during a normal backup cycle.
- The server has the necessary resources (a minimum of two drives and preferably three or more drives) and the capacity to consolidate backups locally.

It is important to note that save set consolidation puts most of the burden on the server. Once the level 1 backup completes, the client is out of the picture. This server load may be unacceptable in some environments and hamper other activities. Save set consolidation does not work for backups of database systems.

3.3.7 Special Data Handling

NetWorker allows additional data handling operations such as compression, encryption and/or password protection to be specified for all or any combination of files in a save set. These operations are applied using NetWorker directives. Directives can be specified as part of a client configuration, in files stored in the client file system, when executing the `save` command from the command line, or from the NetWorker user program when specifying a manual backup. For more information on directives, see the section entitled `NetWorker 6 Administration and Management`.

3.3.8 Cloning

NetWorker provides the ability to make duplicates, or clones, of complete volumes or individual save sets. These clones are frequently sent to offsite storage, used to transfer data to another location or simply retained to enhance the security of important data.

Cloning can be initiated as part of a scheduled backup or on-demand for individual save sets or volumes. The reproduction of data is always from one storage volume to another and does not involve data stored on the clients or server.

Volume cloning entails reproducing complete copies of all the save sets represented on the volume. Using operating system utilities to create exact duplicates of storage volumes is not the same as cloning a volume.
Save sets that are only partially contained on a volume being cloned are recovered in their entirety and written to clone volume(s). Therefore, source volumes in addition to the one specified for the clone operation may be required. This underscores the concept that cloning a volume does not mean that the volume contents are duplicated. Instead cloning a volume means that each of the save sets on the source volume are recovered completely and then rewritten to another destination volume or volumes. By contrast, using operating system utilities—such as the UNIX dd command—to copy a storage volume results in an exact replica of that volume. If the data on the volume consisted of parts of several save sets, the copy will too. In addition, such a copy will not be known to or tracked by NetWorker.

Volume cloning and save set cloning use the same basic mechanisms. Save set cloning recovers a designated save set by reading from as many volumes as necessary then writing the save set data back to the clone volume(s).

Cloning is executed by the nsrclone program as a two-part operation: a recover operation of one or more save sets from a source volume mounted on one device followed by a save (write) operation to another volume mounted on a second device. The cloning operation takes advantage of most of the logic and features implemented for a NetWorker recover as well as for a NetWorker save. De-multiplexing and multiplexing occur automatically during cloning.

De-multiplexing from the source volume occurs as it would during any other recover, except that cloning is more exclusive than a routine recover. Once the cloning operation begins, the recovering nsrmmd is placed in clone-read mode. In this mode, only one clone-read session is permitted on the NetWorker server. In addition, the nsrmmd does not permit multiple recovers to occur from the same volume. If another recover session needs to read the same volume as the clone session, the recover session is delayed until the cloning session is finished with the volume.

As the reading nsrmmd reads and de-multiplexes the save sets from the source, it initiates connections with the nsrmmd reserved for the save/write phase of the operation. The reading nsrmmd can establish more than one connection to the writing nsrmm; so a clone volume can also be multiplexed.

The nsrclone program, working in conjunction with the writing nsrmmd, ensures that no clone volume will contain more than one instance of a particular save set. Thus, an administrator who requests three clones of a save set is guaranteed that each save set clone will be written to a different volume. As the write progresses, the clone save set instances are multiplexed onto the clone volumes. The multiplexed save set data chunks may reflect media differences on the receiving volumes. Volume crossing conditions and multiplexing are handled as they would be during a routine save.

Cloned save sets are tracked only through the media database. The cloning operation does not insert entries into the client file index. During cloning, the location of a cloned save set is added to the existing save set entry in the media database. That is, each save set clone shares the same save set ID number (ssid) as the source save set. All characteristics that are true for the source save set are also true for the cloned save set. If the source save sets are still browsable, the clone status will be browsable. If the source save sets' browse policy have expired, the source and clone save set status are marked "recoverable". To preserve a clone volume after the retention policy of the original save set or save sets has expired, the clone volume must be set to the mode manual recycle.

### 3.3.9 Save Set Staging

Save set staging allows save set data to be transferred from one storage medium to another. The most common use of save set staging is to reduce the time required to complete a backup. This is accomplished by directing the initial backup to a high performance device such as a hard disk. After the backup is completed, it can be staged to a more traditional storage medium, freeing up the disk space to be re-used. The staging process can occur outside the normal backup window, since it does not access online data.

When staging is scheduled, the NetWorker server creates a clone of the save set on whatever medium is specified. If the save set was stored on a file system device, the save set is deleted from the filesystem to
free the space. The NetWorker server tracks the location of the save set in the media database. The retention policy for the save set does not change when the data is staged.

3.3.10 Immediate Save

In a typical NetWorker backup, the client communicates with the server and/or storage node using Remote Procedure Calls (RPCs) transmitted over TCP/IP. In cases where the client being backed up is the NetWorker server or storage node itself, and the data is being written to a local device, the immediate save mechanism is used in place of RPC running NetWorker Power Edition. Immediate save eliminates the overhead of moving local data using the TCP transport.

Immediate save uses shared memory buffers to pass the savestream from the creating **save** program to the receiving **nsrmmd**. The **nsrmmd** program writes immediate save data to the storage medium as the shared memory buffer fills, allowing rapid and efficient backup of local data. An **nsrmmd** can multiplex immediate saves and non-immediate (routine) saves to the same volume.

3.4 OpenTape

NetWorker 6 writes all storage volumes using a format known as OpenTape, which was developed by Legato and has been in continuous use since 1990. The OpenTape format is completely self-describing; each storage volume contains all the information necessary to determine its contents without copying the data back to disk. This capability is extremely useful for many routine administrative operations and can be crucial for disaster recovery.

Unlike many legacy backup formats, OpenTape provides the ability to continue a recover operation after bad sections of media are encountered. All OpenTape data structures are written using XDR (eXternal Data Representation) for portability, and OpenTape supports extremely large save sets using 64-bit data types as necessary.

A storage volume in OpenTape format consists of the volume label followed by multiple volume records. Each NetWorker volume label is 32 KB. NetWorker writes the volume label twice at the beginning of each volume. Duplication of the label protects against accidental overwriting in cases where the primary label is damaged and reserves space for future modifications. The volume label contains the volume identification number and timestamps, as well as all the information needed to ensure the volume can be recovered.

Each record on a volume contains a record header, one or more save set data chunks and one or more note chunks. The record header records information such as the length of the record (frequently 32KB, but high capacity devices are able to write larger records) and the number of save set data chunks contained in the record. An individual record cannot span volumes.
Each save set data chunk is labeled with a header that contains a unique save set id, the offset of its data within the savestream and the length of the data. Because each chunk is individually identified, the save set data chunks stored within the record need not come from the same save set. Multiplexing occurs by interleaving data chunks from different save sets within a single record. (Multiplexing is not used on disk type devices, where it is unnecessary.)

Data chunks cannot cross record boundaries. If a save set contains more data than can be accommodated in a single record (frequently the case), more data chunks can be written to subsequent records on the same or additional volumes.

The note chunks describe the data stored in save set data chunks. They facilitate multiplexing and allow save sets to span multiple volumes. The information contained in note chunks is what makes OpenTape self-describing. The scanner program can read the notes on a volume to recreate client file index and media database entries.

Four types of Note chunks are used:

1. A Start Note is used to signal the start of the first chunk of data from a save set.
2. A Continuation Note marks subsequent data chunks from the save set with pointers back to previous chunks.
3. An End Note is written after the last chunk of data from a save set is written.
4. Sync Notes are written periodically and used in data verification.
Because of the data structures used in OpenTape volumes, the data is stored with great reliability and flexibility. A single save set can span individual records or storage volumes. Large files within a save set can therefore span these boundaries as well.

3.5 Data Recovery

NetWorker Data Recovery takes full advantage of the information stored in the client file index and media database to quickly locate files and recover them to their original location or an alternate location if desired. NetWorker 6 provides two mechanisms for data recovery:

1. Client File Index Based Recovery: An end user or administrator browses the client file index using graphical tools or command line interface (CLI) and selects individual files or directories to recover
2. Save Set Recovery: An administrator or end user recovers an entire save set to the originating client from the NetWorker GUI or CLI

In addition to these methods, NetWorker can readily adapt to unexpected and unusual recovery situations. The scanner program accommodates a wide variety of circumstances in which data has expired and been removed from the client file index or even the media database. Directed recovery enables the recovery of data to a client other than the originating client. Cross-platform browsing can be used in conjunction with directed recovery, allowing Windows systems to browse Unix backups and recover those backups to the same or a different Unix system. Unix systems can recover Windows backups to the same or different Windows client using the recover utility from the command line. This section discusses many of the features of NetWorker recovery.

