VERITAS NetBackup™
Release 3.4
Technical Overview
# Table of Contents

**Product Overview**  .......................................................... 3  
Key Features of VERITAS NetBackup  ....................................... 3  
NetBackup Launch Screen  .................................................... 4  
NetBackup Servers and Clients  ............................................. 5  
NetBackup Centralized Management  ....................................... 5  
VERITAS NetBackup Global Data Manager  ............................. 6  

**Continuous Data Availability Features**  ............................. 8  
Online Backups of Relational Database Management Systems (RDBMS)  ................................................................. 8  
Online Oracle Database Incremental Backups  .......................... 9  
Automatic RMAN Script Generation  ....................................... 10  
Online SAP R/3 Backups  ..................................................... 10  
Lotus Notes Backups  ......................................................... 11  
Online File System Backups  ............................................... 11  
FlashBackup  ........................................................................ 11  
NDMP Backups of Network-Attached Storage (NAS)  .................... 13  
Supported NDMP Configurations  .......................................... 14  
NDMP P-to-NDMP ("NDMP client") Backups  ............................ 14  
EMC Symmetrix Split Mirror Backups  ................................... 15  
Andrew File System (AFS) Backups  ...................................... 15  

**VERITAS NetBackup Backup Concepts**  ............................... 16  
Storage Units  ........................................................................ 16  
VERITAS NetBackup Classes  ............................................... 16  
Scheduling  ........................................................................... 18  
Database Backup Methods  ................................................... 19  
The Basic Backup Process  ..................................................... 20  
Multiplexing Backups  ......................................................... 21  
Automatic Multi-Streaming Clients  ...................................... 22  
Checkpoint/Restart of Backup Sessions  .................................. 23  
Compressing Backup Data  .................................................... 23  
Backing Up Network (CIFS/NFS) Files  .................................... 23  

**Restore Concepts**  ........................................................... 24  
Multiplexing Restores  ......................................................... 24  
Restoring to Alternative Clients  .......................................... 25  
Server-Independent Restores  .............................................. 25  
Restores in Multi-Server Environments  .................................. 25  
Server-Independent Restores in Disaster Recovery Scenarios ....... 26  
True Image Recovery  ........................................................... 27  
Backup/Restore of Moved Directories and Files ....................... 28
NetBackup for Windows NT and Windows 2000 ................................................................................................................. 29
Remote Administration ........................................................................................................................................................................ 29
Microsoft SQL Server Online Database Backup ....................................................................................................................... 29
Microsoft Exchange Hot Backup ................................................................................................................................................... 29
Virus Scanning ......................................................................................................................................................................................... 30
Open File Management ......................................................................................................................................................................... 30
Intelligent Disaster Recovery (IDR) ..................................................................................................................................................... 30

Security .......................................................................................................................................................................................... 31
Authentication ........................................................................................................................................................................................... 31
Authorization ................................................................................................................................................................................................... 31
Encryption .................................................................................................................................................................................................. 32

Device and Media Management ..................................................................................................................................................... 33
Basic Volume Management Process .................................................................................................................................................. 33
Shared Storage Option (Drive Sharing) ................................................................................................................................................ 34
Sharing Tape Libraries ................................................................................................................................................................................. 35
Managing Robot Inventory ........................................................................................................................................................................ 35
Scratch Pools ............................................................................................................................................................................................ 36
Spanning Volumes for Large Images .................................................................................................................................................. 37
Tracking Media Age and Number of Mounts ...................................................................................................................................... 37
Media Overwrite Protection ...................................................................................................................................................................... 37
Verifying Media .................................................................................................................................................................................................. 38
Duplicating NetBackup Media ................................................................................................................................................................. 38
  Duplicating NDMP images .................................................................................................................................................................... 38
Importing Media ................................................................................................................................................................................................ 38

Administration and Use ................................................................................................................................................................. 39
Administrator Interfaces ............................................................................................................................................................................... 39
User Interfaces .................................................................................................................................................................................................. 41
Installation .................................................................................................................................................................................................. 42
Configuration .................................................................................................................................................................................................. 43
Activity Monitoring ................................................................................................................................................................................................ 44
Reports and Logs .................................................................................................................................................................................................. 44
  Operational Reports .................................................................................................................................................................................. 44
  Progress Logs .................................................................................................................................................................................................. 45
  Detailed Activity Logs ............................................................................................................................................................................... 45
  Advanced Reporting ................................................................................................................................................................................................ 45
Error Reporting .................................................................................................................................................................................................. 45
Crash Recovery .................................................................................................................................................................................................. 45
Internal Databases .................................................................................................................................................................................................. 46
Supported Hardware and Software .......................................................................................................................................................... 46

Summary ............................................................................................................................................................................................................. 47

Appendix A: Answers to Common Questions ........................................................................................................................................... 48
Appendix B: Glossary .................................................................................................................................................................................................. 51
Appendix C: Client Backup Coverage Utility ........................................................................................................................................... 53
**Product Overview**

The VERITAS NetBackup™ product family provides a complete set of solutions for protecting data from the desktop to the data center and consists of three distinct yet complementary products: NetBackup™ DataCenter, NetBackup BusinessServer™ and NetBackup™ Professional. NetBackup DataCenter is the classic NetBackup product designed for enterprise environments and high-end applications. NetBackup BusinessServer is a scaled-down version of NetBackup DataCenter optimized for smaller workgroup environments or remote sites. Finally, NetBackup Professional is designed to provide a scalable and practical solution of centrally managing the backup of desktops and laptops within a corporate environment. NetBackup DataCenter and NetBackup BusinessServer are based on the same core architecture and code base, and this document describes these concepts in detail. NetBackup Professional, while an important part of the NetBackup story, is based on a different architecture optimized for desktop backup and recovery and will not be discussed here. Information on the details of NetBackup Professional can be found in other available documentation.

VERITAS NetBackup DataCenter is the industry's leading enterprise data protection solution that provides centralized control from a single management interface. The multi-tier architecture of VERITAS NetBackup DataCenter provides customers with a fast, reliable, data center strength backup and recovery solution that can protect environments that span terabytes to petabytes in size. The NetBackup DataCenter “master” server uses other NetBackup DataCenter “media” servers as workhorses to accomplish backup and recovery tasks in a highly centralized fashion. In contrast, NetBackup BusinessServer, designed for smaller environments, does not need the scalability of this three-tier architecture and instead functions as a standalone master/media server. Despite this key difference, most of the underlying architecture and capabilities of the two products are the same. For simplicity, this document generally will not distinguish between DataCenter and BusinessServer products and will instead simply refer to “NetBackup.”

**Key Features of NetBackup**

Key features in VERITAS NetBackup include the industry's most advanced media management, disaster recovery support, and intuitive Java and Windows NT/Windows 2000 administrative interfaces. In addition to protecting data in a mixed UNIX, Windows NT/Windows 2000 and Novell NetWare environment, VERITAS NetBackup provides advanced, “application aware” solutions for all leading applications including Oracle, Informix, Sybase, DB2, SAP R/3, NCR Teradata, Microsoft SQL Server, Microsoft Exchange and Lotus Notes. VERITAS NetBackup provides high performance backup, archiving, and recovery services for UNIX, Windows NT/Windows 2000, and PC client systems in client/server networks. It can be economically scaled to serve any size operation ranging from a standalone system to an entire enterprise.

Storage devices can be disk, tape, or optical. The Media Manager component of VERITAS NetBackup manages the tape and optical storage and is designed so that secondary storage devices can also be shared by other VERITAS storage products, such as VERITAS Storage Migrator. NetBackup provides extensive and automated support for most tape libraries, which means human intervention is rarely required.

Administrators can set up periodic schedules for automatic, unattended backup operations for clients across the network. These backup operations may be full or incremental. A full backup processes all files, while an incremental backup only processes those files changed since the last full or incremental backup. By carefully scheduling automatic backups, an administrator can achieve systematic and complete backups over a period of time, and optimize network traffic during off-peak hours.

In addition to scheduled backups, administrators can perform manual backups of client data using the same criteria as specified for automatic backups. Manual backup operations are useful in special circumstances, such as backing up a client that missed a previously scheduled backup or preserving a system configuration prior to installing new software.

Client users, too, are able to initiate backup, archive, and restore operations for data on their client systems – without operator or administrator intervention. User-directed backups allow users to protect their files immediately on demand. If files are damaged or accidentally deleted, users can quickly and easily recover any backed up or archived files by restoring them back to their primary disk space.
The NetBackup Master Server maintains a database (called the catalog) which records information about all backup and restore operations. A separate backup procedure is provided to protect the NetBackup catalog to facilitate recovery in case of a disk failure.

VERITAS NetBackup is also closely integrated with VERITAS Storage Migrator™ for sites that need hierarchical storage management. See the VERITAS Storage Migrator Technical Overview for more information.

**NetBackup Launch Screen**

The NetBackup launch screen provides an easy, intuitive entry point into the administrative categories of NetBackup. The seven buttons in the launch screen correspond to backup policy management, storage unit management, volume/media administration, job/activity monitoring, device monitor, reports, and user backups and restores. The launch screen is available on both the Windows and UNIX versions of the product. The Java version is shown in Figure 1 below.

![Figure 1: NetBackup launch screen.](image)
NetBackup Servers and Clients

VERITAS NetBackup includes both client and server software. Server software resides only on the platforms that manage the physical devices used for secondary storage. Client software resides on the individual client workstations containing the data to be backed up (a server can also be a client). In this architecture, client software is responsible for generating the data stream to be backed up and server software directs this data stream to a secondary storage device.

NetBackup Centralized Management

VERITAS NetBackup DataCenter accommodates multiple servers working together in a backup storage domain, under the administrative control of one of the servers in the storage domain. In this relationship, the NetBackup administrative control server is designated to be the “master” server, and the other servers in the storage domain, designated as “media” servers, operate under control of the master server. All NetBackup administrative functions are performed from one location on the master server, and the master server controls all backup scheduling for each media server. Each of the media servers perform the actual backup operations under direction from the master, and backup data stays local to the media servers and their directly attached devices. A master server and its associated media servers are referred to collectively as a NetBackup storage domain, and large networks may have more than one storage domain.

Figure 2: A master server/media server storage domain.

Figure 2 diagrams a simple master/media server configuration. The master in each storage domain serves a single point of administration for all backup operations in the storage domain. Administrators configure backup policies, manage all media and media pools, and configure all local and remote devices in the storage domain from the master without having to log on to or directly access any of the media servers. In addition to retaining backup schedules and other configuration information, the master server contains the backup catalog for the entire storage domain. Users can browse this catalog to locate and restore files.
As also shown in Figure 2, devices configured on the media servers in the storage domain become additional network storage units for backup and restore operations. When clients have large amounts of data, making them media servers is also an effective way of reducing their backup time and lowering network traffic.

