Microsoft Corporation & Dell

Using Network Attached Storage for Reliable Backup and Recovery

*Microsoft Corporation*
*Published: July 2003*

**Abstract**

Tape-based backup and restore technologies have for decades been the primary mechanism by which data is protected from corruption or loss, and it continues to be the best method for archiving data. However, managing multi-server tape-based backups in a local area network (LAN) environment can become problematic as small and midsize businesses grow. Using Dell’s Windows Powered Network Attached Storage (NAS) servers as the means by which to control the backup and recovery process, NAS streamlines management operations, lowers the total cost of ownership (TCO), and offers a rapid backup and restore solution using disk-to-disk backup technology solutions.
The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003. Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Contents

Introduction.................................................................................................................................... 1

Common Causes of Data Loss..................................................................................................... 2
  User Error................................................................................................................................. 2
  Data Corruption......................................................................................................................... 2
  Hardware Failure ....................................................................................................................... 2
  Disaster Recovery....................................................................................................................... 2

Backup and Restore Approaches............................................................................................. 3
  Disk-to-Tape Backups................................................................................................................ 3
  Disk-to-Disk Backups................................................................................................................ 5

Network Attached Storage....................................................................................................... 7
  NAS Servers ............................................................................................................................ 7
  NAS for LAN-based Backups and Restores ............................................................................. 8

Network Backup Components .................................................................................................. 9
  Hardware Components ............................................................................................................ 9
  Software Components ............................................................................................................ 9

NAS Backup Scenarios............................................................................................................. 10
  NAS for Client Backup .......................................................................................................... 10
  NAS for Server Backups ....................................................................................................... 11
  NAS for Remote Site Replication and Central Backup .......................................................... 11

The Dell Windows Powered NAS Backup Solution................................................................. 13
  Dell PowerVault™ NAS Servers ........................................................................................... 13
  Windows Powered NAS ......................................................................................................... 13

Related Links ........................................................................................................................... 16
Introduction

Data is a business’s most valuable resource. Protecting data from corruption, user error, hardware failure, theft or site disaster is widely recognized as a critical part of business operations. Despite this, not all data is equally protected. While backing up data on a relatively small number of servers can be effectively controlled by the system administrator, client data on desktops and notebooks is notoriously vulnerable to loss or corruption—largely because backups are the responsibility of each user and are performed inconsistently.

As businesses expand, the amount of data that requires storage and protection has increased dramatically, and for many businesses this increase has been exponential. At the same time, the window of time during which data can be backed up without negatively impacting business operations has decreased. Both of these factors have combined to make the system administrator’s job of storing and protecting data fundamentally more challenging.

Backup of servers directly to tape has been the primary method of data protection for the better part of the last 50 years. Tapes, inexpensive and mobile relative to disk-based backups, have long provided a cost effective data protection solution. However, as each additional server is brought online to increase storage and production capacity, an additional tape drive must be directly attached to provide backup protection. Not only does this approach drive up equipment costs, but scheduling and administering backups of dozens or hundreds of computers can overwhelm system administrator resources. This problem is all the more challenging when multiple operating systems, each with their own backup protocols, are in use.

Many of these problematic issues can be addressed by moving to a centralized backup model in which a single server is designated as the backup server. This server controls the backup schedule and coordinates writing backups of all the networked servers to a single directly attached tape device, thus allowing for tape drive consolidation. While a general-purpose server can be designated as a backup server, these servers carry an application load and have limited storage capacity.

A more effective solution is to dedicate a network attached storage (NAS) server as the backup engine that controls disk-to-tape backups. NAS servers are dedicated file and print servers because they do not have the application overhead that general-purpose servers carry, and they are highly efficient at moving files between production servers or clients and the storage. They are also designed as high capacity storage devices, with greater scalability than general-purpose servers.