3.5.1 Client File Index-Based Recovery

A client file index-based recovery takes part in two phases: browsing and recovery. NetWorker users browse a representation of a client’s file system, as it existed at a specific point in time and mark files for recovery. After the user submits a recover request, NetWorker automatically handles all the intricacies of the recover operation, ensuring that files are recovered from the correct level backup (which could vary from file to file in a single recover). Files and directories that have been renamed or deleted are also handled correctly. NetWorker prompts for the needed volumes by name (if they cannot be retrieved automatically by an autochanger).

The browsing phase of a client file index-based recovery occurs as two steps:

1. The client-side recover program initiates a request to the NetWorker master service nsrd. After authentication, nsrd passes to the client the encoded credentials needed to directly access the client index service, nsrindexd.
2. The recover program queries nsrindexd for the file and directory information needed to build a view of the file hierarchy in client memory as it existed at the browse time designated by the user. After the view is built, the user marks files or directories for recovery. If a user changes the browse time, the recover program collapses everything in the virtual file system that hasn’t been marked for recovery, then performs a new lookup (via nsrindexd) using the new browse time. In this way, a user can recover two different versions of the same file in the same recovery session. It is likely than an older view of a file system will display files that are not visible in later views. This occurs when files have been deleted over time. Since the browsable view recreates the file system as it existed at a point in time, files that were deleted from the file system but are available for recovery may not be visible when a recent browse time is specified.

After a user marks data for recovery and issues a recovery request, the recover program starts the recovery phase. The recover program builds a list of objects to be recovered, referred to as the rlist. The rlist is passed to an ansrd process for completion. (The master NetWorker service, nsrd spawns ansrd as an agent
for each active recover.) Among other things, **ansrd** determines which volumes are needed for the recover. Each rlist contains the following information for each item to be recovered:

- save time of the backup
- starting offset (location) of the file within the save set, in bytes
- encoded length of the file in the save set, in bytes
- file attributes needed to reconstruct the data

The information contained in the rlist allows **nsrmmmd** to read the appropriate data from each volume. The following steps summarize the activities that occur during the recovery phase:

1. The **ansrd** makes a connection with the designated **nsrmmmd** and passes the rlist to **nsrmmmd**.
2. The **nsrmmmd** mounts the first required volume (or issues a mount notification if the volume is not available in an autochanger)
3. **nsrmmmd** queries **nsrmmdbd** to find the beginning data chunk on the volume.
4. The **nsrmmmd** begins processing the rlist and sends the de-multiplexed recover stream to the client machine **recover** program for rebuilding.
5. As the recovery proceeds, the **recover** program extracts the required files from the recover stream coming from **nsrmmmd** and performs any required processing before writing the files to the file system.
6. If additional required volumes cannot be automatically mounted, **nsrmmmd** initiates mount request notifications.
7. When the recover stream ends, **nsrmmmd** sends a status message to the **recover** program. Any bad spots that were discovered on the volume during the recover are identified in this message.

**Figure 9. Client file index-based recovery**

Files recreated through index-based recovery appear “new” to the client-side **save** program, the first time they are encountered during a backup. Newly recovered files are backed up on the next scheduled backup and inherit the browse policy in effect for the client at the time of the backup.

NetWorker provides several options regarding where to recover data and how to resolve possible conflicts between a recovered data item and an existing on-disk data item. By default, files are returned to their original locations when recovered. NetWorker can be configured to respond to recovery conflicts on an item-by-item basis or automatically, and provides the following options:
- The user can be prompted for the appropriate action to take each time a conflict occurs
- Recovered data can be relocated to an alternate specified location
- The recovered file can be renamed
- The recovered file can be discarded
- The existing file can be overwritten

The **nsrmmd** remains allocated to a recovery operation until the recovery operation is completed. During one **recover** session, a second session may require the same volume. More than one recover operation can share a single volume. The **nsrd** service implements this sharing by assigning the second session to the same **nsrmmd** as it is currently reading the volume. This sharing implementation is referred to as *joining* recover.

### 3.5.2 Save Set Recovery

Client file index-based recovery is the preferred method for most routine situations. Save set recovery is preferred when the files that must be recovered have exceeded the browse policy. (Individual files may still be recovered if the exact pathname and filename are known.) The save set method is also preferred when a large amount of data must be recovered in a short period —for instance, when a disk failure occurs, or when client memory is limited.

Save set recovery lacks the file handling features that are built in to index-based recovery, so care must be taken to recover save sets in order. An administrator may need to manually delete unwanted files and directories that were recovered. Since save set recovery will restore files that were subsequently deleted, it is possible that recovering a full backup followed by a level backup or backups will retrieve more information than a file system can hold.

Save set recover is analogous to the recover phase of index-based recovery as described above. The **nsrd** service checks remote access permissions and licensing, then it passes authorization to **ansrd**, allowing **recover** to connect with the designated **nsrmmd**. The client file index is not consulted, even when browsable entries exist for the data being recovered.

![Figure 10. Save set recovery process.](image)
3.5.3 Directed Recovery

Directed recovery allows backed-up data from one NetWorker client (the source client) to be recovered to another NetWorker client (the destination client). The destination client can be any of the following:

- The source client itself
- Another NetWorker client of the same or similar platform
- The administering computer

Directed recovery facilitates remote administration. Recovers can be carried out without anyone being present at either the source or destination client. Working from a remote machine, an administrator can direct the recovery of files to the machine where they originated or to any similar machine. The ability to recover files backed-up from another system provides the capability to easily access existing configuration files when configuring new systems. Sharing backed-up files is also straightforward. These features are particularly useful on Windows clients that lack built-in utilities like rlogin and ftp that can facilitate direct sharing of files.

To perform a directed recovery, a recover session is started on the request-originating client, initiating the browsing phase of a client file index-based recovery. The client accesses and browses a source client machine’s index and builds a virtual file system for that client in its own memory space. Files to be recovered are marked. Next, the initiating recover session passes all the recovery information (including required portions of the virtual file system) over the network to a second recover session on the destination client where the data is recovered using the methods discussed previously.

Any NetWorker client can browse the files of another NetWorker client for the purpose of directed recovery given the appropriate permissions. However, the ability to actually recover files from one platform type to another is more restricted as indicated in the following table:

<table>
<thead>
<tr>
<th>Source Client Type</th>
<th>Destination Client Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows NT</td>
<td>Windows NT, Windows 2000</td>
</tr>
<tr>
<td>Windows 95/98</td>
<td>Windows NT, Windows 2000</td>
</tr>
<tr>
<td>NetWare</td>
<td>NetWare, Windows NT, Windows 2000</td>
</tr>
<tr>
<td>UNIX/Linux</td>
<td>UNIX/Linux</td>
</tr>
</tbody>
</table>

Table 4. Supported sources and targets for directed recovery.

3.5.4 Scanner

The scanner program can read a NetWorker storage volume directly, without accessing information from the media database. It provides the NetWorker administrator with great flexibility to adapt to unforeseen situations and disasters.

The scanner program can be used to rebuild the media database and/or client file index entries for a particular storage volume or volumes, and is often used to scan in client file index entries to allow index-based recovery of data that has exceeded its browse policy. Entries scanned into the client file index are given browse and retention policies corresponding to those originally in effect for the save set. If a save set originally had a browse time of 1 month and retention time of 3 months, scanning it back in after expiration would make it browsable for an additional 1 month and recoverable for an additional 3 months.

In extreme cases, scanner can be used to recover the media database and client file indexes in their entirety by reading every storage volume. The program can also read and recover data directly. This is useful when transferring data in OpenTape format from one location to another. Scanner can also be used to manually verify the integrity of a NetWorker volume.
3.5.5 Disaster Recovery

NetWorker is designed with disaster recovery as a primary focus. If a disaster occurs—whether it is isolated to a single system, strikes the NetWorker server itself, or affects an entire site—NetWorker is able to respond quickly so that data can be restored and operations can resume in minimal time.

As discussed in the backup section above, the NetWorker databases are regularly protected by the creation of bootstraps. If a disaster strikes the NetWorker server, it must first be recovered to an operational state. This may involve fixing hardware and re-installing operating system software and NetWorker software. Once the NetWorker software is functional, the most recent bootstrap can be recovered from storage media using the `mmrecov` program. Each time a bootstrap is saved, a bootstrap report is printed on the default NetWorker printer. This report contains the information needed to quickly locate the proper storage volume. If this information is not available, the bootstrap can be located using the `scanner` program.

The bootstrap contains the media database and configuration database. Once this information is restored, recovery of the client file indexes can commence. Save set recovers can begin as soon as the bootstrap is recovered as can regular backup operations. Client file index-based recovers are delayed until the appropriate index files are recovered.