The actual location of the backup images in a NetBackup storage domain is totally transparent to NetBackup administrators and users. The Media Manager component of VERITAS NetBackup resides on each NetBackup server and manages secondary storage media and the peripheral devices on those servers.

NetBackup storage domains provide many advanced high availability features that ensure continuous operations in NetBackup environments. For example, if a storage unit (robotics or tape device) on any of the NetBackup servers in the storage domain goes down, the NetBackup master can automatically route the backups to another storage unit in the storage domain. If a media server crashes, another media server can take over the backup operations. If scratch media in the primary storage unit is unavailable, NetBackup can route the backup to another local storage unit or a storage unit connected to another NetBackup server in the storage domain. VERITAS also recommends VERITAS Cluster Server™, a high availability software product, to protect the NetBackup master in case of hardware or system failure. All of these features ensure that all data in a NetBackup storage domain is protected and quickly recoverable in the event of a failure.

**VERITAS NetBackup Global Data Manager™**

In environments where multiple local or remote NetBackup storage domains are implemented, VERITAS NetBackup Global Data Manager™ (GDM) may be used to greatly simplify backup administration tasks. Global Data Manager is an optional software layer that provides centralized management for multiple NetBackup storage domains across a corporate campus or around the world.

![Global Data Manager Architecture](image-url)
Figure 3 diagrams a typical Global Data Manager configuration. As with standard NetBackup, all policy management, media management, and device administration can be performed from one location, the NetBackup Global Data Manager console. Global Data Manager need not be available during backup operations, and the network connection between the GDM and the master servers need not be persistent. Since only administrative updates pass over the network between the storage domain master server and the GDM console system, even wide area networks can easily supply the bandwidth required. Therefore, Global Data Manager is especially appropriate for remote operations such as point-of-sale or branch office environments where centralized control and local data backups are a critical requirement.

The NetBackup catalog information is stored locally on each of the master servers, but catalog browsing and restore operations can be performed from the GDM console or each individual master server.

VERITAS NetBackup Global Data Manager™ may be used to easily integrate the management of all VERITAS backup solutions including VERITAS NetBackup™ DataCenter, VERITAS NetBackup BusinessServer™ and VERITAS Backup Exec™. In this way, Global Data Manager provides an unprecedented degree of centralization and control.

Global Data Manager has been implemented by many of the global leaders in their respective industries. In a thorough departure from conventional backup and recovery solutions, it makes centralized management and monitoring of all NetBackup and Backup Exec storage domains in the enterprise possible.

- **Easy to install and use** — Global Data Manager can be installed quickly without any special training. Since it has the same interface as NetBackup, there is no learning curve. GDM allows organizations to manage every storage domain in the enterprise with consolidated monitoring, reporting and policy management.

- **Scalable and cost reducing centralized management** — Global Data Manager delivers the virtually inexhaustible scalability that expanding organizations need to accommodate their growth in data and storage requirements. Management of more data per administrator optimizes the business investment and reduces the cost of systems ownership.

- **Cross-platform administration** — Global Data Manager provides the flexibility that allows backup administrators to manage data from anywhere. The Java-based console can reside on UNIX or Windows platforms, managing NetBackup DataCenter, NetBackup BusinessServer and Backup Exec systems running within UNIX, Windows or NetWare environments.

Global Data Manager was designed to help worldwide enterprises operate at all times with full integrity and availability of their mission critical data.
Continuous Data Availability Features

Timely access to critical data is often the difference between the success or failure of a business. Data must be available to users when they need it. In today's global economy, critical files and databases must often be available 24 hours per day. If access to a critical system is interrupted for any reason, alternative systems must be able to take over the load automatically and transparently. Disaster recovery capabilities must be available so that if the worst happens and a site is completely disabled, critical data can be restored and available online in a few minutes or, at most, a few hours.

VERITAS NetBackup can be an effective way to provide cost effective disaster recovery protection for mission critical data. NetBackup delivers online high performance backups of database, file system, and application-specific data, with minimal impact on users or applications. In addition to fast backups, NetBackup also provides many methods to recover data quickly. VERITAS NetBackup is an industry leader in providing continuous data availability for all types of mission critical data during backup operations.

Online Backups of Relational Database Management Systems (RDBMS)

VERITAS NetBackup supports high performance, online database and application-specific backups across multiple vendors in addition to providing sophisticated support for older versions of databases (please see the “Database Backup Methods” section below).

NetBackup offers completely online, highly reliable backup solutions for all major databases, including Oracle (RMAN, RMAN Proxy Copy, and EBU), Sybase, Informix, DB2, SAP R/3, Microsoft SQL Server, Microsoft Exchange, and Lotus Notes. With these database solutions, online backups for other major applications such as PeopleSoft, Baan, and SAS are enabled. No matter what the application or environment, NetBackup ensures continuous data availability and complete data protection.

Database backup performance is critical to data availability, even in online database backup configurations. The NetBackup architecture enables multiple parallel data streams to be pushed to a NetBackup server on the local machine or across the network (see Figure 4). On systems where backup media transfer rates far exceed disk or network transfer rates, data streams from multiple disks and clients can be combined into a single stream to drive the offline media at its peak rates - this facility is called multiplexing. Performance scales in a nearly linear manner as additional peripheral devices and backup servers are added incrementally.
NetBackup also minimizes downtime by providing very fast recovery of databases, whole disks, or even entire sites in the event of a disaster. NetBackup maximizes restore performance by recovering multiple data streams in parallel from a multiplexed tape or across multiple tape drives, especially when used with fast tape technologies such as STK 9840, Magstar, DLT, Mammoth, etc. On systems with a locally attached tape device, NetBackup optimizes throughput by utilizing shared memory and other high performance data transfer techniques. Whatever the environment, NetBackup has the flexibility to provide continuous availability of databases or application-specific data with only minimal impact on user response times.

**NetBackup for Oracle Advanced BLI Agent**

Online Oracle database block level incremental (BLI) backups back up only changed file system blocks, virtually eliminating the backup window and significantly reducing the volume of data to be backed up and, more importantly, restored. This allows more frequent backups and continuous data availability while providing dramatically improved backup performance and significantly reducing CPU and network overhead during backups. The functionality brings compelling benefits to large database environments because backups - both in data volume and time - now are only proportional to the amount of changed data, not sheer database size.

Incremental database backups are supported for both Oracle 7 and Oracle 8 databases, including Oracle 8i Proxy Copy integration, whereby NetBackup is given the file names to be backed up rather than the database data itself. NetBackup utilizes functionality within the VERITAS File System that identifies the blocks of data that have changed. Database incremental backups leverage an underlying VERITAS File System technology called Storage Checkpoint. Storage Checkpoint identifies and maintains a list of changed file system blocks as data changes. (i.e., no pre-processing is needed to find changed data blocks as is the case with Oracle 8 RMAN). Through a VERITAS File System API, NetBackup extracts only changed data blocks and can take either differential or cumulative block level incremental backups.
Although the Storage Checkpoint and block level incremental backup technology is not Oracle-specific, VERITAS is first focusing on Oracle environments in strategic cooperation with Oracle. Block level incremental backup support for other major databases and application-specific data environments is planned for future releases of NetBackup.

**Automatic RMAN Script Generation**

Creating RMAN scripts to perform Oracle backup tasks can be a tedious process vulnerable to human error, requiring a certain level of technical sophistication to be done properly. NetBackup has virtually eliminated this process by providing a graphical interface that takes users through the process of configuring Oracle backups. This graphical RMAN script generator allows administrators who are unfamiliar with RMAN to quickly set up Oracle backups in a fraction of the time without having to know the scripting language or debug a script. This capability is currently available for Windows NT/2000 environments and is planned for other platforms in future releases.

**Online SAP R/3 Backups**

With large-scale SAP R/3 environments requiring 24x7 operations, data protection becomes an essential component of any successful SAP R/3 deployment plan. The integration of VERITAS NetBackup and online SAP data backup utilities provides a comprehensive approach to SAP R/3 data protection. Certified by SAP on HP, Solaris, IBM AIX, Compaq Tru64, and Windows NT/2000, the VERITAS NetBackup for SAP R/3 agent provides high performance, online backup of SAP R/3 environments, optimal utilization of large scale device and robotic configurations, and a scalable, distributed design.

Figure 6 diagrams a SAP R/3 backup configuration. SAP R/3 backups can be scheduled and automatically initiated via the NetBackup scheduler or via the SAPDBA interface. NetBackup supports the SAP R/3 BACKINT interface specification for backup, restore and inquire functions from the respective SAP R/3 tools (brbackup, brrestore, and brarchive). BACKINT then starts the required NetBackup programs, monitors the progress of each program, and reports the results back to the SAP R/3 tool upon completion. NetBackup supports SAP R/3 Oracle database backups as either raw partitions or regular files.
Lotus Notes Backups

NetBackup supports online backup of Lotus Notes 4 (Windows NT/2000) and Lotus Notes 5 environments. Lotus Notes 4 environments on Windows NT/2000 can be backed up using standard NetBackup with the Open Transaction Manager. Lotus Notes 5 environments can be backed up online or "Hot" using the NetBackup for Lotus Notes 5 agent which takes advantage of the new Lotus Notes 5 backup API. NetBackup for Lotus Notes 5 provides the following types of backups for Lotus 5 configurations:

- **Full backup** - Online full backups of the common database as well as each users private database area
- **Incremental backup** - Incremental backups of each database (private or full) that has changed since the last full backup
- **User backup** - Backs up a specified user's database as well as the common database.

NetBackup for Lotus Notes provides reliable, consistent online backups of Notes 5 databases.

Online File System Backups

FlashBackup

While your critical enterprise server is up and running and performing its primary function, NetBackup's FlashBackup option can make a lightning-fast backup in a fraction of the time required by conventional backup methods, while still providing data integrity and individual file restorability.
FlashBackup uses snapshot technology to provide high performance, online “file image” backups of mounted file systems while still allowing restores of individual files and directories. FlashBackup significantly enhances backup performance for file servers, web servers, and internet mail servers that have file systems that contain a large number of small files. High performance backups are accomplished with minimal overhead on the host system being backed up. FlashBackup delivers the performance of raw file system backup without losing the flexibility of restores at the individual file and/or directory level.