Using a NAS server also enables disk-to-disk backup solutions. Data from production servers and clients can be temporarily staged on the NAS server before backup to tape. Alternatively, it can remain on the NAS server and be rapidly restored when required. Point-in-time (snapshot) data imaging capabilities provide extremely fast backup and rapid restore advantages for disk-to-disk technology, and make it simple for the system administrator to make more frequent, and therefore, more up-to-date backups than with weekly full backups to tape. Not only are disk-to-disk backups becoming more cost-effective as disk media prices decline, but because of the robustness of the NAS storage disks, disk-to-disk backups can be more reliable than disk to tape backups, thereby increasing data availability.
Common Causes of Data Loss

There is no single most effective way in which to ensure data is protected. The approach to backups and restores depends not only on the organization’s computer and networking resources, but also on the cause and, therefore, the extent of data loss.

The following are the most common causes of data loss.

- User Error
- Data Corruption
- Hardware Failure
- Disaster Recovery

User Error

Users most frequently experience data loss limited to one or a few files, usually caused by deleting or overwriting files. If a user's data is only on the local computer and is not backed up, there is no alternative other than to recreate the data. If the data is on a server, a backup may contain an earlier version of the file which can be restored. (Mirroring data to another disk is not an effective solution for this problem, since the user’s error will also be replicated.) Unfortunately, locating and restoring single files from a tape backup is a time-consuming and costly process.

Data Corruption

Software bugs or virus attacks can be limited to corruption of one or a few files, or can impact an entire application and its associated files. Regardless, recovery from this type of data loss requires restoring data and the application from a point in time prior to the problem. (As before, this precludes mirroring between disks as an option.)

Hardware Failure

Hardware components (cables, power supplies, system boards, and disk drives) are all susceptible to failure. While some hardware losses simply render the data inaccessible, a disk failure can result in the loss of large amounts of critical data. (Similarly, notebooks are at high risk for complete data loss if stolen.) This type of data can be protected through hardware redundancy and mirroring, a method that not only has the advantage of keeping data available (since failover to the mirrored disk is automatic), but also up-to-date (since the mirrored disks remain synchronized until the point of failure). The disadvantages to this approach are the higher costs associated with hardware replication, as well as greater system administration complexity. For small and midsize organizations, the more common solution is to rely on tape backups and full restores of the disk’s data.

Disaster Recovery

Although rare, losing a site to natural or man-made disaster is nevertheless a measurable risk. In the event of a site disaster, tape backups can provide the most effective means to restore data. Alternatively, if the capabilities exist, remote site replication of data is also an effective means of protection.
Backup and Restore Approaches

The most common method of protecting data is to back up from disk to tape. As point-in-time imaging technologies have developed and disk prices have dropped, disk-to-disk backups are emerging as a supplemental means of providing backups.

Disk-to-Tape Backups

The following are methods for performing disk-to-tape backups:

- Direct-attached backup
- Centralized LAN backups
- LAN-free backups

Direct-Attached

The most common method of backing up servers is to directly attach a tape backup unit to each server and to back up the stored data (which is itself either embedded directly in the server, or directly attached to it). Not only is this method simple to configure, but it also provides high performance, since only a single server is using the I/O bandwidth.

Unfortunately, as server storage capacity is exceeded, additional servers must be added, each requiring additional tape drives. Given that the tapes drives are idle the majority of the time, this is not a very cost ineffective solution. It may work well in the short term, but as management of decentralized backups becomes a high cost endeavor, an alternate solution is usually sought.

Centralized LAN Backups

As the number of servers in an organization increases, it is becomes more cost effective to designate a server on the local area network (LAN) as the backup server. This backup server manages backups of all servers on the network, and all data is backed up to tape attached directly to the backup server. This approach effectively consolidates tape backup equipment, and centralizes tape backup management.