Disaster recovery for NetWorker storage nodes and clients follow roughly the same procedures. The failed system must first be brought back online. This may require hardware repairs, operating system software installation, and installation of NetWorker software depending on the nature of the failure. Once the NetWorker software is functioning, data recovery can begin. The `mminfo` command can be run on the server to determine which volumes are required to fully recover a particular client or storage node. Using the appropriate program for the client type, the drives or filesystems to be recovered can be easily designated. This may include the restoration of special backups depending on the platform being recovered. For instance, Windows NT includes a special backup called `System State` that includes the registry and other critical configuration information.

Disaster recovery can be further facilitated using the add-on product NetWorker Recovery Manager. See the later section entitled NetWorker Recovery Manager for details. For complete information on Disaster Recovery, refer to The Legato NetWorker Disaster Recovery Guide.

3.6 NetWorker in Cluster Environments

In a cluster, two or more independent computer systems are connected and appear to network users as a single system. A cluster is usually configured to accommodate failures of any single component including entire systems, allowing application services to continue in the face of hardware or software failures. Because of round-the-clock operations and globalization, enterprises are increasingly turning to clusters to provide the availability and compute capacity they require.

In a typical cluster environment, each physical host or node has private data that must be protected as well as data that is shared with other nodes. (Shared data is typically controlled by a virtual server or servers consisting of two or more cluster nodes.) There may also be cluster-specific databases and configuration data that must be protected. NetWorker can distinguish and back up all these data types.

---

3 Data can be shared via direct-attach SCSI, but the availability of fibre channel and Storage Area Networks dramatically simplifies the sharing of data within a cluster.
Figure 11. Typical cluster environment. Each physical node (Node A and Node B) has local disks that must be backed up. The two nodes also have a set of shared disks used for application data. In this example, NetWorker is itself configured as a highly available application running as a virtual server on Node A. If Node A fails, the NetWorker server will be moved to Node B.

NetWorker provides support for the following Cluster environments:

- Legato Automated Availability Manager
- Microsoft Cluster Server
- Sun Cluster
- Compaq TruCluster
- IBM HACMP
- HP MC ServiceGuard

NetWorker can operate in a cluster environment in two modes:

1. **Cluster Server** in which NetWorker itself is a highly available application within the cluster. Only NetWorker Power Edition supports this mode of operation.

2. **Cluster Client** in which NetWorker client software is installed on cluster nodes. Both NetWorker Power Edition and Network Edition support this mode of operation.

In either mode, NetWorker can effectively back up all cluster data. Once NetWorker has been properly configured to support and recognize a cluster, backup and recover services proceed in a fashion identical to that for non-clustered systems.

For more information on Legato Automated Availability Manager, see the later section, *Legato Automated Availability Manager* or for more information on the other supported Cluster environment, refer to the NetWorker 6.x Administrator's Guide.

## 4 Database and Application Backup

Most Enterprises have mission critical databases and applications that must be backed up regularly. For the specialized data types maintained by these applications, it is not sufficient to use the normal file system backup and recover methods provided by NetWorker. NetWorker capabilities can be extended with specially tailored NetWorker Modules that integrate a wide variety of databases and applications into the NetWorker environment, allowing them to be backed up and managed from a central location. Integrating database backup with NetWorker removes the burden from the database administrator, while still allowing full control of the recovery process. NetWorker Modules increase availability by reducing or eliminating
the need to take down databases and applications for backup. High-performance online backup and recovery ensures that critical database and application files are always available.

NetWorker Modules available for database and application support include:

- NetWorker Module for DB2
- NetWorker Module for EMC Symmetrix for Oracle
- NetWorker Module for EMC Symmetrix for SAP R/3 on Oracle
- NetWorker Module for Informix
- NetWorker Module for Lotus Notes
- NetWorker Module for MS Exchange Server
- NetWorker Module for MS SQL Server
- NetWorker Module for Oracle
- NetWorker Module for SAP R/3 on Oracle
- NetWorker Module for Sybase

A NetWorker Module is installed on the system where the database or application resides. This system must also be configured as a NetWorker client. (The system hosting the application may be configured as a NetWorker server if desired.) The NetWorker Module serves as an intermediary between the application and the NetWorker server. The module works with the native functionality of the database or application to provide complete backup and recovery services.

Most databases and applications provide varying degrees of built-in backup and recovery functionality. NetWorker Modules integrate seamlessly with existing services to provide scheduled, lights-out backup, central administration, advanced media management and optimized performance. For example, the Oracle database provides RMAN (Recovery Manager), which provides low level backup and recovery mechanisms. The NetWorker Module for Oracle utilizes RMAN services to backup and recover Oracle databases and archived redo logs. All Oracle data is stored on NetWorker volumes. Activities initiated through RMAN connect to NetWorker using the services of the NetWorker Module.

Wherever possible, the X/Open Backup Services API (XBSA) is used for communications between the NetWorker server, NetWorker module, and the application. XBSA defines a standard interface allowing storage management applications like NetWorker to interact with databases and other applications that require backup services.

Once the NetWorker Module has been installed and configured, scheduled backups can be initiated by the NetWorker server. Each NetWorker Module is tailored to the application to ensure that all critical application data is backed up no matter where it resides or how it is managed. For databases, this may include transaction logs and other ancillary data items necessary to fully recover a database. For hybrid applications such as Lotus Notes where some data is stored in a database format and other data is stored in flat files, the NetWorker Module uses database methods to backup database files while other files are backed up using standard methods.
If a database or application provides its own interfaces for ad hoc backups, they can be used in addition to NetWorker interfaces to schedule manual backups as necessary. The NetWorker Module mediates the operation and transfers data to the server or storage node as appropriate.

When a database or application must recover data, the request is typically initiated using the interfaces provided with the database or application. In some cases, the NetWorker Module includes a program or script that is executed on the system hosting the application to initiate data recovery.

In either case, the NetWorker Module mediates the transaction, communicating with the NetWorker server to locate and load the correct storage media and initiate the data transfer.
5 Extending NetWorker Core Functionality

The core features of NetWorker are designed to meet a wide variety of customer needs. However, some specialized functions are optional or beyond the scope of the core product. The NetWorker environment can be customized through the activation of optional functionality or the addition of a wide variety of products to meet specific needs such as those created by NAS devices, SANs and clusters. Optional features can be activated simply by the entry of an appropriate license key. Add-on products require the installation of additional software in addition to the core NetWorker software. This section explores a number of these products, discussing when they are needed and how they operate.

Optional features include Dynamic Drive Sharing (DDS), NDMP Client Connection, and NetWorker Archive. These are discussed first, followed by information on the wide array of NetWorker add-on products.

5.1 NetWorker Dynamic Drive Sharing (DDS)

NetWorker DDS is an optional NetWorker feature. A typical NetWorker datazone consists of a NetWorker server, one or more storage nodes, multiple clients and associated tape libraries and/or standalone drives. Libraries and drives are typically attached to individual systems as indicated in figure 14.

![Figure 14. A typical NetWorker environment with direct-attached tape libraries](image)

By default, NetWorker 6.1 Network and Power Editions allow server and storage nodes to share the same tape library, but each individual tape drive must be dedicated for the use of one particular host4 and cannot be shared. Libraries can be shared through multiple SCSI connections or by connecting the device to a SAN as illustrated in Figure 15.

---

4 In releases prior to NetWorker 6.1, that functionality was sold separately as the Shared Library Option.
Figure 15. NetWorker datazone with a SAN-attached library shared between server, a storage node and two SAN storage nodes. (One or more drives must be permanently allocated to each system unless DDS is in use.)

DDS allows sharing of the same tape drives among multiple hosts (the server, storage nodes, SAN storage nodes, and NAS devices with NDMP). A system initiating a backup is allocated a drive only for the time it takes for its backup activity to complete. Upon completion, the drive is available for use by other hosts.

In addition to allowing physical drives to be shared, DDS also allows some or even all of the storage volumes in an autochanger to be shared among multiple storage nodes. All tape volumes in a library could be made available for use by any storage node that shares that library. A subset of the total set of tapes does not have to be pre-allocated to each storage node. Because all NetWorker tapes are written in OpenTape™ format, even storage nodes with different operating systems (for example, NT and Solaris) can write data to the same tapes, allowing even better utilization of a library. This functionality is unique to Legato NetWorker.

In a DDS environment, there are multiple device definitions—one for each node sharing the drive—all pointing to a single physical drive. Each device definition points to only one physical drive. Each physical drive may have multiple device definitions. The DDS software manages these definitions, and controls access to physical drives so that two systems can't access the same drive at the same time. A simplified NetWorker DDS configuration is shown in Figure 16.
The server and storage nodes dynamically share access to the two drives over the SAN. The arrow from the server to the tape library indicates that the NetWorker server controls the robotics in the library. However, it is not required that the server control the robotics; any storage node can be configured to do so.