Both full and incremental FlashBackup backups are supported and are performed with a single sweep of the source disk, eliminating unnecessary head movement. All restores are performed with a single pass of the media, which optimizes restore times.

Figure 7 illustrates the FlashBackup backup process. FlashBackup delivers the high performance of a raw partition backup (i.e. it bypasses the buffered I/O of the file system) and dramatically reduces CPU utilization during the backup process. A disk “snapshot” capability provides a consistent view of the live disk during backup. This provides a point-in-time backup of the disk, even though users may continue to change the contents of the disk during the backup operation.

FlashBackup can dramatically enhance backup performance – especially in environments with large numbers of small files. Backup performance improvements of 6x -10x are commonplace in NFS file server, web server, and pop mail server environments. For example, Figure 8 graphs backup times for a customer with a large number of files on their file system that reduced their backup window from 72 hours using a standard backup to 11 hours using the FlashBackup option.

---

1 Supported file systems include Solaris running UFS or the VERITAS File System, HP-UX running Online JFS or the VERITAS File System**, and Auspex. Support for other platforms is planned for future releases.

2 When FlashBackup is used with VERITAS File System, the online snapshot capability of VERITAS File System is used. When FlashBackup is used with Solaris UFS or HP-UX Online JFS, FlashBackup provides the online snapshot capability.
NDMP Backups of Network Attached Storage (NAS)

VERITAS NetBackup provides online data backup and restore to a locally attached storage device for network-attached storage (NAS) hosts using the Network Data Management Protocol (NDMP). Currently supported NAS hosts include Network Appliance (NetApp), EMC Celerra, and the Auspex NS2000. In a NetBackup NDMP configuration, only control and catalog information is transferred over the network. This is a critical requirement in NAS host environments where file servers can store a terabyte or more of online data, which makes network-based backups infeasible or even impossible.

In a typical NetBackup/NDMP configuration, a NetBackup server sends backup, recovery and robotic control commands via the NDMP protocol to the NAS file server, which contains locally attached disks, tape drives, and optionally, robotics units. The NetBackup catalog maintains a complete listing of the backup image. The NAS NDMP host performs the actual NDMP backup/restore utility that runs on the NAS file server and carries out the NDMP commands from NetBackup. Large robotics devices can be shared between NAS file servers or between NetBackup master/media servers and NAS file servers.
Supported NDMP Configurations

The following sections describe specific supported NDMP configurations and capabilities, providing unparalleled flexibility in defining and implementing a NAS backup strategy.

NDMP-to-NDMP (“NDMP client”) Backups

NetBackup supports backups between NDMP hosts. Sometimes it is not cost effective to directly attach a tape drive or library to each NDMP host, especially in environments where there are many smaller NAS servers. In these situations, an “NDMP host” (Netapp, etc) backs up directly to another NDMP host with a locally attached tape device (see Figure 10).

Figure 9: NetBackup backups of NAS servers via NDMP.

Figure 10: NDMP-to-NDMP backups.
Library sharing between NetBackup and NDMP Hosts

NetBackup can share a tape library between the NetBackup server and one or more NDMP NAS servers, or just between the NDMP NAS servers themselves. For more information, see the "Media Manager Library Sharing" section.

EMC Symmetrix Split Mirror Backups

VERITAS NetBackup directly backs up EMC Symmetrix disk arrays using the EMC Timefinder API to provide data synchronization and 3rd-mirror break-off. The NetBackup server attaches directly to the EMC Symmetrix array (SCSI or fibre connection), detaches the 3rd mirror and backs it up offline while the host application continues to run unaffected. NetBackup utilizes the EMC Timefinder API to manage the break-off of the mirror before the backup starts and re-attach or synchronize the 3rd mirror once the backup is complete. Initially, only Oracle database backups on raw partitions are supported. Other application support on EMC arrays is planned for future releases. To customize backup support for other applications in the interim, please contact VERITAS Enterprise Consulting Services.

![Figure 11: NetBackup split mirror backup for EMC Symmetrix arrays.](image)

See the Split Mirror Backup section in the VERITAS NetBackup for EMC Administrator’s Guide for more details.

Andrew File System (AFS) Backups

Andrew File System (AFS) volume level backup and restore is supported in NetBackup. NetBackup utilizes the AFS "VOSdump" and "VOSrestore" utilities to implement the backup and restore operations. Both full and incremental AFS backup operations are supported.

AFS is supported on the Solaris and HP-UX clients. Other platforms may be added in future releases. File-level AFS backups are not currently supported.
VERITAS NetBackup Backup Concepts

The following sections explain the basic concepts involved in backup operations.

Storage Units

VERITAS NetBackup associates all storage devices and media with logical storage units. As used by NetBackup, the term storage unit refers to a logical entity that includes one or more physical storage devices that are of a specific type and media density and attach to a specific host. There are three categories of storage units:

- Directly attached standalone or robotic media storage units that contain tape or optical devices and are managed by the VERITAS NetBackup Media Manager.
- Remote standalone or robotic storage units controlled by the VERITAS NetBackup Media Manager via Network Data Management Protocol (NDMP).
- Disk file system storage units consisting of a designated directory in the file system that will receive the backup or archive data.

During configuration, the administrator first completes any necessary device and media configuration and then groups all devices and media into appropriate VERITAS NetBackup storage units. For example, on a specific host, a Hewlett-Packard optical disk library could be in one storage unit and a ATL tape library could be in another.

During backups and restores, VERITAS NetBackup specifies the media required and Media Manager automatically finds it and mounts it in a device within an available storage unit.

The storage unit concept makes it easier to configure backups because the administrator can simply assign the storage unit with the type of storage needed for a client backup, rather than worry about specific devices. It also provides a virtual approach to backup storage because if more storage of that type is needed, it will be automatically and transparently utilized after being added to the Media Manager and VERITAS NetBackup configurations (see the Media Manager Scratch Pool section below).

VERITAS NetBackup Classes

An important feature of VERITAS NetBackup is the capability to configure backup classes. A class consists of one or more clients that have similar backup needs. Every VERITAS NetBackup client must belong to at least one class and often belongs to more than one. Classes are sometimes referred to as policies.

The major advantage offered by VERITAS NetBackup classes is that the administrator can group clients into classes and then configure backups for the entire group, rather than one client at a time. In addition, since a client can belong to more than one class, the administrator can establish different schedules for different files on the same client or assign a client to one class for automatic backups and another for user-directed backups and archives.

When new clients are installed, they can be added to an existing class or the administrator can define new classes for new clients on a one-by-one basis. An easy way to create a new class is simply to clone and modify an existing one.
The properties that the administrator configures for each class include:

- **Client List** — lists the set of clients in the class. When a new client is added to VERITAS NetBackup, the administrator can simply add the client's host name to the appropriate class and the client software can optionally be installed automatically over the network.

- **File List** — lists the set of files to include in automatic backup operations for the class. It is not a requirement that all files on the list exist on all clients and it is often convenient to make the file list a superset of the desired files. The file list does not apply to user-directed backups because the user personally selects those files at the time of the backup. The administrator or user can also specify a list of files to exclude from each client backup. The exclude list is not part of the class definition and is unique for each client.

- **Schedules** — lists the set of schedules pertaining to the class (refer to the next section for a detailed description of schedules).

- **Storage Unit** — specifies the type of storage device to receive the file backups. This is optional. If unspecified, backups and archives can go to any available storage unit.

- **Volume Pool** — specifies the set of volumes (media) to use for storing the backups. If unspecified, backups and archives use the default NetBackup volume pool.

- **Class Attributes** — the following are class-specific attributes
  - **Maximum Jobs per Class** — specifies the number of client jobs from this class that can be performed concurrently. Administrators can use this parameter to "balance" network load.
  - **Collect True Image Recovery Information** — specifies whether NetBackup will collect the information necessary to support true image recovery of directories saved by clients in this class.
  - **Class Type** — specifies the type of class you are configuring. You will use the Standard class type for most UNIX clients. The other class types cover special cases. For example, you would specify Exchange backup type to backup Microsoft Exchange clients or Oracle-OEBU backup type to back up ORACLE databases on clients that have ORACLE.
  - **Encryption** — specifies whether or not to enable client-level encryption during backup operations. Both US Domestic (56 bit DES) or international (40 bit DES) encryption types are supported. Encryption is a separately priced NetBackup option.
  - **Image Compression** — specifies whether or not to use software image compression during backup operations.
  - **Backup Network Drives** — specifies whether to allow backups of remote files that are NFS mounted on the client.
  - **Cross Mount Points** — specifies whether or not VERITAS NetBackup is to cross file systems to back up directory paths and files.
  - **Priority** — specifies the priority of backups for this class relative to the other classes. This is useful to ensure that the most important data is backed up first.
  - **Active** — specifies whether or not NetBackup will allow backups or archives for this class. This is useful for temporarily deactivating a class during, for example, network troubleshooting or repair.

All class definitions are stored in the configuration database on the master server. In networks with more than one storage domain of VERITAS NetBackup servers, clients can belong to classes on more than one master server. Although clients will normally use only one master server, the ability to use others can be an essential feature if a client's regular master server goes down and there is critical data to back up.
Scheduling

Each VERITAS NetBackup class has a set of schedules to control its backups and archives. These schedules are part of the class definition and each schedule for a class affects the entire list of clients and files in that class.

A typical schedule might call for a weekly full backup followed by incremental backups every other day, as illustrated in Figure 12.

Among the attributes that the administrator specifies for each schedule are:

- **Type of Backup** — specifies the types of backups available to the type of class you are configuring. For example, most UNIX clients will be in a standard class and you can select from full or incremental backup, user-directed backup, or user-directed archive. The NetBackup incremental type backs up all files changed since the last backup (full or incremental). The cumulative incremental type backs all files changed since the last full. The full or incremental backups are started automatically by the NetBackup scheduler on the master server. User-directed backups and archives are started by the user on the client system or can be script-driven.

- **Start Time and Duration** — specifies the backup window, which is the time period during which backups can occur for this schedule. The start time defines the times and days of the week when the window opens. The duration defines how long the window stays open. For example, the administrator could schedule automatic full backups to occur during early morning hours on weekends, when the increase in network traffic will have the least effect on users.