Figure 1. LAN-based backups to a NAS backup server.
Centralized backups can be controlled by two types of servers.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General-Purpose Backup Server</td>
<td>In this scenario, any of the production servers on the LAN can be designated as a backup server. The server retains all of its normal server capabilities—that is, the server is still a general-purpose server, supporting client applications. However, when backups are required, this is the backup server that carries out the operation. While this approach is quite functional, it is not optimal, primarily because of the storage overhead associated with a fully loaded application server. A better solution is to use a dedicated backup server.</td>
</tr>
<tr>
<td>Dedicated Backup Server</td>
<td>A dedicated backup server is loaded with the backup application and does not contain any of the applications users normally access on a general-purpose server. This optimizes backup performance, since, unlike with a general-purpose production server, competition for computing resources does not occur. A NAS server is a highly effective backup solution because it is already a dedicated file and storage server.</td>
</tr>
</tbody>
</table>

The drawback to LAN backups is that all data must pass over the network to the backup server. Because backups are intensive I/O operations, it is possible that the performance of application servers will be negatively impacted by the degraded network bandwidth, especially the first time a full backup is made. While this may not be a problem if the volume of data on the servers is moderate (and isn’t a problem when making incremental backups in which only the file changes are saved), in situations where high volumes of data are passing across the network, users may notice slow speeds.

This problem can be addressed in a number of ways. The least costly solution is to restrict backups over the LAN to times when there is low application traffic. If the backup window is small (or eliminated), an alternate solution is to install a second LAN dedicated to backup and restore traffic only. Another solution is to upgrade from existing networks (typically 100 megabit/second Ethernet) to Gigabit Ethernet, which increases data transmission speeds to 1000 Mb/s, vastly improving congestion problems. The most optimized solution is to install a dedicated storage network or SAN (storage area network). This solution is also the most costly.

**LAN-Free Backups**

As organizations continue to experience a need for even greater storage capacity and data protection, NAS servers can be integrated into a SAN environment, allowing tape backups over the SAN instead of the LAN. In this setup (which requires a dedicated Fibre Channel switch and cables for the SAN), the NAS server is a file server “head,” and the storage capacity resides on the SAN. If there are multiple NAS servers, this approach has the advantage of making the tape device available to any of the NAS servers plugged into the SAN.
Limitations of Tape Backups and Restores

Tape-based backups have been the primary backup technology for more than 40 years, and the market continues to grow as capacities continue to improve. While remaining the best solution for long-term data archiving, there are some limitations to tape-based backups that the system administrator must plan for to ensure that tape restores are effective.

- **Cold Backups.** If backups are done when applications are open and the production servers are writing to disk, data can become corrupted. In order to perform a complete backup, the open application must be shut down, which may stop production. The other alternative is to not backup this application data at all. Cold backups, performed when the data is not in use, require a backup window to be done correctly.

- **Shrinking Backup Window.** One of the biggest difficulties with tape-based backups is the length of time it takes to complete a backup. As more businesses have continued to increase the amount of their data, the window of time allotted for incremental backups (usually done nightly) and full backups (done across weekends) have shrunk dramatically. For those operations required to be operational 24x7, backup windows have been eliminated altogether.

- **Unprotected Client Data.** Client data on desktops and notebooks, unless copied to the server by the individual user, are usually not backed up to tape. In those cases where client data is backed up to tape, the cost of restoring an individual file can be exorbitant.

Although system administrators often focus on making sure data is backed up, the real issue is whether data can be correctly restored. Unfortunately, despite intensive management, tape backups often perform poorly and have unpredictable restore success. Poor quality media, interruptions during the backup process, or other causes can result in the failure to restore backed up data. Unfortunately, there is no way of knowing whether a backup is successful. The only way to determine whether tape media, tape drives and backup applications are all working as intended is to back up data and do some trial restores before a crisis occurs.

Assuming restores are demonstrated to work effectively, the process of restoring from tapes is time intensive. Generally tapes are stored offsite, some distance away from the main facility. The correct tapes must be located, and in the case of incremental backups, restored in order. Even with the best equipment, tapes still must be read sequentially, making it a challenge to locate and restore individual files rapidly.