5.2 NDMP Client Connection

Network Data Management Protocol (NDMP), which was jointly developed by Legato and Network Appliance, is a standard protocol that provides backup and recover services for network-attached devices. NDMP is ideally suited for the backup and restore of network attached storage (NAS) systems and is now recognized as the preferred method of managing data for NAS.

NDMP in NetWorker 6 is offered as an optional product—Legato NetWorker NDMP Client Connection—providing backup and restore support for NDMP-compliant NAS devices.

NetWorker NDMP Client Connection software provides backup and recover support for NDMP-compliant NAS devices. Sharing of tape libraries between NDMP and non-NDMP backups is also allowed.
Figure 18. Three-party NDMP Configuration. Data flows from NAS Device #2 over the network to NAS device #1 and then to tape. Metadata is sent from NAS Device #2 to the backup server. NDMP control information flows between the backup server and both NAS devices.

NetWorker is able to backup or recover NDMP hosts running NDMP version 1, 2 or 3. Three configurations are supported. In addition to the standard local and three-party configurations, a system running NDMP can be backed up to a tape device attached only to the NetWorker server. NetWorkerNDMP Client Connection does not currently support the disk-to-disk and tape-to-tape copying feature described in version 3 of the NDMP specification.

Figure 19. Configuration for transferring data between a NAS device and a library attached to a NetWorker server. Data from the NAS device passes to the NetWorker server and is written to the tape library by the NDMP Tape Service provided by NetWorker SnapImage.

NetWorker Advantages for NAS Devices
Legato provides NAS devices with as much of the functionality of its standard client/server product as possible while maintaining strict adherence to the NDMP specification. The NetWorker implementation of NDMP provides many of the important features of standard NetWorker including scheduled backup, index management, configurable browse/retention policies, media management, Administrative and User GUIs, file by file recover and save set recover. The NDMP specification does not define all of the features that Legato customers have come to expect, so some features could not be supported. Some features that are not explicitly defined in the specification were provided using the basic features of NDMP as building blocks.

Directed Recovery

This configuration currently requires installation of the Legato NetWorker SnapImage Module on the NetWorker server.
Directed recovery is one important feature that is not explicitly defined by NDMP although it is supported by NDMP. Using directed recovery the NetWorker server can retrieve data from any DSP and direct that data to another DSP (or a different directory or file system on the same host). This capability can be important for disaster recovery. The whole process can be done remotely from an administering NetWorker system. No one needs to be physically present at the NetWorker server, or either DSP.

Direct Access Restore (DAR)
DAR provides the ability to keep track of tape position for individual files in NDMP backups so that the tape server can seek directly to the file during restore. This process eliminates the time consuming process of scanning tapes searching for the specific individual files to restore.

Legato NetWorker NDMP 6.1 and later releases support Direct Access Restore (DAR). A single file or even an entire set of files can be restored more quickly through DAR. Support for DAR involves recording seek offsets for individual files in the save set. In typical NDMP implementations, NDMP backups and restores do not do this; consequently a single file restore requires reading through an entire save set.

Library Sharing
Sharing of tape libraries between DSP appliances of the same type and sharing of tape libraries between NDMP and non-NDMP backups are supported with Legato NetWorker NDMP.

Dynamic Drive Sharing (DDS)
DDS provides the ability to dynamically share individual tape devices in an autochanger attached to a SAN. NetWorker 6.1 and later allows dynamic drive sharing (DDS) between DSPs of the same type, for example, between NetApp filers or EMC IP4700 appliances. Drive sharing between NDMP and non-NDMP appliances in a SAN is supported. All of the components in the SAN must be supported by all vendors for Legato to support DDS for the configuration.

![Figure 20 – NetWorker Server, Storage Node and NAS-NDMP share tape devices in a SAN.](image-url)
Complete details of NDMP and the implementation of NDMP in NetWorker can be found in the white paper, *NDMP Support in NetWorker 6*.

### 5.3 NetWorker Archive

The primary purpose of archiving data is to conserve online disk storage while ensuring that the data stored on the archived media is reliable, safe, and easily retrievable. Data archival is performed in addition to scheduled backups, to provide a higher level of security for mission-critical data. Data archival is typically performed on files and directories that are closely associated, such as quarterly financial data or source code trees. Archival is frequently used at the completion of a project or at the end of a defined period such as a quarter or fiscal year.

NetWorker Archive works in a manner similar to backup but is used under different circumstances. Archive is typically used whenever a permanent copy of a set of data is required from a single point in time. For instance, at the close of a quarter a financial organization might archive all records from the quarter and store them permanently off-site.

Permanence is one of the primary features of archives. Archives are not subject to the browse and retention policies of backups. Online copies of archived data are often deleted after an archive is created, although this is not required. By definition, archives are always equivalent to full backups. There is no such thing as an incremental archive.

When NetWorker archives data, it takes a snapshot of the specified save sets as they existed on the client at a single point in time and writes the data to one or more archive volumes. Archives and backups do not share the same storage volumes. With each archive request, an administrator can optionally create a short description or *annotation* (up to 1024 characters) of the archived data. NetWorker stores the archive description with each save set entry in the media database but not on the archive volume. After the archive completes, NetWorker verifies the stored data. If verification is successful, the administrator is prompted to delete the source save sets.

Archives can be scheduled to occur at particular times using methods similar to those for scheduling backups. Scheduled archives can be configured to automatically *groom* (delete) archived save sets if desired. The operation of archive differs somewhat for PC versus Unix clients. By default, archives from PC clients generate entries in the client file index, while archives of Unix clients do not. Archive recovery typically involves restoring the entire archive as a unit. However, if client file indexes have been written, the archive can be browsed and individual files can be restored.

### 5.4 Legato Automated Availability Manager

Legato Automated Availability Manager (LAAM) is a suite of clustering software services that provide high availability and centralized management for clusters of computers. A cluster is a cooperating group of computers. With LAAM, these systems need not be of the same model or even the same platform.

LAAM provides a general framework for monitoring almost any application, providing failover to a secondary server should trouble arise. In addition, a variety of modules are available that are tailored to meet the specific needs of mission critical databases and applications. LAAM offers the ability to accommodate system maintenance, load fluctuations, business workflow cycles, and human error.

LAAM is designed to function in a wide variety of cluster environments including shared-disk and shared-nothing configurations. Shared-disk configurations utilize direct-attached SCSI disks or Storage Area Networks (SANs). In SAN configurations, up to 100 nodes can be configured in a single cluster domain. When failure occurs in a shared disk environment, a secondary server immediately takes control of critical application data.
Shared-nothing configurations utilize a local area network (LAN) or wide area network (WAN) with data replication and synchronization provided by Legato wanCluster. Replicating data at a remote site provides disaster recovery and follow-the-sun capabilities for global operations.

LAAM maintains a replicated database, to ensure that all nodes in the environment can access all domain information. Each database copy contains records of all defined components, their configuration and their runtime states, so each cluster node has access to all necessary information at all times, enabling immediate rule-based decision making. NetWorker offers full support for backups of data maintained in a Cluster environment. See the previous section NetWorker in Cluster Environments, for more details.

5.5 *NetWorker SnapImage*

NetWorker SnapImage is an add-on product that combines the functionality of image backups with a snapshot capability to provide consistent, high performance online backups. NetWorker SnapImage is ideally suited for the backup of applications such as mail systems that generate large numbers of small files. The processing overhead of backing up huge numbers of small files with traditional methods can be prohibitive. SnapImage facilitates online backup and greatly increases backup performance while lessening the impact on application performance. Systems running Solaris and HP-UX are supported.

The snapshot function of NetWorker SnapImage ensures that a stable, consistent version of the file system is backed up. A block-level snapshot of the file system is taken at the commencement of the backup, allowing the backup to proceed using a point-in-time static view of the file system. This snapshot does not disrupt file system access. As data blocks within the file system are modified the writes are intercepted by the \textit{wi} (write intercept) driver. The original data stored in those blocks is cached. SnapImage uses a separate raw disk partition for the cache. Backups reading the snapshot retrieve the original blocks from the cache whenever modified data is encountered. Since modified data blocks are written to the file system as normal, if anything does go wrong with the process the file system is not adversely affected. A new snapshot can simply be taken and the backup re-started.