- **Frequency** — specifies the period of time that will elapse until the next backup operation can begin on this schedule. If, for example, the frequency is seven days and a successful full backup occurs on Wednesday, the next full backup does not occur until the following Wednesday. The frequency can be set to a value that preserves all critical changes in the files. If data changes often, the frequency can be short. For more stable files, the frequency can be longer. Incremental backups will have a shorter frequency than full backups.
• **Retention Level** — indicates a specific time period for keeping backup or archive copies of files before deleting them from secondary storage. The default retention periods range from one week (Level 0) to infinite (Level 9); however, the retention periods may be set to any specific value by the NetBackup administrator. The retention level also denotes a schedule’s priority within the class, with Level 9 schedules having the highest priority and Level 0 the lowest.

• **Storage Unit** — specifies the storage device to receive the file backups. This option overrides the storage unit specified at the class level and provides the flexibility for putting backups from different schedules on different storage units. For example, it may be desirable to put full backups and incremental backups on different types of media.

• **Maximum MPX per Drive** — specifies the maximum number of simultaneous jobs that a client in the class can attempt to multiplex onto a single drive.

• **Volume Pool** — specifies the set of volumes (media) to use for storing the file backups. This option overrides the pool specified at the class level and allows the administrator to keep images from different schedules on separate sets of volumes.

The above attributes give the administrator great latitude. Schedules can range from very basic to schemes that are sophisticated enough to meet the most demanding backup requirements.

---

**Database Backup Methods**

VERITAS NetBackup supports three methods of backing up relational database management systems: raw (cold), warm, and online (hot). Cold database backup involves shutting down the database and using the raw partition of file system backup capability of NetBackup. Warm database backups use pre- and post-processing scripts of NetBackup to place the database in “online backup” mode, then proceed to back up the database raw partition or database file. Online database backups for Oracle, Microsoft SQL Server, IBM DB/2, Sybase, and Informix use the VERITAS NetBackup database backup agents. VERITAS NetBackup currently supports the Oracle Recovery Manager (RMAN), as well as the Oracle Enterprise Backup Utility (EBU), Microsoft SQL Server, Informix On-Bar, Sybase Backup Server, and IBM DB/2. Specifics of the database backup methods supported by NetBackup are outlined below.
• Raw database backups (database files or partitions) are configured and executed in the same manner as file backups. The performance resulting from backing up cold databases is generally greater than that achieved when backing up through the UNIX file system or through the data extraction utilities supplied by RDBMS vendors.

• Warm database backup is similar to raw database or file backup method described above, except that the database is placed in “hot backup” mode via the capability of NetBackup to preprocess scripts prior to the raw partition or database file backup. After the backup is completed, the database is returned to normal mode via a NetBackup post-processing script.

• Hot database backup requires a VERITAS NetBackup Database backup agent and a corresponding database vendor backup utility. NetBackup database backup agents exist for Oracle (Oracle EBU/RMAN), Microsoft SQL Server, Sybase, Informix, and IBM DB2 databases. An example is VERITAS NetBackup for Oracle. This product interfaces to Oracle RMAN and takes advantage of VERITAS NetBackup and Media Manager features. Administrators can use VERITAS NetBackup interfaces to schedule and execute Oracle database backups in much the same manner as they can standard disk files. The Media Manager manages the storage devices and media.

![Diagram of NetBackup online database backup.](image)

Because VERITAS NetBackup spans backup images across multiple tapes or disks, it can back up very large database files with any of the above methods.

**The Basic Backup Process**

When the classes and their associated schedules are configured, the clients in a class can be backed up in any of the following ways:

• Automatic scheduled backups start automatically at the times specified by the administrator during schedule configuration.

• Immediate manual backups of a selected class and schedule can be started at any time by the administrator by using the administrative GUI or the command line interface.

• User-directed backups and archives begin when a user on a client starts the operation through the user interface.
In all cases, the client generates the backup image as a data stream using TCP/IP sockets and sends it to either the VERITAS NetBackup master or media server. The receiving server directs the data stream to the appropriate attached storage device.

While the backup operation is progressing, the client directs another data stream to the master server which catalogs information about the files contained in the backup image and is stored in the NetBackup image catalog. The image catalog and other VERITAS NetBackup databases are backed up in a separate operation, explained under “Crash Recovery” section below.

The process VERITAS NetBackup uses to write images to secondary storage depends on whether the target storage unit is a disk file or a peripheral managed by Media Manager. In the latter case, Media Manager assists the backup operation by handling the volume and drive allocation and mounting as explained later under “Media Manager.” VERITAS NetBackup records the volume information in its file database for use during a subsequent restore.

When backing up to magnetic disk, VERITAS NetBackup writes images to the file path specified during configuration of that storage unit and records the path of the image in its file database. The disk manager handles the actual writing of data in the disk file.

**Multiplexing Backups**

NetBackup can run multiple backups simultaneously and stream the data to one or more devices. The backup streams can be from locally attached disks or from multiple clients over the network.

As jobs finish, NetBackup dynamically adds more to the device. Sites can tune the configuration to the level of multiplexing desired on each device and for each schedule.

Multiplexing can dramatically increase performance and allow implementation of a few fast devices, instead of many slow devices. This optimizes the usage of high-speed tape devices and improves overall performance and data availability.

In conjunction with multiplexed backups, NetBackup also restores multiplexed tape images in parallel. Please see the multiplexed restore section below for more details.
Automatic Multi-Streaming Clients

A single NetBackup backup class can automatically create multiple simultaneous client backup sessions and dramatically increase the performance of the backup. Parallel backup sessions are initiated based on client system mount points or individual entries (explicit or via wildcards) in the NetBackup class file list.

The automatic multi-streaming client feature can be administrator defined to dynamically “auto-discover” newly created folders and partitions on a client.
Checkpoint/Restart of Backup Sessions

NetBackup's multistreaming capability enables failed streams of a multistreamed backup to be restarted in the event of a backup failure. Once service is resumed, the backup will restart the failed stream rather than restarting the entire backup job. Checkpoints may be set at file system mount points or at file and/or directory paths as defined in the NetBackup class “file list” (see the “NetBackup Classes” section above). Additional checkpoint options will be supported in future releases.

From a restore perspective, each checkpoint creates a complete and standalone NetBackup image on tape that can be used for restore regardless of whether or not the rest of the backup session is completed.

Checkpoint/restart is not supported for restores at this time. In addition, checkpoint/restart is not supported for manual backups or user initiated backups.

Compressing Backup Data

VERITAS NetBackup is capable of compressing data as part of the backup operation. The compression and decompression takes place on the client and its effectiveness depends on the type of data being compressed. In the right circumstances, compression can significantly reduce both storage requirements and network traffic. In general, most customers find the hardware compression provided by tape devices a much simpler and efficient method of compression.

Backing Up Network (CIFS/NFS) Files

VERITAS NetBackup optionally backs up files that are resident on a PC network file server or NFS file server mounted on a VERITAS NetBackup client. This is useful for backing up remote files or an unsupported client platform that has files NFS mounted on some other VERITAS NetBackup client system (Figure 18).

Normally, it is undesirable for a client backup operation to include such files because the data transfer goes through the network protocol (IPX, TCP/IP, or NFS). It is better to back up the data on the platform where the files physically reside, making backup through NFS/CIFS unnecessary.

Figure 18: Using NFS mounts to back up unsupported clients.
**Restore Concepts**

Client users can, at any time, browse their backed up files and select the ones they want to restore. When a user initiates a restore, the request passes from the client to the master server. Once the server validates the request, the restore operation becomes fully managed by the server, which identifies the storage device and volume containing the backed up files by querying the backup catalog. The server then automatically transmits the files back to the client disk.

The process VERITAS NetBackup uses to retrieve images from secondary storage depends on whether the storage unit is a disk file or a peripheral managed by Media Manager. In the latter case, Media Manager assists the backup operation by handling the volume and drive allocation and mounting. When the media is mounted, the VERITAS NetBackup server reads the backed up data from the media and sends the requested portions of the image to the client.

When restoring files backed up to magnetic disk, VERITAS NetBackup finds the image path stored in its file database during the backup operation, and sends the requested portions of the image to the client. The disk manager handles the actual reading of backed up data from the disk file.

Figure 19 shows the data flow in restore operations.

![Figure 19: NetBackup restore data flow.](image)

**Multiplexing Restores**

VERITAS NetBackup supports the parallel multiplexed (simultaneous) restore of multiplexed backup images. To enable multiplexed restore, the tape must have been written with multiplexing enabled during the backup. Any subset of the number of “plexes” of the backup multiplexes may be restored in parallel. For example, if five backup sessions were multiplexed to the tape during the backup, any number of backup sessions up to the five could be restored in parallel with a single pass of the tape.
Multiplexed restores are especially useful in the case of databases. Often database backup performance can be optimized by multiplexing multiple sessions during the backup. However, many online database backup utilities require that if multiple backup sessions were run in parallel, they must be restored in parallel. Therefore, to enable multiplexed database backups, the backup product must support the multiplexed restore capability.

Any restore requests of a multiplexed backup image that are submitted inside an administrator-defined time window may be restored in parallel. For example, assume eight clients were multiplexed to a single tape during backup. If the restore of three of those clients was requested inside the administrator defined time window (default: 30 seconds), all three clients would be restored simultaneously.

**Restoring to Alternative Clients**

The administrator on the master server can direct restores for any client (administrator-directed restores) or give a user on one client permission to browse and restore files that were backed up from another client. This feature is convenient, for example, when a workstation is down and the user wants to restore backed up files to another workstation and continue working. The administrator on the master server can also direct files from the master server to any client.

**Server Independent Restores**

NetBackup supports restores using a NetBackup server other than the server used to write the backup. This provides easier access to data for restores in multi-server environments, and better failover and disaster recovery capabilities.

**Restores in Multi-Server Environments**

The server-independent restore feature of NetBackup greatly simplifies operations and improves timely access to data in NetBackup master/media server storage domain environments, where storage devices (drives or robotics) may be connected to any server in the storage domain or where a large library is shared between servers (see Figure 21). Server independent restore applies to the following multi-server situations:
Figure 21: Server-independent restores.

- Two or more servers are sharing a robot, each with connected drives. When a restore is requested, one of the servers is temporarily inaccessible. Under direction of the master server, any available server in the storage domain can be used to restore the file.

- Two (or more) servers have standalone drives of the same type. When a restore is requested, one of the servers is temporarily inaccessible. The operator can mount the tape in a drive connected to any available server and restore the file.

Server-Independent Restores in Disaster Recovery Scenarios

In situations where there is a remote disaster recovery site, the server-independent restore feature can dramatically reduce the time required to resume normal business operations in the event of a site failure.