**Disk-to-Disk Backups**

Back up one disk drive to another is not a new backup solution; what is new is the increased affordability of disks relative to tapes, as well as a number of disk-based technologies which directly address some of the limitations with tape backups. Although disk-to-disk backups can provide a valuable supplement to the tape backup process, they are not yet a replacement for tape-based backups, which are still the most effective method of archiving data.
Disk-to-disk backups can exploit a relatively new technology: “frozen imaging” of data. With the appropriate software on the NAS device, point-in-time images (also called snapshots) can be made by either mirroring or copy-on-write technologies\(^1\). Both techniques have the following advantages:

- **Open File Backups.** Users no longer have to stop working while applications are shut down in order to prevent writes to the data during the backup process. Instead, NAS backup software with point-in-time imaging capabilities serves to complete all in-progress data transactions, write all previously cached data to disk, and pause new writes to disk, thus ensuring data consistency without ever taking the application offline. The process of creating the point-in-time copy takes only seconds (even for gigabytes of data), compared with the hours that it can take to do backups directly to tape.

- **Rapid Restores.** Restores of point-in-time copies from the NAS storage disk are considerably faster than restores from tapes. Access to disks is direct, whether they are physically on site or accessed remotely. In contrast, tapes must be physically retrieved from an offsite storage vault. Unlike tapes which must be read sequentially, data on disk is read by direct random access. While restoring massive amounts of data from tape is fast and effective, restoring smaller amounts of data—especially individual files—can be more efficient and less expensive when restoring from disk.

- **Remote Replication.** While tapes can be taken offsite for disaster recovery purposes, application data written to the primary disk can be replicated to secondary disks at off-site locations via a network connection, without any need for physical transport. Unlike tape backups which are inherently out-of-date, replication to remote sites ensures that data is maximally up-to-date, since it essentially occurs in real-time. The replication process, whether synchronous or asynchronous, ensures high fidelity copies of the data.

- **Synchronous Replication.** The data on the primary disk is identical to the data on the secondary disk(s) at all times. Each new update to disk can only proceed when the previous update is completed. The advantage of this method is that data at the secondary failover sites is always up-to-date. However, synchronous replication is negatively impacted when network load is high, since the application must wait for each write to complete before transactions can resume. In addition, because network performance degrades over long distances, this method is only useful over relatively short distances (10 km or less).

- **Asynchronous Replication.** The data written to the secondary disk(s) can lag behind writes to the primary disk. This method allows the application to resume processing before writes to the secondary disk are complete, thus enabling multiple updates to occur concurrently. While asynchronous replication means that the secondary failover site(s) can be slightly out of date, the system administrator can limit the extent to which the secondary sites fall behind. (This process, known as throttling, is accomplished by stalling the application writes until the secondary disk writes catch up.) Asynchronous replication is the optimal method for high volume networks or distances exceeding 10 km.

\(^1\) The mirroring (or split mirror) technique makes a copy of the entire disk or volume. In contrast, the copy-on-write technique copies the only the changed data.
Network Attached Storage

Until the advent of network attached storage, storage was either embedded directly into the server, or was external to the server, but still directly attached to it. This approach has two significant drawbacks:

- It scales poorly, since meeting the increased demand for storage capacity must be dealt with by adding additional servers
- The file processing functions (such as data storage and retrieval) directly compete with applications for system resources.

NAS technology fundamentally changes this model by removing storage from the production servers and placing it on separate devices that directly attach to the Ethernet LAN\(^2\) or to a Fibre Channel connected storage area network (SAN).

NAS Servers

NAS servers are dedicated (and often optimized\(^3\)) file servers that function to store and retrieve files for production servers. Whereas general-purpose production servers are loaded with applications that consume storage, NAS servers are stripped of unnecessary hardware (there is no monitor, keyboard or mouse) and software applications, and use only those components of the operating system\(^4\) required for file serving, thus maximizing the disk space available for storage.

NAS servers have many advantages:

- **Rapid Installation.** NAS appliances are preconfigured with the necessary software for effective storage management and seamless integration into the existing network. Unlike general-purpose servers which can be complex and time-consuming to install, often requiring network downtime, NAS servers can be plugged directly into the network cable—with no impact on network operations—configured and up and running in less than 15 minutes. All NAS server management is conducted through a web browser interface, rather than having to use the command line interface more common to general-purpose servers.