Image or block-level backup typically copies a file system or disk partition to tape block by block without paying attention to file-level details. (Storage devices such as disk drives are typically divided into blocks to facilitate management and I/O. Block sizes vary, but typically range from 512 bytes to 4KB.) NetWorker SnapImage extends the functionality of traditional image backup with mechanisms to ensure that only populated blocks are written to storage rather than the entire image of the file system.\footnote{A \texttt{dd}-compatible option can be used to create image backups in \texttt{dd} format. The \texttt{dd} utility can then be used to restore the backups if necessary. When this option is used, all blocks in the file system are backed up.}
Figure 21. NetWorker SnapImage provides block-level image backup. A server can backup local data (direct or SAN-attached) to tape, or can provide backup services to backup a remote server using NDMP to transfer data across a network.

Incremental backups can also be performed with NetWorker SnapImage, unlike traditional image backup methods. During an incremental backup, only blocks that have changed since the previous backup are saved. This method can be much more space efficient than standard backup methods. Under standard methods, if a small change is made to a file, the entire file—possibly consisting of hundreds or thousands of data blocks—is backed up. With NetWorker SnapImage, only the block or blocks that contain modifications need be saved.

In order to perform incremental backups, SnapImage maintains a Block Level Incremental (BLI) bitmap in system RAM to record which blocks have been modified since the last backup. This bitmap can be preserved during normal system reboots. However, a system crash will result in the loss of this data and necessitate a full backup.

Recovering single files is not possible with traditional image backups. Typically, if a single file or a small set of files must be recovered from an image backup, the entire image is restored to a spare partition and the necessary files are recovered from there. As file systems get larger and larger this process becomes prohibitive due to time and resource constraints.

NetWorker SnapImage overcomes this limitation. Before a backup commences, SnapImage scans the file system and stores the block locations for each file allowing any individual file to be restored as necessary.

NetWorker SnapImage records block level information in the /usr/ndmphome/mdcache directory using two separate files. One keeps track of blocks backed up, and the files those disk blocks represent. The other file keeps track of where the blocks are located on the disk. This provides the ability to map files selected for recovery to a list of disk blocks, and hence to the locations where those blocks exist on tape. This information is separate from that in the client file index's media database.

NetWorker SnapImage uses the NDMP protocol for all external communications. The NetWorker server must be NDMP-enabled through the installation of NDMP Client Connection software. If NetWorker SnapImage is to use a tape device connected to the NetWorker server or another system, SnapImage must be installed on that system as well. This is necessary because NetWorker SnapImage implements the NDMP tape server function required to receive NDMP data streams and direct the data to tape. The presence of the NDMP tape server provides an added benefit in that a system with NetWorker SnapImage installed can be used for remote NDMP backup of Network Attached Storage (NAS) systems.
5.6 Celestra

Legato Celestra builds on the functionality of NetWorker SnapImage to create the first truly serverless backup product. The Celestra architecture has gained widespread acceptance in the storage industry, becoming a de facto standard for serverless backup. More than 50 vendors have joined the Celestra Consortium to promote an open, integrated architecture for effective data movement and management of Storage Area Network (SAN) environments.

Key to the functioning of Celestra is the SCSI Extended Copy Specification\(^7\), which allows vendors to develop products that can inter-operate. Developed by Legato, the specification allows any device that implements it to copy data directly from disk to tape, eliminating server involvement.

Celestra is implemented as two separate components. The Celestra Power Agent, which runs on the server that controls the data, and the Celestra Data Mover, which implements extended copy and performs the data movement. When backup begins, Celestra Power syncs the file system, takes a snapshot, and builds a file system block list. Metadata is collected and forwarded to the NetWorker server for indexing. These operations are analogous to the operations performed by NetWorker SnapImage (see previous section for a more detailed discussion). Celestra Power is able to complete these tasks rapidly with little incremental burden to the data server, allowing applications to run unimpeded.

When its tasks complete, Celestra Power sends the block list to the Data Mover. The Data Mover is an independent device that reads the blocks on the block list directly from disk and writes them directly to tape, bypassing the LAN. The Data Mover is currently implemented as a software module that runs on a standalone Sun or HP workstation. As device vendors—such as fibre channel switch makers—implement Extended Copy, a workstation dedicated to the Data Mover function will cease to be necessary. The Data Mover function will simply be subsumed as part of the SAN infrastructure.

\(^7\) The SCSI protocol is used on SANs when managing data storage, so the copy specification applies to both SANs and direct-attached SCSI devices. Because SAN configurations can support greater numbers of attached devices, SAN is the preferred choice for Celestra, but limited configurations using direct-attached SCSI disks are also possible.

Figure 22. NetWorker SnapImage in use to backup a NAS filer.
Figure 23. Celestra Power Agent and Celestra Data Mover being used for backup.

Like NetWorker SnapImage, Celestra provides hot backup of active file systems, with no user lockout or system downtime and with optimum efficiency. During full backup, only populated blocks are written to tape, not the entire disk image (unless a dd-format backup is specified). During incremental backup, only changed blocks are backed up, not entire files. Backup operations can be completed in less time and—because there is no disruption to access—performed more often, reducing data loss exposure. Directories and individual files can be recovered directly from tape. If a disaster occurs, full image recoveries are written directly from tape to disk, dramatically reducing restore times and downtime costs. Celestra uses NDMP to communicate with external applications. This allows Celestra to interface with any NDMP-compliant backup software product, not just NetWorker, however no other applications have been certified at this time.

The Celestra Module for Oracle (CMO) extends the functionality of Celestra to protect Oracle databases. CMO places the database in a consistent state before backup begins to ensure integrity. Then—as with a standard Celestra backup—the Celestra Power Agent creates a snapshot of the partition(s) containing the database, creates a block list for backup, and passes that block list to a Data Mover to copy the designated blocks direct from disk to tape. CMO interfaces directly with NetWorker, which provides automated backup scheduling, autochanger support, media handling and centralized administration.

5.7 Open File Manager

Open File Manager (OFM) from St. Bernard Software is an add-on that enables NetWorker to back up open files on Windows and NetWare servers in a consistent state regardless of the access mode or file-locking status set by other applications. In a typical NT or NetWare backup, files that are opened by another application are locked by the O/S and can't be backed up. If files are read while writing is in progress, there is a serious risk of the file being saved in an inconsistent state. With OFM, changes made during the backup do not affect the correctness of backed up files and no interruption in service is experienced by users.

Before an open file is backed up, OFM ensures that there are no transactions pending and the file is in a consistent state. Once consistency is assured, backup begins. If modifications are written to a file while the backup of that file is in progress, OFM stores the original data in a disk cache accessible to NetWorker. The original data from the files that are modified is cached, and the modifications are written to disk. NetWorker backs up the cached original blocks of data rather than the modified data, ensuring that the file is backed up in a consistent state that corresponds exactly to the state of the file at the time the backup began. This method of ensuring data consistency is analogous to the snapshot methods used by NetWorker SnapImage and Celestra as discussed in the previous two sections.
Original data can be maintained in the cache until backup verification is complete (if desired) or the space used by each file can be released as the backup of that file completes.

**Figure 24.** Open File Manager. Applications continue to write data files as necessary. OFM caches the original versions of all modified data blocks in a special disk cache. NetWorker reads the unmodified data from the cache as necessary to ensure that the file image copied to storage is consistent.

### 5.8 NetWorker Recovery Manager

Recovery Manager is an add-on product providing single-point, disaster recovery for NetWorker servers and clients running Windows or Solaris. Before a disaster occurs, the software automatically collects, catalogs, and stores all the information necessary to boot and reconfigure a protected computer’s basic operating system.

For Solaris platforms, the Recovery Manager Repository is a program that collects and stores all information about each Recovery Manager’s client. This information resides on the Recovery Manager server, making it accessible if a client is damaged. If a Recovery Manager client is damaged, then client can be recovered using the information in the repository. For each client computer, the repository stores the following piece of information:

- SCSI Ids
- Disk partition information
- Filesystem information
- SCSI controller information
- NetWorker version
- NetWorker server bootstrap save set information (if applicable)

On Windows platforms, the Recovery Manager Storage Adapter is a program that collects and stores all of the information needed to boot a Windows computer and recovers its basic operating system. This information constitutes a mini-operating system (MOS) image file for the computer, which is used to create a recovery boot CD-ROM. Each MOS image file is composed of three major parts:

- File activity logger (FAL) - which collects a list of all of the files that are loaded into the system and then determines which files are absolutely necessary to boot the computer, such as filesystem drivers, I/O drivers and device drivers for network and SCSI cards.
- Disk partition information
- Custom defined files
• **musthave.lst** - allows administrator to include any personal or application files in the MOS image that are required in the first stage of recovery along with the "must have" files identified by the FAL.
• **Blacklist.lst** - allows administrator to determine which files Recovery Manager will not restore when recovering the system. By default, this list is empty.

