

Data Protection Solutions for Network Attached Storage

VERITAS Backup Exec™ 9.0 *for Windows Servers*

TABLE OF CONTENTS

Background 3

Why Use a NAS Device? 4

What about Storage Area Networks (SAN)? 5

NAS, VERITAS and Microsoft Windows Server Appliance Kit 6

Value of Using VERITAS Backup Exec With NAS Devices 7

Supported Environments 8

Backup Strategies 9

 NAS Device Operating Systems 9

 Backup Exec Support of NAS 9

 A. NAS devices using the Windows Server operating system 9

 B. NAS devices using an operating system emulating Windows Servers 9

 C. NAS devices using standard supported versions of Linux and UNIX 10

Configurations 11

 1. NAS (file server or appliance) 12

 2. NAS protecting itself in a SAN 13

 3. NAS as a file server protected by Backup Exec Remote Agent for Windows Servers 14

 4. NAS as a backup appliance in a LAN 15

Known Issues With NAS Devices 17

BACKGROUND

The popularity of NAS devices continues to grow at a faster rate than general-purpose servers. As a result, it is becoming increasingly important to develop a strategy to adequately protect NAS devices. The goal of this document is to help users find the best way to address their storage requirements with products available today. By using the backup applications currently available, NAS devices can be properly protected, ensuring that corporate data is safe and can be restored quickly.

Network attached storage (NAS) devices are specialized server appliances used only to store data. They are designed to allow users to add storage to their local area networks easily and cost effectively. Many vendors are introducing new NAS products targeting markets ranging from entry level to the enterprise. More data is being stored on these NAS devices, so it's critical to protect this data via backup.

NAS devices are different from traditional network servers. They are referred to as "headless" since they do not have a keyboard, mouse or display screen. These devices are designed as single-purpose "plug and play" storage for networks and do not require a full-featured operating system. Many NAS devices use operating systems that emulate different server environments, including Microsoft Windows NT, Windows 2000, Windows Server 2003 and UNIX, or use modified standard operating systems such as Microsoft Windows Server Appliance Kit (SAK).

This document examines several alternatives for protecting NAS resources on the LAN or SAN and explores the alternative of evolving the NAS hardware into a storage appliance — that is, utilizing the capacity of the NAS appliance in conjunction with VERITAS Backup Exec™ and a tape device to protect itself and remote resources on the network. The solutions presented demonstrate, in varying degrees, the benefits of maximizing the use of the NAS appliance's capacity and the speed for both backup and recovery which results an increased in centralized storage management and reduced media costs. The overall benefit is a greater return on the storage solution while minimizing storage costs.

WHY USE A NAS DEVICE?

Network attached storage separates storage resources from general-purpose application servers to simplify storage management and improve the reliability, performance and efficiency of the network, thus increasing an organization's overall productivity.

Much of the computing power of general servers is wasted in the file serving operation. According to a study by Carnegie Mellon University, most servers require 25 percent of available CPU cycles for file I/O. Being a file server has everything to do with the efficiency of the I/O data path, not computing power.

NAS appliances are fixed-function servers that are optimized for a specific function. The filer is the simplest example of a NAS appliance. Filers focus all of their processing power solely on file service and file storage. Filers are self-contained, intelligent devices (running an operating system that attaches directly, usually to an existing LAN). A file system is located and managed on the NAS device and data is transferred to clients over industry-standard network protocols (TCP/IP or IPX) using industry-standard file sharing protocols (SMB/CIFS, NCP, NFS, AFP or HTTP). This intelligence on the NAS device enables true data sharing among heterogeneous network clients.

More commonly, the term NAS appliance is given to servers optimized for a specific application such as Web hosting database application, e-mail or data protection. Worldwide, NAS appliance servers running file sharing and data protection applications represent more than 54 percent of all appliance servers shipped, by revenue, according to IDC.²

As networks continue to grow and evolve, network administrators are looking for ways to improve efficiency. Areas they look to improve include:

Installation	NAS enables you to add storage anywhere on your network in minutes simply by plugging in a network cable, applying power and configuring a few settings. There is no server reconfiguration or network downtime.
Architecture	A streamlined architecture where NAS filers are designed for one function: to serve data to clients in heterogeneous environments, powered by an operating system that is optimized for file I/O activity.
Server I/O Bottlenecks	Separating storage from the server reduces the file serving activity and I/O bottlenecks and increases server bandwidth. CPU cycles can be allocated to handle application requests, resulting in improved client response time.
Efficient Allocation and Use of Resources	NAS provides a common pool of storage that can be shared by multiple servers and clients, regardless of their file system or operating system. No additional software or client licenses are required for clients to access storage, thus existing network investments can be leveraged.
Data Reliability and Availability	According to Dataquest more than 60 percent of server failures are caused by storage-related problems. Network downtime resulting from server failure costs organizations thousands of dollars per hour. Separating storage resources from the server decreases both the number of server-connected hardware components and the amount of file I/O activity. This reduces the probability of server downtime and increases the reliability of the network and application servers. NAS servers operate independent of network servers and communicate directly with the client, keeping files available, even when network servers are unavailable.
Lower Total Cost of Ownership	The features detailed above all result in a lower total cost of ownership by simplifying and centralizing storage management, improving reliability, increasing network performance and efficiency to improve the overall productivity of the organization.