- **Support for Heterogeneous Environments.** NAS servers make pooled storage available to multiple operating systems, thus making it unnecessary to maintain multiple machines for separate storage, lowering costs and streamlining management. Windows Powered NAS servers from Dell support CIFS and NFS file sharing protocols (among others) enabling file serving of both Windows and Unix files.

- **Server Consolidation.** By shifting the file serving and storage burden off of the general-purpose servers onto high storage capacity NAS servers, overall equipment costs and associated

---

\(^2\) The network can also be a wide area network (WAN), virtual private network (VPN) or Dial-up network.

\(^3\) An optimized file server has been configured with specialized hardware by an original equipment manufacturer (OEM) to make the file-serving process very fast.

\(^4\) Unlike Dell’s Windows Powered NAS, not all NAS servers come loaded with an operating system, which can limit their functionality.
licensing expenses decline. Moreover, pooling storage on a NAS server both makes it both simpler for users to access files as well as streamlining storage management.

- **Improved Server Performance.** Production servers, relieved of the burden of file serving, experience less bandwidth congestion and improved performance, which translates directly into improved response time for the end users.

- **Highly Available Data.** NAS servers can be designed with redundant components such as failover Ethernet controllers and hot-swappable drives to ensure that storage remains available even in the event of a hardware failure. The separation of storage functions from production work ensures that in the event of storage problems, the production servers remain online. Conversely, should there be a problem with a production server, files are still available through the NAS device.

**NAS for LAN-based Backups and Restores**

Because all the file serving and storage requirements on the LAN are already directed to the NAS server, it is a simple and highly effective step to bundle backup software into the NAS and thus enable centralized backups and restores. Using NAS as a backup device provides the following additional advantages:

- **Consolidation of Backup Equipment.** With storage attached to the network rather than directly attached to the server it is no longer necessary to attach a tape device to each server for backups. Tape equipment can be consolidated directly onto NAS servers. This allows businesses to invest in a limited number of high quality tape devices and to maintain them in environments controlled for temperature and humidity.

- **Streamlined Backup Management.** Using the NAS device to control the backup and restore processes simplifies management by centralizing backup operations. System administrators no longer have to go to each individual machine to execute backups. Using a web-based interface, the NAS device can be scheduled to backup all servers to tape such that no write conflicts between servers arise.

- **Client System Backups.** Notebooks are not typically configured for tape backups, and rarely do users consistently back up desktops or notebooks. NAS backup servers provide a means by which to automate the backup process for these client systems.

- **Effective Management of Backup Windows.** All backups are scheduled and controlled through the NAS server. Data is backed up from NAS disk to tape when network traffic is minimal.

- **Disk-to-Disk Backups.** Disk-to-disk backups (see previous section) are enabled by backing up client data to the NAS server. Disk-to-disk backups are faster than disk to tape thus reducing the backup window time. When point-in-time software capabilities are used, backups can be accomplished in seconds. For backed up data that must be frequently accessed, disk-to-disk restores are much less time consuming than restores from tape.

The next sections outline the hardware and software needed to enable backups, and several scenarios in which NAS controlled backups provide a highly effective data protection solution.
Network Backup Components

Network backups are more complex in design than direct attached tape backups. The following sections explain the components necessary to back up over a network, and the types of backups that can be done.

Hardware Components

The hardware components of networked backup systems determine how fast backups and recovery can occur. The following are the critical components of network backups.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Systems</td>
<td>The systems requiring data backup. Also known as data source systems.</td>
</tr>
<tr>
<td>Backup System</td>
<td>The system on which the software controlling backups resides. Also known as backup engine or host backup server.</td>
</tr>
<tr>
<td>Tape Devices</td>
<td>Provide the primary storage medium for backed up data. These can be combined with tape autoloader subsystems to simplify tape management.</td>
</tr>
<tr>
<td>Network Wiring</td>
<td>The wiring components between the client and the backup systems include network interface cards (NICs), switches, hubs and cabling. In the small and medium size business setting, an Ethernet-based network is the most common infrastructure.</td>
</tr>
</tbody>
</table>