In the event of a disaster, Recovery Manager works in conjunction with NetWorker backup and recovery software to guide an administrator through the system recovery process including:

• Reformat and re-partition the hard disk
• Reinstall and reconfigure the Windows operating system (for Windows clients only)
• Recreate the file systems
• Reinstall and reconfigure the NetWorker backup and recover software
• Recover the system’s application and data files to their pre-disaster state using the latest NetWorker backup files

### 5.9 **AlphaStor**

AlphaStor provides drive sharing and advanced media management across multiple NetWorker datazones. NetWorker customers often implement multiple NetWorker servers to maximize backup performance. This means there are multiple client-file indexes and media databases, introducing multiple points of media administration and increased complexity. AlphaStor reduces this complexity by providing a single and consolidated view of all NetWorker media, as well as other storage media.

AlphaStor’s integration to NetWorker is seamless, allowing for fast, smooth implementation and immediate access to AlphaStor’s extended media management functionality. When used in conjunction with NetWorker, AlphaStor provides:

• A simple-to-use, browser-based interface for Data Center operation personnel
• Onsite and offsite tape rotation management and tracking
• The ability to schedule, track, and automate movement of all media, regardless of location, based on defined policies and utilizing tape retention policies defined within NetWorker
• Ability to share tape devices and libraries across multiple NetWorker servers and storage nodes.
• A consolidated view of all media and drive usage.
• Consolidated reporting of tape pools and media by location.
• Support for Storage Area Networking (SAN) environments.

AlphaStor interfaces with NetWorker via the AlphaStor Data Mover Interface Module, keeping tape information in sync between AlphaStor and NetWorker databases. AlphaStor maintains information not provided in the standard NetWorker databases, (such as rotation schedules, on/offsite locations, etc.) as well as device and library information. When NetWorker requests a tape device (mount), AlphaStor determines what device to use and returns the device path to NetWorker.

AlphaStor is implemented to integrate with NetWorker using the same interfaces as GEMS SmartMedia. (See the following section, GEMS, for more information on SmartMedia.) NetWorker is configured to work with either product through the creation of a virtual jukebox. AlphaStor takes over the management of the physical library (or libraries), offloading those tasks from the NetWorker Servers and storage nodes.

A virtual jukebox tracks the volumes that have been allocated to be used by a NetWorker Server. The virtual jukebox also maintains a list of volumes managed by AlphaStor that the NetWorker Server can access. The number of “slots” in the virtual jukebox increases as volumes are allocated and decreases as volumes are removed. Only a single virtual jukebox is required in each NetWorker datazone regardless of the number of physical devices present in the AlphaStor environment. This dramatically simplifies the configuration and management of media and devices across multiple NetWorker datazones.
5.10  GEMS

The Legato Global Enterprise Management of Storage (GEMS) Product Family is a suite of management software products that enable information systems managers to provide global management, consistency and control of distributed storage and data protection across an enterprise. From GEMS enabled systems, organizations can centrally configure, control, and manage storage resources across platforms, networks and geographically dispersed sites. GEMS products employ advanced administration policies to streamline management of media, devices, and systems, and simplify the management of data protection and data movement software. GEMS products provide a higher level of control that complements the data protection services of NetWorker. Using GEMS, multiple NetWorker data zones across an enterprise can be managed.

**GEMS SmartMedia** is a standards-based service for enterprise-wide management of removable media and devices. SmartMedia allows different applications to share common libraries and drives, which increases utilization and reduces hardware administration costs. SmartMedia reduces the complexity and costs associated with removable media. An enterprise can choose fewer larger media devices, rather than providing individual smaller devices to go with each application requiring removable media. SmartMedia acts as middleware between applications and robotic library hardware.

Using SmartMedia, heterogeneous applications—including backup, archive, HSM and other homegrown applications or scripts—can share the same tape libraries and even the same devices within those libraries. SmartMedia provides media management, mediates device access, and maintains pools of storage volumes for each individual application.

NetWorker communicates with SmartMedia through a virtual jukebox. SmartMedia takes over the management of all defined autochangers, relieving the NetWorker server or storage node from this task. The virtual jukebox tracks volumes that have been allocated for use by a NetWorker server. The virtual jukebox also maintains a list of volumes managed by SmartMedia that the NetWorker server can access. The number of slots in the virtual jukebox increases as volumes are allocated and decreases as volumes are de-allocated.

The number of devices added to the virtual jukebox defines the maximum number of SmartMedia volumes that the NetWorker server can access simultaneously. This number is an upper boundary because devices managed by SmartMedia are shared. Consequently, they might not always be available.

SmartMedia is based on OpenVault™ technology licensed from Silicon Graphics®, Inc. Both SmartMedia and OpenVault are the basis of IEEE’s Storage System Standards Working Group (SSSWG) efforts to standardize a Media Management System (MMS) definition. Legato actively participates in the SSSWG efforts and intends to maintain conformance with the written IEEE standards for MMS. The first five standards for MMS were released by the IEEE in 2000. (Those standards are numbered 1244.1 through 1244.5). For more information, refer to the IEEE SSSWG web site, www.ssswg.org.

Other GEMS products include:

**GEMS Frameworks** software: provides integration between NetWorker and popular system management frameworks including HP IT/Operations, Tivoli Management Software, and CA Unicenter TNG.

**GEMS Storage Resource Manager** (SRM) provides web-based automated enterprise-wide reporting for online storage capacity, consumption and availability. SRM uses agent-based technology and a standard web browser interface. It automatically monitors all disks, RAID systems, partitions, directories, and files in Windows, UNIX and Linux environments.

**GEMS Console** is an affordable, easy-to-install-and-use web-enabled management application. It provides central monitoring, administration, and reporting for Legato NetWorker servers. GEMS Console centralizes Legato NetWorker events and associates priority icons with each. With its cross-platform browser interface, GEMS Console can centrally administer any NetWorker server from any system running...
Netscape Navigator or Microsoft Internet Explorer, automatically displaying the success or failure of each
day’s backups.

5.11 NetWorker HSM

NetWorker HSM (Hierarchical Storage Management) is an add-on product providing a flexible and automatic framework for migrating infrequently accessed online data to less expensive nearline or offline media. Although disk storage is becoming increasingly cheaper, it creates many less obvious expenses such as the labor involved in installing and configuring additional disks, identifying inactive files, and manually freeing up disk space. The cost of the electricity and physical space required for a sizable disk farm are also substantial. On many networks, 20% or less of stored data is actually accessed in any given month. These factors can make HSM attractive for a variety of applications. HSM is currently available for systems running Solaris, Compaq Tru64 Unix, and Windows NT/2000.

Conceptually HSM is straightforward. HSM allows infrequently accessed files to be automatically and transparently migrated from more expensive, high performance storage media to less expensive, slower storage devices such as optical libraries, tape drives, and tape libraries. When migrated files are accessed, they are automatically copied back from the slower medium onto disk. The migration process is transparent to the user or application accessing the file. NetWorker HSM can provide a nearly unlimited storage pool with continuous access to all data. (Of course, access to data stored on slower media incurs some delay while the data is located and transferred back to primary storage.)

Under HSM, data migrates from a client’s file system to a migration pool. The trigger for data migration is based on an administrator’s definition of a high-water mark and a low-water mark each specified as a percentage of total disk space. The high-water mark defines the threshold when automatic migration begins. Migration continues until all eligible files are migrated or until the low-water mark is reached. For example, HSM might be configured to begin migration when a file system exceeds 70% capacity (the high water mark) and to cease migration when the file system drops below 40% capacity. Files can be selected for migration based on some or all of the following criteria:

- File system
- time of last access
- minimum file size
- file owner
- file group

HSM operation occurs in five distinct phases:

1. When NetWorker launches, files are identified as migration candidates, based on the administrator-defined migration configuration resources.
2. When a scheduled group backup runs, the client’s migration candidate files are evaluated for pre-migration. The evaluation occurs whether or not the candidate files will participate in the backup, and regardless of file space issues.
3. For files that qualify for pre-migration, data is copied to a migration pool whose acceptance criteria match the characteristics of the data.
4. If the administrator-defined HSM high-water mark is reached, NetWorker initiates actual migration. NetWorker replaces the on-line candidate files with a stub (or symbolic link) that points to the pre-migrated file.
5. When a user accesses a migrated file, HSM issues a recall command, which uses the migration stub to locate and recover to the client machine the needed file.

Pre-migration qualification and copying activities consume system resources, but this predictable, extra drain can be factored into an environment’s overall backup strategy. Migration policies can be modified if the resource drain affects users. The positive trade-off comes later when a critical need for disk space
arises. Then, migration activity occurs immediately without resource drain, since copies of the files have already been made in the migration pool.

Figure 25. Operation of NetWorker HSM. Based on defined criteria files from HSM clients are replaced with HSM stubs (A’, B’, C’, D’). The real files (A, B, C, D) are migrated through the HSM server and stored on tape or optical media. The server itself can migrate data in a similar manner (E’, E).