Figure 22: Recovering data from a disaster site.
In disaster recovery strategies where a set of backup tapes are transferred to a remote site, the following simple series of steps enables quick data availability at the remote site:

1. Using a NetBackup-supplied utility on the primary server, create a copy of the NetBackup catalog and the media database associated with the backup tapes being transferred from the primary server. This tape and the backup data tapes should be transferred to an offsite location or a vault. This operation should be repeated periodically as part of the ongoing disaster recovery process.

2. In the event of a site disaster, move the tapes (primary or duplicate) from the vault (or library on the primary server) and transfer them to the remote site.

3. At the remote site, load the NetBackup catalog and media database from the tape created in step (1) above via a NetBackup-supplied utility and load the tapes into the library or tape drives at the remote site.

4. Restore the backup data to the desired client through the disaster recovery server.

**True Image Recovery**

True image recovery allows users to restore only their current files in the event that disaster recovery is required. This capability can be configured on a class-by-class basis so that NetBackup will track file deletion activity and optionally prevent the restore of deleted files if a directory or file system restore is requested. Without true image recovery, files that were included in previous backups but subsequently deleted may also be restored.

True image recovery provides installations with the option of tracking the environment as it existed at the last backup so that during recovery only current data is recovered. For example, if a server were to be recovered on a Tuesday, a combination of the last full backup tapes (Sunday) and Monday’s incremental would be used to recover the server. However, TIR would ensure that only the data that existed during the time of the Monday incremental backup was restored. This would keep any data that became obsolete (deleted) between the Sunday full and Monday incremental.

For example, in Figure 23, NetBackup restores 141 files, including the latest versions of 90 files that were modified. The 22 files that were deleted are ignored. Without true image recovery, NetBackup would restore 163 files.

![Figure 23: True image recovery.](image)
The true image scheme utilized by NetBackup avoids creating large backup catalogs typical of competitive true image backup offerings by keeping older true image catalogs on tape rather than all on disk.

**Backup/Restore of Moved Directories and Files**

Moved, renamed, or newly installed files and directories are detected and backed up during incremental backup operations by comparing the new file and directory names relative to those contained in the previous full or incremental backup. A catalog of the previous full or incremental backup is saved on the NetBackup client.

Some client disk space is required to store partial backup catalogs. This is an optional feature since additional system resources are required.
NetBackup is available for Windows NT and Windows 2000 as both a server and client. The NetBackup client software for
NT/2000 provides backup and disaster recovery services for mission critical NT/2000 systems, including NTFS and FAT file
system types, Microsoft SQL Server databases, and Microsoft Exchange application environments. Online file system backups
are supported through the use of Open Transaction Manager included with NetBackup DataCenter at no extra cost and
offered as an option to NetBackup BusinessServer. NetBackup also supports online full and partial (hive level) backup and
restore of the NT registry, as well as the ability to restore individual keys within the registry if needed. All of the unique
Windows 2000 attributes and data types are protected as well, including the System State, Active Directory, reparse points,
disk quota information and other Windows 2000 attributes.

The Windows NT/2000 NetBackup Server software is a re-implementation of NetBackup to the Windows NT/2000 platform
rather than simply a port from UNIX. The user and administrative GUIs have been completely redesigned to the Wins32
interface specification and the Microsoft Windows style guide. NetBackup also utilizes Microsoft standard services such as
the NT Event log and InstallShield installation.

Just as important, the NetBackup server on Windows delivers the same enterprise class capabilities and performance as the
UNIX version of NetBackup. For example, a Windows NT/2000 NetBackup master server can administer all the UNIX and
Windows NetBackup servers across a LAN or WAN from a single screen, greatly reducing administrative costs. Large robotics
devices can be shared between Windows and UNIX servers. Your NetBackup investment can grow as your Windows
environment grows by simply adding another remote NetBackup server and local robot and managing it from the centralized
management interface.

Remote Administration

NetBackup administrators can remotely administer UNIX or Windows NT/2000 NetBackup servers without having to
physically be located at the server's console. System administrators can manage any UNIX or Windows NT/2000 NetBackup
servers from any UNIX or Windows NT/2000 system using basic NetBackup server software. No third party remote access
software is required.

Microsoft SQL Server Online Database Backup

VERITAS NetBackup supports high speed, online backups of Microsoft SQL Server Release 6.5 and 7.x databases and all
associated log files, including SQL Server 2000. DBAs can quickly restore the complete SQL server database or individual files
and file groups to any point in time with the easy to use administration GUI.

Microsoft Exchange Hot Backup

VERITAS NetBackup utilizes the Microsoft Exchange APIs to perform online backups of the Microsoft Exchange Information
Store and Directory along with all associated transaction log files. NetBackup supports advanced Exchange roll-forward and
roll-back operations to enable Exchange databases to be restored to any point in time, a key requirement of many large-scale
Exchange environments.

VERITAS NetBackup for Exchange utilizes the Exchange Messaging API (MAPI) to enable “brick-level” backups of Exchange
mailboxes, allowing individual mailboxes, folders or e-mail messages to be easily recovered. Administrators no longer need to
rely on a spare server to restore individual messages from Exchange.
Virus Scanning

The Network Associates (McAfee) Viruscan technology is bundled in the NetBackup for Windows NT/2000 client. It scans for viruses during backups and restores or both (configurable). It is integrated via the Viruscan APIs. Virus scanning is an optional capability, and by default is enabled in NetBackup. McAfee virus software is now available for backup and restore for Windows NT/95/98/2000.

Options for virus scanning during backup include:

- **Perform virus scanning** — Files are scanned, but infected files are neither cleaned nor backed up.
- **Clean infected files** — Files are scanned, and infected files are cleaned and backed up. Infected files that could not be cleaned are not backed up.
- **Backup infected files** — Files are scanned, and infected files are cleaned and backed up. Infected files that could not be cleaned are also backed up.

Options for virus scanning during restore include:

- **Perform virus scanning** — Files are scanned, but infected files are neither cleaned nor restored.
- **Clean infected files** — Files are scanned, and infected files are cleaned and restored. Infected files that could not be cleaned are not restored.

Open File Management

Open file management functionality via the Open Transaction Manager (OTM) is bundled in the NetBackup for Windows NT/2000 and NetWare clients at no additional charge with DataCenter and as a chargeable option with BusinessServer. OTM presents a stable, coherent, point-in-time snapshot view of one or more volumes or physical drives for NetBackup to access during a backup. This is an optionally installed and configured feature.

Intelligent Disaster Recovery (IDR)

For Windows NT/2000 environments, the Intelligent Disaster Recovery (IDR) option provides a means to perform a “bare metal” restore of a crashed system without first restoring the Windows operating system. The process works via four floppy disks that NetBackup creates along with the Windows NT/2000 CD. They are used to rebuild the Windows system and initiate a remote (over the network) recovery of the entire server. The NetBackup client is contained on one of the prepared floppy disks or the prepared CD from which the whole system can be restored from the boot media and the backup image. It is a simple three-step process for administrators to restore a Windows NT/2000 system using IDR:

- Boot the NT/2000 system from the four NT/2000 boot disks (this will partition and format the drives, followed by a reboot).
- Use the NBU agent and network drivers contained on the fourth floppy to restore the rest of the system from an existing NetBackup server over the network.
- Reboot the system.

Boot of non-networked systems (i.e. locally attached drive support) is not currently supported. Bare metal restore from directly attached tape devices is planned for a future release.
Storage management applications have often been characterized as the biggest security loophole in a secure data environment. Once the data leaves the confines of the physical system environment by way of a backup or data migration, the data security policies and procedures often do not follow.

NetBackup addresses security concerns in the enterprise storage management environment by providing customers with a wide range of security options. These include authentication, authorization, data encryption, and auditing. Each can be tailored to meet a customer's specific needs. Data can be encrypted before it is sent across the network and/or before it is stored on tape.

**Authentication**

VERITAS NetBackup authenticates via a peer-to-peer protocol between NetBackup master servers, remote servers, and clients to validate that systems are who they say they are and protect against “spoofing.” The authentication will take place after a NetBackup connection has been established but before any NetBackup transactions have taken place.

For NetBackup, the standard authentication method is a one-time password (challenge/response) mechanism based on the U.S. Navy's OPIE protocol. The one-time password method was chosen for NetBackup authentication because it is secure, portable, and exportable.

**Authorization**

VERITAS NetBackup protects data from unauthorized access through the use of secure client hosts to restrict client-server communications, and administrator-imposed restrictions on restore operations.

Users do not have direct access to the volumes containing their backed up files and cannot choose their own media volumes. The VERITAS NetBackup server, not the user, chooses the secondary storage media. In addition, Media Manager only allows VERITAS NetBackup to have access to these volumes, and imposes access control to protect the backed up files from unauthorized viewing or use by other applications.

Under normal conditions, VERITAS NetBackup prohibits users from either viewing or restoring other people's files. By default, VERITAS NetBackup enforces normal file viewing and restoration restrictions in which client users may view or restore only those files that they personally backed up or archived from that client.

Administrators, however, have the flexibility to modify these restrictions to meet special site requirements. The administrator may relax file access restrictions by giving designated clients on a server access to backup or archive images created on any other designated clients. For minimum security, the administrator can disable all restrictions, permitting access by any client.
Encryption

NetBackup protects critical data from unauthorized access and tampering while in transit as well as when it is resident on backup media. NetBackup performs the data encryption on the client, transfers the data across the network and stores it on tape in the encrypted format. On restores, the data is read from media and transferred across the network to the client before decrypting. The encryption algorithm is fully exportable, available in both 56 bit DES for the United States and for export to most countries, and a restricted 40 bit DES version for countries with import restrictions, such as France.

Optional Data Encryption

- 56 bit U.S. encryption
- 40 bit non-U.S. encryption

Figure 24: NetBackup data encryption.
Device and Media Management

One of the most impressive features of VERITAS NetBackup is the Media Manager. This powerful software manages the wide array of tape and optical storage devices and media supported by VERITAS NetBackup. Media Manager is also easy to configure and administer, thanks to a graphical user interface that allows the administrator to centrally manage and control device and media information for all VERITAS NetBackup master and media servers on the network.

The Media Manager also allows users and other VERITAS storage management applications, such as VERITAS Storage Migrator, to share its secondary storage devices. This eliminates the need for dedicated devices, and helps administrators make the best use of their storage equipment investments.

Basic Volume Management Process

The three main elements of Media Manager are shown in Figure 24.

• **Robot Management** — supports robotic secondary storage devices.

• **Device Management** — lets you share secondary storage devices among different users and applications.

• **Media Management** — tracks the location of all removable media and secondary storage devices in your system, and gathers media usage statistics.