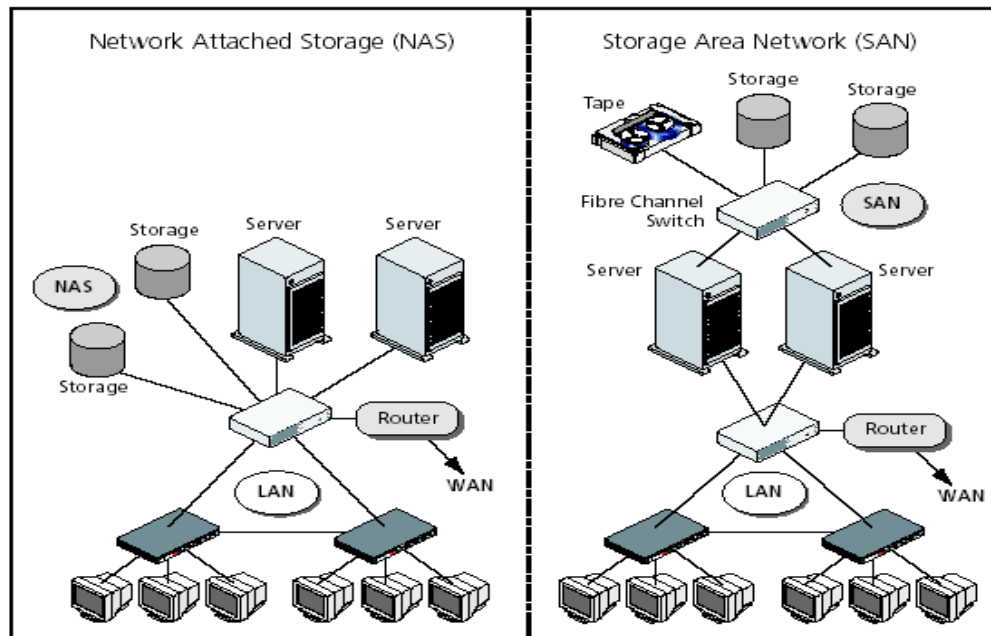
"Taming the Storage Growth Beast with Network Attached Storage (NAS)," 2000, International Data Corporation

WHAT ABOUT STORAGE AREA NETWORKS (SAN)?

SAN and NAS represent two different storage technologies and attach to your network in different places.

NAS is a defined *product* that sits *between your application server and your file system*. NAS devices are connected to servers using the generic LAN. Data is transferred via standard (Ethernet, FDDI, ATM, etc.) network interface using network file system (NFS) or common Internet file system (CIFS) protocols, and data requests are made at the file level over the LAN.

SAN is a defined *architecture* that sits *between your file system and your underlying physical storage*. A SAN is a discrete network of servers and storage devices (RAID, tape libraries, switches, hubs, etc.) attached via a high-speed I/O interconnect such as fibre channel (FC). Data is transferred via serial I/O (SCSI commands), and raw data requests are made directly to disk at the block level over the discrete network. All storage transactions are processed on a separate network with dedicated bandwidth for data.



Although it is important to understand the differences between NAS and SAN, it is possible, and increasingly popular, to create environments with a combination of the two. A NAS device can be added to a SAN simply by adding a host bus adapter (HBA) to the NAS device and plugging the NAS device to a FC switch/router, which adds the NAS device into the SAN fabric.

Trends in network technology support the concept of NAS/SAN convergence. Network speeds (gigabit Ethernet, fibre channel) are now surpassing storage speeds, blurring the lines of underlying infrastructure between NAS and SAN. Another factor driving convergence is the creation of the open standards initiative Direct Access File System (DAFS). DAFS is a file system protocol based on virtual interface standards fostered by Intel. DAFS is agnostic to gigabit Ethernet or fibre channel mediums.

NAS Characteristics	SAN Characteristics
<ul style="list-style-type: none"> NAS defines a device 	<ul style="list-style-type: none"> SANs describe a topology
<ul style="list-style-type: none"> Transfers files 	<ul style="list-style-type: none"> Transfers blocks
<ul style="list-style-type: none"> Data is typically accessed by clients 	<ul style="list-style-type: none"> Data is typically accessed by servers
<ul style="list-style-type: none"> File system resides in the NAS device 	<ul style="list-style-type: none"> File system resides in the server
<ul style="list-style-type: none"> Connected with Ethernet 	<ul style="list-style-type: none"> Connected with FC (or SCSI)
<ul style="list-style-type: none"> Uses network protocols 	<ul style="list-style-type: none"> Uses SCSI protocols
<ul style="list-style-type: none"> 10/100 Mbps or 1 Gbps data transfer rates 	<ul style="list-style-type: none"> 1 Gbps / 2 Gbps data transfer rates

NAS, VERITAS AND MICROSOFT WINDOWS SERVER APPLIANCE KIT

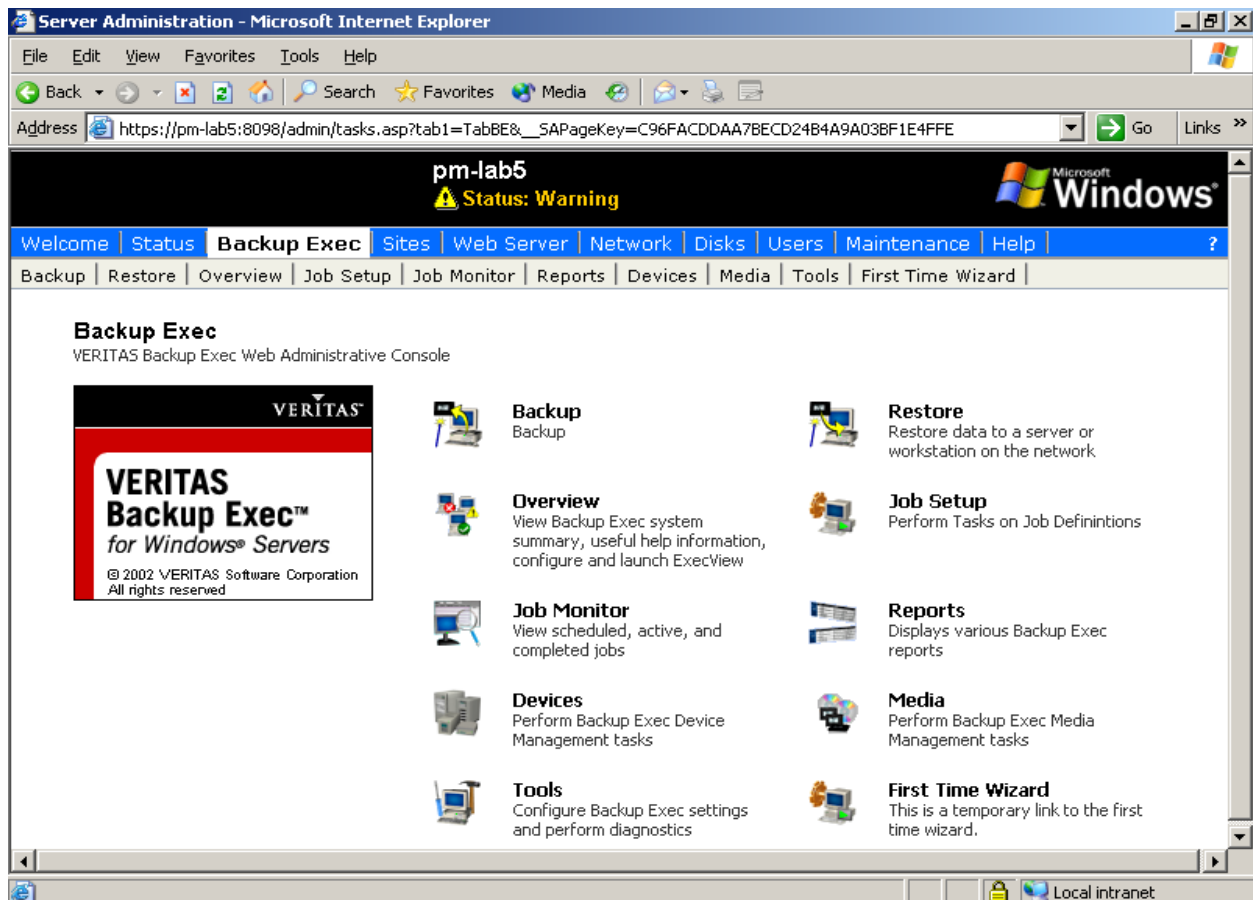
VERITAS has leveraged its strategic relationship with Microsoft to be the first vendor to offer a backup application that is fully integrated into the Windows Server Appliance Kit (SAK). The SAK has been optimized to use key Windows Server features that enable an organization to build a very reliable, scalable and manageable enterprise-wide solution on a single platform. The SAK integrates seamlessly with existing IT infrastructure and the Web.

Ease of deployment is another key advantage. Appliances powered by Windows SAK are capable of being deployed in 15 minutes. With the SAK Web interface an administrator can easily configure settings and other administrative tasks from anywhere on the network.

VALUE OF USING VERITAS BACKUP EXEC WITH NAS DEVICES

VERITAS Backup Exec™ is designed for departmental workgroups and distributed environments of small to midsize corporate customers. This coincides with the target market for Windows SAK NAS appliances. One thing that all NAS devices have in common is that they offer high volumes of data storage — and all of this data must be protected.

Administrators can manage their backup appliance through the remote Web administrator interface of the Windows SAK — no new operating system to learn, no additional user interface to become familiar with. This new generation of NAS devices offers a high-performance, low-cost option to traditional tape backup.



Utilize a web browser interface to perform all administration tasks.

SUPPORTED ENVIRONMENTS

Support For:

- Windows 2000 (Server, Advanced Server, and Datacenter)
- SAK Server and Advanced Server 2.0 and higher
- Windows Server 2003 web user interface

Managed VERITAS Backup Exec Via:

- Web-based Backup Exec plug-in to SAK and Windows Server 2003 web user interface via Internet Explorer 5.0 or later
- Standard Backup Exec user interface via Windows 2000 Terminal Services
- Standard Backup Exec user interface via Remote Administrator option

VERITAS Backup Exec – Key Functionality Matrix with Windows SAK & Windows Server (2003)

Functionality	Backup Exec Standard User Interface via Terminal Services or Remote Administration	Backup Exec Web Administration Console
Manage Backup Exec via Web Browser		X
Protect Local NAS Device	X	X
Protect Remote Resources	X	X
Perform ADAMM Functions	X	X
LAN-Free Backup Support	X	X
Protect Backup Exec – Supported Databases	X (1)	X (1)
Advanced Open File Option	X	X
Library Expansion Option	X	X
Intelligent Disaster Recovery	X (2)	X (2)
Intelligent Image Option	X	X

(1) Microsoft licensing of SAK limits the hosting of Exchange or SQL Server on Windows SAK devices

(2) Requires mouse, keyboard, monitor and bootable device on NAS filer running Windows Server operating system. Please Note: Several NAS vendors have their own disaster recovery method that includes a disaster recovery CD.

* Terminal Services extends the model of distributed computing by allowing PCs to operate in a server-based computing environment.

BACKUP STRATEGIES

NAS DEVICE OPERATING SYSTEMS

The operating system used by a NAS device is the critical factor in determining what level of protection Backup Exec provides. For Backup Exec data protection, NAS devices can be divided into the following groups:

- NAS devices using the Windows Server operating system
- NAS devices not using the Windows NT or Windows 2000 operating system, that properly emulates Windows
- NAS devices using standard supported versions of Linux/UNIX

BACKUP EXEC SUPPORT OF NAS

VERITAS offers alternative solutions to protect various configurations of NAS filers. These are discussed in detail below, and shown with a sample configuration. The version of Backup Exec that will provide the required functionality to protect data in those environments is then highlighted.

A. NAS devices using the Windows Server operating system

If the NAS device is using Windows NT, 2000, SAK, or Windows Server 2003 Backup Exec will see it as any other Windows server on the network. All Backup Exec options will behave as if they were on a traditional Windows server or workstation.

The only exception to this is VERITAS Backup Exec Intelligent Disaster Recovery Option™. Since most NAS devices are headless, disaster recovery technology cannot be used. Disaster recovery requires that a bootable device (tape, CD-ROM or disk), keyboard and monitor be attached to the server. If these components are attached to a NAS device using any of the Windows Sever configurations above, Backup Exec Intelligent Disaster Recovery Option will be supported. If these hardware components are not present, disaster recovery will require that a multiple step approach be used to replace a defective NAS device and restore data. The restoration process must follow a certain procedure: the operating system must first be installed, followed by the backup application and then performing a restore of the data from the last full backup and subsequent incremental or differential backups.

B. NAS devices using an operating system emulating Windows Servers

If the NAS device is using an operating system properly emulating Windows servers, the emulation is transparent to Backup Exec. Files or directories can be backed up and restored with their appropriate attributes for the emulated operating system just as they can for any shared network volume.

Backup Exec's level of data protection for devices with these operating systems does not support:

- Backup Exec Intelligent Disaster Recovery Option
- Backup Exec Remote Agent (CAL) for Windows Servers
- Backup Exec Advanced Open File Option w/CAL

Databases

NAS operating systems that are not Microsoft Windows server operating systems, yet can emulate one of these, can be used to store data for a database and this data can be protected using Backup Exec. Even though the actual applications cannot run on the NAS device, applications can access the data through a network share.

If the NAS device is used to store data for a database, the database application must be hosted on a different Windows system and refer to the NAS device as a shared network resource. Backup Exec can back up and restore these NAS device-based shares as it can shares on a Microsoft server platform. Backup Exec uses special application components (database agents) that are designed to interact and back up database information using specific interfaces for that particular database. Since the database agent interacts with the database server application and not the actual data, the underlying operating system is transparent and the agent can operate normally through the database server application on another system to protect data stored on the NAS device.

C. NAS devices using standard supported versions of Linux and UNIX

Backup Exec can protect these devices using our standard Linux/UNIX client agent.

CONFIGURATIONS

The chart below outlines the more common examples of how Backup Exec and NAS devices may be configured to protect NAS devices. Following each description we provide a summary of which version(s) of Backup Exec are ideally suited to provide protection.

NAS Backup Strategies Using VERITAS Backup Exec™			
Strategy	Operating System on Appliance		
	Windows NT, 2000, SAK, Server 2003	Windows Emulation*	UNIX - Linux
1. NAS Protecting Itself in a LAN	BE		
2. NAS Protecting Itself in a SAN	BE	BE	BE
3. NAS as a File Server Protected by Backup Exec Remote Agent (CAL) for Windows Servers	BE	BE	BE
4. NAS as a Backup Appliance in a LAN	BE		
5. NAS as a Backup Appliance in a Dedicated Backup LAN	BE		
BE = Backup Exec 9.0 for Windows Servers			
*Does not offer Intelligent Disaster Recovery functionality, as the application cannot capture system state information. These NAS devices can be protected by installing Backup Exec client on any other computer with a Windows operating system and configuring the backup job to protect the NAS device via a CIFS/NFS mount.			

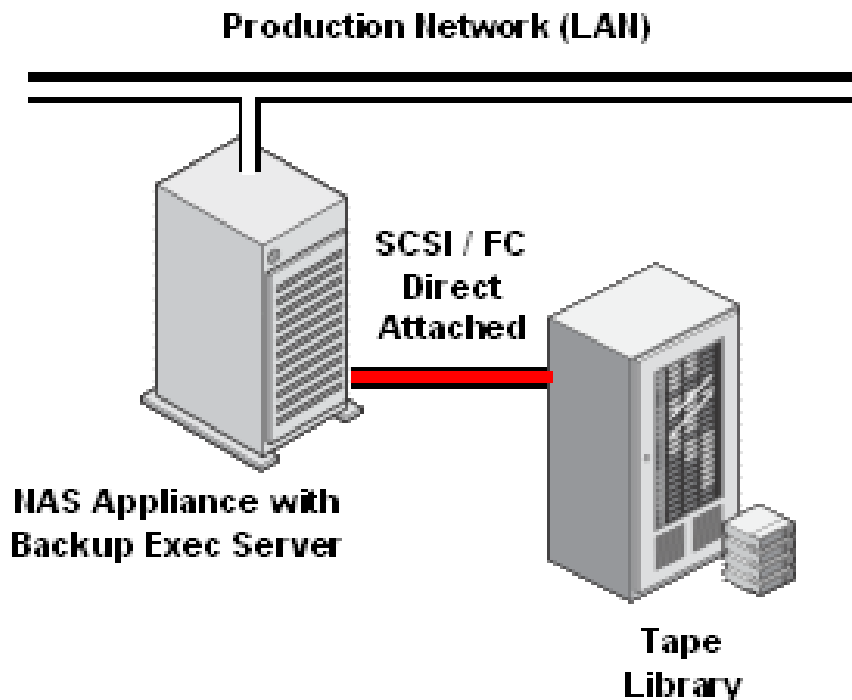
1. NAS (file server or appliance)

Typical customer environment — small to midsize customers with relatively small amounts of data

This is the most basic use of Backup Exec to protect a NAS device itself. Simply load Backup Exec (media) server onto the NAS device. If the NAS appliance is using less than 50 percent disk capacity, a backup can be run locally to itself (disk to disk). Backing up data in this manner provides only partial protection for events such as accidental file deletion, uninstall and data corruption. Additional steps must be taken to provide protection for storage media (disk) failure or disasters. To offer the added protection, directly attach, via SCSI or fibre channel connection, a tape device (drive or library).

Benefits of direct-attached backups are:

- Faster backup and restore performance
- No additional LAN traffic to protect the NAS device



2. NAS protecting itself in a SAN

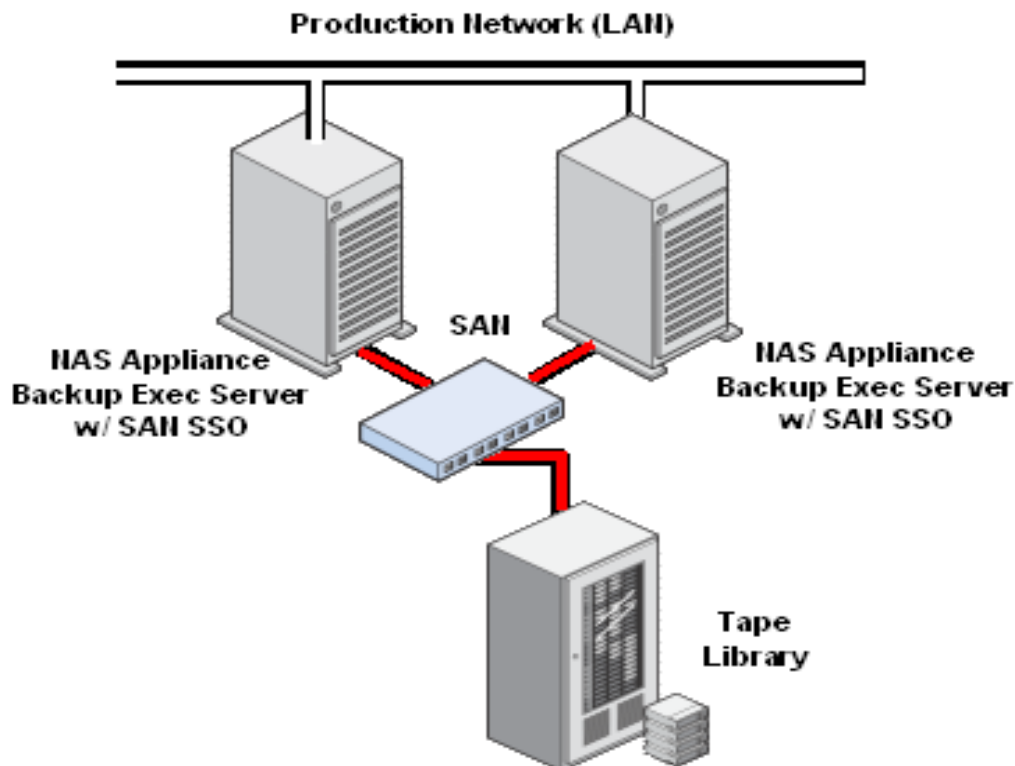
Typical customer environment — midsize to large corporations with large amounts of data

Backup Exec is installed on the NAS device. The backup data flow is from the NAS device to the SAN-attached tape resources. The typical configuration for the SAN disk/tape farm is as follows: A host bus adapter (HBA) card resides in the NAS device; the HBA is connected to a fibre channel switch or hub; the data can now be transported over long distances via fiber cable to a router or bridge, where the data packets are converted back to SCSI protocol for the disk and/or tape storage device(s). The tape storage device can be a tape drive or more commonly, a tape library with multiple tape drives.

You can configure your backup to run from disk to disk, and then schedule a post process to back up the secondary storage to tape providing higher redundancy and disaster recovery capability if tapes are stored at a remote location.

Benefits of this configuration include:

- Faster backup and restore performance
- LAN-free backup — elimination of backup traffic on your LAN
- Dynamic share tape drives between NAS devices
- Consolidation of your backup operation
- Lower total cost of ownership through the reduction of removable media and media management
- Additional protection via remote tape storage for true disaster recovery capability

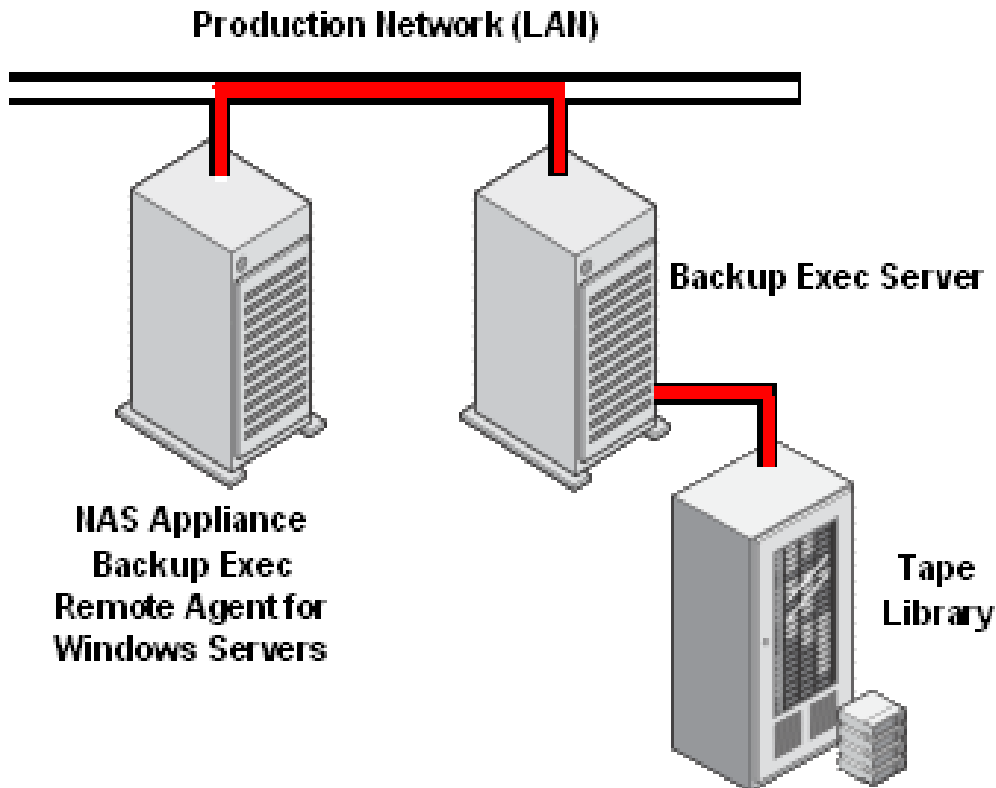


3. NAS as a file server protected by Backup Exec Remote Agent for Windows Servers

Typical customer environment — small to midsize and departmental customers

Backup Exec (media) server is installed on a server running a Microsoft Windows-based operating system. The NAS device can be running any operating system. If the NAS device is running a supported operating system, then a Backup Exec Remote Agent (CAL) is installed on the NAS device. If the NAS device is running a non-Windows operating system but properly emulating Windows NT or Windows 2000 then the backup jobs are configured to back up the NAS device as a network share. Clients are connected to the backup server via a LAN connection. The backup data flow is via the LAN from the client to the Backup Exec server, which then directs the backup to a tape drive or tape library.

The benefit of protecting the NAS appliance in this manner is the centralization of the backup data to tape device, while maintaining the optimum file I/O for the NAS appliance.



4. NAS as a backup appliance in a LAN

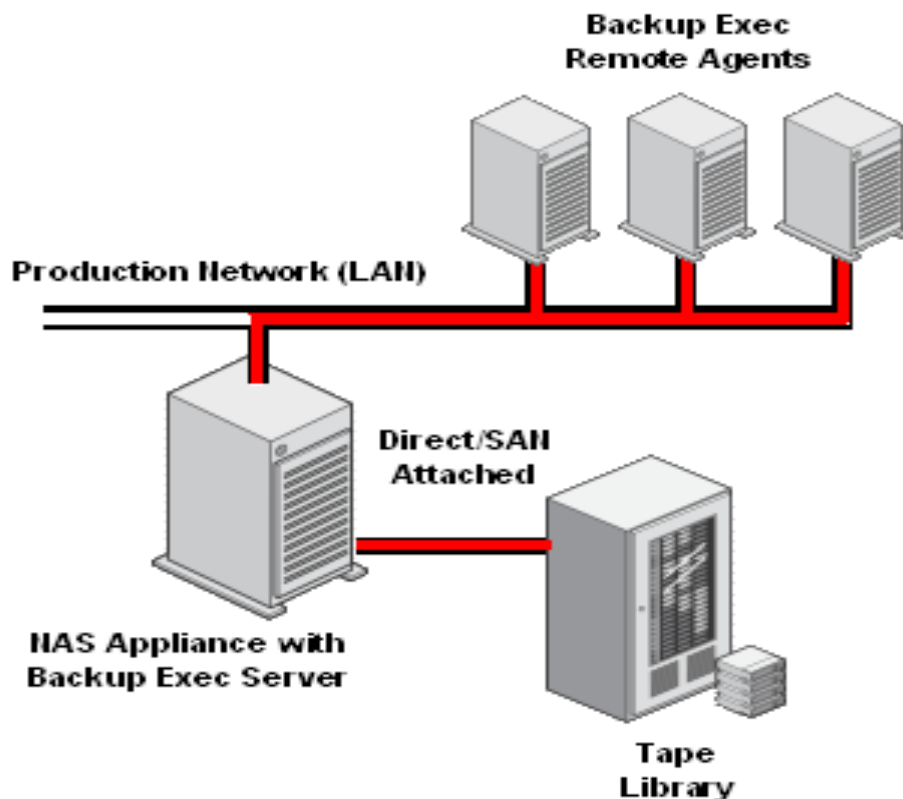
Typical customer environment — small and midsize corporations

Backup Exec is installed on the NAS device. The NAS backup appliance must be running a Microsoft Windows operating system. The backup data flow is from the LAN-attached client to the NAS backup appliance. The client LAN data being protected can be a disk array or another NAS device.

You can configure your backup to run from client disk to backup appliance disk, and then schedule a post process to backup the secondary storage to tape providing higher redundancy and disaster recovery capability if tapes are stored at a remote location.

Benefits of this configuration include:

- Better backup and restore performance than a conventional tape backup solution
- Less LAN traffic than with a tape backup solution
- Lower total cost of ownership through the reduction of removable media and media management
- Additional protection via remote tape storage for true disaster recovery capability



5. NAS as a backup appliance in a dedicated backup LAN

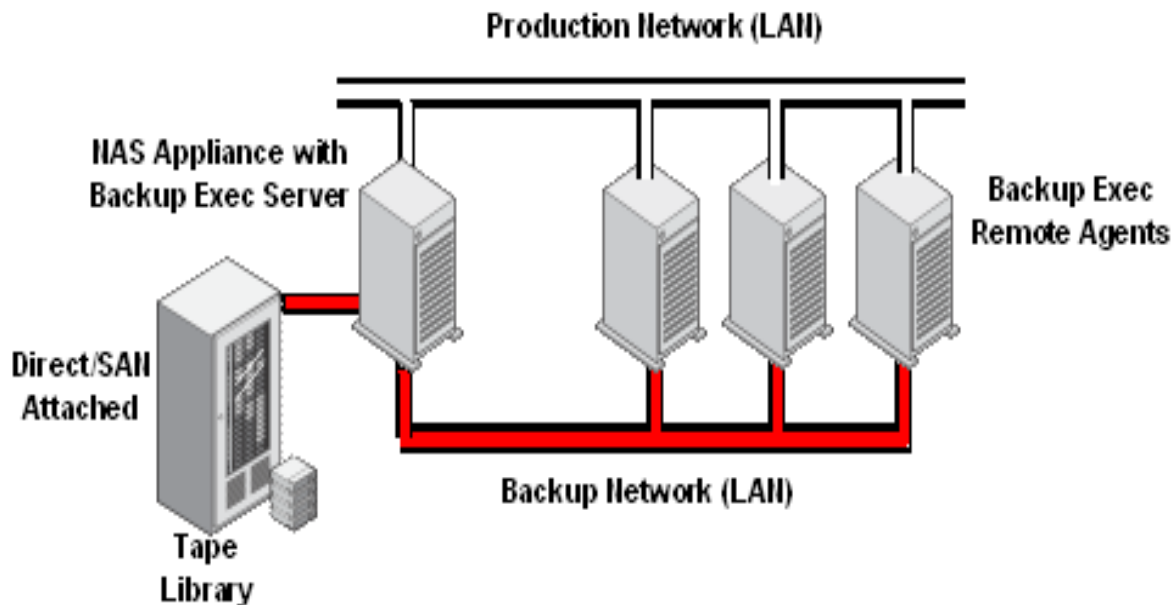
Typical customer environment — midsize to large customers

Backup Exec is installed on the NAS device. The NAS backup appliance must be running a Microsoft Windows operating system. Each of the protected servers must have two network interface cards (NICs) installed. One NIC is connected to the standard corporate LAN, and the second is connected to dedicated backup LAN. The backup data flow is via the backup LAN from the client to the NAS backup appliance. The backup LAN disk being protected can be a disk array or another NAS device.

You can configure your backup to run from client disks to backup appliance disk, and then schedule a post process to back up the secondary storage to tape providing higher redundancy and disaster recovery capability if tapes are stored at a remote location.

Benefits of this configuration are:

- Faster backup and restore performance than conventional tape backup solution
- Significantly less LAN traffic than with a conventional tape backup solution by isolating backup traffic
- Additional protection via remote tape storage for true disaster recovery capability



KNOWN ISSUES WITH NAS DEVICES

For NAS appliances utilizing an operating system that properly emulates Windows Servers the following restrictions apply:

- Backup Exec cannot be hosted on the NAS device
- File and directories can be backed up and restored with the appropriate attributes of the emulated operating system and the data appears as any shared network volume to Backup Exec
- The emulation is transparent to Backup Exec

Due to the dependency of the operating system, NAS appliances that properly emulate Windows Servers may still experience technical difficulty utilizing the following Backup Exec agents and options, and are not currently supported by VERITAS in this environment:

- Intelligent Disaster Recovery Option
- Remote Agent (CAL) for Windows Servers
- Remote Agent (CAL) for NetWare
- Advanced Open File Option

Backup Exec offers no protection for NAS appliances using other operating systems.

For additional updated information, check our support Web site at support.veritas.com.

VERITAS Software Corporation
Corporate Headquarters
350 Ellis Street
Mountain View, CA 94043
650-527-8000 or 866-837-4827

For additional information about VERITAS Software, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at www.veritas.com.