Software Components

The software components determine how effectively the hardware is used. Software components include.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Scheduler</td>
<td>Allows system administrator to manually configure or automate backups. Scheduling jobs ensures that no two servers try to write to tape at the same time.</td>
</tr>
<tr>
<td>Backup Agent Software</td>
<td>Software running on the client system that works with the backup system to provide filing functions.</td>
</tr>
<tr>
<td>Data Mover Agent</td>
<td>Software that enables data to be copied from the source to the backup device. These agents—often called “push” or “pull” agents—can reside on either the client, where the data is pushed to the backup system, or on the backup system, where data is pulled by the host off the client.</td>
</tr>
</tbody>
</table>
NAS Backup Scenarios

In all of these scenarios, backups are done over the network, whether LAN, WAN, VPN or dial up. In each case, backup “engine” software is loaded onto the NAS server to control the backup process, and backup agents are loaded onto the data source hosts to push the data to the backup engine.

In each of the scenarios below, the backup engine software can be either CA BrightStor ARCserve Backup or VERITAS Backup Exec. In contrast, the backup agent software is specific to the source device: desktops, notebooks or servers, for instance, require specific agent software.

NAS for Client Backup

Because of heavy daytime use, backups of desktops and workstations are scheduled for after hours, when user activity is generally light. In contrast, because notebooks are generally taken home in the evening, they must be backed up during the day when they are docked at the worksite. Different client agents are required for these two scenarios.

Desktops and Workstations

1. The system administrator loads the client agent software (either CA BrightStor ARCserve Backup or VERITAS Backup Exec) onto each desktop computer or workstation.
2. The system administrator schedules the NAS device to back up data sources after hours.
3. Data is transmitted over the LAN to the NAS device, which schedules pass-through to the tape device (disk to tape) for sequential backups of each desktop and workstation.

Notebooks

1. The system administrator loads the mobile backup software (either CA BrightStor Mobile Backup or VERITAS NetBackup Pro) onto each notebook.

---

5 The specific capabilities of each backup product differs. Consult with Dell for product details.
2. Docked notebooks flag the NAS system.

3. NAS initiates the transfer of data across the network to storage on the NAS device (disk-to-disk backup; can be used for fast recovery).

4. NAS schedules after-hours backup to tape drive (disk to tape).

**NAS for Server Backups**

Specialized backup software is required to back up multiple networked servers across different platforms. Both VERITAS Backup Exec and CA BrightStor ARCserve offer remote server agents optimized for backup of multiple servers (in a cross-platform setting) to the NAS backup server. This backup option requires a backup window.

For those businesses that require 24x7 operations, the application and hot agents offered by BrightStor and VERITAS provide open file backup capabilities using point-in-time (snapshot) imaging.

1. The system administrator loads the backup software agent on each application server.

2. The system administrator schedules backups, which are completed without application downtime.

3. Snapshots can be taken off data stored on the NAS server.

4. Snapshots can be stored on the NAS device (disk-to-disk backups) to provide fast recovery capabilities.

5. Snapshots can be backed up from the NAS device to the tape device for archiving.

**NAS for Remote Site Replication and Central Backup**

Organizations with geographically dispersed divisions or branches can take advantage of NAS backup and remote site replication technology as a means of providing a centralized disaster recovery solution. At each site, data from production servers is stored on a NAS device (see Figure 1). This data can then be synchronously or asynchronously transmitted across the network to a
centralized storage and backup NAS server. This NAS server in turn controls backups to the centralized tape device.

Replication software for each remote NAS server can be NSI Double-Take, CA BrightStor High-Availability Manager, or VERITAS Storage Replicator. As before, the tape backup software on the central NAS backup server is either CA BrightStor ARCserv Backup or VERITAS Backup Exec.

1. Replication software loads onto each remote site’s NAS server.
2. Data from each remote NAS server is transmitted synchronously or asynchronously across network to the NAS central backup server (disk-to-disk).
3. The NAS device controls backups to the target tape device (disk to tape).
The following sections describe the Dell Windows Powered NAS backup solution.

**Dell PowerVault™ NAS Servers**

Dell PowerVault Network Attached Storage (NAS) solutions help simplify your storage environment. They are designed to provide great flexibility by making centralized storage accessible across the local area network (LAN).