The term volume as used in VERITAS NetBackup refers to the physical storage media on which VERITAS NetBackup stores its backups, such as a tape or optical disk. The Device Manager controls the actual mounting of volumes on the tape or optical storage devices in response to requests from VERITAS NetBackup or others. These requests specify both the volume name and device density.

![Figure 25: Volume management.](image-url)
The Device Manager always uses the volume database to get information about the volume. If the request involves a robot, this information includes the specific robot that has the volume and the slot location of the volume within the robot. The device then issues a mount command to the robotic daemon controlling that robot, which automatically mounts the specified volume and returns control to VERITAS NetBackup. No operator intervention is required, provided the required volume is physically in the robot.

If the volume is not in the robot, the Device Manager alerts the operator by sending a mount request to the console. The operator then finds the volume and inserts it in the robot so the operation can proceed.

Barcode verification is also supported for robots with barcode readers. This provides an extra measure of confidence that the correct volume is being mounted.

With a standalone drive, VERITAS NetBackup attempts to use the media that is in the drive. If the drive does not contain media, the Device Manager alerts the operator by sending a mount request to the console. The operator then finds the volume, mounts it manually, and assigns it to the request.

The Media Manager allocates a previously unassigned volume to VERITAS NetBackup whenever a new volume is required for either a standalone or robotic drive. Volumes allocated to VERITAS NetBackup come from the volume pool designated for the specific backup files, which by default is the NetBackup volume pool. The term volume pool refers to a distinct set of volumes that are assigned for a specific use.

Volume Pools make it possible to keep only one type of image on a volume. For example, you could create separate pools for archives and backups. A case where separate volume pools are mandatory is when another application, such as VERITAS Storage Migrator, is also using Media Manager.

Once a volume is allocated to VERITAS NetBackup, no other application can use it until all images written on the volume have expired. The VERITAS NetBackup administrator specifies the retention period for the files and can choose to either keep all images with the same retention period on the same volume or to keep a mix of different retention periods on a volume.

In addition to assigning volumes, the media manager tracks the location of both online and offline volumes and keeps this information in the volume database.

**Shared Storage Option (Drive Sharing)**

The NetBackup Shared Storage Option allows individual tape drives (standalone or in a robotic library) to be dynamically shared between multiple NetBackup master or media servers. Drives can be dynamically allocated across NetBackup servers as backup/restore operations dictate. This software option requires appropriate hardware connectivity, such as a SCSI multiplexer or fibre switch/hub storage area network (SAN). If the robotic control is SCSI-based, one host controls the robotics (see the “Sharing Tape Libraries” section below). Other applications such as VERITAS Storage Migrator and user tape requests can also share tape drives.

Figure 26 below diagrams an example of a shared drive configuration. Multiple NetBackup servers (master servers or media servers) are grouped around one or more multi-drive libraries connected by a fibre or SCSI switch. During setup, drives that are to be shared between NetBackup servers are defined as shared drives by the system administrator. Drives not designated as shared drives are dedicated to a single server. All of the shared drives are available to any of the NetBackup servers in the SAN. When a backup session is initiated on a specific NetBackup server, that server requests the appropriate number of drives from the shared drives available. Assuming the number of requested drives are available, the drives are allocated to that server, the electrical connection is configured in the switch, and the backup proceeds. When the backup session completes, the drives are de-allocated, freeing them for use by other NetBackup servers. The same process repeats as other NetBackup servers initiate backup or restore operations. Once all of the shared drives are allocated, the backup/restore session is queued until the requested number of drives are available.
Sharing Tape Libraries

VERITAS Media Manager, included with NetBackup, provides the capability for multiple backup servers to share a multi-drive tape library. One NetBackup server acts as the “robotics controller,” and other NetBackup servers request tape mount and dismount services from the robotics controller. In this configuration, each NetBackup server maintains dedicated data paths to maximize performance without sacrificing the cost effectiveness and economies of scale of large tape libraries.
Libraries attached to a “NDMP media server” (direct-attached to the NAS NDMP host) can also be shared between multiple NDMP NAS servers and one or more NetBackup servers, as shown in Figure 28 below. Drive sharing is not supported for NDMP NAS hosts. As with the NetBackup server case above, the library robotics may be controlled by either the NetBackup server or one of the NAS NDMP hosts.

![Figure 28: Sharing robotics libraries between NetBackup and NDMP NAS servers.](image)

### Managing Robot Inventory

Managing the contents of robots is a critical task and can be very difficult when a site has a large number of robotic volumes. Media Manager provides options that are designed to make this task much easier. Some of the important capabilities that Media Manager gives to the administrator are:

- **Automatically populate the volume database for a new robot.**

  In a new configuration, the administrator can load a robot with new media and then have Media Manager automatically add the volumes to its volume database.

  If barcodes are being used, Media Manager automatically registers the new media according to the barcodes. By defining rules based on barcodes, the administrator can have Media Manager initialize volume database entries with specified values for volume pool, media type, maximum number of mounts, and volume description.

- **Update the volume database after changing the contents of a robot.**

  After adding or removing volumes, the administrator can have Media Manager physically inventory a robot and then automatically update the volume database so it coincides with the results of the inventory. When volumes are moved in or out of the robot, Media Manager updates the database to show the new location.
The administrator can also generate reports that show:

- What is physically in a robot?
- Discrepancies between what is physically in a robot and what is shown in the volume database.

**Scratch Pools**

Media manager enables administrators to configure/enable scratch pools. When applications such as VERITAS NetBackup and Storage Migrator need additional (new) media, they can obtain new media from the scratch pool. Scratch pools can be local to a single storage unit (library), or can be configured across multiple storage units. This allows administrators to add all new tape volumes to the scratch pool, rather than statically assigning new media for use by specific applications.

When configured in a NetBackup master/media server storage domain, the media pool capability can significantly reduce operator effort. For example, assume that one of the libraries in a NetBackup storage domain has run out of free media to use. Utilizing the scratch pool feature, NetBackup can automatically and transparently acquire a scratch tape in any library in the NetBackup storage domain that has free media available, and use it as the media for the backup.

**Spanning Volumes for Large Images**

When a backup image is too large to fit on a single volume, VERITAS NetBackup fills each volume to capacity and then automatically spans the image to another volume. This makes the most efficient use of media and is especially useful when backing up large images, such as are commonly encountered with databases. If for some reason, spanning volumes is not desired, the administrator can disable it.

**Tracking Media Age and Number of Mounts**

Because the possibility of media failure increases with age and use, Media Manager keeps statistics on how old the media is and how often it has been mounted. The administrator can choose to expire the physical media based on date or a specified number of mounts.

If VERITAS NetBackup suspects a media failure (usually due to repeated write failures) it suspends use of that volume. Similarly, it will shut down a storage device if a drive fails. In either case, VERITAS NetBackup logs the reason for the action in the error database and notifies an operator to correct the problem.

**Media Overwrite Protection**

Many environments have media written by applications other than VERITAS NetBackup. In these instances, it is important that the old media not be accidentally overwritten thus destroying what could be valuable data. To prevent this from occurring, VERITAS NetBackup provides overwrite protection for a number of different formats, including tar, cpio, and ANSI labeled.

By default, VERITAS NetBackup refuses to overwrite a protected format. It is possible to override this behavior, however, so a site can reuse the media for VERITAS NetBackup images if desired. This option can be useful when phasing over to VERITAS NetBackup from an application that uses one of these protected formats.
Verifying Media

A verification option allows the administrator to read NetBackup media and compare its contents to the online catalog of information in VERITAS NetBackup.

Duplicating NetBackup Media

By using the duplicate option, an administrator can create a second copy of media containing VERITAS NetBackup images. This is convenient for making copies for offsite storage.

Administrators have the option of duplicating a multiplexed primary image into non-multiplexed (tar-compatible) images on secondary media, OR retain the multiplexed format of the primary image on the secondary media. The secondary media can be an exact copy of the primary media, or contain any subset of the (multiplexed) backup images contained on the primary multiplexed media. For example, if the primary media was created with seven multiplexed images, the secondary media may contain from one to seven multiplexed images. The duplicates are created with a single pass of the primary tape regardless of the number of multiplexes being copied, which often dramatically speeds up the duplication of multiplexed primary images.

In addition, both the primary and secondary copies of a backup image can have its own unique expiration period.

Duplicating NDMP images

The NetBackup bpduplicate command can also duplicate backup images created on Network Appliance servers via NDMP. To perform the duplication operation, the NetBackup server must share a library with the Network Appliance NDMP host, or the Network Appliance NDMP host tapes must be transferred to a library attached to a NetBackup server. See the “Sharing Large Robotics Libraries” section above for more information on library sharing between NetBackup servers and NDMP hosts.

Importing Media

An import option allows administrators to import VERITAS NetBackup database information from VERITAS NetBackup media that has expired or was created on another master server. One example of using this option is to move backups or archives to a master server at another location. The import option can also be used to regenerate the NetBackup catalogs from regular backup media. This is normally not required because of the special processes that NetBackup provides for backing up its databases, but it is an extra measure of insurance.
Administration and Use

VERITAS NetBackup and Media Manager provide a comprehensive and logically designed set of interfaces that make it easy to perform all required administration, backup, or restore tasks. There are GUI (graphical user interface), menu-driven, and command line versions of most interfaces.

The graphical user interfaces provide the greatest ease of use with icons, pull-down menus, and full mouse support. These interfaces are Java or Microsoft Windows-based, depending on the platform. Graphical “wizards” assist in the installation and configuration of devices, media, and classes.

The menu-driven interfaces are character-based for individuals who do not have terminals with GUI capabilities. These interfaces are also designed for ease of use and allow an administrator to easily perform tasks, such as checking or altering the configuration from home via a dial-up modem.

In addition to what can be done from the GUI and menu interfaces, many operations can be started from the command line, thus facilitating the use of scripts.

Administrator Interfaces

The administrator interfaces provide access to all information necessary to configure and manage VERITAS NetBackup and Media Manager. You can perform this administration from a single point (Figure 29), regardless of the number of servers or clients in the NetBackup configuration.

![Single Console: Single system view of all NetBackup servers](image)

- Backup schedules & classes
- Volume & tape management
- Remote device management
- Consolidated backup catalog

Figure 29: Centralized administration.
Figure 30 is a screen from the VERITAS NetBackup Windows administrator interface. The administrator uses this particular screen to view, modify, or add backup schedules to the VERITAS NetBackup configuration. Double-clicking on any of the schedules in the right hand window enables the administrator to modify a pre-existing schedule in a logical and easy-to-use format. The menu version provides equivalent functionality.

Figure 30: GUI Screen for viewing, modifying or adding schedules.

The Media Manager also has graphical user interfaces for managing its devices and media. Figure 31 shows the screen for managing devices. The administrator uses this screen to check and alter the status of devices. The menu version shows similar information.

Figure 31: GUI screen for managing storage devices.
Other screens allow the administrator to configure media for use under Media Manager or to perform other tasks related to Media Manager configuration and administration.

A site administrator can even define custom menus and menu commands for the administrator graphical user interfaces. These menus will appear on the main window of the interface and contain whatever commands the administrator has added to them.

Several wizards have been designed to step novice users through common setup and configuration tasks. These wizards simplify and accelerate the process of adding devices, media or backup classes and reduce the likelihood of error.

**User Interfaces**

Users can initiate backups, restores, and archives from their client workstation without logging into the server and without administrator intervention (Figure 32).

![NetBackup user interface](Figure 32: NetBackup user interface.)

Figure 33 shows a typical user interface screen for VERITAS NetBackup users. This example shows the restore screen where users can scroll through the list of backed up or archived files and select those to be restored on the client disk. A menu version of this interface provides the same functionality from a character-based terminal. In addition, a command line interface enables users to create their own shell scripts to perform client-directed operations.
Installation

It is possible to install and configure VERITAS NetBackup on stand-alone systems or on heterogeneous client/server networks supporting hundreds of clients. The administrator first installs software on the master server, then on media servers (if any), and finally on the clients.

The entire install process is automated by Windows InstallShield wizards or installation scripts. When the software is installed the administrator configures VERITAS NetBackup by using the administrator interfaces.

For UNIX clients, software is initially read into the server and subsequently pushed to the clients across the network as shown in Figure 34. This greatly speeds the installation process because there is no need to install client software from CD on individual clients. The administrator installs software upgrades in the same manner, quickly and easily across the network. Windows NT/2000 clients are installed from an NT Domain or AD server or CD. PC and Macintosh client software is quickly and easily installed on each client via CD. It is also possible to install the software so LAN file servers can share NetBackup program files with its clients.
Configuration

During initial configuration, the administrator can start with the default options, which were carefully chosen to meet most of the requirements for typical installations. From this point, well-designed administrator interfaces and wizards along with online help and ample documentation make it easy to customize the setup for a specific site.

The main tasks involved in completing the configuration are:

- Identify the storage devices that are available to Media Manager (serialized hardware is automatically discovered)
- Register media for use as volumes by Media Manager
- Define the type and density of devices that will be in the storage units
- Define VERITAS NetBackup classes including:
  - Clients in each class
  - Files to back up on the clients
  - Backup schedules

The interfaces provide change options that make it easy for the administrator to modify the values set during the initial configuration. Tape drives and robotic devices are automatically discovered (as long as the hardware supports device serialization - most current hardware does).
Activity Monitoring

The VERITAS NetBackup Activity Monitor allows administrators to monitor progress and status of backup and archive jobs. Figure 35 shows the job window with statistics about a selected job. Job control is also provided in that the administrator can kill jobs, which is useful in correcting problem situations, such as when a job is hung or too many jobs are in the system.

In some instances, it may be desirable to produce a report about current and completed jobs without using the Job Monitor interface. The administrator can do this by executing a command from the system prompt or from a script.

![Activity monitor window.](image)

Figure 35: Activity monitor window.

Reports and Logs

VERITAS NetBackup provides many standard reports and logs to verify the completion of backup operations. In addition, users and administrators can set up additional logs if a site requires them.

VERITAS NetBackup can also be configured to notify users and administrators via electronic mail of an operation’s success or failure.

Operational Reports

The administrator has online access to many operational reports through the administrator interfaces. A Backup Status Report provides status and error information on backups completed within a particular time period. The Client Backup Report gives details on each client backup operation. A Log Entry Report lists all activities that occurred during a specified time period. The subset of log entries that indicate problems appears in the Problems Report. Also available to the administrator are various media reports, such as which images are on the media.
Progress Logs

Progress logs on the client allow easy monitoring of all user backup, archive, and restore operations. By creating a separate progress log for each user-directed backup, archive, or restore, users can monitor these operations and detect any problems that may occur. Client users can also receive electronic mail notification of operational results. If users rely on mail notification as a more concise way to receive job status, they need to use the logs only on an exception basis to help isolate problems.

Detailed Activity Logs

At the discretion of the administrator, VERITAS NetBackup will produce detailed activity logs for VERITAS NetBackup programs running on each server and client. These logs are helpful if the standard status and error reports prove to be inadequate for understanding and resolving particularly troublesome problems.

Advanced Reporting

For extensive graphical reporting, the VERITAS Advanced Reporter provides NetBackup users with a wealth of historical and trending information in a variety of formats. These tools allow for more effective capacity planning, performance optimization, and service level assessment. Advanced Reporter is available as a chargeable option to NetBackup.

Error Reporting

Error information is presented in message dialogs through the interfaces and also in various VERITAS NetBackup reports and logs. Over 200 distinct error codes help speed any problem resolution that may be necessary.

In most cases, informational messages in the VERITAS NetBackup reports give detailed description of what led to an error. A Troubleshooting Guide provides analysis and suggests corrective actions that can be taken to correct error conditions.

Crash Recovery

Whenever data in primary storage becomes lost for any reason, users can restore their files from any backup or archive copy still residing on secondary storage. This is true for data loss resulting from accidental file deletion as well as from system failures.

If the VERITAS NetBackup or Media Manager databases are also damaged, the administrator can restore them using special procedures. These databases contain all of the information about the backup and archive files on secondary storage and special backup procedures are employed to ensure their availability.
Internal Databases

VERITAS NetBackup and Media Manager provide interactive online access to all of the internal database information needed to manage its operations efficiently.

There are four NetBackup databases: configuration, file, error, and media. The media database is the only type not stored on the master server. Each server with a storage unit has a media database.

- The configuration database has server, class, client, storage unit, and schedule definitions.
- The file database has the names of backed up or archived files, the volume(s) containing those files, and the associated dates.
- The error database contains the error logs used to generate reports.
- The media database on each NetBackup server has information on the NetBackup media used by the storage units on that server.

In addition, Media Manager maintains three of its own databases - a device database, a robotic database, and a volume database.

- The device database has information about the tape and optical disk storage devices included in the VERITAS NetBackup configuration.
- The robotic database has information about the robotic controls for those devices.
- The volume database has the location of each volume containing backed up or archived files. It operates in conjunction with media databases located on each of the servers attached to the secondary storage devices.

Supported Hardware and Software

The list of hardware and software platforms supported by VERITAS NetBackup and the peripheral storage devices supported by Media Manager is continually growing as new products come on the market. For specific answers on a particular client or server platform, operating system, or peripheral device, refer to www.veritas.com or contact your VERITAS sales representative or reseller.
Summary

VERITAS NetBackup brings the same level of storage management support to the world of open systems as is found in traditional centralized mainframe installations. It is possible to fully automate file backup and archive schedules across entire networks.

Client users are more productive because they no longer need to spend time backing up their own files. Administrators and operators no longer need to support user-directed restores. Everyone can be confident that data is safe because of systematic backups. If primary data is lost, recovery is quick and sure.

User-friendly and intuitive, graphical user interfaces simplify both administration and use. An activity monitor and comprehensive logging and reporting reduce efforts required to track and troubleshoot problems if they occur.

Master and media server storage domains along with Media Manager ensure that secondary storage devices are used to best advantage. Backup storage is shared and managed automatically across the network. The broad range of device and media support also makes it easier to find suitable devices when adding storage capacity.

VERITAS NetBackup was engineered for high performance, scalability, flexibility, and ease of use. It is the ideal solution for backup, archiving, and recovery of mission critical data, which is the most critical storage management task for any organization.
Appendix A

Frequently Asked Questions

Does VERITAS NetBackup provide full automation for backup and restore operations without operator intervention?

Yes. Operational involvement is not required if peripherals are configured and the needed media is online. Backups are performed by a scheduler process (not cron) based on administrator-specified schedules.

Users can restore files on demand through any of three interfaces – graphical, full-screen menu, or command line – by perusing lists of backed up files and selecting which ones they want to restore. This selection is by file or directory name, and does not require any knowledge of the media involved. The server determines this automatically as part of the restoration process.

Does VERITAS NetBackup have the ability to restart a failed backup?

With frequency-based scheduling, automated backups begin within a specified period or backup window. VERITAS NetBackup performs a specified number retries during the time that the backup window is open. The number of retries is a configurable option.

Do you provide media bar code support?

We support bar codes on robotic devices that contain bar code readers.

Which network protocols does VERITAS NetBackup support?

VERITAS NetBackup uses TCP/IP for transporting data.

Does VERITAS NetBackup allow users to exclude files from being backed up?

Yes. Each user may establish his or her own exclude list of client files to skip.

Does VERITAS NetBackup allow for backups spanning tapes and tape devices?

With VERITAS NetBackup an individual tape or optical disk may contain multiple backups, and an individual backup may span multiple tapes or disks.

Does VERITAS NetBackup have the ability to create duplicate tape sets?

An optional feature of NetBackup called the Vault Extension allows making a second copy of media containing VERITAS NetBackup images fast and easy.

What is the measured performance of both backup and restore operations for entire file systems with NetBackup?

There are many important variables that affect performance, such as network load, client and server capabilities, file system characteristics, file size, and the number and type of peripherals configured.

VERITAS has measured from 1 MB per second for backup and restore on a single Exabyte 8500XL drive, all the way up to 1 TB/hr on a hot Oracle Database backup (to 24 STK Redwood drives). This just illustrates how much performance can vary, depending on the network and computing environment.
How much data can VERITAS NetBackup back up to a single peripheral in an 8-hour shift?

This depends on the sustained transfer rate achieved.

For a file system backup to an 8500XL, the following calculations indicate the aggregate data you could back up in eight hours at typical transfer rates:

- 8.6 GB at 300 KB per second
- 12.9 GB at 450 KB per second
- 23.0 GB at 800 KB per second
- 28.8 GB at 1 MB per second

For a raw partition backup to a DLT 4000, at a transfer rate of 2.3 MB per second, you could back up 72 GB in eight hours.

The above numbers do not count the time needed to locate and mount the media. Also, in both cases, adding another drive would increase throughput by a factor of 1.5 to 1.8.

How many clients do your current customers typically backup on a single server? What is your experience in production with multiple NetBackup servers?

Media servers, operating under the control of a single master server, help decrease network traffic and make more peripherals available. Several current customers are backing up more than 5000 clients to domains of NetBackup servers, and are continually adding more client workstations to the configuration.

How many peripheral devices can VERITAS NetBackup use in parallel?

VERITAS NetBackup can concurrently utilize as many peripherals as can be configured (disregarding performance considerations and system limitations). For example, VERITAS’ test environment has a single Sun IPC using the following peripherals simultaneously:

- Exabyte 10i (1 drive)
- Exabyte 60 (2 drives)
- HP Optical Library (2 drives)
- Metrum RS-48 (2 drives)

In this configuration, VERITAS NetBackup can perform seven backups in parallel.

What dynamic load balancing features does the VERITAS NetBackup scheduling process provide?

You can balance network loads by adjusting the "Max Jobs/Class" attribute of the client class definition. This can give clients in one class preference over those in another class. If you group your client workstations by network location, this could balance networks of differing capabilities.

Does VERITAS NetBackup work simply and easily with a single tape drive if no robotic peripherals are available in the network?

VERITAS NetBackup, working in conjunction with Media Manager, provides an operator interface that tracks the status and mount requests for a stand-alone tape drive. Mounting previously labeled or used media will allow automatic assignment of a single drive.

The real advantage of Media Manager, however, is its powerful ability to coordinate the operation of multiple robotic peripherals, which lets you increase the capacity of small networks as your needs grow.
Do you support the automatic scheduling of cleaning cartridges in robotic peripherals?

Media Manager not only supports automatic cleaning schedules in robotic tape peripherals but also tracks cleaning and usage information for devices that do not have mountable cleaning cartridges.

How does VERITAS NetBackup provide easy verification of backup success?

Optional e-mail notification is available to both the administrator and individual client users citing backup successes and failures. In addition, reports are available that list the backup status of all clients and list all backed up files available for restoration. Either of these reports can be limited to a particular client and date range. Daily summary reports are also available. In addition, the administrator can use the media verification option to compare media contents to what is recorded in the VERITAS NetBackup database.

How is standard UNIX security maintained for backups, restores, and database browsing?

VERITAS NetBackup provides UNIX-level security for files during backup, list, and restore operations. In addition, the owner, group, and permission attributes are maintained in the backups so it is available to be properly reset during a restore.

In addition, client data security is enhanced if VERITAS NetBackup is installed on secure clients that are not required to trust the server to log in as root.

Can VERITAS NetBackup restore files to any machine regardless of original machine name or IP address (in case the original machine no longer exists)?

It is possible to restore files to alternate clients with VERITAS NetBackup. An administrative action is necessary to allow this to happen, and the client user doing the restoration must identify the client from which the data was originally backed up.

Can VERITAS NetBackup be integrated with a file migration product?

VERITAS Storage Migrator is a separate VERITAS product that you can integrate with VERITAS NetBackup. This product manages server disk space by migrating data to secondary storage while still providing transparent access to files.

How is media handled if file backup and file migration are integrated?

Both VERITAS NetBackup and the VERITAS hierarchical storage management products use Media Manager as their media management utility. This provides a common interface across all peripheral devices, whether cartridge tape or optical disk, and enables other programs and applications to share these devices.

Does VERITAS NetBackup support permanent logging of error messages?

VERITAS NetBackup maintains a history of error messages in its error database. The default value is 28 days, but the administrator may modify this to provide a permanent record of the error message log.

Can you generate catalog information about your backups from the backup media itself?

Yes, there are two ways to do this. If the administrator follows the recommended procedures for backing up the NetBackup catalogs, the information contained is easily restored by using the VERITAS NetBackup bprecover command. If for some reason these procedures are not followed, recovery takes longer but can be done by importing the media containing the database backups.
Glossary

administrator: a user granted special privileges to configure, install, and manage VERITAS NetBackup.

archive: duplicating a primary storage file in secondary storage, then deleting the file from primary storage. Performed in order to retain data for a long period of time (see “backup”).

backup: duplicating a primary storage file in secondary storage without deleting it from primary storage. Performed to protect data from system failures and accidental loss (see “archive”).

backup image: the collection of data VERITAS NetBackup saves for a client during each backup or archive operation, including all the associated files, directories, and catalog information.

backup window: the time period during which automatic backups and user-directed backups and archives can occur.

class: (see "client class").

client class: a group of clients designated by the administrator that shares common backup characteristics. Sometimes referred to as a policy.

command line interface: the client-based user interface provided by VERITAS NetBackup to control backup and restore operations by means of individual commands and shell scripts (see “graphical user interface,” “menu interface”).

software compression: the act of reducing the backup image size on the client to minimize data storage requirements and network traffic (see “decompression”).

configuration database: the VERITAS NetBackup database containing server, client, and storage unit definitions, client class definitions, and schedules.

daemon: a UNIX process, apart from the kernel, that performs a particular task.

decompression: the act of reconstructing compressed data during a restore operation (see “compression”).

device database: the Media Manager database containing information about the tape and optical disk storage devices included in the VERITAS NetBackup configuration (see “robotic database,” “volume database”).

file database: the VERITAS NetBackup database containing information describing past backups and archives.

frequency: the designated time that should elapse between successful backups for a particular VERITAS NetBackup schedule.

full backup: a backup of every specified file on a client (see “incremental backup”).

graphical user interface (GUI): the administrator or client-based user interface provided by VERITAS NetBackup conforming to OSF/Motif conventions (see “menu interface,” “command line interface”).

incremental backup: a backup only of those specified client files that have been changed since the previous backup operation (see “full backup”).

master server: server that performs all administrative actions and is responsible for all backup scheduling (see “media server”).

media server: a server operating under control of the master server that manages additional secondary storage units (see “master server”).
**menu interface:** the administrator or client-based user interface provided by VERITAS NetBackup for individuals who do not have GUI capabilities (see "graphical user interface," "command line interface").

**multiple volume device:** a physical storage device not requiring manual intervention to change volumes because of built-in robotic controls (see "single volume device").

**multiplexing:** streaming data from multiple, simultaneous backups to the same device.

**NFS mounts:** files residing on a remote node that are mounted on the local node through the Network File System (NFS) protocol.

**primary storage:** online magnetic disk storage connected directly to a client or server where new or active data is maintained (see "secondary storage").

**raw partition restore:** physical backup of a partition of a disk drive.

**removable media:** a tape cartridge or optical disk that is not permanently mounted in a secondary storage device.

**restore:** the act of returning a previously backed up or archived file to primary storage from secondary storage.

**retention level:** a factor specifying how long backups or archives are to be saved before being deleted.

**robotic:** performing a complex mechanical task ordinarily ascribed to human beings (such as choosing one of several removable media and loading it into the drive of a secondary storage device).

**robotic database:** the Media Manager database containing information about the robotic controls for the storage devices included in the device database (see "device database," "volume database").

**secondary storage:** supplemental storage connected to a storage server where data from primary storage is backed up or archived (see "primary storage," "removable media").

**secure client:** a client that does not require a /.rhosts file entry for the server (see "trusting clients").

**single volume device:** physical storage device requiring manual intervention to change volumes (see "multiple volume device").

**standalone device:** physical storage device requiring manual intervention to change volumes (see "single volume device").

**storage domain:** a single NetBackup master server and its associated media servers

**storage media:** any object upon which data can be stored, such as tapes, tape cartridges, and magnetic or optical disks.

**storage unit:** as used by VERITAS NetBackup, a logical entity that includes one or more storage devices that are of a specific type and media density and attach to a specific host.

**true image recovery:** restores only files that were in the directory at the date and time of a specific backup. Previously deleted files are ignored.

**trusting client:** a client that has a /.rhosts file entry for the server (see "secure clients").

**user:** a person operating a client workstation (see "administrator").

**volume:** any physical storage medium such as a tape or optical disk.

**volume database:** the Media Manager database containing information about the volume handling during backup and restore operations (see "device database," "robotic database").
Appendix C

Client Backup Coverage Utility

The client coverage backup utility can produce three reports that gather various types of information about the clients being backed up by the server. The reports are:

- System Backup Coverage Report
- Class Hardware/OS Report
- Hosts Report

The File System Backup Coverage Report detects file systems that are not backed up by any class and file systems that are backed up by more than one class. Currently, this report is only supported for UNIX clients.

The Class Hardware/OS Report displays hardware and operating system information for clients. The Hosts Report indicates which hosts are in a NetBackup class on the server.

The new check_coverage script can be found in `/usr/openv/netbackup/bin/goodies`.

Refer to the example reports below.

File System Backup Coverage Report (UNIX only)

```
Key: * - Class is not active
UNCOVERED - Mount Point not covered by an active class
MULTIPLE - Mount Point covered by multiple active classes
CLIENT: honeypot
Mount Point Device Backed Up By Class Notes
----------- ------ ------------------ -----
/ /dev/dsk/c1t0d0s0 pooh
/acasl /dev/dsk/c1t2d0s0 UNCOVERED
/export/home /dev/dsk/c1t1d0s0 pooh
/openv /dev/dsk/c1t1d0s1 tigger
/opt /dev/dsk/c1t0d0s5 kanga MULTIPLE
/opt /dev/dsk/c1t0d0s5 roo MULTIPLE
/packages /dev/dsk/c1t2d0s1 UNCOVERED
/test2 /dev/dsk/c1t0d0s7 pooh
/usr /dev/dsk/c1t0d0s6 UNCOVERED
/var /dev/dsk/c1t0d0s1 *piglet UNCOVERED
```

Class Hardware/OS Report

```
Key: * - Class is not active
CLIENT - hostname (uname information)
VERSION - NetBackup version running on the client
CLIENT: honeypot (sun4u/SunOS 5.6 Generic)
VERSION: NetBackup-Solaris2.6 3.1GA
```

DOCUMENT_ID: ENB_941210342
kanga Sun4/Solaris2.6
*piglet Sun4/Solaris2.6
pooh Sun4/Solaris2.6
roo Sun4/Solaris2
Tigger Sun4/Solaris2.6

Hosts Report

---------

Key: YES - In a NetBackup class
NO - Not in a NetBackup class

NO 123.456.777.21 abc.your.company.com abc
YES 123.456.789.1 bcd.your.company.com bcd
YES 123.456.789.2 cde.your.company.com cde
YES 123.456.789.3 def.your.company.com def
YES 123.456.789.4 efg.your.company.com efg
YES 123.456.789.5 fgh.your.company.com fgh
NO 123.456.789.6 ghi.your.company.com ghi
NO 123.456.789.7 hij.your.company.com hij