Scheduled group backups of client data only back up migration stubs for files that have been migrated to storage. Independent backups of migrated data must be performed to protect that data. Recalling migrated files for backup would defeat the purpose of HSM, and possibly trigger unnecessary file system full problems. NetWorker backup is designed to work with NetWorker HSM to avoid this problem.

NetWorker recover operations of a save set (or a file) recover only the stub, or the symbolic link, of a migrated file. This stub-only recover ensures that the recovery operation will not overflow available space on the client machine. To recreate a file that has been migrated, the user must attempt to access the file, which will initiate an HSM recall.

6 NetWorker 6 Administration and Management

The administration and management features of complex software are at least as important as the technology they control. Without interfaces that are clear and easy to use, software is nearly worthless. NetWorker provides a variety of interfaces and control options and uses a variety of powerful abstractions to facilitate interactions with the software. This section describes NetWorker’s user interfaces, configuration and management issues, security, and other topics that are essential administrative requirements of enterprise-class software.
6.1 Interfacing with NetWorker

NetWorker provides a number of different interfaces tailored to meet a variety of needs. The majority of administrative tasks can be carried out using NetWorker’s graphical user interface programs. On Unix platforms this program is referred to as nwadmin; on Windows it is simply referred to as NetWorker Administrator program. A command line interface is available on Unix and Windows platforms. This interface allows NetWorker to be administered remotely through telnet or similar connections and facilitates script writing to automate common tasks. Of course, some users simply prefer this type of interface. No matter what the platform of the NetWorker server, it can provide services to clients of any supported platform.

Figure 26. NetWorker Administrative Interface for Unix.

Unix platforms also support a character-based interface—nsradmin—that can be utilized to administer NetWorker remotely or from systems that are unable to run the graphical program. Because this type of interface is uncommon in Windows environments, no similar interface is available for NetWorker servers running Windows.
NetWorker users on client systems can also choose between graphical interfaces or the command line. On Unix platforms, the graphical program `nwbackup` and `nwrecover` provide access to most end-user functions, while on Windows platforms, users can access all NetWorker features from the NetWorker User program on the Start menu. In either environment, common utilities like `save` and `recover` can be executed from the command line.

### 6.2 NetWorker Configuration and Management

NetWorker configuration and management is based on the use of a number of powerful abstractions that allow an administrator to manage large numbers of clients, storage devices and storage volumes efficiently. Operations or policies can be applied to large groups of clients or volumes at once, saving the administrator from having to re-apply the same operations repeatedly. At the same time, NetWorker interfaces provide the flexibility to tailor operations to meet specific needs of individual clients as necessary. Default and pre-configured values that work well for most situations ease initial startup and ongoing configuration.

As an example, NetWorker allows an administrator to place multiple clients in a `backup group`. The default and/or customer settings for the group apply to all group members. Any operation on the group automatically applies to all clients in the group. For instance, an administrator can define a schedule and apply it to the group so that it automatically takes effect for all clients in the group.

NetWorker manages `volume pools` in a similar fashion. Any number of storage volumes can be lumped into a pool. All selection criteria applied to the pool apply to each member. This greatly simplifies the process of managing large numbers of individual storage volumes.

#### 6.2.1 Resources and Attributes

Everything controlled by NetWorker—clients, storage devices, backup schedules, policies, etc.—is considered a NetWorker `resource`. Each resource has one or more `attributes` that control features of the resource. Attributes may themselves be resources. For instance, a client resource can have schedule and policy resources as attributes. This may seem at first confusing, but the way resources and attributes are defined within NetWorker provides great uniformity and is crucial to the flexibility and power of the interface.
The following table defines some of the key resources used within NetWorker.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>Defines the NetWorker features enabled for this NetWorker server.</td>
</tr>
<tr>
<td>Server</td>
<td>Identifies the local NetWorker server characteristics. Only one server resource can exist per NetWorker server.</td>
</tr>
<tr>
<td>Notification</td>
<td>Names and defines a trigger-and-action pair of events: a specific NetWorker event is associated with a specific server response, defined either by a default or customer setting.</td>
</tr>
<tr>
<td>Client</td>
<td>Identifies a unique set of data items associated with a unique system/machine (filesystems, disk volumes, directories, or files) for backup and assigns specific backup instructions to the set.</td>
</tr>
<tr>
<td>Policy</td>
<td>Names and defines a time period that can be associated with administrator-specified data lifecycle policies for data.</td>
</tr>
<tr>
<td>Directive</td>
<td>Defines file-processing activities that the NetWorker server performs during backup of a client.</td>
</tr>
<tr>
<td>Device</td>
<td>Describes a device that is either locally connected or connected to a storage node that is managed by the NetWorker server.</td>
</tr>
<tr>
<td>Pool</td>
<td>Names a collection of volumes and specifies the acceptance criteria that backup data must meet to be written to this named collection.</td>
</tr>
<tr>
<td>Label Template</td>
<td>Provides instructions for the NetWorker software to follow to create a label for a volume. Each pool is associated with a specific label template.</td>
</tr>
<tr>
<td>Staging</td>
<td>Names and defines the NetWorker policy of moving data from one storage medium to another.</td>
</tr>
<tr>
<td>Group</td>
<td>Names and defines a unique collection of client resources that participate in a group backup operation. Clients can follow different backup schedules within the group operation, but all clients in the group start the operation at the same time.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Names and defines a backup schedule that can be assigned to a client or group resource. The schedule dictates the days that the data is to be backed up and the level of each backup.</td>
</tr>
<tr>
<td>Autochanger</td>
<td>Describes a device that can mount and write to multiple volumes automatically. Contains a robotic arm and one or more tape devices, holds multiple volumes for writing, and can mount them into it's tape devices automatically</td>
</tr>
</tbody>
</table>

Table 5. Common NetWorker Resources

![Figure 28. Dependencies of various NetWorker resources.](image_url)
Configuring NetWorker for backup and recovery simply involves defining the appropriate resources. At a minimum, the NetWorker Server, any attached devices and any clients must be configured. Since many default and pre-configured values are provided, the initial configuration tasks are quite simple. Over time, the configuration can be tailored to meet specific business needs and to adapt to growth.

### 6.2.2 Notifications and Reports

The NetWorker server sends notifications to inform an administrator about events taking place in the NetWorker environment. A notification describes a specific NetWorker event (which functions as a trigger) and a specific action that the NetWorker software implements in response to that event. NetWorker provides a large number of pre-configured notifications, and custom notifications can be configured as needed.

Each notification consists of an event, an action, and a priority. Typical events include the need to mount or unmount storage volumes, the completion of a backup group, or the need to perform device cleaning. The administrator can configure a variety of actions to take when an event occurs. Standard actions include writing to log files and sending messages to the NetWorker management console and/or a designated printer. Events can also be trapped and sent to an SNMP management console. NetWorker provides great flexibility in configuring actions so that almost any program can be executed when an event occurs. This makes it possible to have important event notifications trigger e-mail or paging alert systems.

Some events result in the creation of detailed reports. For instance, each time a backup group completes, a savegroup completion report is generated. This report provides status information for all save sets initiated during that backup session. A separate bootstrap creation report is created each time NetWorker creates a bootstrap. By default, this information is sent to a printer so that it is available for disaster recovery if necessary. A variety of other NetWorker utilities exist for creating ad hoc reports covering various areas of NetWorker operations such as volume or device status, or the state of the client file index and media database. More advanced reporting for NetWorker can be achieved using GEMS Reporter. (See the previous section entitled *GEMS* for more information.)

### 6.2.3 Schedules

NetWorker provides great scheduling flexibility to help accommodate ever shrinking backup windows. Pre-configured schedules are provided which implement commonly used backup schedules, but these can be modified or new schedules can be created to meet any requirements. Backup begins at the time designated for a backup group, then each client’s backup schedule tells the NetWorker server what level of backup operation to perform on a given day. For instance, on Fridays a full backup might be performed while incremental backups are performed the rest of the week. Schedules can be very simple or very complex. All clients can share the same schedule, or each client can have its own unique schedule.

Although the process of creating and using backup schedules is straightforward, careful planning is necessary to create an optimal backup scheme. The following questions have to be considered:

- How much data must be backed up?
- How big is the backup window?
- What is the aggregate bandwidth of available backup devices?
- How many storage volumes are available?
- Does it matter how many volumes are required to recover from a disaster such as a disk crash?

The answers to these questions may dictate the final backup schedule. For instance, if bandwidth is limited or the backup window is small, it may make sense to stagger backup schedules to smooth out the load. If all full backups are performed on the same day, that can result in a dramatic increase in backup load on that day versus implementing schedules that spread those backups across multiple days.
6.2.4 Browse and Retention Policies

Browse and retention policies are used to control the data lifecycle for data backed up and stored by NetWorker. Changes to these policies can have a great impact on data security, and the amount of storage required.

The NetWorker browse policy determines how long information about files is retained in the client file index, and therefore controls how long users can browse and recover individual files. The retention policy determines how long save set data is actually stored before being eligible to be overwritten.

After a save set exceeds its browse policy, NetWorker must decide when to delete all records associated with that save set from the client file index. If no other save sets depend on the save set in question, the records are deleted immediately. However, if other save sets are dependent on a save set that has exceeded its browse policy, the records for that save set are not removed until all the dependent save sets have also exceeded their browse policy. For example, a full backup will remain browsable until all the incremental backups that depend on it exceed their browse policy. This ensures that a file can be reconstructed to any point in time encompassed by the browse period.

Once the client file index entries have been removed, users can no longer browse the save set to recover individual files. The entry for the save set remains in the media database, and the save set data is retained on the storage medium available for recovery at least until the retention policy for that save set is exceeded. When the retention policy of the save set and all save sets that depend on it are exceeded, the save set status in the media database is changed to recyclable. However, the save set is retained on the storage volume until all save sets on that volume have been marked as recyclable. When this occurs, the mode on the

Figure 29. Staggering full backups to decrease load.
storage volume itself is changed to recyclable and the volume is available for re-use. The data is not actually deleted until the volume is re-used, and so data may continue to be available for recovery long after the retention policy has been exceeded. Only when the volume is actually re-used are the save set entries removed from the media database.

![Figure 30. Three week retention policy. The save sets backed up during the first week are not marked recyclable until the end of week 4, after all dependencies from week 1 have expired.](image)

### 6.2.5 Directives

Directives are special programs NetWorker applies to client save set data to initiate additional data processing. A directive tells NetWorker to run an Application Specific Module (ASM), a program containing instructions to assist the backup process, maximize the efficiency of a backup, or handle special files. Directives can be written to accommodate almost any data processing situation, greatly increasing the flexibility of NetWorker to accommodate special situations.

Directives can be used to reduce the amount of data backed up by skipping files or compressing data, possibly eliminating the need to change volumes on the days full backups are performed. NetWorker directives specify instructions to NetWorker backup programs such as `save` or `nsarchive`. These instructions may be applied at either a directory or file level, depending on the context. During restore operations, the actions of NetWorker directives are reversed, restoring the data to its original state.

NetWorker comes with a number of predefined directives to perform the following functions:

- Always include a file for backup regardless of schedule
- Skip certain files or types of files
- Perform client-side compression
- Password protect or password protect and encrypt files during backup (NetWare and Windows only)

NetWorker also includes a set of standard directives that are used for clients of a specific type. For instance, the Unix directive instructs NetWorker to skip core files, backs up mail files without causing the
messages to appear as read, and performs other platform specific operations for Unix clients. These standard directives can be modified as necessary.

Directives can be integrated into a backup operation in three ways:

1. A directive can be specified as an attribute in the client configuration resource.
2. Directives can be specified in files that reside on the client and that are encountered by `save` as it walks the file system during a backup operation. (Directive files are identified by their filename, .nsr.)
3. Directives can be specified at the command line when `save` is invoked.

6.2.6 Storage Node Configuration and Management

As mentioned previously, storage nodes are independent computer systems that host storage devices—standalone devices, autochangers, or silos—for use by NetWorker. The NetWorker server may direct a client to save its data to a storage node. However, a client still sends its metadata directly to the server so the client file index and media database can be updated. Storage nodes can greatly increase the parallelism in a NetWorker environment, and help to compartmentalize data.

Storage nodes are configured by first installing the storage node software and then configuring the devices attached to the storage node. Once the devices are configured, the NetWorker server can perform normal storage tasks such as mounting and labeling volumes on the storage node devices the same as for locally attached devices.

Once a storage node has been configured, the NetWorker client configurations must be updated to take advantage of it. The client resource contains an attribute for **Storage Node Affinity**. For each client, an administrator defines a list of one or more storage nodes (or the NetWorker server itself). When a scheduled client backup occurs, the list is scanned top to bottom until a storage node is found that has an available device and a volume belonging to a suitable volume pool. If a suitable volume is already in use on a storage node on the list, the client data may also be multiplexed to that volume.

6.3 Security and Licensing

NetWorker uses its security and licensing mechanisms to ensure that data is protected from unauthorized access. NetWorker security can be configured with very tight limits where the utmost security is required or looser limits where greater flexibility is needed.

Security within NetWorker is based on:

- Limiting Administrative access to NetWorker Software
- Authenticating user access and limiting privileges
- Enforcement of licensing mechanisms to ensure only authorized clients have data access
- Password protection and encryption of sensitive data (NetWare and Windows only)
- Firewall support

Most NetWorker operations—particularly those involving configuration changes and media management—can only be performed by someone with Administrator privileges. This level of access can be tightly restricted for the highest security, or relaxed for greater ease of use.

User privileges and access to NetWorker data are closely controlled. All communications between client and server are authenticated using NetWorker authorization tokens. For example, consider the negotiation between a client `save` program and `nsrd`. When `save` begins negotiation with `nsrd` it passes the required authorization information about the backup (through the LGTO_AUTH call), including:
• Client machine licensing identification
• The client resource name
• The save set name(s)
• The backup level
• The group parameter(s) specified for this save, if any

In response, **nsrd** performs the necessary look-ups in the configuration resource database to:

• Verify that the initiator of the save request has the required execution permissions
• Provide the authorization tokens needed to establish necessary communications
• Select a volume pool and perform other tasks related to the backup

Verifying client licensing at the time of client authorization not only enforces proper licensing of the NetWorker product, it also provides another layer of security by making it nearly impossible for an unauthorized client to spoof the NetWorker server. By default, NetWorker clients can only view and recover their own data. This restriction can be relaxed if desired by granting access to specific additional users.

On Windows and NetWare clients, the most sensitive files, or entire save sets, can be password protected or password protected and encrypted using NetWorker directives. Data that is encrypted cannot be recovered without the password, even by the NetWorker Administrator. (See the previous section entitled *Directives* for more information.) Although this feature is not available for Unix clients, such clients can easily encrypt and decrypt important files using built-in utilities prior to backup if necessary.

Firewalls have become an integral part of the security systems of most companies. As the importance of the Internet has increased, many companies have found they are deploying more and more resources outside the firewall to host websites and provide other services. These systems still require regular backups. NetWorker firewall support enables backups to clients and storage nodes on the other side of a packet filtering firewall from the NetWorker server. A packet filtering firewall looks at each packet entering or leaving the network and accepts or rejects it based on defined rules.

NetWorker defines a range of *service ports* on the server or storage node on which it listens for client requests. *Connection ports* are used to connect to the server during backup and recovery processes. The allowable range of port numbers for each can be restricted to increase security further. The firewall must be configured to allow inbound and outbound TCP/UDP traffic for the defined ports.

NetWorker uses licensing to ensure only authorized use of NetWorker software takes place. The licensing mechanism also provides some additional security from unauthorized access to NetWorker data as mentioned above. NetWorker software licensing operates in one of three modes:

• *Evaluation mode* which provides a free, 30-day trial
• *Enabled mode* which initiates a 45-day extension to the evaluation mode upon entry of an enabler code
• *Authorized Mode* that provides fully licensed and unrestricted use of NetWorker software after input of a Legato Authorization Code.

Proper licensing for all NetWorker software components is verified each time the software is activated. NetWorker licensing can be managed locally at each NetWorker server, or it can be managed centrally using the Legato License Manager, which provides a central control point (on a single computer) for managing the licenses of all NetWorker clients and servers. Installation of the License Manager is an option when installing the NetWorker software. The License Manager is required on only one NetWorker server.

7 Conclusion
Legato NetWorker is the preferred solution for addressing the data protection needs of large and small heterogeneous enterprise environments. It delivers superior results in manageability, performance, and scalability. It provides fast, reliable and complete data backup and recovery for all systems, databases and Enterprise servers running critical applications.

Legato NetWorker delivers the functions most needed by heterogeneous operations, such as serverless backup, library sharing and drive sharing for LANs or SANs. NetWorker includes an advanced indexing architecture that dramatically increases performance and scalability in backup and recovery operations. NetWorker features support for NDMP, fast reliable disaster recovery management, and end-to-end tape media management. NetWorker supports a broad list of platforms including NetWare, Linux, Unix and Windows and an extensive list of media devices – tape drives and libraries. It provides robust cluster support for Legato Automated Availability Manager, Sun Clusters, Hewlett Packard MCSG, Compaq TruCluster, IBM HACMP and Microsoft Cluster Services. It is simply the best solution for guaranteed data protection. Legato NetWorker is the cornerstone of reliable storage management.