NAS servers are self-contained, intelligent devices that attach directly to your existing LAN. A file system is located and managed directly on the NAS server, and data is transferred to clients over industry-standard network protocols (TCP/IP) using industry-standard file-sharing protocols. These flexible, multi-platform devices can be easily and seamlessly integrated into your network, providing a dependable and affordable way to back up your critical data.

**PowerVault 725N**

*Workgroup Level NAS Server*

The PowerVault 725N network attached storage server is an ideal solution for backing up clients and servers, consolidating existing storage and adding incremental storage to your network for use by clients or servers. The PowerVault 725N can provide up to 1 TB of preconfigured storage and can be managed from any remote, web-accessible location.

**PowerVault 770/775N**

*Workgroup to Enterprise Level NAS Server*

The PowerVault 775N and 770N can be easily integrated into most network environments and their incredibly dense form factors are designed to fit into space-constrained offices. Additionally, they can connect to Dell/EMC Fibre Channel storage systems to help provide external disaster recovery and business continuity options. For added protection and value, optional clustering capabilities allow you to build an infrastructure for optimum availability.

- **PowerVault 770N.** Tower or 5 unit rackmount form factor, with an embedded Gigabit Ethernet NIC, and is scalable from 876GB to 17.2 TB with SCSI and over 40 TB with Fibre Channel.
- **PowerVault 775N.** 2 unit rackmount form factor with dual embedded Gigabit Ethernet NICs, and is scalable from 438GB to 16.7TB with SCSI and over 40TB with Fibre Channel.

**Windows Powered NAS**

Windows Powered NAS powers the Dell PowerVault NAS Servers offered by Dell. Windows Powered NAS is built upon the Windows 2000 Advanced Server platform, but uses only the parts of the operating system necessary for file serving and storage, thus enabling such capabilities as point-in-time copies (snapshots), storage management and heterogeneous support. This model allows OEM partners like Dell to optimize file serving abilities to match customer requirements.
Using Windows as the NAS operating system means that many critical features are built into the NAS unit rather than having to be added on. These include file security features, administration, and file management features including:

- **Full integration with Active Directory, the directory service for the Windows platform.** By providing both a database in which to store information about objects on the network—such as applications, files, printers and users—and a consistent way to name, describe, locate, access, and secure information across distributed computer systems, Active Directory simplifies administration, enhances security and extends interoperability.

- **Journaling.** Transaction logging capabilities in the NTFS file system logs change to the directory structure and files, thereby enhancing data integrity.

- **File Level Security.** NTFS enables the administrator to put security access control lists on each directory and file, such that individuals and groups have specific privileges.

- **File Sharing/Locking.** Individuals or applications can open a file for reading while another user or application is writing to it elsewhere.

- **Encrypted File System.** Enables the user to encrypt their files for extra security. The encryption is transparent to authorized users, but unauthorized users are unable to access or read files.

- **Disk Quotas.** Enables system administrators to monitor disk space usage to ensure that systems do not unexpectedly reach capacity. Capacity can be monitored by both volumes and users.

- **File Replication Service.** Enables system administrators to copy and maintain files and shared folders on multiple servers simultaneously. FRS controls synchronization of data, and works both locally and remotely.

- **Distributed File System.** Allows system administrators to create a single unified system that enables effective location of and access to files and folders shared across multiple servers. With a unified “namespace,” users are able to locate and use files as readily as if the information were only on a single machine. DFS can also help provide load balancing for files or folders that are accessed frequently.
Summary

Dell's Windows Powered NAS provides both robust file serving and backup capabilities, thereby enabling both server and tape device equipment consolidation. The NAS server is an out-of-the-box solution that can be deployed in minutes, without network downtime. The minimal management of NAS servers can be accomplished through a web browser, rather than having to use command-line interfaces. NAS servers provide simple cross-platform file sharing and backups, greatly simplifying management of multiple platforms, making it a necessary and valuable part of your complete enterprise backup solution.
Related Links

See the following resources for more information: