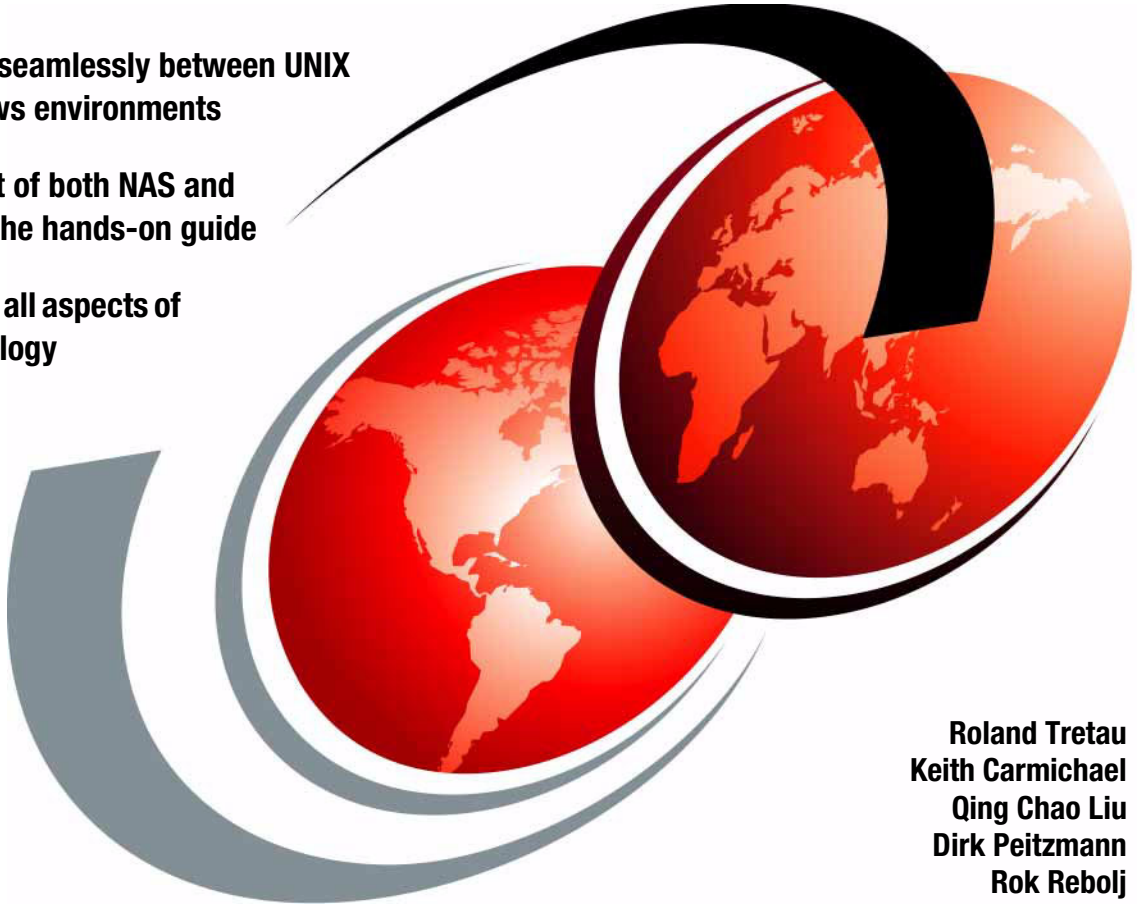
IBM

The IBM TotalStorage NAS Gateway 500 Integration Guide

- Share data seamlessly between UNIX and Windows environments
- Get the best of both NAS and SAN using the hands-on guide
- Understand all aspects of NAS technology



Roland Tretau
Keith Carmichael
Qing Chao Liu
Dirk Peitzmann
Rok Rebolj

Redbooks

ibm.com/redbooks

International Technical Support Organization

The IBM TotalStorage NAS Gateway 500 Integration Guide

March 2004

SG24-7081-00

Note: Before using this information and the product it supports, read the information in “Notices” on page xxiii.

First Edition (March 2004)

This edition applies to the IBM TotalStorage NAS Gateway 500 Release 1.0 as of January 2004.

Note: This book is based on a pre-GA version of a product and may not apply when the product becomes generally available. We recommend that you consult the product documentation or follow-on versions of this redbook for more current information.

Contents

Figures

Tables

Examples

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AFS®
AIX 5L™
AIX®
AS/400®
DB2®
DFS™
Enterprise Storage Server®
ESCON®
@server™
@server ™
FlashCopy®
FICON®
IBM®
ibm.com®
iSeries™
Netfinity®
PAL®
PowerPC®
Predictive Failure Analysis®
pSeries®
RACF®
RAMAC®
Redbooks™
Redbooks (logo) ™
RS/6000®
S/390®
SANergy®
SysBack™
Tivoli®
TotalStorage®
xSeries®
zSeries®

The following terms are trademarks of other companies:

Intel and Intel Inside (logos) are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM® Redbook describes how to install and configure the very latest IBM storage solution and concept, the IBM TotalStorage® Network Attached Storage (NAS) Gateway 500, in heterogeneous environments.

The IBM TotalStorage NAS Gateway 500 series is an innovative Network Attached Storage device that connects clients and servers on an IP network to Fibre Channel storage, efficiently bridging the gap between LAN storage needs and SAN storage capacities. The IBM TotalStorage NAS Gateway 500 is a storage solution for UNIX/AIX/Linux, Apple, and Microsoft® Windows® environments. In this book, we show how to integrate the IBM TotalStorage NAS Gateway 500 and explain how it can benefit your company's business needs.

This book is an easy-to-follow guide which describes the market segment that the IBM TotalStorage NAS Gateway 500 is aimed at, and explains NAS installation, ease-of-use, remote management, expansion capabilities, high availability (clustering), and backup and recovery techniques. It also explains cross platform storage concepts and methodologies for common data sharing for UNIX/AIX/Linux, Apple, and Microsoft Windows environments.

This book makes use of the IBM TotalStorage NAS initiative in the marketplace and defines its position and value-add. Also discussed is how the reliability, availability, scalability, and security of the IBM TotalStorage NAS Gateway 500 has the potential to be at the heart of an enterprise's data storage system.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

The team, from left to right: Qing Chao, Rok, Roland, Keith, and Dirk

Roland Tretau is a Project Leader with the IBM International Technical Support Organization, San Jose Center. Before joining the ITSO in April 2001, Roland worked in Germany as an IT Architect for Cross Platform Solutions and Microsoft Technologies. He holds a Master's degree in Electrical Engineering with a focus in Telecommunications. He is a Red Hat Certified Engineer (RHCE) and a Microsoft Certified Systems Engineer (MCSE), and he holds a Masters Certificate in Project Management from The George Washington University School of Business and Public Management.

Keith Carmichael is an advisory IT Availability Professional from IBM South Africa. He has been with IBM for seven years. Keith's current responsibilities include Technical Support for PCs, xSeries® as well as managing the Parts Repair Centre. He is a Microsoft Certified Professional (MCP). His areas of expertise are Microsoft Windows NT/2000/2003, xSeries and Netfinity® servers,

desktops, ThinkPads, and thin clients. Keith holds a National Diploma in Electrical Engineering.

Qing Chao Liu is an Advisory IT Special list in IBM China. He has five years of experience in supporting IBM PC, IBM xSeries, and IBM pSeries® servers. He holds a Bachelor's degree in Computer Science from the University of Science and Technology of China. Qing Chao has several operating system and networking based certifications, such as AIX® Advanced Technical Expert, MCSE, CCNP, TLCE (Turbo Linux certified engineer) and the certification from Linux Professional Institute.

Dirk Peitzmann is a Senior IT Specialist with IBM Systems Sales in Munich, Germany. He has nine years of experience providing technical pre- and postsales solutions for IBM pSeries (RS/6000®) and IBM TotalStorage. Dirk is a certified Specialist AIX System Administrator, AIX System Support Specialist, and IBM Tivoli® Storage Manager Consultant. He holds a Master's degree in Computer Sciences from the University of Applied Science in Isny, Germany.

Rok Rebolj is a Systems Engineer and Instructor in Slovenia. He has nine years of experience in the IT field. He holds a degree in Electronics Engineering from the University in Ljubljana. His areas of expertise include IBM Netfinity and xSeries servers, Storage Networking, and Systems Management. He holds several hardware and operating system-based certifications (xSeries CSE, StorageWorks ACE, MCSE, MCT).

Thanks to the following people for their contributions to this project:

Yvonne Lyon, Deanna Polm, Barry Kadleck, Charlotte Brooks, Gustavo Castets
International Technical Support Organization, San Jose Center

Wendy Sandin, Julie Anne Knight, Maxey von Senden, William Bostic,
Kevin Galloway, Justin Irwin, Rainer Wolafka, Jeffry Larson, Ivan Olguin,
Nathan Seiter, Scott Washabaugh, Ellen Grusy, Dominic Pruitt, Bill Wilson,
Robert Vining, Neal Jones, Scott Hovey
IBM U.S.

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or clients.

Your efforts will help increase product acceptance and client satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an Internet note to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. QXXE Building 80-E2
  650 Harry Road
  San Jose, California 95120-6099

Part 1

Network Attached Storage concepts and hardware

In this part of the book, we introduce the IBM NAS Gateway 500 system and related hardware, as well as some concepts about Network Attached Storage.

1

The main concept behind Network Attached Storage

Given the expansive growth in both storage and network technology, it is not surprising that an easy-to-implement and scalable solution has been developed to meet the various storage needs.

Network Attached Storage (NAS) exploits the existing intermediate speed messaging network with a very easy-to-integrate storage solution.

In this book, we focus on NAS as a storage networking solution. Reading this book should adequately equip you to implement a NAS solution using one or more of the products we describe to meet your networked storage requirements.

This introductory chapter covers the following topics:

- How this book is organized
- Local Area Networks
- Open Systems Interconnection (OSI) model
- File systems and I/O
- Network Attached Storage (NAS)
- Industry standards

1.1 How this book is organized

Basically, here is how the material in this book is presented:

- First we provide the concepts and technical knowledge needed and offer a brief overview of the IBM products we used (Part 1, “Network Attached Storage concepts and hardware” on page 1).
- Next we explain how to configure the SAN storage for the NAS Gateway 500 to use (Part 2, “SAN storage configuration” on page 45).
- After that we show the first steps for getting connected with the IBM TotalStorage NAS Gateway 500. We start with basic steps up to the two node cluster configuration. We also take a look at the basic user and security management features. Then we describe how to integrate the IBM TotalStorage NAS Gateway 500 product into your enterprise as a high performance open systems storage solution (Part 3, “Implementation” on page 113).
- Then we talk about some backup and restore considerations, and we show various backup and restore options. Next we show how the NAS Gateway 500 can be used with Tivoli Storage Manager (Part 4, “Backup and recovery” on page 287).

Most of this book is a hands-on guide to implementing the IBM TotalStorage NAS Gateway 500 as part of a storage networking solution, but before we can leap into the how-to section, it is important that you understand a few of the basic concepts about networks and storage.

Note: If you are a seasoned storage networking professional and are already very familiar with this subject, feel free to skip ahead to Part 2, “SAN storage configuration” on page 45. However, if you would like a quick primer, you will need to read these first three chapters. They provide the background information you need to understand, not only how to proceed with the integration, but also what you stand to gain from doing so.

1.2 Local Area Networks

A Local Area Network (LAN) is simply the connection of two or more computers (nodes) to facilitate data and resource sharing. They proliferated from the mid-1980s to address the problem of “islands of information” which occurred with standalone computers within departments and enterprises. LANs typically reside in a single or multiple buildings confined to a limited geographic area which is spanned by connecting two or more LANs together to form a Wide Area Network (WAN).

LAN designs are based typically on open systems networking concepts, as described in the network model of the Open Systems Interconnection (OSI) standards of the International Standards Organization (ISO). The OSI model is shown in detail in Figure 1-4, “Comparing the Internet protocol suite with the OSI reference model” on page 7.

LAN types are defined by their topology, which is simply how nodes on the network are physically connected together. A LAN may rely on a single topology throughout the entire network but typically has a combination of topologies connected using additional hardware. The primary topologies defined for Local Area Networks are:

Bus topology

In a bus topology, all nodes are connected to a central cable, called the bus or backbone. Bus networks are relatively inexpensive and easy to install. Ethernet systems use a bus topology (Figure 1-1).

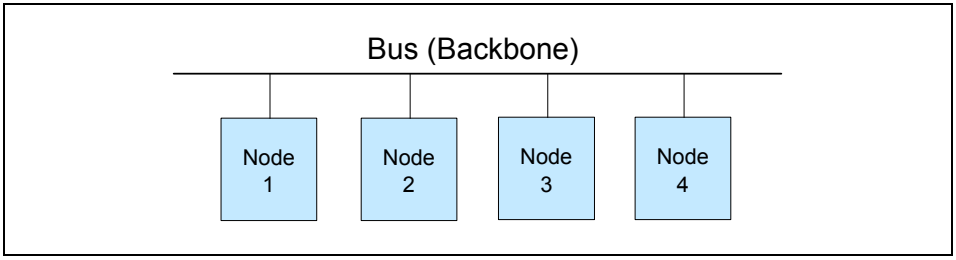


Figure 1-1 Bus topology

Ring topology

Nodes in a ring topology are connected via a closed loop such that each node has two other nodes connected directly to either side of it. Ring topologies are more costly and can be difficult to install. The IBM Token Ring uses a ring topology (Figure 1-2).

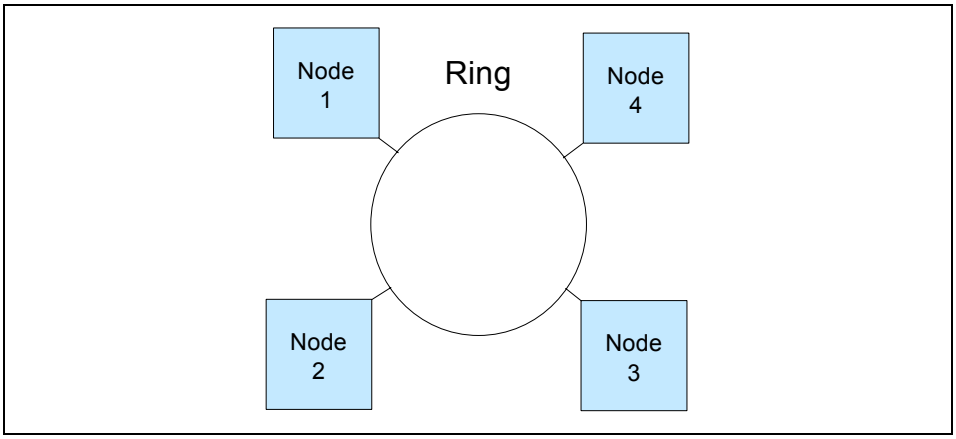


Figure 1-2 Ring topology

Star topology

A star topology uses a centralized hub to connect the nodes in the network together. Star networks are easy to install and manage. However, bottlenecks occur since all of the network traffic travels through the hub. Ethernet systems also use a star topology (Figure 1-3).

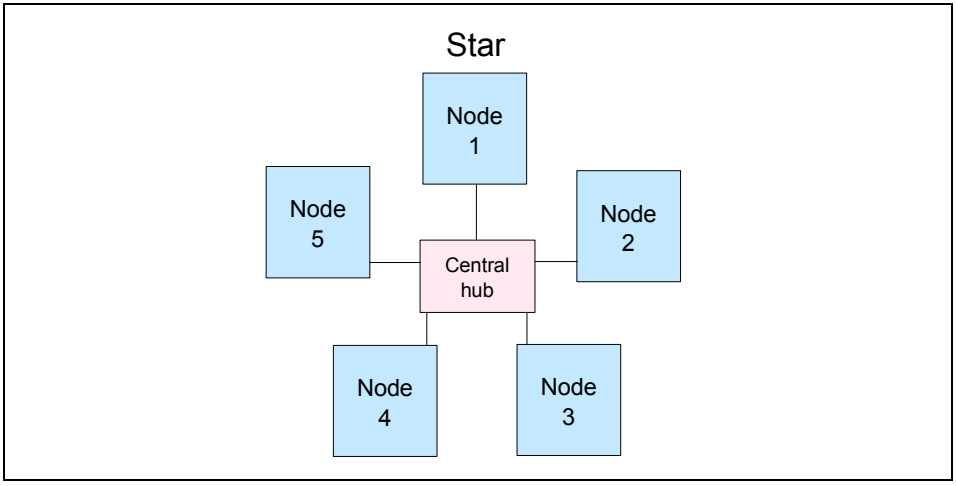


Figure 1-3 Star topology

Today, Ethernet topologies are predominant. International Data Corporation (IDC) estimates more than 85% of all installed network connections worldwide are Ethernet. It is popular due to its simplicity, affordability, scalability, and manageability. Ethernet includes definitions of protocols for addressing, formatting and sequencing of data transmissions across the network and also describes the physical media (cables) used for the network.

1.3 Open Systems Interconnection (OSI) model

The Open Systems Interconnection (OSI) model describes the layers in the network required for communication between computers. OSI is a seven layered model illustrated with the Internet protocol suite (or stack) in Figure 1-4. Each layer is responsible for a certain set of tasks associated with moving data across the network. Most Ethernet networks (including ours) communicate using the TCP/IP protocol. In this section, we discuss TCP/IP and how it relates to the OSI model, since it is the default communication protocol for the IBM TotalStorage NAS Gateway 500.

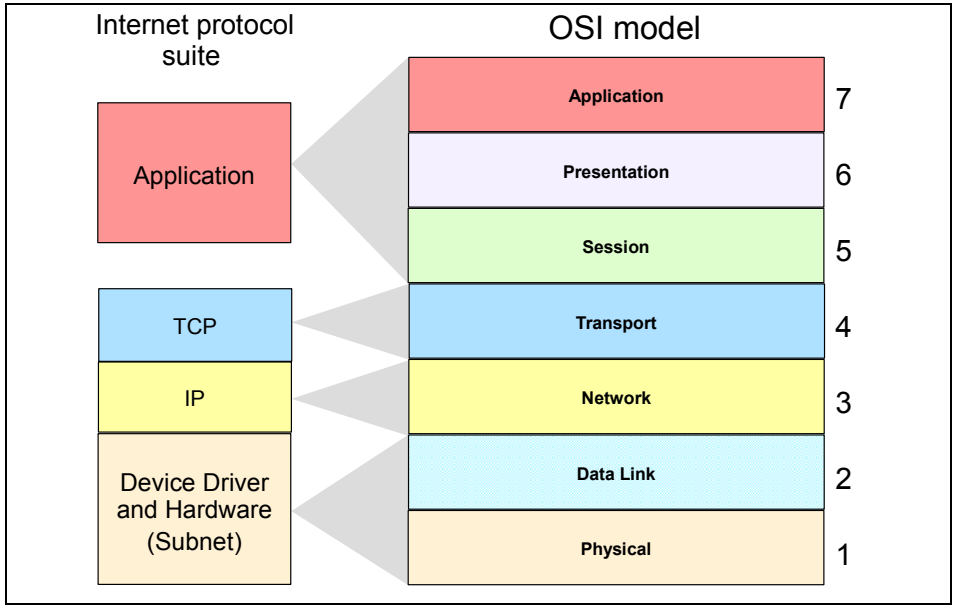


Figure 1-4 Comparing the Internet protocol suite with the OSI reference model

1.3.1 Device driver and hardware layer

Also called the Subnet layer, the device driver and hardware layer comprises both the physical and data link layers of the OSI model. It is considered the hardware that is part of each node on the network. The hardware handles the electrical and mechanical aspects of data transfers, moving the bits across a physical link. The data link layer packages packets of data into frames, ensures that they arrive safely to the target destination, and encompasses error detection and correction.

1.3.2 Internet Protocol layer

In the OSI model, the Network layer finds the best route through the network to the target destination. It has little to do in a single discrete LAN; but in a larger network with subnets, or access to WANs, the Network layer works with the various routers, bridges, switches, gateways, and software, to find the best route for data packets.

The Internet Protocol (IP) layer in the Internet protocol suite performs the functions of the network layer. It is the common thread running through the Internet and most LAN technologies, including Ethernet. It is responsible for moving data from one host to another, using various “routing” algorithms. Layers above the network layer break a data stream into chunks of a predetermined size, known as packets or datagrams. The datagrams are then sequentially passed to the IP layer.

The job of the IP layer is to route these packets to the target destination. IP packets consist of an IP header, together with the higher level TCP protocol and the application datagram. IP knows nothing about the TCP and datagram contents. Prior to transmitting data, the network layer might further subdivide it into smaller packets for ease of transmission. When all the pieces finally reach the destination, they are reassembled by the network layer into the original datagram.

IP connectionless service

The IP is the standard that defines the manner in which the network layers of two hosts interact. These hosts may be on the same network, or reside on physically remote heterogeneous networks. IP was designed with inter-networking in mind. It provides a connectionless, best-effort packet delivery service. Its service is called connectionless because it is like the postal service rather than the telephone system.

IP packets, like telegrams or mail, are treated independently. Each packet is stamped with the addresses of the receiver and the sender. Routing decisions are made on a packet-by-packet basis. On the other hand, connection-oriented, circuit switched telephone systems explicitly establish a connection between two users before any conversation takes place. They also maintain the connection for the entire duration of conversation.

A best-effort delivery service means that packets might be discarded during transmission, but not without a good reason. Erratic packet delivery is normally caused by the exhaustion of resources, or a failure at the data link or physical layer. In a highly reliable physical system such as an Ethernet LAN, the best-effort approach of IP is sufficient for transmission of large volumes of information. However, in geographically distributed networks, especially the Internet, IP delivery is insufficient. It needs to be augmented by the higher-level TCP protocol to provide satisfactory service.

The IP packet

All IP packets or datagrams consist of a header section and a data section (payload). The payload may be traditional computer data, or it may, commonly today, be digitized voice or video traffic. Using the postal service analogy again, the “header” of the IP packet can be compared with the envelope and the “payload” with the letter inside it. Just as the envelope holds the address and information necessary to direct the letter to the desired destination, the header helps in the routing of IP packets.

The payload has a maximum size limit of 65,536 bytes per packet. It contains error and/or control protocols, like the Internet Control Message Protocol (ICMP). To illustrate control protocols, suppose that the postal service fails to find the destination on your letter. It would be necessary to send you a message indicating that the recipient's address was incorrect. This message would reach you through the same postal system that tried to deliver your letter. ICMP works the same way: It packs control and error messages inside IP packets.

IP addressing

An IP packet contains a source and a destination address. The source address designates the originating node's interface to the network, and the destination address specifies the interface for an intended recipient or multiple recipients (for broadcasting).

Every host and router on the wider network has an address that uniquely identifies it. It also denotes the sub-network on which it resides. No two machines can have the same IP address. To avoid addressing conflicts, the network numbers are assigned by an independent body.

The network part of the address is common for all machines on a local network. It is similar to a postal code, or zip code, that is used by a post office to route letters to a general area. The rest of the address on the letter (that is, the street and house number) are relevant only within that area. It is only used by the local post office to deliver the letter to its final destination.

The host part of the IP address performs a similar function. The host part of an IP address can further be split into a sub-network address and a host address.

Time to Live (TTL)

The IP packet header also includes Time to Live (TTL) information that is used to limit the life of the packet on the network. It includes a counter that is decremented each time the packet arrives at a routing step. If the counter reaches zero, the packet is discarded.

1.3.3 TCP layer

The transport layer is responsible for ensuring delivery of the data to the target destination, in the correct format in which it was sent. In the event of problems on the network, the Transport layer finds alternative routes. It is also responsible for delivering the sequence of packets in the correct order. In the Internet protocol suite, the protocol operating in the transport layer is the Transmission Control Program (TCP).

The application data has no meaning to the Transport layer. On the source node, the transport layer receives data from the application layer and splits it into data packets or chunks. The chunks are then passed to the network layer. At the destination node, the transport layer receives these data packets and reassembles them before passing them to the appropriate process or application.

The Transport layer is the first end-to-end layer of the TCP/IP stack. This characteristic means that the transport layer of the source host can communicate directly with its peer on the destination host, without concern about 'how' data is moved between them. These matters are handled by the network layer. The layers below the transport layer understand and carry information required for moving data across links and subnetworks.

In contrast, at the transport layer or above, one node can specify details that are only relevant to its peer layer on another node. For example, it is the job of the transport layer to identify the exact application to which data is to be handed over at the remote end. This detail is irrelevant for any intermediate router. But it is essential information for the transport layers at both ends.

1.3.4 Application layer

The functions of the Session, Presentation, and Application layers of the OSI model are all combined in the Application layer of the Internet protocol suite. It encompasses initial logon, security, final termination of the session, interpretation services (compression, encryption, or formatting), and delivery of the network messages to the end user program.

The Application layer is the layer with which end users normally interact. It is responsible for formatting the data so that its peers can understand it. Whereas the lower three layers are usually implemented as a part of the OS, the application layer is a user process. Some application-level protocols that are included in most TCP/IP implementations, include:

- Telnet for remote login
- File Transfer Protocol (FTP) for file transfer
- Simple Mail Transfer Protocol (SMTP) for mail transfer

1.3.5 Protocol suites

A protocol suite (or protocol stack), as we saw in the Internet protocol suite, is organized so that the highest level of abstraction resides at the top layer. For example, the highest layer may deal with streaming audio or video frames, whereas the lowest layer deals with raw voltages or radio signals. Every layer in a suite builds upon the services provided by the layer immediately below it.

Note: You may see the different terms Internet protocol suite, *TCP/IP suite*, or *TCP/IP stack*. These are simply names for the same thing, the group of network layers to describe how two nodes on the Internet communicate.

The terms protocol and service are often confused. A *protocol* defines the exchange that takes place between identical layers of two hosts. For example, in the IP suite, the transport layer of one host talks to the transport layer of another host using the TCP protocol. A *service*, on the other hand, is the set of functions that a layer delivers to the layer above it. For example, the TCP layer provides a reliable byte-stream service to the application layer above it.

Each layer adds a header containing layer-specific information to the data packet. A header for the network layer might include information such as source and destination addresses. The process of appending headers to the data is called encapsulation. Figure 1-5 shows how data is encapsulated by various headers. During de-encapsulation the reverse occurs; the layers of the receiving stack extract layer-specific information and process the encapsulated data accordingly. The process of encapsulation and de-encapsulation increases the overhead involved in transmitting data.

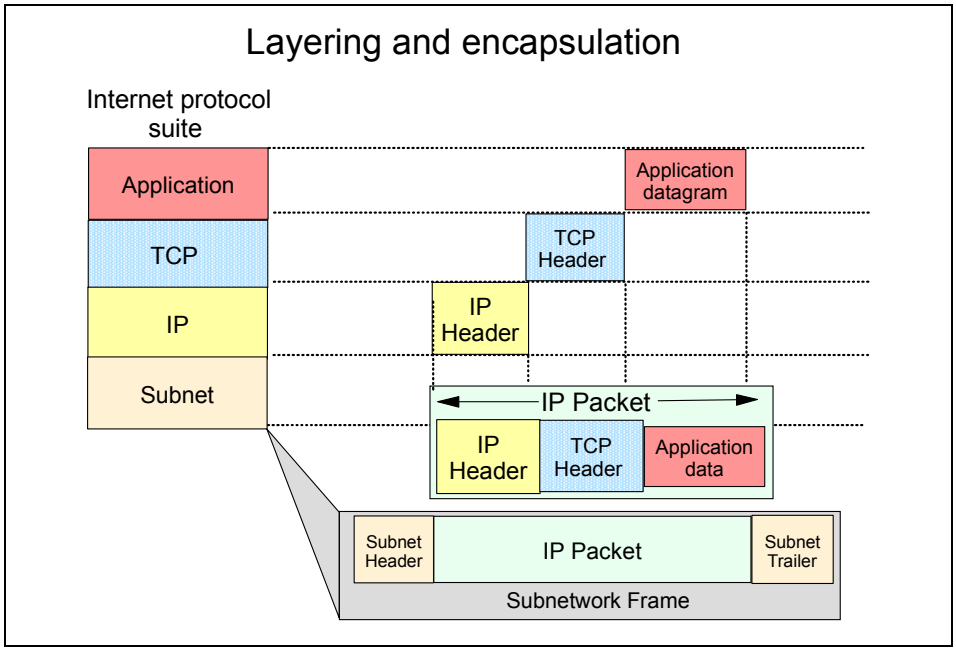


Figure 1-5 Layering and encapsulation

1.4 File systems and I/O

In this section we describe the most common file level protocols and attempt to untangle the confusion surrounding the various I/O concepts.

1.4.1 Network file system protocols

The two most common file level protocols used to share files across networks are Network File System (NFS) for UNIX and Common Internet File System (CIFS) for Windows. Both are network based client/server protocols which enable hosts to share resources across a network using TCP/IP. Users manipulate shared files, directories, and devices such as printers, as if they were locally on or attached to the user's own computer. The IBM TotalStorage NAS Gateway 500 is designed to support both NFS and CIFS. CIFS is an optional feature.

Network File System (NFS)

NFS servers make their file systems available to other systems in the network by *exporting* directories and files over the network. Once exported, an NFS client can then “mount” a remote file system from the exported directory location. NFS controls access by giving client-system level user authorization based on the assumption that a user who is authorized to the system must be trustworthy. Although this type of security is adequate for some environments, it is open to abuse by anyone who can access a UNIX system via the network.

For directory and file level security, NFS uses the UNIX concept of file permissions with *User* (the owner’s ID), *Group* (a set of users sharing a common ID), and *Other* (meaning all other user IDs). For every NFS request, the IDs are verified against the UNIX file permissions.

NFS is a *stateless* service. Therefore, any failure in the link will be transparent to both client and server. When the session is re-established the two can immediately continue to work together again.

NFS handles file locking by providing an *advisory lock* to subsequent applications to inform them that the file is in use by another application. The ensuing applications can decide if they want to abide by the lock request or not. This has the advantage of allowing any UNIX application to access any file at any time, even if it is in use. The system relies on “good neighbor” responsibility which, though often convenient, clearly is not foolproof. This is avoided by using the optional Network Lock Manager (NLM). It provides file locking support to prevent multiple instances of open files.

Common Internet File System (CIFS)

Another method used to share resources across a network uses CIFS, which is a protocol based on Microsoft’s Server Message Block (SMB) protocol. Using CIFS, servers create *file shares* which are accessible by authorized clients. Clients subsequently connect to the server’s shares to gain access to the resource.

Security is controlled at both the user and share level. Client authentication information is sent to the server before the server will grant access. CIFS uses access control lists that are associated with the shares, directories, and files, and authentication is required for access.

A *session* in CIFS is oriented and *stateful*. This means that both client and server share a history of what is happening during a session, and they are aware of the activities occurring. If there is a problem, and the session has to be re-initiated, a new authentication process must be completed.

CIFS employs opportunistic locks *(oplocks)* to control file access. Depending on the type of locking mechanism required by the client, CIFS offers nodes the ability to cache read or write data from the file being accessed to improve network performance. Exclusive rights to the file prevents other nodes on the network from gaining access to that file until it is closed. During a CIFS session the lock manager has historical information concerning which client has opened the file, for what purpose, and in which sequence.

1.4.2 Understanding I/O

A major source of confusion regarding NAS is the concept of *File I/O* versus *Block I/O*. We try to shed a little light on this subject here. Understanding the difference between these two forms of data access is crucial to realizing the potential benefits of any SAN-based or NAS-based solution.

When a partition on a hard drive is under the control of an operating system (OS), the OS will format it. Formatting of the partition occurs when the OS lays a file system structure on the partition. This file system is what enables the OS to keep track of where it stores data. The file system is an addressing scheme the OS uses to map data on the partition. Now, when you want to get to a piece of data on that partition, you must request the data from the OS that controls it.

For example, suppose that Windows 2000 formats a partition (or drive) and maps that partition to your system. Every time you request to open data on that partition, your request is processed by Windows 2000. Since there is a file system on the partition, it is accessed via File I/O. Additionally, you cannot request access to just the last 10 KB of a file. You must open the entire file, which is another reason that this method is referred to as File I/O.

Block I/O (raw disk) is handled differently: There is no OS format done to lay out a file system on the partition. The addressing scheme that keeps up with where data is stored is provided by the application using the partition. An example of this would be DB2® using its tables to keep track of where data is located rather than letting the OS do that job. That is not to say that DB2 cannot use the OS to keep track of where files are stored. It is just more efficient, for the database to bypass the cost of requesting the OS to do that work.

Using File I/O is like using an accountant. Accountants are good at keeping up with your money for you, but they charge you for that service. For your personal checkbook, you probably want to avoid that cost. On the other hand, for a corporation where many different kinds of requests are made, an accountant is a good idea. That way, checks are not written when they should not be.

When sharing files across a network, something needs to control when writes can be done. The operating system fills this role. It does not allow multiple writes at the same time, even though many write requests are made. Databases are able to control this writing function on their own so in general they run faster by skipping the OS although this depends on the efficiency of the implementation of file system and database.

For a more in-depth study of these topics, refer to the redbook, *IP Storage Networking: IBM NAS and iSCSI Solutions*, SG24-6240.

1.5 Network Attached Storage (NAS)

Storage devices which optimize the concept of file sharing across the network have come to be known as Network Attached Storage (NAS). NAS solutions utilize the mature Ethernet IP network technology of the LAN. Data is sent to and from NAS devices over the LAN using TCP/IP.

By making storage devices LAN addressable, the storage is freed from its direct attachment to a specific server and any-to-any connectivity is facilitated using the LAN fabric. In principle, any user running any operating system can access files on the remote storage device. This is done by means of a common network access protocol, for example, NFS for UNIX servers, and CIFS for Windows servers.

A storage device cannot just attach to a LAN. It needs intelligence to manage the transfer and the organization of data on the device. The intelligence is provided by a dedicated server to which the common storage is attached. It is important to understand this concept. NAS comprises a server, an operating system, plus storage which is shared across the network by many other servers and clients. So NAS is a *device*, rather than a *network infrastructure*, and shared storage is either internal to the NAS device or attached to it.

1.5.1 File servers

Early NAS implementations in the late 1980s used a standard UNIX or NT server with NFS or CIFS software to operate as a remote file server. In such implementations, clients and other application servers access the files stored on the remote file server, as though the files are located on their local disks. The location of the file is transparent to the user.

Several hundred users could work on information stored on the file server, each one unaware that the data is located on another system. The file server has to manage I/O requests accurately, queuing as necessary, fulfilling the request and returning the information to the correct initiator. The NAS server handles all aspects of security and lock management. If one user has the file open for updating, no-one else can update the file until it is released. The file server keeps track of connected clients by means of their network IDs, addresses, and so on.

1.5.2 Designated Network Attached Storage

More recent developments use application specific, specialized, “thin server” configurations with customized operating systems, usually comprising a stripped down UNIX kernel, reduced Linux OS, a specialized Windows 2000 kernel, or a specialized AIX/UNIX system as with the IBM TotalStorage NAS products. In these reduced operating systems, many of the server operating system functions are not supported. The objective is to improve performance and reduce costs by eliminating unnecessary functions normally found in the standard hardware and software. Some NAS implementations also employ specialized data mover engines and separate interface processors in efforts to further boost performance.

These specialized file servers with a reduced OS are typically known as NAS systems, describing the concept of an application specific system. NAS products, like the IBM TotalStorage NAS Gateway 500, typically come with pre-configured software and hardware, and with no monitor or keyboard for user access. This is commonly termed a “headless” system. A storage administrator accesses the systems and manages the disk resources from a remote console.

One of the typical characteristics of a NAS product is its ability to be installed rapidly using minimal time and effort to configure the system. It is integrated seamlessly into the network as shown in Figure 1-6. This approach makes NAS products especially attractive when lack of time and skills are elements in the decision process.

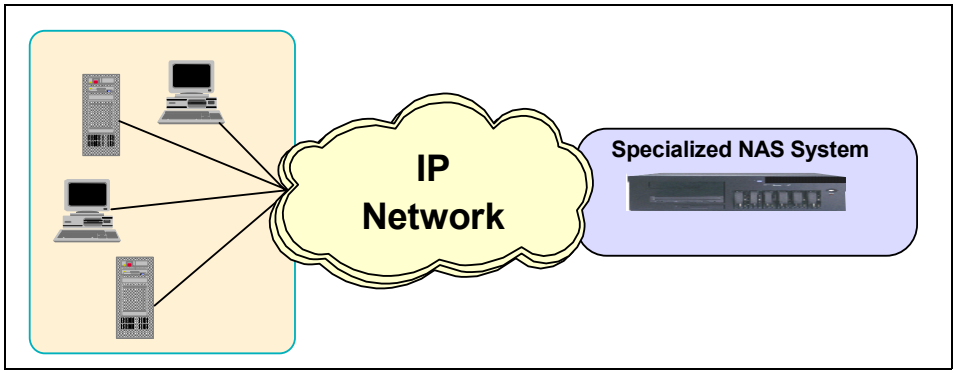


Figure 1-6 The role of NAS in your storage network

So, a NAS system is an easy-to-use device, which is designed for a specific function, such as serving files to be shared among multiple clients. It performs this task very well. It is important to recognize this fact when selecting a NAS solution. The NAS system is not a general purpose server, and should not be used (indeed, due to its specialized OS, probably cannot be used) for general purpose server tasks. However, it does provide a good solution for appropriately selected shared storage applications.

1.5.3 NAS uses File I/O

One of the key differences of a NAS disk device, compared to direct access storage (DAS) is that all I/O operations use file level I/O protocols. File I/O is a high level type of request that, in essence, specifies only the file to be accessed, but does not directly address the storage device. This is done later by other operating system functions in the remote NAS system.

A File I/O request specifies the file and the offset into the file. For instance, the I/O may specify “Go to byte ‘1000’ in the file (as if the file was a set of contiguous bytes), and read the next 256 bytes beginning at that position”. Unlike Block I/O, there is no awareness of a disk volume or disk sectors in a File I/O request. Inside the NAS system, the operating system keeps track of where files are located on disk. The OS issues a Block I/O request to the disks to fulfill the File I/O read and write requests it receives.

Network access methods, NFS and CIFS, can only handle File I/O requests to the remote file system. I/O requests are packaged by the node initiating the I/O request into packets to move across the network. The remote NAS file system converts the request to Block I/O and reads or writes the data to the NAS disk storage. To return data to the requesting client application, the NAS system software re-packages the data in TCP/IP protocols to move it back across the network. This is illustrated in Figure 1-7.

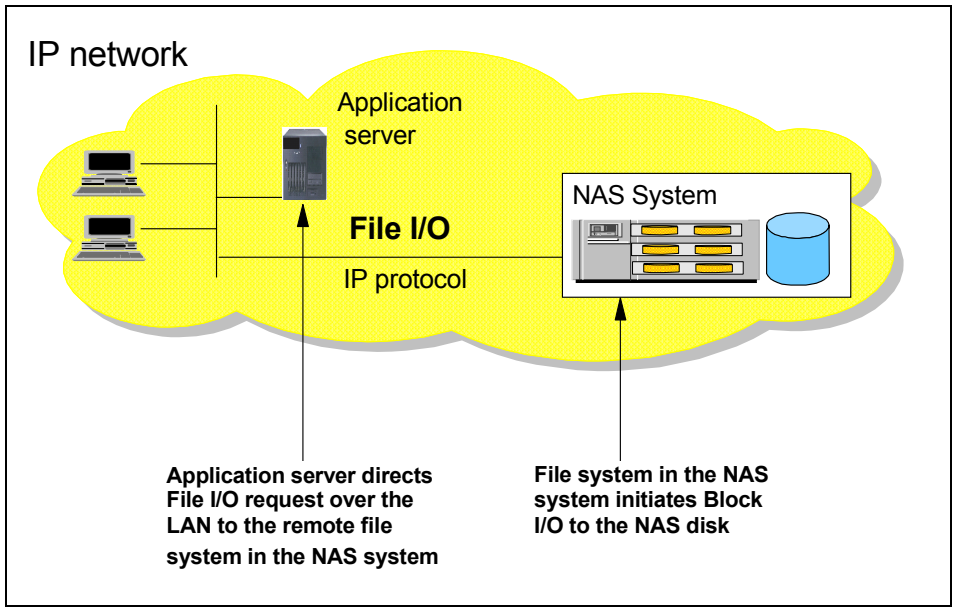


Figure 1-7 NAS devices use File I/O

1.5.4 NAS benefits

NAS offers a number of benefits that address some of the limitations of directly attached storage devices, and that overcome some of the complexities associated with SANs.

Resource pooling

A NAS product enables disk storage capacity to be consolidated and pooled on a shared network resource, at great distances from the clients and servers which will share it. Thus a NAS device can be configured as one or more file systems, each residing on specified disk volumes. All users accessing the same file system are assigned space within it on demand. This contrasts with individual DAS storage, when some users may have too little storage, and others may have too much.

Consolidation of files onto a centralized NAS device can minimize the need to have multiple copies of files spread on distributed clients. Thus overall hardware costs can be reduced.

NAS pooling can reduce the need to physically reassign capacity among users. The results can be lower overall costs through better utilization of the storage, lower management costs, increased flexibility, and increased control.

Exploits existing infrastructure

Because NAS utilizes the existing LAN infrastructure, there are minimal costs of implementation. Introducing a new network infrastructure, such as a Fibre Channel SAN, can incur significant hardware costs. In addition, new skills must be acquired, and a project of any size will need careful planning and monitoring to bring it to completion.

Simple to implement

Because NAS devices attach to mature, standard LAN implementations, and have standard LAN addresses, they are typically extremely easy to install, operate, and administer. This plug-and-play operation results in lower risk, ease of use, and fewer operator errors, all of which contributes to lower costs of ownership.

Enhanced choice

The storage decision is separated from the server decision, thus enabling the buyer to exercise more choice in selecting equipment to meet the business needs.

Connectivity

LAN implementation allows any-to-any connectivity across the network. NAS products may allow for concurrent attachment to multiple networks, thus supporting many users.

Scalability

NAS products can scale in capacity and performance within the allowed configuration limits of the individual system. However, this may be restricted by considerations such as LAN bandwidth constraints, and the need to avoid restricting other LAN traffic.

Heterogeneous file sharing

Remote file sharing is one of the basic functions of any NAS product. Multiple client systems can have access to the same file. Access control is serialized by NFS or CIFS. Heterogeneous file sharing may be enabled by the provision of translation facilities between NFS and CIFS, as with the NAS Gateway 500.

Improved manageability

By providing consolidated storage, which supports multiple application systems, storage management is centralized. This enables a storage administrator to manage more capacity on a system than typically would be possible for distributed, directly attached storage.

Enhanced backup

NAS system backup is a common feature of most popular backup software packages. For instance, the IBM TotalStorage NAS Gateway 500 provides IBM Tivoli Storage Manager client software support. Some NAS systems have some integrated advanced backup and restore features such as Split-Mirror backup, **backsnap** and **snapback** commands. This enables multiple point-in-time copies of files to be created on disk, which can be used to make backup copies to tape in the background. This is similar in concept to features such as the IBM snapshot function on the IBM RAMAC® Virtual Array (RVA).

1.5.5 Other NAS considerations

On the converse side of the storage network decision, you need to take into consideration the following factors regarding NAS solutions.

Proliferation of NAS devices

Pooling of NAS resources can only occur within the capacity of the individual NAS system. As a result, in order to scale for capacity and performance, there is a tendency to grow the number of individual NAS systems over time, which can increase hardware and management costs.

Software overhead impacts performance

As we explained earlier, TCP/IP is designed to bring data integrity to Ethernet-based networks by guaranteeing data movement from one place to another. The trade-off for reliability is a software intensive network design which requires significant processing overheads, which can consume more than 50% of available processor cycles when handling Ethernet connections. This is not normally an issue for applications such as Web-browsing, but it is a drawback for performance intensive storage applications.

Consumption of LAN bandwidth

Ethernet LANs are tuned to favor short burst transmissions for rapid response to messaging requests, rather than large continuous data transmissions. Significant overhead can be imposed to move large blocks of data over the LAN. The maximum packet size for Ethernet is 1518 bytes. A 10 MB file has to be segmented into more than 7000 individual packets. Each packet is sent separately to the NAS device by the Ethernet collision detect access method. As a result, network congestion may lead to reduced or variable performance.

Data integrity

The Ethernet protocols are designed for messaging applications, so data integrity is not of the highest priority. Data packets may be dropped without warning in a busy network, and have to be resent. Since it is up to the receiver to detect that a data packet has not arrived, and to request that it be resent, this can cause additional network traffic.

With NFS file sharing there are some potential risks. Security controls can fairly easily be by-passed. This may be a concern for certain applications. Also the NFS file locking mechanism is not foolproof, so that multiple concurrent updates could occur in some situations.

Impact of backup/restore applications

One of the potential downsides of NAS is the consumption of substantial amounts of LAN bandwidth during backup and restore operations, which may impact other user applications. NAS devices may not suit applications which require very high bandwidth. To overcome this limitation, some users implement a dedicated IP network for high data volume applications, in addition to the messaging IP network. This can add significantly to the cost of the NAS solution.

1.5.6 Total cost of ownership

Because it makes use of both existing LAN network infrastructures and network administration skills already employed in many organizations, NAS costs may be substantially lower than for directly attached or additional SAN-attached storage. Specifically, NAS-based solutions offer the following cost-reducing benefits:

- They reduce administrative staff requirements.
- They improve reliability and availability.
- They bridge the gap between UNIX and Windows environments.

Reduced administrative staff requirements

Implementing single or clustered NAS systems to manage your networked storage concentrates the administrative tasks and thereby reduces the number of people required to maintain the network. Since the NAS system is a headless system, administration is usually performed via a Web-based GUI interface accessible from anywhere on the network. In addition, more capacity can be managed per administrator, thus resulting in a lower cost of ownership.

Improved reliability and availability

In today's business world, it has become the de facto standard to provide clients with access to information 24 hours per day, 7 days per week, allowing very little time available for unplanned outages. The IBM TotalStorage NAS Gateway 500 offers the ability to provide excellent availability with options for clustered models.

Bridges the gap between UNIX and Windows environments

Most companies today contain heterogeneous operating environments. A NAS solution offers clients the ability for true cross-platform file sharing between Windows and UNIX clients by offering support for CIFS and NFS. This becomes increasingly important when application data becomes more common across platforms.

1.6 Industry standards

There is a clear client need for standardization within the storage networking industry to allow users to freely select equipment and solutions, knowing that they are not tying themselves to a proprietary or short term investment. To this end, there are extensive efforts among the major vendors in the storage networking industry to cooperate in the early agreement, development, and adoption of standards. A number of industry associations, standards bodies, and company groupings are involved in developing and publishing storage networking standards. The most important of these are the Storage Networking Industry Association (SNIA) and the Internet Engineering Task Force (IETF).

In addition, IBM, IBM Business Partners, and other major vendors in the industry, have invested heavily in inter-operability laboratories. The IBM laboratories in Gaithersburg (Maryland, USA), Mainz (Germany), and Tokyo (Japan) are actively testing equipment from IBM and many other vendors, to facilitate the early confirmation of compatibility between multiple vendors servers, storage, and network hardware and software components.

1.6.1 Storage Networking Industry Association

The Storage Networking Industry Association (SNIA) is an international computer industry forum of developers, integrators, and IT professionals who evolve and promote storage networking technology and solutions. SNIA was formed to ensure that storage networks become efficient, complete, and trusted solutions across the IT community.

SNIA is accepted as the primary organization for the development of SAN and NAS standards, with over 150 companies and individuals as its members, including all the major server, storage, and fabric component vendors. SNIA is committed to delivering architectures, education, and services that will propel storage networking solutions into a broader market.

IBM is one of the founding members of SNIA, and has senior representatives participating on the board and in technical groups. For additional information on the various activities of SNIA, see its Web site at:

http://www.snia.org

1.6.2 Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (for example, routing, transport, and security).

For more information on the IETF and its work groups, refer to:

http://www.ietf.org

2

Products overview

This chapter provides a brief overview of each of the IBM products used during the development of this redbook. The IBM Enterprise Storage Server® (ESS), the IBM Fibre Array Storage Technology (FAStT) and the IBM SAN Fibre Channel Switch. The hardware configurations of each of the products used in our environment are not covered here, but are addressed in the subsequent chapters.

2.1 IBM TotalStorage NAS Gateway 500

The new IBM TotalStorage NAS Gateway 500 is part of the overall IBM Storage Networking offering of hardware, software, and services. IBM network attached storage (NAS) products provide you with additional building blocks to increase the flexibility, efficiency, and effectiveness of your storage networking solutions.

The IBM TotalStorage NAS Gateway 500 provides network file serving. It allows client computer systems residing on a traditional Internet Protocol (IP) communications network to access disk storage residing on a Fibre Channel Storage Area Network (SAN). It does this by supporting network file protocols such as Network File System (NFS), Common Internet File System (CIFS), Hypertext Transmission Protocol (HTTP), and File Transfer Protocol (FTP). It receives file requests from client computer systems on the communications network using these network file protocols and satisfies these requests by accessing the disk storage on the SAN. In addition, it supports the IBM TotalStorage SAN Volume Controller and the IBM TotalStorage SAN Integration Server.

The NAS Gateway 500 is an optimized, high performance server designed to provide shared data to both clients and servers in Windows, UNIX, and mixed environments. Attached directly to both the LAN and the SAN, the NAS Gateway 500 off-loads general file sharing from other servers, freeing those servers to handle more resource-intensive application processing. Adding the NAS Gateway 500 to the LAN and SAN does not affect any other systems in either of these networks, and upgrading other servers, clients, or applications does not impact the NAS Gateway 500.

The NAS Gateway 500 is a specialized NAS device acting as a high-bandwidth conduit. It connects LAN-attached clients and servers to the SAN through high-speed Fibre Channel paths.

The NAS Gateway 500 can be a valuable addition to your storage network strategy because:

- It is easy to use and install.
- It is a headless device — it requires no keyboard, mouse, or display to configure and maintain.
- It supports CIFS, NFS, FTP, and HTTP.
- It has a Snap Shot function for point-in-time backups.
- It includes Web-based GUI administration tools as well as a command line interface.

2.1.1 NAS Gateway 500 connectivity

The NAS Gateway 500 comes shipped with standard hardware. Since the NAS Gateway 500 is a NAS device designed for a specific purpose, it is equipped with the hardware required to integrate it directly into your network. There is optional hardware available to improve performance, connectivity, and availability.

The NAS Gateway 500 is designed to work in heterogeneous environments right out of the box. Figure 2-1 visually demonstrates how the built-in features of the NAS Gateway 500 allow it to plug into almost any environment.

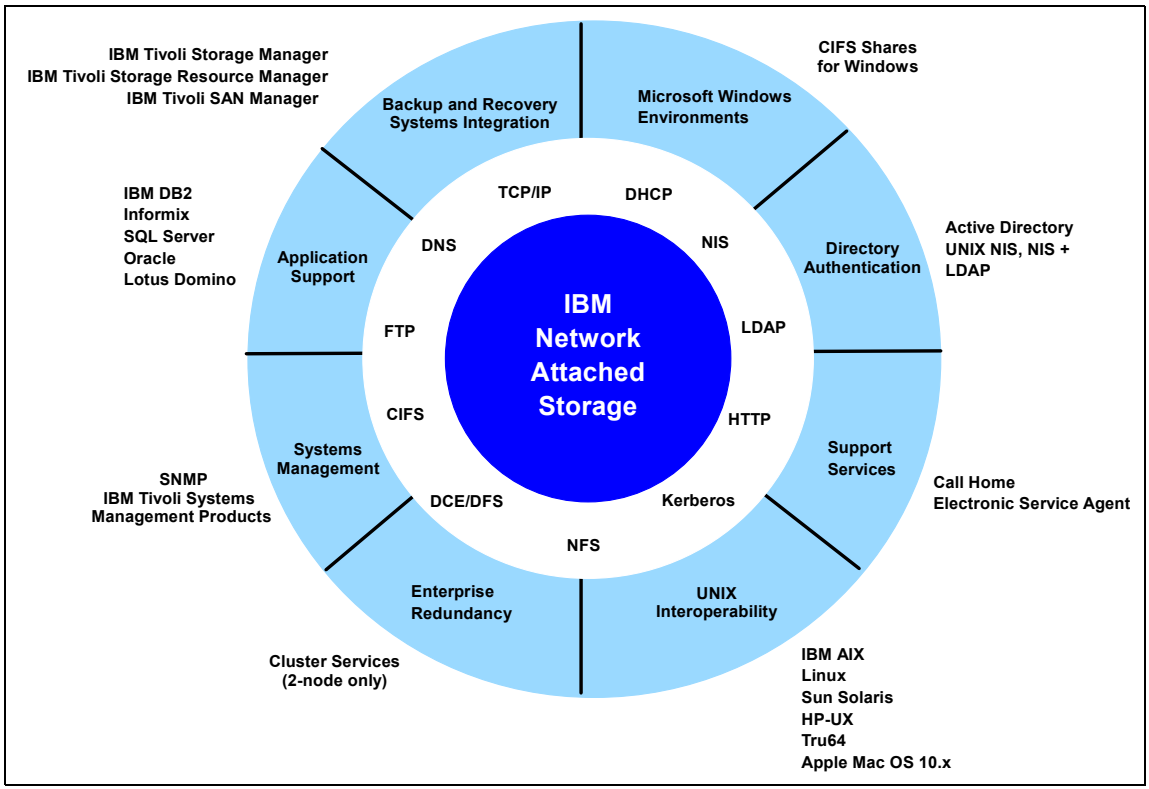


Figure 2-1 Visualization of features of the NAS Gateway 500

2.1.2 IBM NAS Gateway 500 sample storage connectivity

The NAS Gateway 500 supports connectivity to a variety of IBM storage products. Figure 2-2 shows sample connectivity between the NAS Gateway 500 and the ESS, FAStT, or the SAN Volume Controller. The NAS Gateway 500 can attach one storage type at a time.

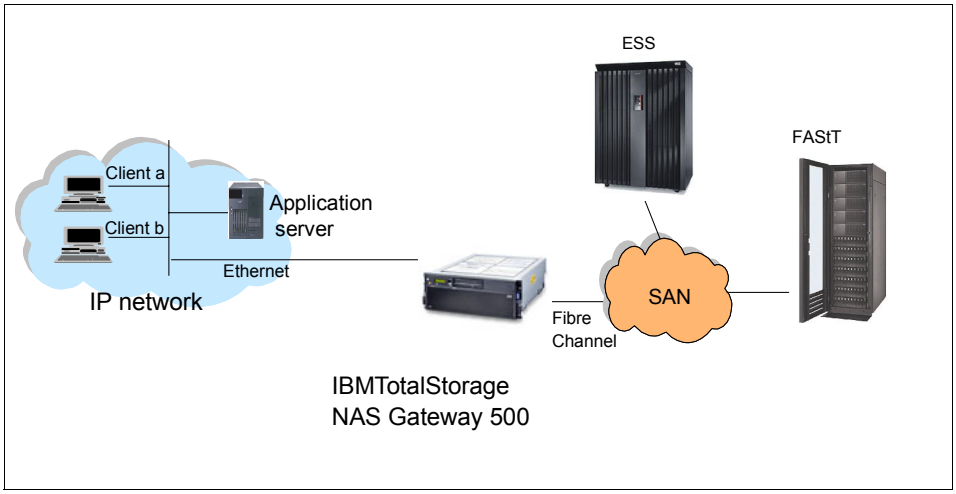


Figure 2-2 NAS Gateway 500 connectivity with ESS, or FAStT

The NAS Gateway 500 high-speed system connects your Ethernet LAN to storage resources on your SAN. These are high-performance models which are designed to link application servers, transaction servers, file servers, and end-user clients to storage resources located on the SAN, 24 hours a day, 7 days a week.

2.1.3 NAS Gateway 500 features

The NAS Gateway 500 is a rack-mounted storage server that connects LAN servers and clients to a storage area network (SAN) and allocates storage on approved SAN devices. It is capable of operating in a single-node (one server) configuration or dual-node (two servers) clustered configuration. The internal disk storage is for the operating system and associated software.

The NAS Gateway 500 is meant to be utilized with an intelligent disk storage subsystem, such as the IBM Fibre Array Storage Technology (FAStT) product line or the IBM Enterprise Storage Server (ESS) product line. The back-end disk storage subsystem is separate from the NAS Gateway 500 and provides the disk storage for client data.

The NAS Gateway 500 supports the attachment of:

- IBM FAStT product line
- IBM Enterprise Storage Server
- IBM TotalStorage SAN Volume Controller
- IBM TotalStorage SAN Integration Server

The amount of storage that can be attached to the NAS Gateway 500 is only limited by the amount of storage supported by a single disk storage subsystem. For FAStT900 that amount is 56 TB. For Enterprise Storage Server, Model 700, that amount is 32.8 TB.

2.1.4 Hardware components

The NAS Gateway 500 is a rack-mounted device occupying 4 rack units (see Figure 2-3). The base hardware contains a number of design features that increase reliability and availability, including hot-swappable redundant power supplies, redundant cooling, hot-plug PCI-X adapters, Predictive Failure Analysis®, a dedicated service processor to monitor the main processors, extended error handling on the PCI bus, and redundant CPUs with dynamic processor deallocation that allows a processor to be taken offline without a reboot. It is also possible to order multiple adapters to provide redundant data paths. All memory is error correcting.

Figure 2-3 NAS Gateway 500 front view

The basic hardware building block is a Node (Engine). Each node can have two or four processors, and these are referred to as 2-way or 4-way processors.The processor books are mechanical assemblies that contain a two-way processor card. The two 1.45Ghz Power 4+ processors on this card share a common 1.44 MB L2 cache and share a common 8 MB L3 cache. Single Nodes can be clustered into Dual Node systems, but a Dual Node system should not be confused with a 2-way processor.

Memory (each engine)

- 16 GB for a two-way system (4 GB minimum)
- 32 GB for a four-way system (8 GB minimum)

Hard disk drives (HDDs)

- One or two Ultra 160 10,000 rpm 36.4 GB hard disk drives. Only one drive is used if mirroring feature code is not installed. Otherwise, two hard disk drive bays are used. Hard disk drives are used for the operating system and application programs such as UPS shutdown programs.

Adapters

- 1-Port Gigabit Ethernet SX Adapter 1000 Mbps
- 2-Port Gigabit Ethernet SX Adapter 1000 Mbps
- 1-Port Gigabit Ethernet TX Adapter 10/100/1000 Mbps
- 2-Port Gigabit Ethernet TX Adapter 10/100/1000 Mbps
- 1-Port 2 Gigabit Fibre Channel HBA
- 2-Port 2 Gigabit Fibre Channel HBA

Interoperability

Connection to the disk storage subsystem can be made directly from the NAS Gateway 500 to storage controllers, or can be made through Fibre Channel switches or directors. While using clustering, no direct connection can be used. The following switches and directors are supported:

- Cisco MDS 9216 Multilayer Fabric Switch (IBM 2062 Model D01)
- Cisco MDS 9509 Multilayer Directors (IBM 2062, Models D07 and T07)
- CNT FC/9000 Fibre Channel Directors (2042 Models 001, 128, and 256)
- IBM TotalStorage SAN Switches (2109 Models F16, F32, M12 and 3534 Model F08)
- McDATA ED/5000 Fibre Channel Director (2032–001)
- McDATA Intrepid 6064 Enterprise Fibre Channel Director (2032-140)
- McDATA Intrepid 6140 Enterprise Fibre Channel Director (2032-064)
- McDATA Sphereon 4500 Fabric Switches (2031 Models 016, 032, 216, 224, and 232)
- Brocade SilkWorm 2400
- Brocade SilkWorm 2800
- Brocade SilkWorm 3800
- Brocade SilkWorm 3900
- Brocade 12000
- Brocade SilkWorm 2010 with full-fabric switch upgrade

2.1.5 Software components

The NAS Gateway 500 system software consists of a tightly integrated collection of system software that provides the features and functions necessary for an enterprise-class highly-scalable Network Attached Storage (NAS) gateway. These features and functions include an industrial strength operating system, a highly scalable file system, flexible user interfaces, robust data protection capabilities, storage management facilities, systems management, and performance management features.

Operating system

The NAS Gateway 500 system software utilizes the IBM AIX 5L™ 5.2B operating system. This is the IBM version of the UNIX operating system. The NAS Gateway 500 utilizes a 64-bit AIX kernel in order to leverage the 64-bit processing power of the IBM Power 4+ processor technology inside the NAS Gateway 500. The operating system provides normal operating system facilities, such as process and thread scheduling, memory (real and virtual) management, I/O management, network management, and user/group management.

File system

The NAS Gateway 500 system software utilizes the Enhanced Journaled File System (JFS2) as the underlying file system for NAS volumes. JFS2 is a highly scalable journaled file system in which changes to the metadata associated with files and directories are committed to the file system log first before being written to the file system. The file system log is used to insure the integrity and consistency of the file system at all points in time. The file system log is used in case of system failure to insure that the file system is consistent (all the internal data structures associated with the file system are consistent) when the system is restarted following a system crash or when the NAS volumes (file systems) are failed-over to another NAS Gateway 500 in a clustered high-availability configuration.

User Interfaces

The NAS Gateway 500 system software provides three user interfaces:

- Command Line Interface (CLI):

  The command line interface (CLI) provides the necessary commands to configure, monitor and manage the NAS Gateway 500. The CLI is often preferred by experienced system administrators, especially those familiar with UNIX operating systems.

- System Management Interface Tool (SMIT):

  The Systems Management Interface Tool (SMIT) provides a menu-driven environment for managing the NAS Gateway 500. The administrator is presented with a set of menus for managing specific functional areas within

the product, such as administrators, client access, networking, devices, file serving, and general system environment.

- Web-based System Manager (WebSM):

  The Web-based Systems Manager (WebSM) is a Web-based graphical user interface (GUI) for configuring, monitoring and managing the NAS Gateway 500. WebSM can be used to remotely manage one or more NAS Gateway 500s. This user interface is likely to be preferred by system administrators that are more comfortable working with a graphical user interface.

Data protection

The NAS Gateway 500 system software includes a number of features for data protection:

- Local volume mirroring
- File system snapshot and rollback capability
- NAS volume mirroring
- IBM Tivoli Storage Manager backup and recovery capability

  The system software includes the IBM Tivoli Storage Manager client and storage agent. Clients using the IBM Tivoli Storage Manager to provide distributed backup and recovery capabilities across their enterprise, can seamlessly integrate the NAS Gateway 500 into their IBM Tivoli Storage Manager environment.

Storage management

The system software includes the IBM Tivoli Storage Resource Manager agent. IBM Tivoli Storage Resource Manager is an enterprise-wide storage resource management application. Clients utilizing IBM Tivoli Storage Resource Manager for enterprise-wide storage resource management, can seamlessly integrate the NAS Gateway 500 into their IBM Tivoli Storage Resource Manager environment.

SAN management

Because the NAS Gateway 500 is a gateway product that is intended to be used in conjunction with a fibre-channel attached disk storage subsystem, it includes the IBM Tivoli Storage Area Network Manager agent. This agent works in conjunction with the IBM Tivoli SAN Manager software product to provide the client with an enterprise-wide view of their SAN.

Optional software features

The NAS Gateway 500 system software currently provides the following optional software features (please check the NAS Gateway 500 Web site for updates):

- CIFS file serving:

  The CIFS file serving optional software feature provides a CIFS file server. The CIFS file server allows client computer systems running versions of the

Windows operating system to access the file systems (shares) exported by the NAS Gateway 500 using the Microsoft Common Internet File System (CIFS). CIFS is sometimes referred to as the Server Message Block (SMB) network file protocol. If clustered, CIFS must be installed on both nodes.

- Clustering:

  The optional clustering software feature allows two NAS Gateway 500s to be clustered together in a dual-node high availability (HA) configuration. The purpose of clustering is to improve data availability, by continuing to provide access to the file systems (through network file protocols) even in the event that one of the two NAS Gateway 500s fails. The optional clustering software feature must be ordered on both of the NAS Gateway 500s being used in a dual-node high-availability clustered configuration. In addition, if you are using CIFS, the CIFS option must be ordered for both nodes.

2.1.6 NAS Gateway 500 volumes

In order to begin NAS Gateway 500 volume management, your SAN disks must be configured and defined as physical volumes ready for use in a NAS volume.

After storage has been set up and allocated using FAStT or ESS system, a NAS Gateway 500 volume can be created and configured for file serving. During the creation process, you can specify the maximum number of snapshots that will be allowed for this volume and the total percentage of the file system that should be reserved for the snapshots. Additionally, in a clustered system, you can specify which host will be the priority owner for the volume. A NAS volume can span across multiple disks. This allows users the ability to create multiple volumes for multiple purposes, with varying storage sizes.

A resource group is a set of resources handled as one unit for failover purposes. In the NAS Gateway 500, the resource group would contain the volumes, NFS exports, CIFS shares, and the IP address(es) used to access those volumes. Currently, there is one resource group associated with each node. This facility allows high-availability in the case of a node failure, such that the other node will be able to pick up the volumes associated with failed node.

Once created, the following tasks can be applied to a NAS Gateway 500 volume:

- Changing (name or owning resource group) a volume
- Deleting a volume
- Defragmenting a volume
- Exporting (remove only the definition but keep the content) a volume
- Importing an existing volume into a system
- Extending the size of a volume
- Copying a volume
- Replacing a disk within a volume

- Mounting a volume
- Unmounting a volume
- Mirroring a volume
- Unmirroring a volume
- Synchronizing a volume
- Listing NAS volumes in a system
- Viewing NAS volume statistics

The snapshot functions

The NAS Gateway 500 snapshot captures a consistent block-level image of a volume at any given point in time. The snapshot remains the same even if the source volume changes. The snapshot can then be used to create a backup of the volume. The snapshot also provides the capability to access files or directories as they were at the time of the snapshot. The snapshot can be generally viewed as a mechanism of backing up a specific NAS volume.

You can create a snapshot at a specified time or after a particular action takes place on a recurring basis. You can take individual snapshots at specific times even if no one is available to administer the NAS Gateway 500. You can take monthly, weekly, daily, or hourly snapshots. The snapshot command also has the capability of calling a separate backup command to back up the newly created snapshot immediately to a specified location in storage and then delete it.

2.1.7 NAS Gateway 500 file serving

The NAS Gateway 500 provides network file-serving capabilities by supporting the following network file protocols:

- Network File System (NFS Version 2 and 3) for predominately UNIX/Linux environments:

  The system software supports the latest NFS protocol update, NFS Version 3, and provides an NFS Version 2 client and server. The system software is, therefore, backward compatible with an existing install base of NFS clients and servers. Typically, the NAS Gateway 500 is the NFS server providing file access to other clients; however, it is also possible for the NAS Gateway 500 to be a client to another NFS server.

- Common Internet File System (CIFS) for Windows environment:

  The NAS Gateway 500 contains optional Common Internet File System (CIFS) server software to provide file sharing to Windows clients. When started, the CIFS server responds to SMB/NetBIOS requests on all operational TCP/IP interfaces. The User Mapping wizard helps you create Windows-to-UNIX username mappings, which allows Windows users to transparently access CIFS shares.

- Hypertext Transmission Protocol (HTTP):

  The NAS Gateway 500 has HTTP file sharing protocol preloaded on the system. It allows clients with a Web browser to access files stored on the NAS Gateway 500.

- File Transfer Protocol (FTP):

  The FTP file share protocol is enabled by default at system startup on the NAS Gateway 500.

2.1.8 Integrated data protection

The IBM NAS Gateway 500 helps safeguard the most valuable asset of an organization — its data — by providing features such as:

- LAN free backup support using IBM Tivoli Storage Manager
- NAS Gateway 500 dual path SAN implementation usage of SDD/RDAC
- Backup of RootVG to external storage (NIM server, tape or DVD-RAM)
- Recovery of system to manufacturing state and restoring back to pre-disaster state with **`restnasb`** and snapshot rollbacks
- User recovery of files with snapshots

The IBM Tivoli Storage Manager Client/Agent, IBM Tivoli Resource Manager Agent and IBM Tivoli SAN Manager Agent are preinstalled on the product.

2.1.9 IBM Tivoli Storage Manager integration

SAN technology provides an alternative path for data movement between the IBM Tivoli Storage Manager client and the server. Shared storage resources (disk, tape) are accessible to both the client and the server through the SAN. Data movement is off-loaded from the LAN and from the server processor and allows for greater scalability. LAN-free backups decrease the load on the LAN by introducing a Storage Agent.

For more information on IBM Tivoli Storage Manager concepts, please refer to the following IBM Redbook: *IBM Tivoli Storage Management Concepts*, SG24-4877-03, available at:

`http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg244877.html?Open`

2.1.10 High availability configuration using redundant storage

The clustering is accomplished using the High Availability Clustered Multiprocessing (HACMP) software. The dual-node clustered configuration is normally an active/active configuration. By active/active, it means that each of the NAS Gateway 500s is actively processing network file requests for the file systems (NAS Volumes) that it owns and is exporting for network file access.

Each NAS Gateway 500 is exporting a different set of file systems for network file access. In the event that one of the NAS Gateway 500s were to experience a failure, the resources (file systems, disk volumes, and IP addresses) owned by the failed node are transferred to the remaining node. Therefore, network file access to the file systems exported by the failed node continue to be processed by the remaining node. The key benefit of an active/active configuration is that both nodes are actively processing network file system requests, so each node is performing productive work

The IBM TotalStorage NAS Gateway 500 cluster is a 2-node solution serving over a single physical network, meaning that all Ethernet ports defined to the cluster must be routable to each other. If desired, both machines can be actively serving volumes in an active-active configuration, though they will not be serving the same volumes

The IBM TotalStorage NAS Gateway 500 solution uses the IP Address Takeover (IPAT) through IP Aliasing feature of HACMP 5.1 rather than traditional IPAT. IP aliasing is faster than traditional IPAT, and it allows for multiple file serving IP addresses to be assigned to the same node or even to the same Ethernet adapter. Figure 2-4 shows a typical cluster configuring including redundant fabric and storage.

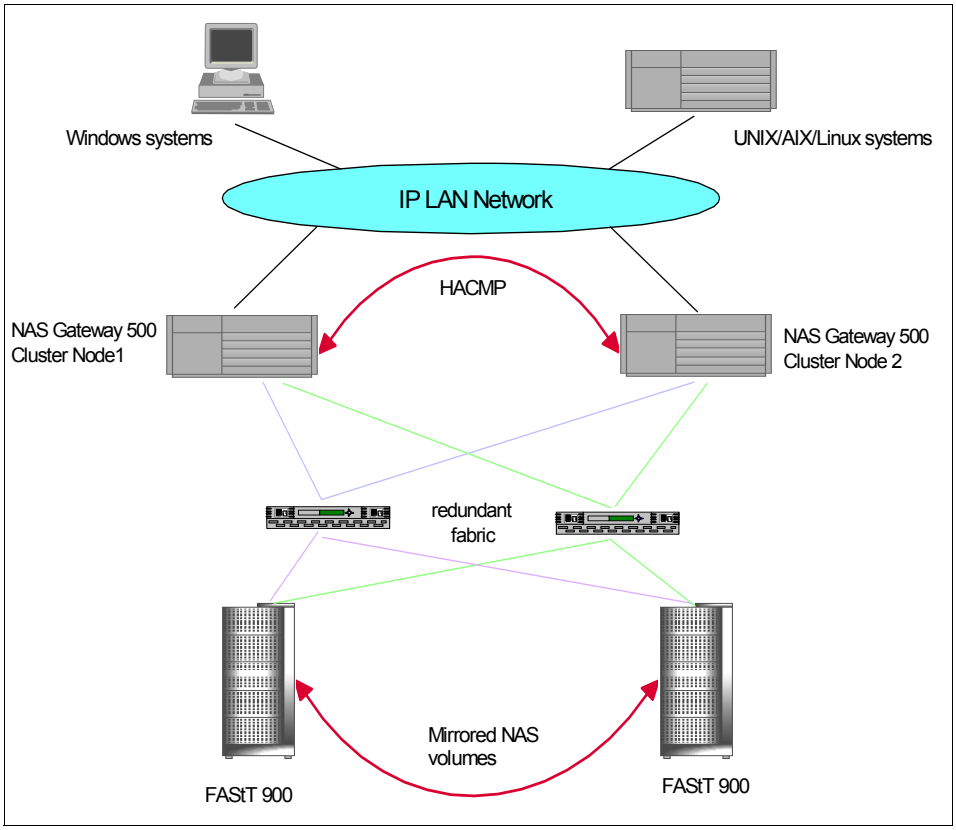


Figure 2-4 High available configuration

To keep a mirrored copy of a volume in the case of a disk failure, use the **mirvol** command. This allows the information on a NAS Volume to be synchronized on another disk or set of disks. You can have up to two mirrored copies of a NAS volume.

2.1.11 More information

You can find more information about IBM NAS Gateway 500 from these following Web sites:

http://www.storage.ibm.com/snetwork/nas/500/index.html
http://www.storage.ibm.com/snetwork/nas/index.html
http://www.storage.ibm.com/solutions/globalservices/index.html

For more information about the cluster configuration, refer to the *HACMP for AIX, Concepts and Facilities Guide* at:

http://publibfp.boulder.ibm.com/epubs/pdf/c2348640.pdf

2.2 IBM Enterprise Storage Server (ESS)

This topic provides a brief overview of the major IBM Enterprise Storage Server (ESS) components, features, and benefits. For more detailed information, please refer to the redbook, *The IBM Enterprise Storage Server*, SG24-5645, or to the product Web site:

http://www.storage.ibm.com/disk/ess/index.html

2.2.1 Overview

The IBM TotalStorage Enterprise Storage Server (ESS) Model 800 (see Figure 2-5) helps set new standards in performance, automation, and integration as well as capabilities that support continuous availability to data for the on-demand world. This storage system also supports many advanced functions, which can be critical for increasing data availability during planned outages and for protecting data from planned and unplanned outages. These advanced functions can provide important disaster recovery and backup protection.

Figure 2-5 IBM TotalStorage Enterprise Storage Server (ESS) Model 800

2.2.2 Product highlights

These are only a few of the product highlights. Again, please refer to product specific Web sites and redbooks for more details:

- Supports storage sharing for IBM @server™ pSeries® and UNIX®, Microsoft® Windows NT®, Microsoft Windows® 2000, Microsoft® Windows Server® 2003, Novell NetWare, Linux® and SGI® IRIX® platforms; IBM @server™ iSeries™ and AS/400® platforms; and IBM @server™ zSeries® and S/390® platforms.

- Supports fast data transfer rates with attached hosts via ESCON®, FICON®, Fibre Channel, 2 Gigabit Fibre Channel/FICON or Ultra SCSI
- Designed to provide outstanding performance with dual cluster RISC SMP processors, large cache and serial disk attachment
- Uses redundant hardware, mirrored write caches and RAID-5 and RAID-10 protection for "disks" to support high availability for mission critical business applications

2.3 IBM Fibre Array Storage Technology (FAStT)

This topic provides a brief overview of the major IBM FAStT components, features and benefits. For more detailed information, please refer to the redbook, *Fibre Array Storage Technology - A FAStT Introduction*, SG24-6246 or to the product Web site:

http://www.storage.ibm.com/disk/fastt/index.html

2.3.1 Overview

IBM FAStT900 Storage Server delivers breakthrough disk performance and outstanding reliability for demanding applications in compute intensive environments. The FAStT900 is designed to offer investment protection with advanced functions and flexible features. Designed for today's on-demand business needs, the FAStT900 offers up to 32TB of Fibre Channel disk storage capacity with the EXP700. FAStT900 Offers advanced replication services to support business continuance and disaster recovery. The FAStT900 is an effective storage server for any enterprise seeking performance without borders (see Figure 2-6).

Coupled with the EXP100, it allows you to configure RAID protected storage solutions of up to 56 TB to help provide economical and scalable storage for your rapidly growing application needs for limited access, data reference, and near-line storage.

Figure 2-6 IBM TotalStorage FAStT900 Storage Server

2.3.2 Product highlights

These are only a few of the many product highlights. Again, please refer to product specific Web sites and redbooks for more details:

- Data protection with dual redundant components, multiple RAID levels, LUN masking, and enhanced management options.
- Storage Consolidation for SAN, NAS, and direct-attach environments.
- Investment protection throughout the FAStT family of storage systems.
- Future releases are planned to support intermix of EXP100 and EXP700 disk drive enclosures to a FAStT900.
- Support for IBM AIX ® , Microsoft ® Windows® 2000, Windows NT® , Windows Server 2003, Novell™ Netware™, Sun Solaris , HP-UX, Red Hat Linux, VMWare, Linux IA64.
- Supports EXP700 or EXP100 drive enclosures to preserve investment in FAStT storage.
- Scales up to 32 terabytes (TB) of Fibre Channel disk capacity using flexible combinations of 18.2, 36.4, 73.4 and 146.8 GB drives with EXP700, or up to 56 terabytes (TB) of Serial ATA disk capacity with EXP100.

2.4 IBM TotalStorage SAN Switch M12

This topic provides a brief overview of the major IBM TotalStorage SAN Switch M12, features, and benefits. For more detailed information, please refer to the redbook, *Designing and Optimizing an IBM Storage Area Network Featuring the IBM 2109 and 3534*, SG24-6426-00, or to the product Web site:

http://www.storage.ibm.com/ibmsan/products/2109/m12/index.html

2.4.1 Overview

IBM TotalStorage SAN Switch M12 provides one or two 64-port, 2 Gigabit per second director with high availability features including non-disruptive CP failover and firmware activation. It provides mainframe server FICON, UNIX and Intel®-based server Fibre Channel switching for high availability, scalable large enterprise SANs with a common management system. Advanced Security can help create a secure storage network infrastructure. Fabric Manager 4.1 feature can simplify management of complex fabrics. Compatibility with the Brocade Silkworm family of switches can enable interoperability with a wide range of non-IBM server and storage devices (see Figure 2-7).

Figure 2-7 IBM TotalStorage SAN Switch M12

2.4.2 Product highlights

These are only a few of the many product highlights. Again, please refer to product specific Web sites and redbooks for more details:

- Designed to provide superior performance with up to 2 Gigabit/sec (Gbps) throughput and Inter-Switch Link (ISL) Trunking with aggregate speed up to 8 Gbps.
- High port density packaging helps save rack space.
- FICON Director switching with Open/FICON intermix and FICON cascading provides consolidated enterprise SAN infrastructure.
- High availability director, scalable from one 32-port switch to two 64-port switches with 128 ports, is designed to enable large enterprise SANs
- Intelligent fabric management simplifies deployment, management, and network growth.
- Advanced security with comprehensive, policy-based security capabilities can improve availability and simplify operation.
- Offers advanced fabric services such as end-to-end performance monitoring and fabric-wide health monitoring.

2.5 IBM TotalStorage SAN Volume Controller

This topic provides a brief overview of the major IBM TotalStorage SAN Volume Controller, features, and benefits. For more detailed information, please refer to the redbook, *IBM TotalStorage, Introducing the SAN Volume Controller and SAN Integration Server*, SG24-6423-00, or to the product Web site:

`http://www.storage.ibm.com/software/virtualization/svc/index.html`

2.5.1 Overview

The IBM TotalStorage SAN Volume Controller is designed to reduce the complexity and costs of managing storage networks. It allows users to virtualize their storage and helps increase the utilization of existing capacity and centralize the management of multiple controllers in an open-system SAN environment. The SAN Volume Controller now supports attachment to non-IBM storage systems. Now storage administrators can reallocate and scale storage capacity and make changes to more underlying storage systems without disrupting applications.

2.5.2 Product highlights

The IBM TotalStorage SAN Volume Controller is designed to:

- Provide a centralized control point for managing an entire heterogeneous SAN, including storage volumes from disparate vendor devices.
- Help optimize existing IT investment by virtualizing storage and centralizing management.
- Reduce downtime for planned and unplanned outages, maintenance and backups.
- Increase storage capacity utilization, uptime, administrator productivity and efficiency.
- Provide a single set of advanced copy and backup services for multiple storage devices.

2.6 IBM TotalStorage SAN Integration Server

This topic provides a brief overview of the major IBM TotalStorage SAN Integration Server, features, and benefits. For more detailed information, please refer to the redbook, *IBM TotalStorage, Introducing the SAN Volume Controller and SAN Integration Server*, SG24-6423-00, or to the product Web site:

`http://www.storage.ibm.com/software/virtualization/sis/index.html`

2.6.1 Overview

The SAN Integration Server is designed to help integrate IBM virtualization technology, Fibre Channel switches, and storage Redundant Array of Independent Disks (RAID) technologies into a preconfigured, comprehensive solution. Delivered and installed as a single unit, it offers upgrade options for connectivity, storage capacity, and performance levels. The solution was developed to provide the benefits of SAN with the ease of single-system manageability. SAN Integration Server will initially be capable of scaling to over 100 terabytes (TB) of storage capacity and connecting up to 42 hosts.

2.6.2 Product highlights

The IBM TotalStorage SAN Integration Server is designed to:

- Provide an integrated, pre-configured, and easily implemented storage solution.
- Give users a centralized control point for managing an entire heterogeneous SAN, including storage volumes from disparate vendor devices, from one console.
- Reduce downtime for planned and unplanned outages, maintenance and backups.
- Provide a single set of advanced copy and backup services for multiple storage devices.
- Offer a system architecture where storage capacity, server connectivity, and performance are independently scalable to better accommodate changing business needs.

Part 2

SAN storage configuration

This part of the book provides a step-by-step walkthrough, explaining how to integrate the IBM TotalStorage NAS Gateway 500 into a storage network. We also show how to connect the NAS Gateway 500 to various storage devices.

3

NAS Gateway 500 storage considerations

This chapter provides a step-by-step walkthrough, explaining how to integrate the IBM TotalStorage NAS Gateway 500 into a storage network.

Important: Setting up SAN storage should be your first step. You will not be able to share any data without SAN attached storage.

3.1 Sharing SAN-based storage

We start with a step-by-step walkthrough that shows how to connect to NAS Gateway 500 to the ESS and FAStT after re-initializing the system.

3.2 To SAN or not to SAN

With both the FAStT and the ESS, we describe connecting via the SAN and a point-to-point connection (although we did not do both methods simultaneously). The configurations of the FAStT, the ESS, and the NAS Gateway 500 are all identical regardless of how they are attached. But please be aware that they use different multi-path drivers. We will configure the switch early on, to show the steps specific to setting up our SAN environment. We will be using the IBM 2109 as our fabric device. Additionally, we will be setting up a zone to isolate our devices from devices being used for other purposes.

3.2.1 Finding the World Wide Name

You can obtain WWNs of the Fibre Channel adapters installed on NAS Gateway 500 via either a Web browser, WebSM, or command line tools. Here we explain how to do it using these various methods.

Obtaining WWNs using a Web browser

If your external storage requires entry of the World Wide Name (WWN) for the Fibre Channel host bus adapters installed in your NAS Gateway 500, they can be obtained by opening a Web browser and entering:

```
http://hostname/NAS500GetWWN.html
```

Here, hostname is the hostname or IP address of your NAS Gateway 500 system. In case your NAS Gateway 500 is not within the same IP subnet, you should use the full qualified domain name that is used with DNS name resolution; for example:

nasgateway500.servers.mycompany.com

Obtaining WWNs via WebSM

Connect to the NAS Gateway 500 via WebSM, and login with the root account. On the left pane, expand the IP address of your NAS Gateway 500 under **Management Environment**. Expand **Devices**, and then expand **All Devices**, as shown in Figure 3-1.

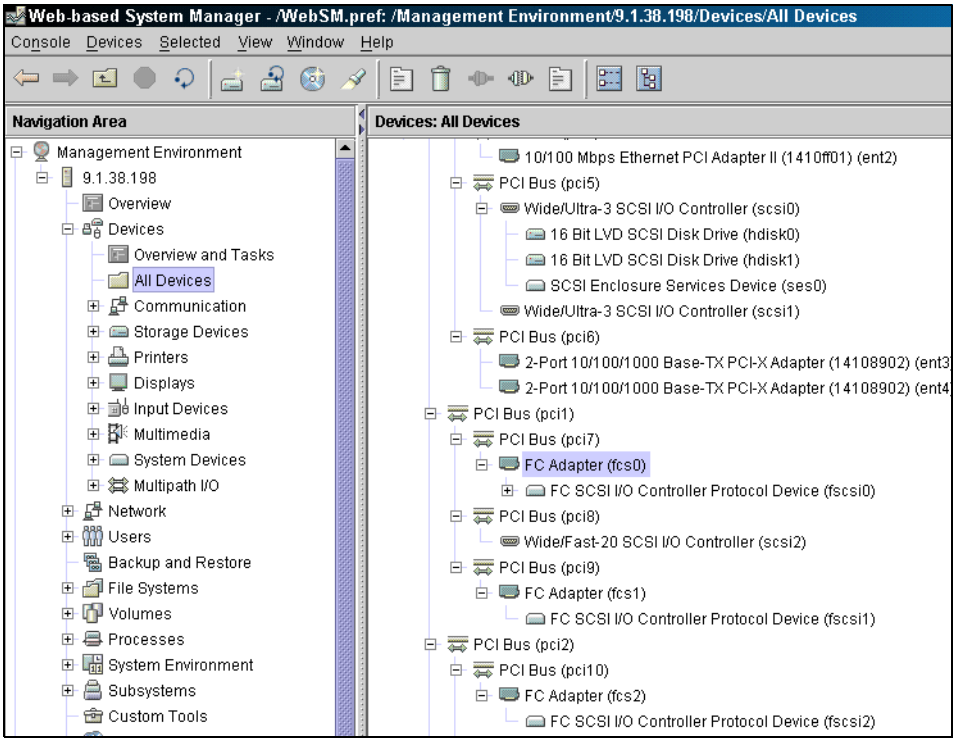


Figure 3-1 Expand all devices

Find the **FC Adapter (fcsx)** devices on the right pane, right-click each of these devices, and select **Vital Product Data**. The vital product data of this Fibre Channel adapter will shown. Scroll up in the window and find the Network Address field. This is the WWN of this adapter (see Figure 3-2).

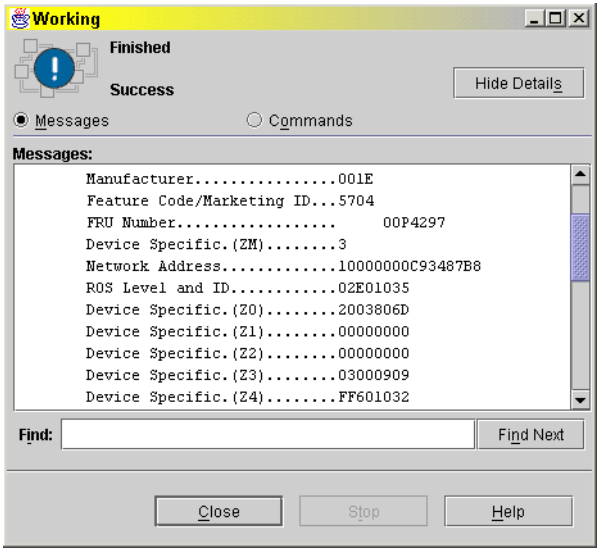


Figure 3-2 The vital product data of a Fibre Channel adapter

Obtaining WWNs via command line

Login the NAS Gateway 500 as root, from a serial terminal. Run the command **`lscfg -vpl "fcs*" |grep Network`** to get the WWNs of all Fibre Channel adapters installed (see Example 3-1).

Example 3-1 lscfg -vpl "fcs" |grep Network*

```
(/)-->lscfg -vpl "fcs*" |grep Network
        Network Address.....10000000C93487CA
        Network Address.....10000000C934863F
        Network Address.....10000000C93487B8
        Network Address.....10000000C934864F
```

You can also use the command **`lscfg -vpl "fcs*" > foo.txt`** to put all vital product data of the Fibre Channel adapters installed on NAS Gateway 500 to a text file. You can keep this file for future usage. Here we give part of this file in Example 3-2. You can find WWN, location information, microcode level, part number, and plenty of other information about your Fibre Channel adapters in this file.

Example 3-2 The vital product data of a Fibre Channel adapter

```
fcs2             U0.1-P2-I6/Q1  FC Adapter

        Part Number.................00P4295
        EC Level....................A
        Serial Number...............1E323088E2
        Manufacturer................001E
        Feature Code/Marketing ID...5704
        FRU Number..................     00P4297
        Device Specific.(ZM)........3
        Network Address.............10000000C93487CA
        ROS Level and ID............02E01035
        Device Specific.(Z0)........2003806D
        Device Specific.(Z1)........00000000
        Device Specific.(Z2)........00000000
        Device Specific.(Z3)........03000909
        Device Specific.(Z4)........FF601032
        Device Specific.(Z5)........02E01035
        Device Specific.(Z6)........06631035
        Device Specific.(Z7)........07631035
        Device Specific.(Z8)........20000000C93487CA
        Device Specific.(Z9)........HS1.00X5
        Device Specific.(ZA)........H1D1.00X5
        Device Specific.(ZB)........H2D1.00X5
        Device Specific.(YL)........U0.1-P2-I6/Q1

fcs3             U0.1-P2-I5/Q1  FC Adapter

        Part Number.................00P4295
        EC Level....................A
        Serial Number...............1E3230890F
        Manufacturer................001E
        Feature Code/Marketing ID...5704
        FRU Number..................     00P4297
        Device Specific.(ZM)........3
        Network Address.............10000000C934863F
        ROS Level and ID............02E01035
        Device Specific.(Z0)........2003806D
        Device Specific.(Z1)........00000000
        Device Specific.(Z2)........00000000
```

3.3 SAN storage considerations

Before you start to plan for, configure, or install your environment or additional software (like multipathing) on the NAS, consider your environment and which configuration you need.

Keep the requirements of all components in mind. All participating products must be checked for their interoperability. These are the storage subsystem, the Fabric (SAN Switches), the NAS Gateway 500 itself (HBA, HACMP, Base OS) and the multipathing software.

Note: All configuration and installation steps in the following steps are specific for the software and hardware we used in our lab. Changes and differences may appear with newer versions and levels.

Be clear about:

- Infrastructure (connectivity of the NAS you are employing)
- Devices (storage devices connected to the NAS Gateway 500)
- HBAs (that you are using in your NAS Gateway 500) (FC 6239 / FC 6240)

3.3.1 Infrastructure

Planning and implementing the infrastructure of the NAS Gateway 500 bears a basic relationship to the SAN environment. More information on planning and implementing a SAN environment can be found in the IBM Redbook, *Designing and Optimizing an IBM Storage Area Network*, SG24-6419, and the redbook, *IBM SAN Survival Guide*, SG24-6143.

This part of the redbook just alludes to some important issues. The NAS Gateway 500 can be attached in several ways: direct attached connectivity, or via a Storage Area Network (SAN).

Direct attached connectivity is cheaper, but much less flexible and scalable. Switched Fabric connectivity allows you zoning, fabric security, a very flexible environment, and sharing of devices between other systems.

Regarding availability, you should consider using multiple paths to the Storage devices. This involves more than just using two Fibre Channel Adapters in the NAS Gateway 500.

Figure 3-3 shows various connectivity considerations, using five graphics arranged from left to right.

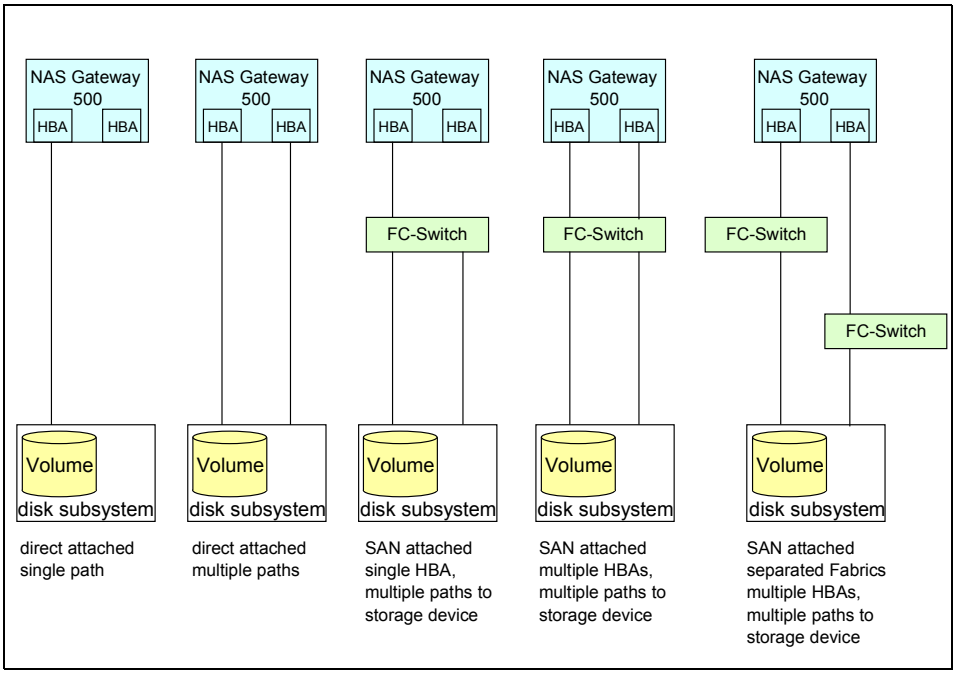


Figure 3-3 Connectivity considerations

The leftmost graphic represents the simplest solution. It provides one Fibre Channel link to the storage device with direct attached connectivity. This link is dedicated (server - storage) and in case of a failure (link; HBA) it is not redundant. The throughput is limited to one link.

The second graphic illustrates a direct attached connectivity with multiple paths to the storage device. This case implies the need for multipathing software. The server can access the volume in the storage device by both links. The hdisk (in our NAS Gateway 500 environment) would be detected by the configuration manager twice. The configuration manager (**cfgmgr**) runs at system start and on demand by issuing the **cfgmgr** command. To avoid the dual disk issue, the multipathing software has to be applied.

The graphic in the middle describes a single switch connectivity with one server-switch link and two links to the subsystem. This configuration also needs multipathing software, because the volume is accessible through both switch-storage links. If only one connection between switch and storage is used, the multipathing software will not be necessary. But keep in mind that just one connection could limit availability and throughput.

The second graphic from the right side describes a SAN based configuration using multiple HBAs from server to switch, and multiple connections between switch and storage device. This configuration additionally needs a multipathing software and is very flexible regarding the sharing of ports between multiple initiators (servers). The only weak point is the switch; if it fails, all connections are cut off.

The graphic on the very right side demonstrates the most flexible, redundant, and performing configuration. All components are redundant (even the server can be redundant via HACMP). The usage of two separated fabrics provides reliability and prevents outage even if one fabric fails (in the picture, a single Fibre Channel switch). Multipathing software is obligatory.

Detailed information about how to set up ESS Volumes and Host assignments can be found in Chapter 6, “ESS storage configuration” on page 93.

Before you proceed, make sure the NAS Gateway 500 is correctly cabled and connected. Verify the SAN zoning.

3.3.2 Storage devices

This section deals with considerations on which storage devices are connected to the NAS Gateway 500. Be sure to use a supported configuration. Take a look at the interoperability matrix of the NAS Gateway 500, which can be found in the Web at:

`http://www.storage.ibm.com`

We describe the configuration of volumes by means of examples in Chapter 6, “ESS storage configuration” on page 93.

Depending on the storage subsystem, you will choose the multipathing software. Be sure your configuration needs multipathing, because it may not be supported to run multipathing software with only one path.

Attention: Check the interoperability matrixes and Web documents for which multipathing software is suitable for your disk subsystem.

At the time of writing this book, MPIO was not supported in a clustered environment in conjunction with ESS. So we will describe how to install and set up SDD (Subsystem Device Driver)

The NAS Gateway 500 is shipped with pre-installed multipathing drivers (RDAC and MPIO):

- RDAC (This is Multipathing Software for FAStT storage subsystems).
- MPIO (multi-path I/O) is a technology that was introduced as part of the AIX 5.2 operating system.

If you want to connect to an ESS using multiple paths, you must use Subsystem Device Driver (SDD). The MPIO Driver also does this for an unclustered NAS Gateway 500 attached to ESS. Subsystem Device Driver (Multipathing Software for the ESS) is not pre-installed on the NAS Gateway 500. However, you can connect FAStT storage to your NAS Gateway 500 without adding additional software.

You can download the latest version of SDD from the Net. Check for the latest Version:

`http://www-1.ibm.com/servers/storage/support/software/sdd.html`

Verify if the provided SDD Version is supported with the NAS Gateway 500, check prerequisites of SDD in the readme files, and installation documentation. Restrictions and prerequisites may appear. Look for required PTFs. You should also verify prerequisites regarding the ESS Interoperability Matrix:

`http://www.storage.ibm.com/disk/ess/supserver.htm`

Look for entries regarding the NAS Gateway 500.

We needed to use Licensed Internal Code (LIC) Level 2.2.0 or higher in the ESS.

Tip: If you have to upgrade the ESS microcode regarding the prerequisites, plan this before attaching to the NAS Gateway 500.

3.3.3 Host attachment scripts

If all prerequisites are met, we can go on with the procedure. Before installing the Multipathing Software SDD, we had to install ESS attachment scripts on the NAS nodes. The following procedure describes how to prepare for the attachment scripts and how to install them.

Migration steps from MPIO environment to SDD environment

If you install the Host attachment scripts (**ibm2105.rte**) the first time on the NAS Gateway 500, you first have to remove the MPIO drivers. On a command line, check if the attachment scripts are installed:

```
lslpp -La | grep ibm2105
```

Figure 3-4 displays the situation where MPIO (**ibm2105mpio.rte**) is installed, and the ESS Host attachment scripts (**ibm2105.rte**, which is a prerequisite for SDD) are not yet installed. Both versions will not coexist on the NAS Node, so you have to unconfigure and remove the MPIO package.

```
(/)-->lslpp -La | grep ibm2105
  ibm2105mpio.rte            1.0.0.0    C     F    IBM 2105 Host Attachment for
(/)-->
```

Figure 3-4 Check installed file set

To unconfigure MPIO devices, determine which disks to remove.

On a command prompt, issue the following command as root user:

`lsdev -Cc disk`.

Attention: In our case, the first two disks (16 Bit LVD SCSI Disk Drive) **hdisk0** and **hdisk1** are the operating system disks (internal SCSI disks). You must ***not*** remove them. Please be aware that these numbers cannot be guaranteed and might change if you have more disks in your system.

Use the command **`rmdev -dl hdiskX -R`** to delete all MPIO disks (for example, **`rmdev -dl hdisk2 -R`**). The command deletes the disk from the ODM, including all child devices.

Figure 3-5 shows an environment with only the internal disks. Please be aware that the numbers may change.

```
(/)-->lsdev -Cc disk
hdisk0 Available 1S-08-00-8,0 16 Bit LVD SCSI Disk Drive
hdisk1 Available 1S-08-00-9,0 16 Bit LVD SCSI Disk Drive
(/)-->
```

Figure 3-5 All MPIO devices removed

Now you can remove the **ibm2105mpio.rte** file set. Open a command line as root and enter the command:

`installp –u ibm2105mpio.rte`

This will remove the MPIO file set as shown in Figure 3-6.

```
0503-409 installp:  bosboot verification starting...
installp:  bosboot verification completed.
0503-408 installp:  bosboot process starting...

bosboot: Boot image is 18292 512 byte blocks.
0503-292 This update will not fully take effect until after a
         system reboot.

    * * *  A T T E N T I O N  * * *
    System boot image has been updated. You should reboot the
    system as soon as possible to properly integrate the changes
    and to avoid disruption of current functionality.

installp:  bosboot process completed.
+-----------------------------------------------------------------------------+
                                Summaries:
+-----------------------------------------------------------------------------+

Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
ibm2105mpio.rte             1.0.0.0         ROOT        DEINSTALL   SUCCESS
ibm2105mpio.rte             1.0.0.0         USR         DEINSTALL   SUCCESS
(/usr/sys/inst.images)-->
```

Figure 3-6 MPIO successfully removed

The NAS node is now prepared for the **ibm2105.rte** installation.

You can find the appropriate scripts on a CD in your ESS. Ask your ESS administrator to get the CD or file sets.

We downloaded the file sets from the Web site. To access the scripts, go to:

http://www-1.ibm.com/servers/storage/support/software/sdd.html

Follow the link: **ESS host attachment scripts**, then go to: **ESS Host Attachment Script for SDD on AIX** -> open Web Page:

http://www-1.ibm.com/support/docview.wss?rs=540&context=ST52G7&q=host+script&uid=ssg1S4000106&loc=en_US&cs=utf-8&lang=en+en

Download: **AIX Host Attachment Script**.

In our case, this was: Platform AIX 32.6.100.18 English Byte Size 102400 Date 11/21/2003)

Download **ibm2105.rte.tar** from Web page to the local directory on your NAS node into the directory:

/usr/sys/inst.images

Change to the directory: **cd /usr/sys/inst.images** and extract the downloaded file:

```
tar -xvf ibm2105.rte.tar
```

Then create a new table of contents file (**.toc**) used later by the installation procedure:

```
inutoc .
```

Run the install SMIT menu (with the fastpath):

```
smitty install_latest
```

Specify the path (you can use the **.** because we changed the directory before, or specify the full path: Press **Esc+4** and select the appropriate directory as shown in Figure 3-7 (**Input device: /usr/sys/inst.images (Installation Directory)**.

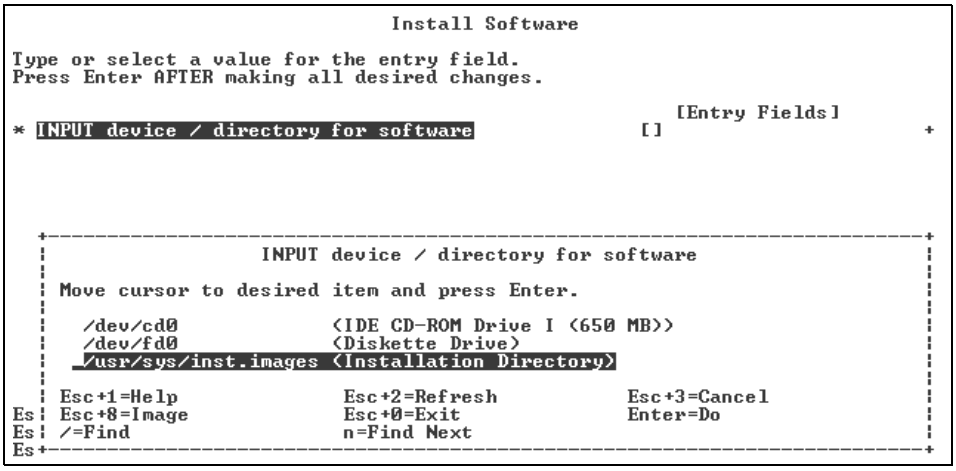


Figure 3-7 SMIT install latest

Place the cursor on **SOFTWARE to install** and press **Esc+4** as shown in Figure 3-8.

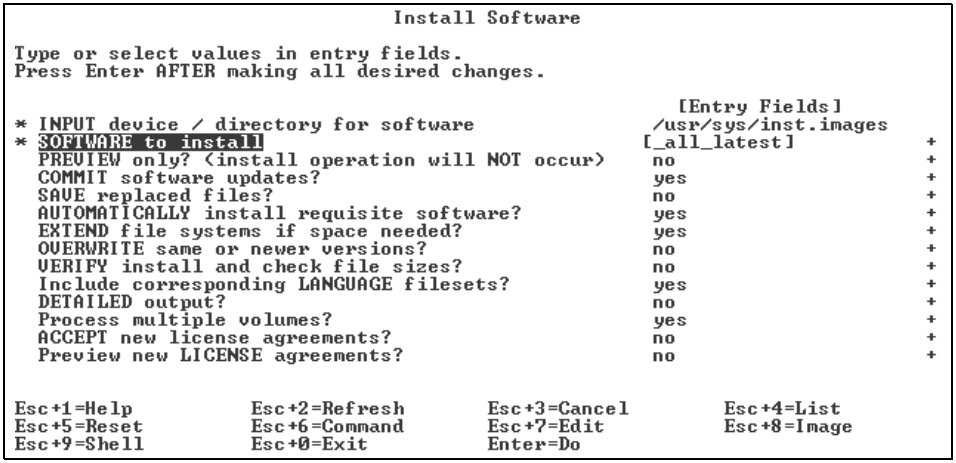


Figure 3-8 SMIT installation menu

Then move the cursor to **ibm2105** press **Esc+7** to select (the **>** should appear in front of the **ibm2105** software). Then press Enter (Figure 3-9).

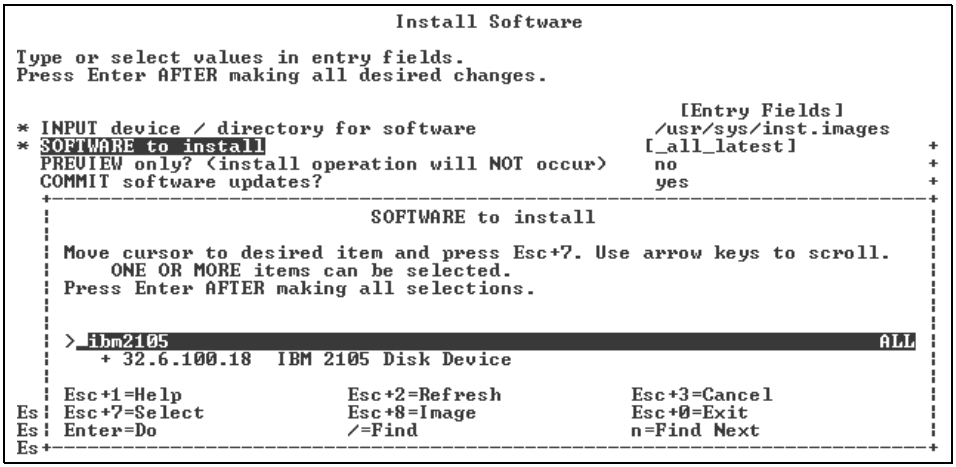


Figure 3-9 Choose the file set to install

Press Enter and the installation will occur (Figure 3-10).

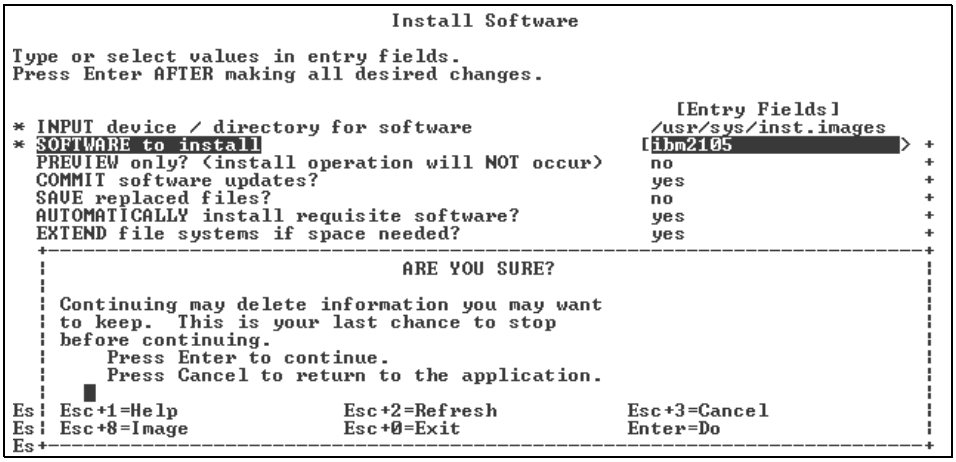


Figure 3-10 Confirm the Installation

The installation should end with success as shown in Figure 3-11.

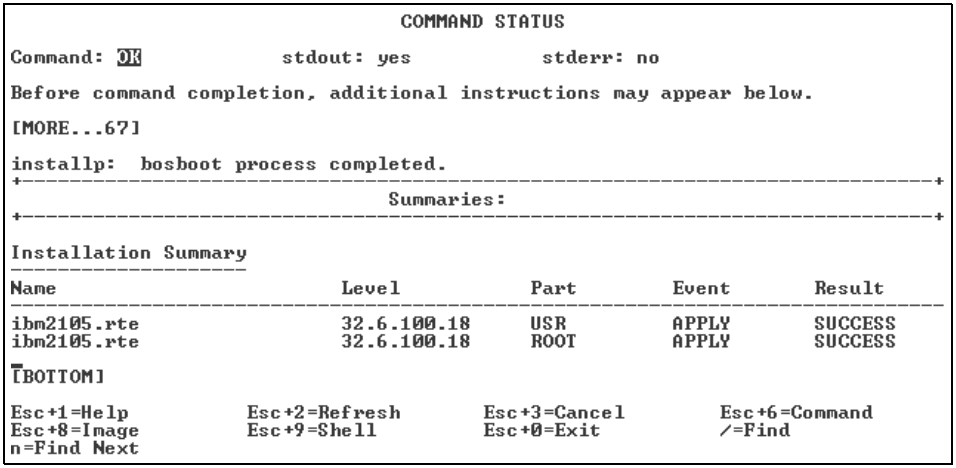


Figure 3-11 Successfully installed the file set

To be sure, you can verify if the file set is installed (Figure 3-12).

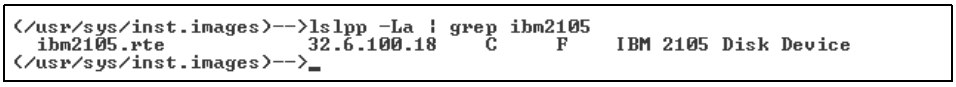


Figure 3-12 Installed Host attachment scripts

If the ESS and SAN are correctly set up, and volumes are assigned to the NAS Gateway 500, you may see some disks if l**sdev -Cc disk** is run. All disks residing on the ESS should display in the description: **hdiskx..... FC2105xxx**.

The system disks hdisk0 (and hdisk1 if the system has two internal disks) should not have the 2105 description.

Tip: At this point we do not advise you to configure volume groups, logical volumes, or file systems on ESS disks. This should be done after SDD is installed. If volume groups are created before, the administrator has to convert the *hdisk* Volume group to a *vpath* volume group (see the **hd2vp** command in the SDD documentation).

If the physical volumes on an SDD volume group's physical volumes are mixed with hdisk devices and vpath devices, you must run the **dpovgfix** utility. Otherwise, SDD will not function properly. Issue the **dpovgfix vg_name** command to fix this problem.

3.3.4 Subsystem Device Driver

Part of the migration from MPIO environment to SDD was described in 3.3.3, "Host attachment scripts" on page 55. More information about installing and using SDD can be found in the *Subsystem Device Driver User's Guide*.

If all steps described above are done successfully, we can proceed as follows. SDD drivers are provided with the ESS, but it is advisable to look for the latest version in the Internet. The SDD file sets (non-concurrent HACMP), readme, and documentation can be found at:

http://www-1.ibm.com/servers/storage/support/software/sdd.html

Follow the link: **Download Subsystem device drivers** and choose the appropriate version (Remember that NAS Gateway is AIX powered).

Check the documentation, readme, and Web site for prerequisites concerning SDD.

At the time of writing this book, the file set was named (Version 1.5.0.0):

devices.sdd.52.rte.tar

We downloaded it to the NAS node via **ftp**, then we unpacked it as shown in Figure 3-13.

```
(/usr/sys/inst.images)-->tar -xv -f  devices.sdd.52.rte.tar
x devices.sdd.52.rte, 1177600 bytes, 2300 media blocks.
(/usr/sys/inst.images)-->
```

Figure 3-13 Extracting the SDD archive

Change directory to **cd /usr/sys/inst.images** and run **inutoc** to create a new **.toc** file in this directory, as shown in Figure 3-14.

```
(/usr/sys/inst.images)-->tar -xv -f  devices.sdd.52.rte.tar
x devices.sdd.52.rte, 1177600 bytes, 2300 media blocks.
(/usr/sys/inst.images)-->ls -al
total 5096
drwxr-xr-x   2 bin      bin             256 Dec 04 05:04 .
drwxrwxr-x   4 bin      bin             256 Dec 02 16:04 ..
-rw-r--r--   1 root     system          242 Dec 03 12:47 .toc
-rw-r--r--   1 ipsec    ldap        1177600 Oct 27 18:28 devices.sdd.52.rte
-rw-r-----   1 root     system      1187820 Dec 04 05:03 devices.sdd.52.rte.tar
-rw-r--r--   1 ipsec    ldap          95232 Sep 26 18:07 ibm2105.rte
-rw-r-----   1 root     system       102400 Dec 03 12:34 ibm2105.rte.tar
-rw-r-----   1 root     system        36189 Dec 04 05:00 rd_aix.txt
(/usr/sys/inst.images)-->inutoc .
(/usr/sys/inst.images)-->ls -al
total 5096
drwxr-xr-x   2 bin      bin             256 Dec 04 05:04 .
drwxrwxr-x   4 bin      bin             256 Dec 02 16:04 ..
-rw-r--r--   1 root     system          698 Dec 04 05:06 .toc
-rw-r--r--   1 ipsec    ldap        1177600 Oct 27 18:28 devices.sdd.52.rte
-rw-r-----   1 root     system      1187820 Dec 04 05:03 devices.sdd.52.rte.tar
-rw-r--r--   1 ipsec    ldap          95232 Sep 26 18:07 ibm2105.rte
-rw-r-----   1 root     system       102400 Dec 03 12:34 ibm2105.rte.tar
-rw-r-----   1 root     system        36189 Dec 04 05:00 rd_aix.txt
(/usr/sys/inst.images)-->
```

Figure 3-14 Creating a new .toc file

Fibre Channel Adapter drivers had already been installed with the Basic setup (recovery CDs). If you are going to upgrade SDD, please refer to the *SDD User's Guide for the IBM ESS* and the IBM SAN VC document for details on upgrading SDD on AIX 5.2.

The following installation guideline is intended for a fresh installation only.

Make sure to be logged in as root user.

Issue **smitty install_latest** at a command prompt.

Choose **.** (if you changed the directory to **/usr/sys/inst.images**) before; otherwise press **Esc+4** and select the directory.

You will see a screen similar to the one shown in Figure 3-15.

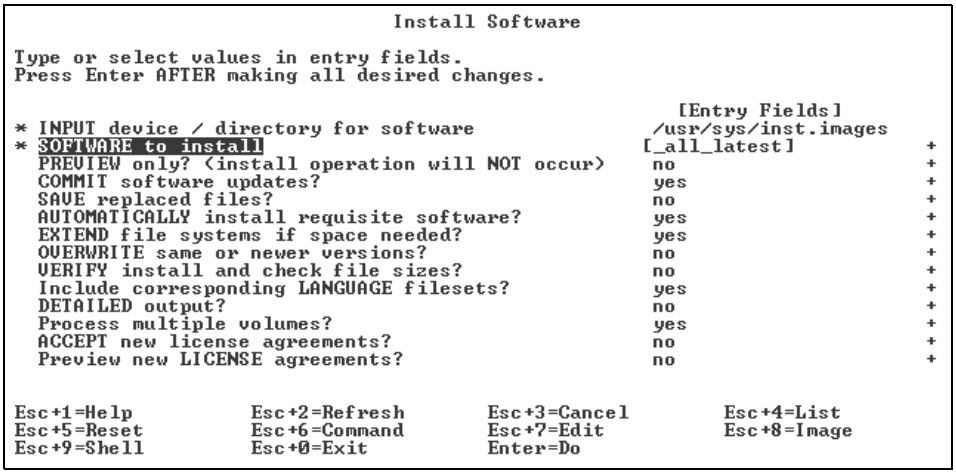


Figure 3-15 SMIT install menu

Place the cursor on **SOFTWARE to install** and press **Esc+4**.

Use the up and down key to place the cursor on **devices.sdd.52** and press **Esc+7** to select this file set. The **>** sign will show the selected item. See the sample in Figure 3-16.

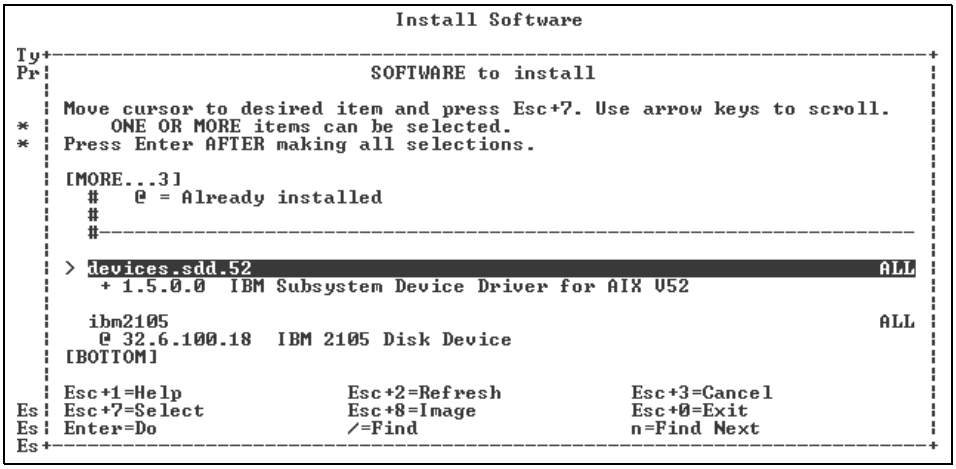


Figure 3-16 Choose the SDD file set

Press Enter to come back to the installation menu as shown in Figure 3-17.

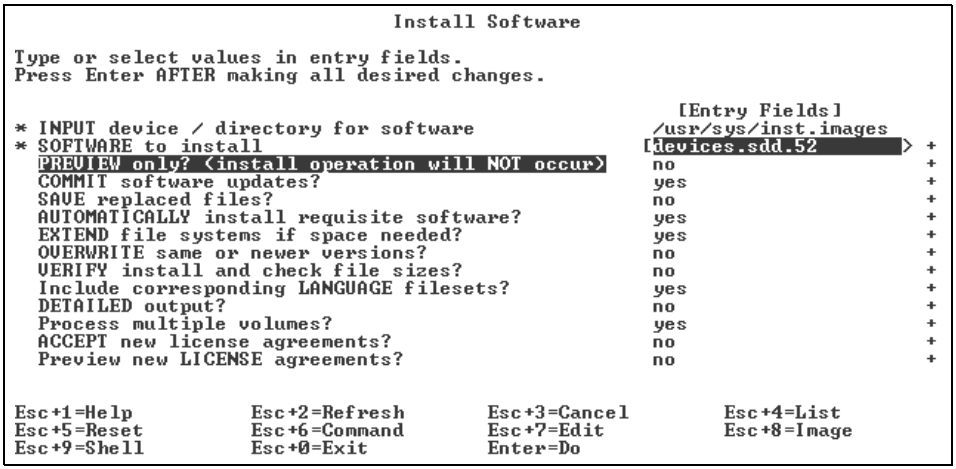


Figure 3-17 Proceed with the installation

Note: If you want to do a preview first, select yes in the **PREVIEW only?** field.

Proceed by pressing Enter. SMIT will ask you to confirm the installation. Press Enter again.

The installation should finish successfully as shown in Figure 3-18.

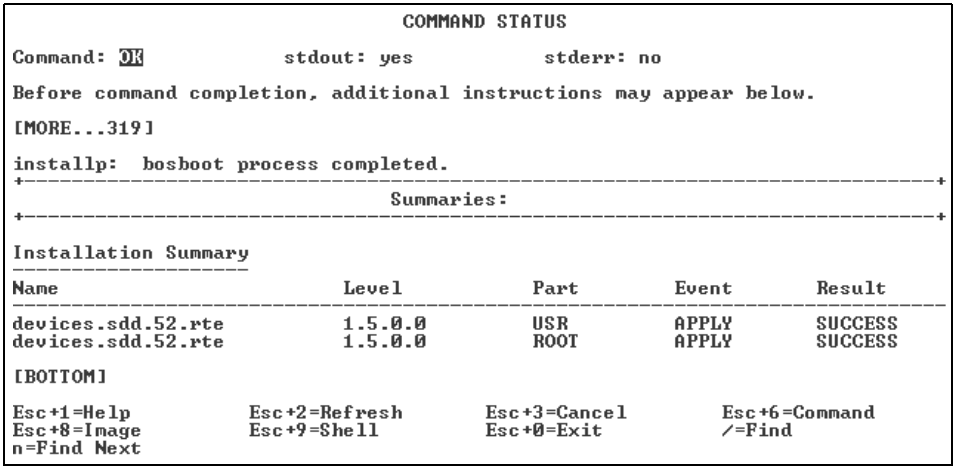


Figure 3-18 SDD Installation succeeded

Verify if the file set is installed, as shown in Figure 3-19.

```
(/usr/sys/inst.images)-->lslpp -La ¦ grep sdd
  devices.sdd.52.rte          1.5.0.0    C     F    IBM Subsystem Device Driver
(/usr/sys/inst.images)-->
```

Figure 3-19 SDD installations verification

Be sure the ESS is configured and attached correctly, and that zoning in your SAN environment is correct. Now you can run the Configuration Manager (**cfgmgr**) on a NAS Gateway 500 command line.

Important: Do only use the **cfgmgr** command located at /opt/nas/bin/cfgmgr.

If everything is correct, you should see 2105 disks (hdisks and vpath devices with FC2105xxx description) if you run the command:

```
lsdev -Cc disk
```

Also try the following very useful SDD commands:

```
datapath query adapter
datapath query device
lsvpcfg
```

After SDD is successfully installed, you can configure NAS volumes. Keep in mind that SDD provides the new commands **mkvg4vp** and **extenvg4vp**).

Note: You should have only **pvid**'s on vpath devices (**lsdev -Cc disk**).

4

SAN zoning

It is not our intention to point out *every* detail required to set up and/or configure the IBM 2109, but we will hit the highlights. To learn more about this subject, please refer to the description in the *IBM SAN Survival Guide*, SG24-6143.

4.1 Zoning the IBM 2109

Using a browser, go to the **Fabric View** of your 2109 by typing its IP address into the address bar of your browser. This should bring up a screen similar to the one in Figure 4-1.

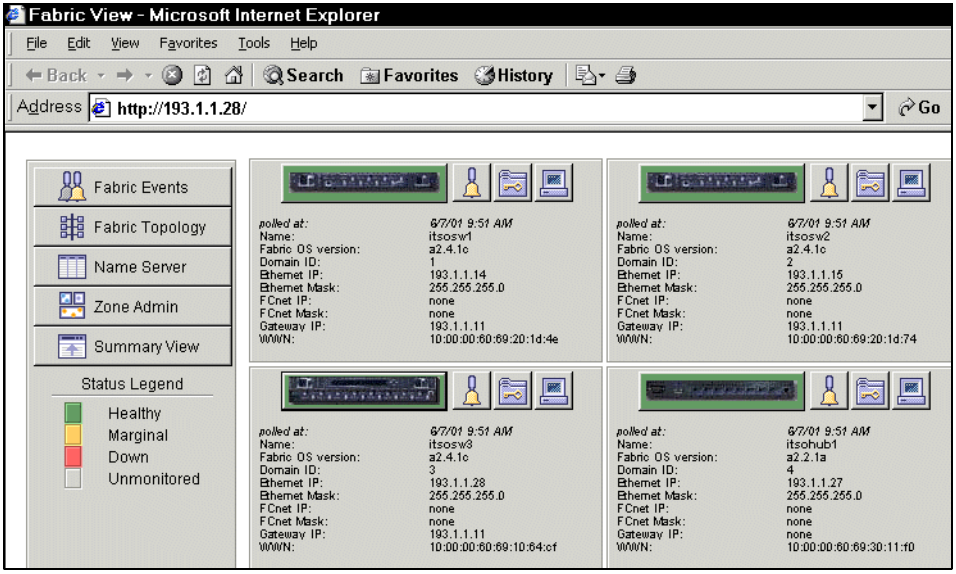


Figure 4-1 Fabric View of the 2109

Now select the switch to configure and press the **Zone Admin** button in the left pane. You will need to supply the user name and password in the dialog, and click **OK** (see Figure 4-2).

Figure 4-2 Zone login

Once you've logged in, create an alias. We are simply re-naming an existing alias, so our screen shown in Figure 4-3 may be different from yours.

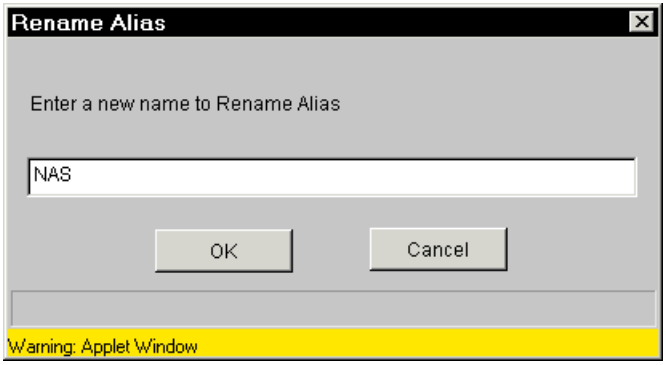


Figure 4-3 Rename alias

Next, we will add the World Wide Name (WWN) of the devices to be associated to this alias. **Highlight** the WWN of the devices in the list on the left, as shown in Figure 4-4.

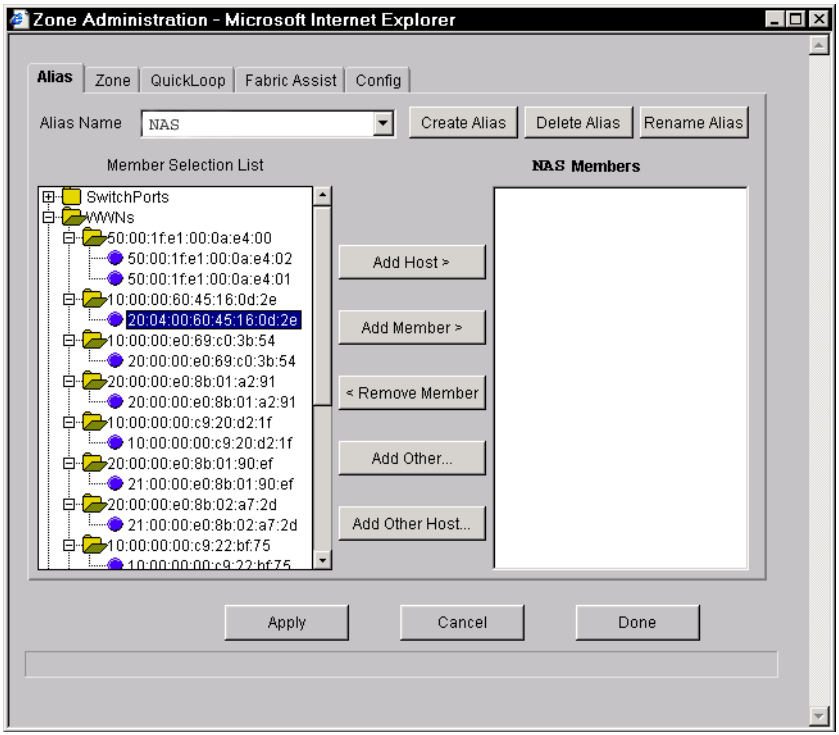


Figure 4-4 Locate WWN

Now associate the WWN to the alias you have created by pressing the **Add Member** button, as shown in Figure 4-5.

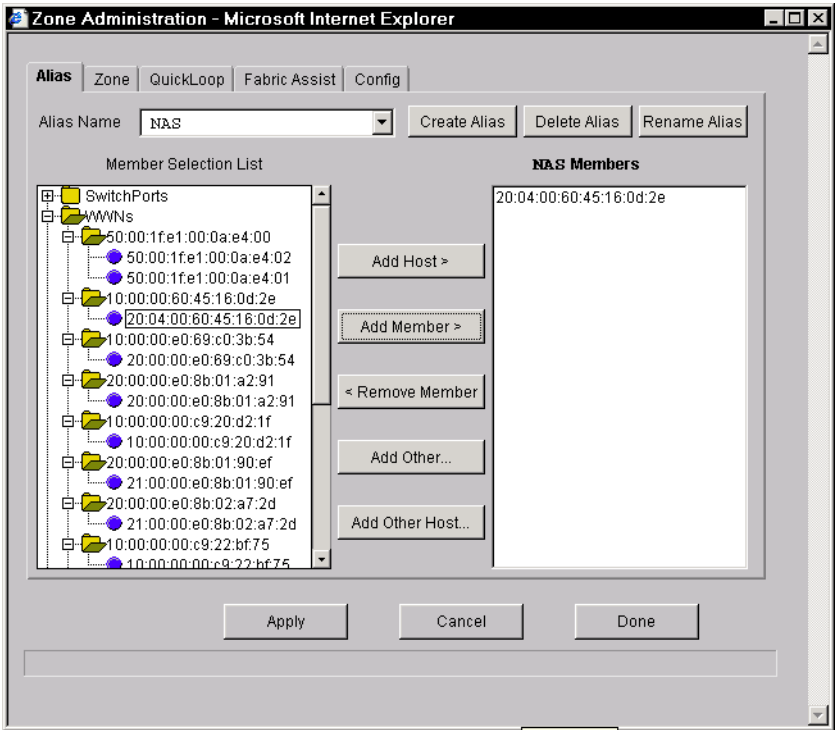


Figure 4-5 Add members

Next, we will make a zone to put the alias in. Select the **Zone** tab and click **Create Zone** as shown in Figure 4-6.

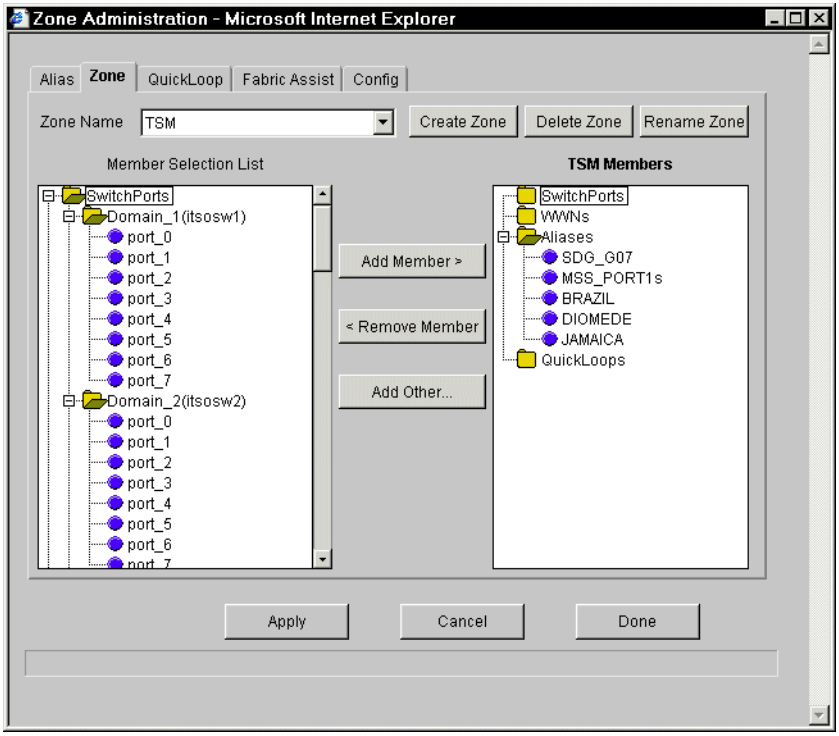


Figure 4-6 Zone creation

Enter the name of the zone you are going to add and click **OK** as shown in Figure 4-7).

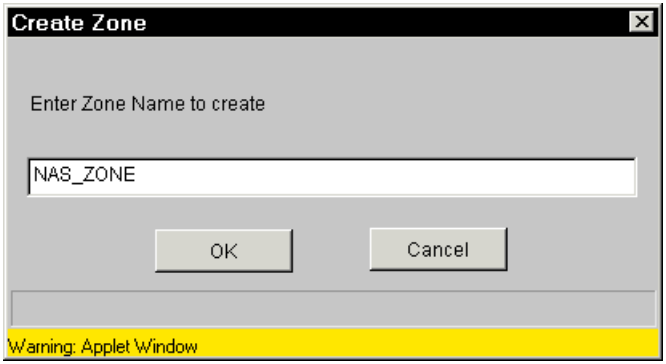


Figure 4-7 Create Zone

Now we can add the alias we created earlier to this zone. Open the **Aliases** folder and **highlight** the alias to add as shown in Figure 4-8.

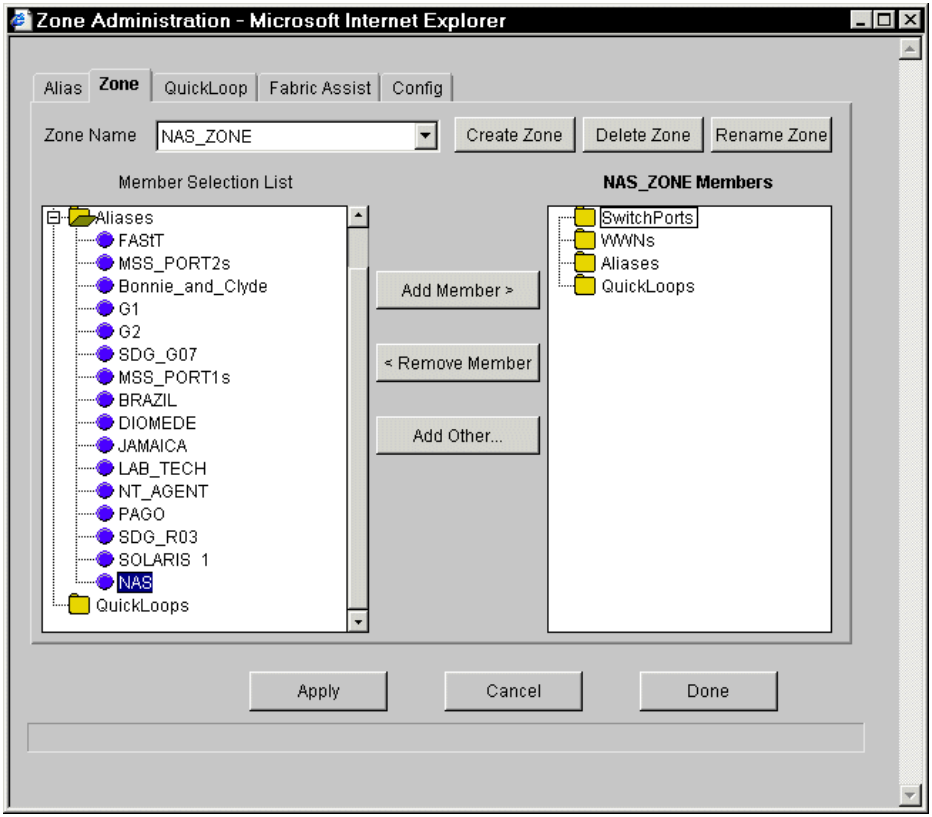


Figure 4-8 Select alias

Click the **Add Member** button. Your screen will look similar to the one shown in Figure 4-9.

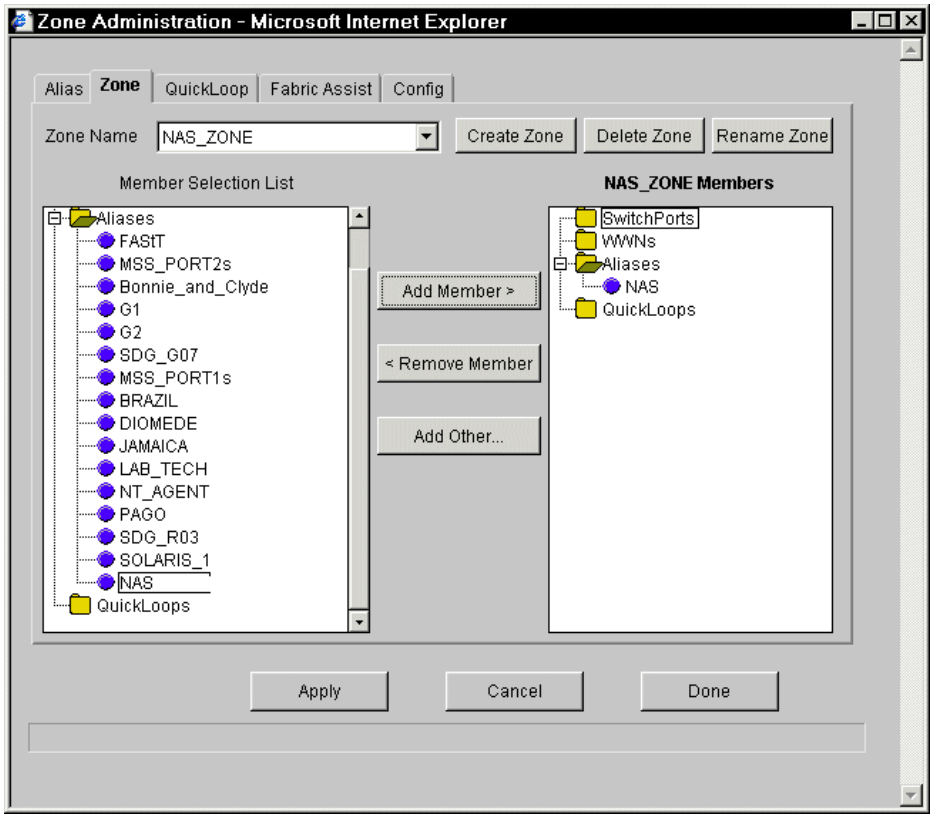


Figure 4-9 Add alias to zone

To finish this zoning process, choose the **Config** tab, **highlight** the configuration to add to the new zone to by using the **Config Name** pull-down menu, open the **Zones** folder, and **highlight** the newly created zone as shown in Figure 4-10.

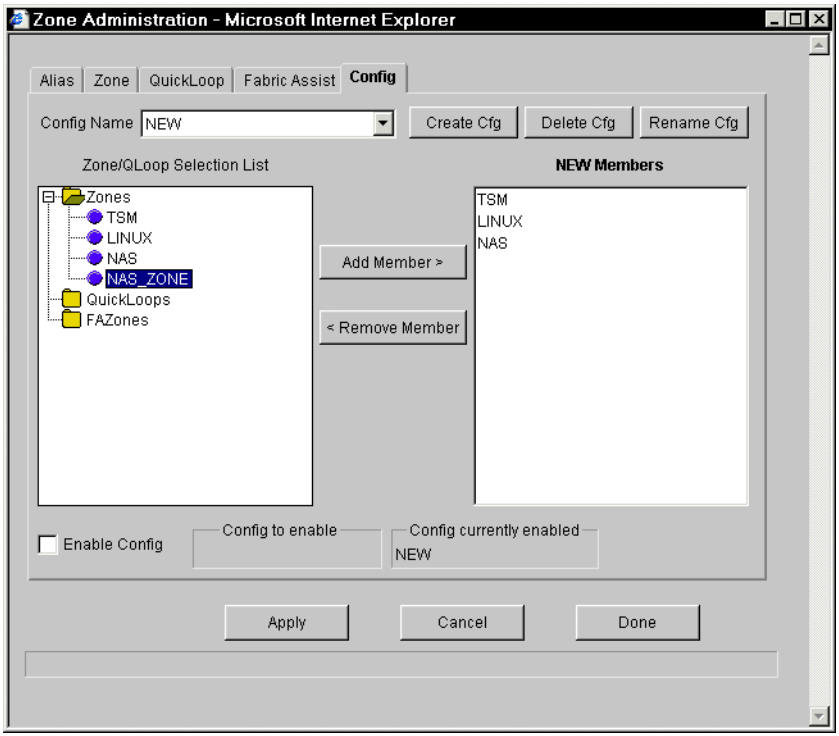


Figure 4-10 Select zone to add

Click the **Add Member** button, and then click the **Apply** button, as shown in Figure 4-11.

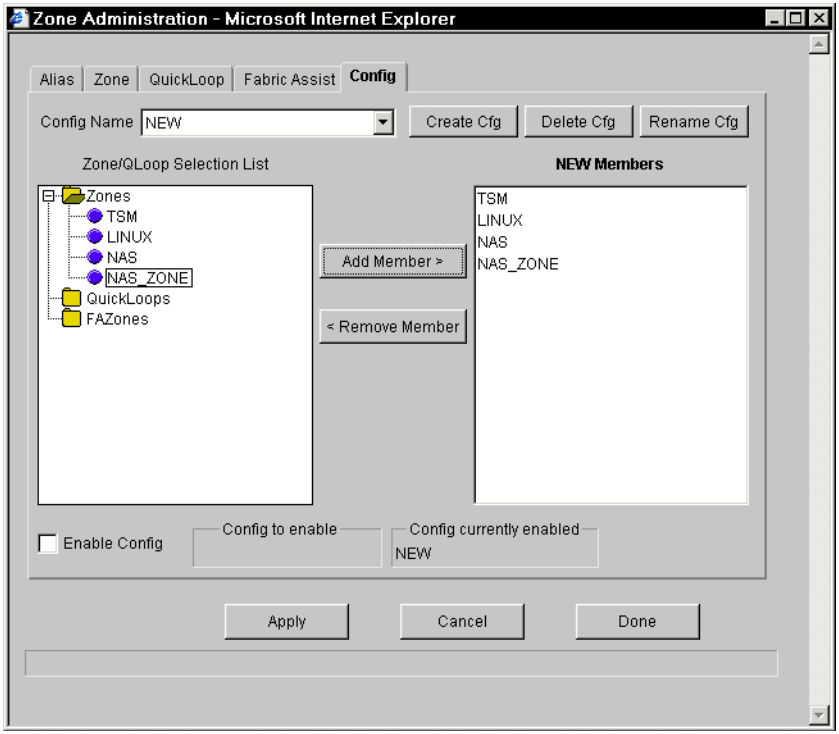


Figure 4-11 Add zone to configuration

Note: Only the zones listed in the NEW Members panel on the right will be active once the **Apply** button is pressed.

5

FAStT storage configuration

If you are performing this setup in a production environment, there are many planning steps you would need to go through before proceeding. We do not cover all of those steps here; we just focus on the setup steps which occur after planning. If you need more comprehensive background information, we recommend that before proceeding, you take a look at the redbook, *Fibre Array Storage Technology - A FAStT Introduction*, SG24-6246.

Note: FAStT600 and FAStT900 have a chargeable HOST Kit for AIX. Be sure you have installed the appropriate license on your FAStT.

Getting storage space in the FAStT to appear as drives to the NAS Gateway 500 is a detailed process. Again, you will have to do some planning to make the FAStT storage space meet your requirements. Just as an example, we will create RAID5 drives from the free space in our FAStT.

5.1 Creating logical drives

We are launching the **IBM FAStT Storage Manager** client from the system that is used to perform work on the FAStT as shown in Figure 5-1. If the **IBM FAStT Storage Manager** is not installed on your PC, you can download it from the following Web site:

`http://www.storage.ibm.com./disk/fastt/index.html`

Just select your FAStT storage system and click **Product Support**. You will find the latest version of the Storage Manager software there.

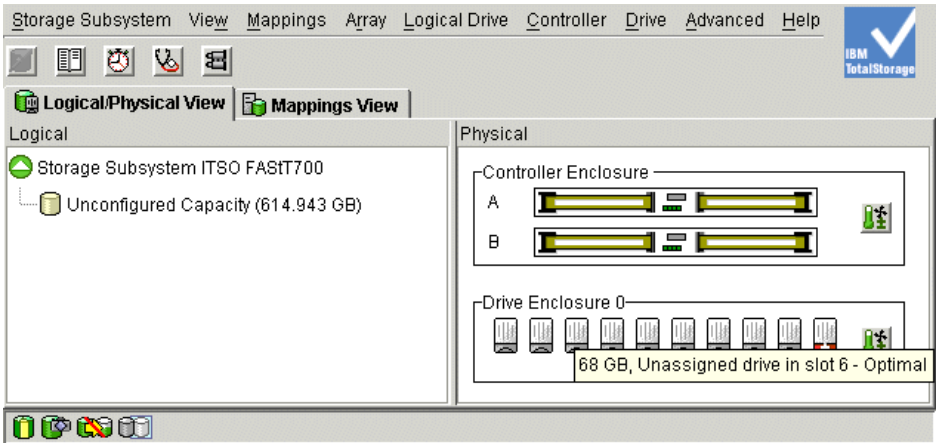


Figure 5-1 Storage Manager main screen

Now we ***highlight*** the device and right-click the unconfigured drives as shown in Figure 5-2. Click the menu **Create Logical Drive**.

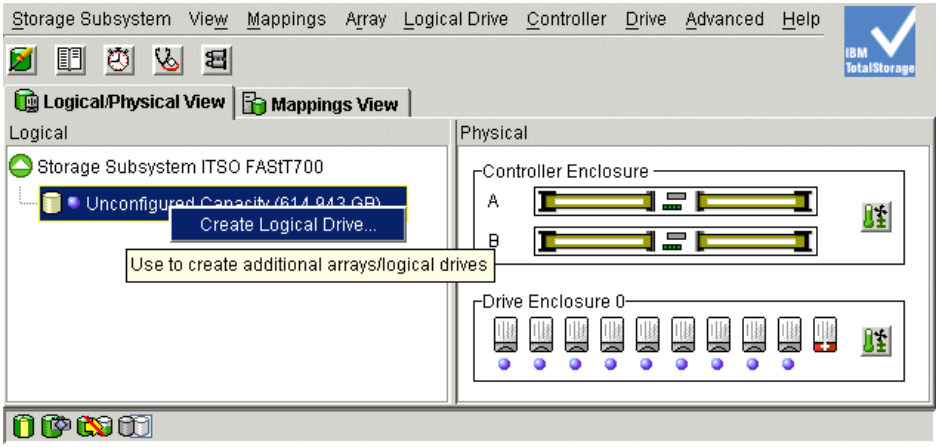


Figure 5-2 Subsystem management

The Default Host type window will be opened as shown in Figure 5-3. Select AIX as the connection type for the NAS Gateway 500. Click **OK**.

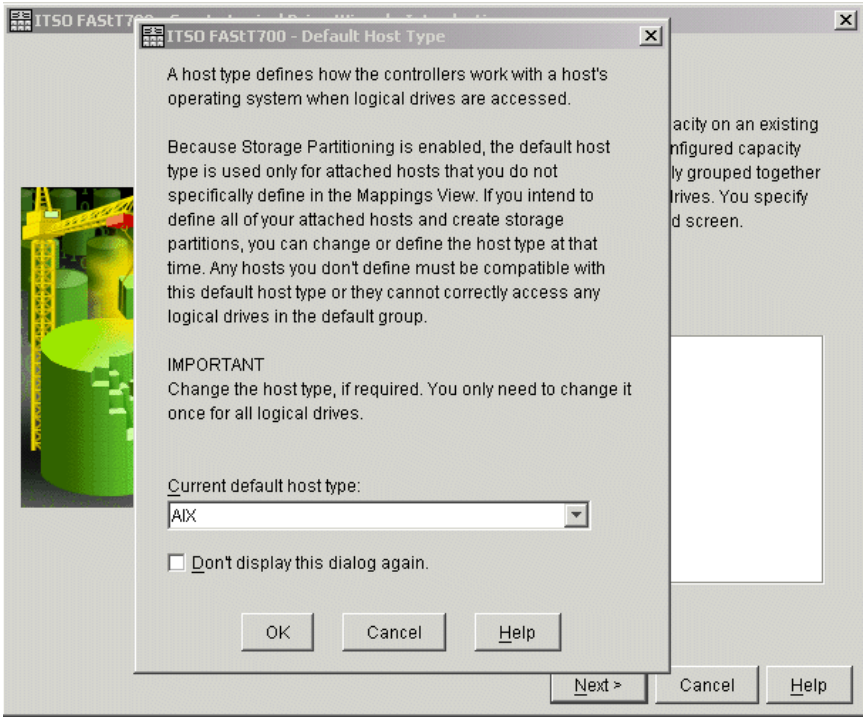


Figure 5-3 Default host type

The Create Logical Drive Wizard will now be opened as shown in Figure 5-4. As there is no storage configuration on this FAStT, we will start with **Unconfigured capacity (create new array)**, then click **Next**.

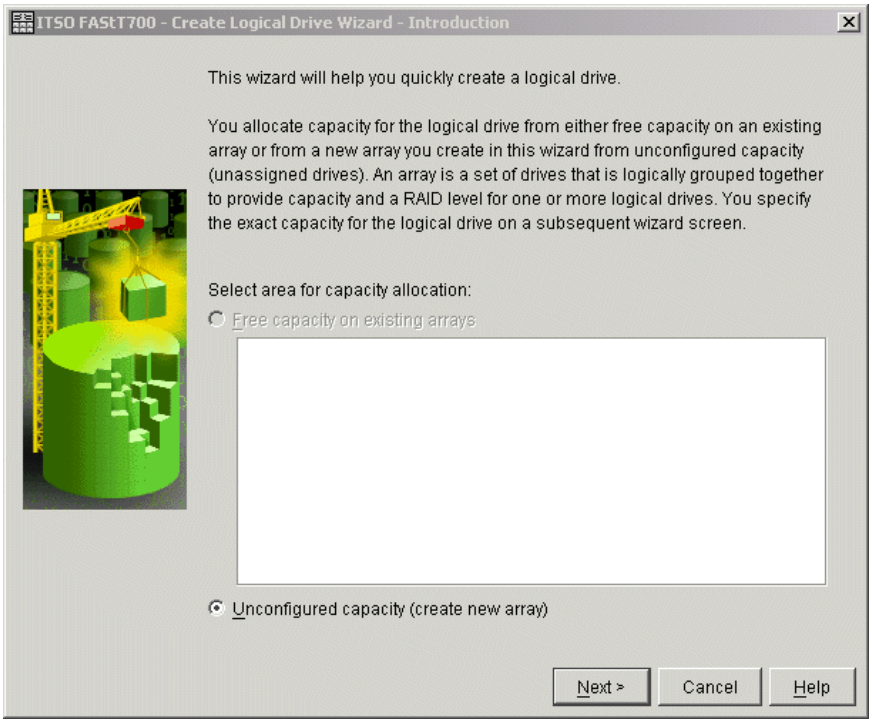


Figure 5-4 Logical drive wizard

We have selected to do a manual configuration of the amount of drives we want to include and the RAID level as shown in Figure 5-5. Select the amount of drives and the RAID level that is required.

Note: The **Next** button will not be available until the selection is made and the **Apply** button is selected.

Click **Apply**.

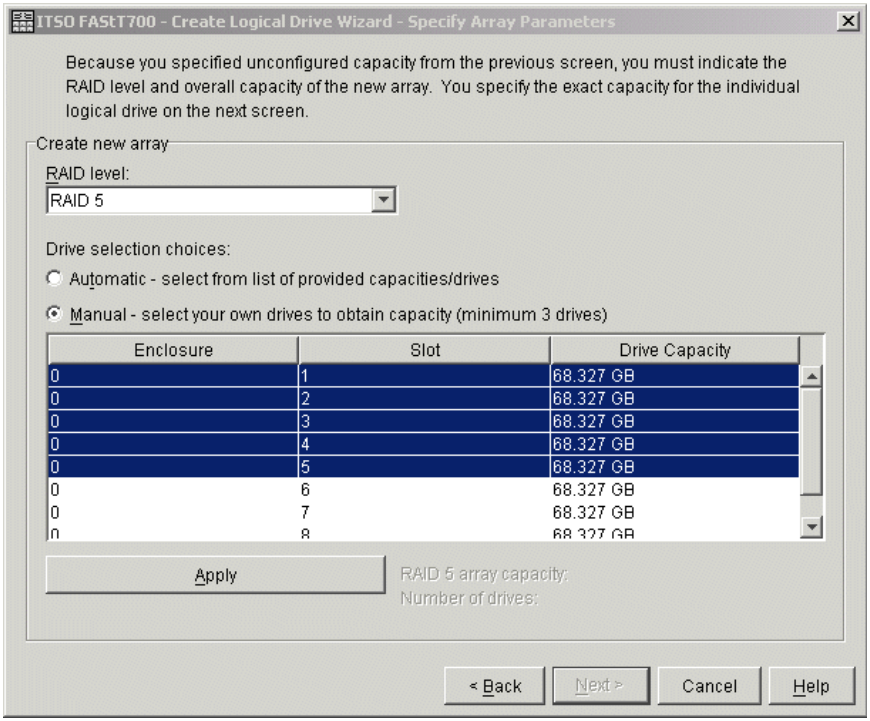


Figure 5-5 Specify array parameters

Select **Next** as shown in Figure 5-6 to apply the setting.

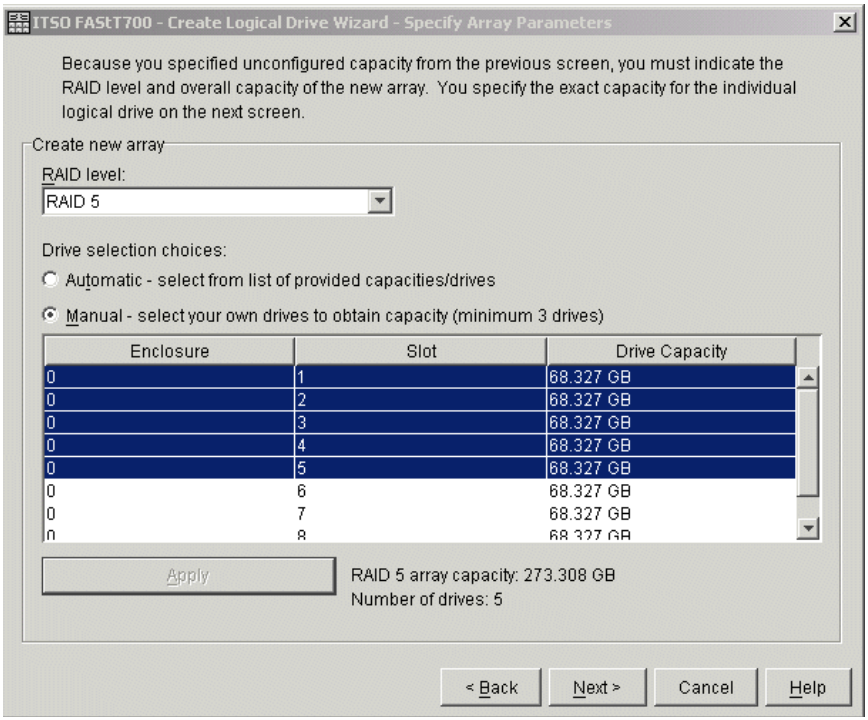


Figure 5-6 Array creation

The **Logical Drive Parameters** window will be opened as shown in Figure 5-7, select the drive size and type in the drive name that will be assigned to the logical drive. Click **Finish**. The drive will now be created.

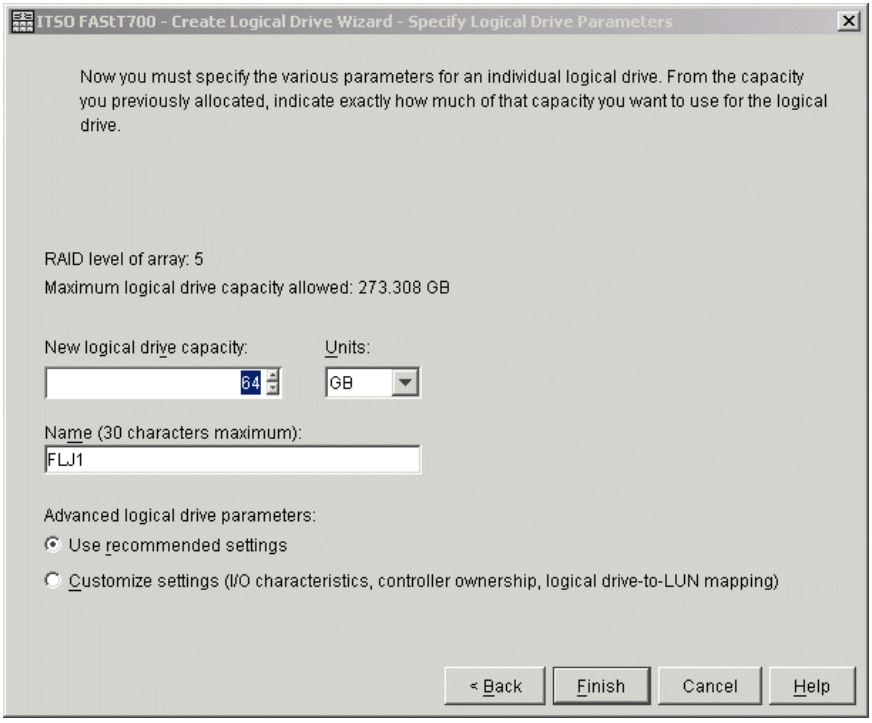


Figure 5-7 Logical drive Parameters

To create more drives, select the required setting. Or, to exit and close the window, select **NO** as shown in Figure 5-8.

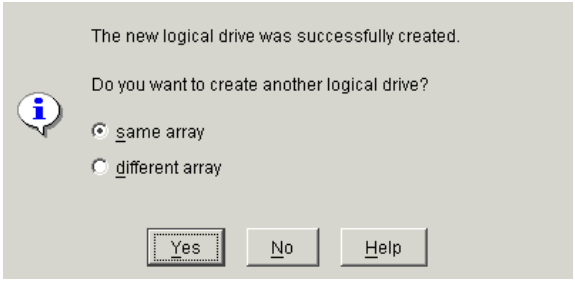


Figure 5-8 Logical drive option window

The storage and logical drive has now been created as shown in Figure 5-9. It shows the drives and controller that has been assigned to the logical drive as well as the RAID level.

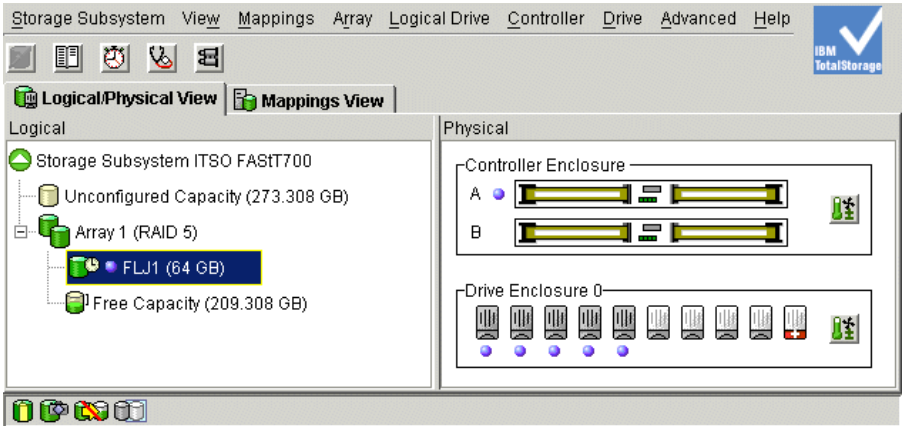


Figure 5-9 View created storage

5.2 Defining hosts

Select the **mappings view** as shown in Figure 5-10 to start configuring the required mappings for the NAS Gateway 500.

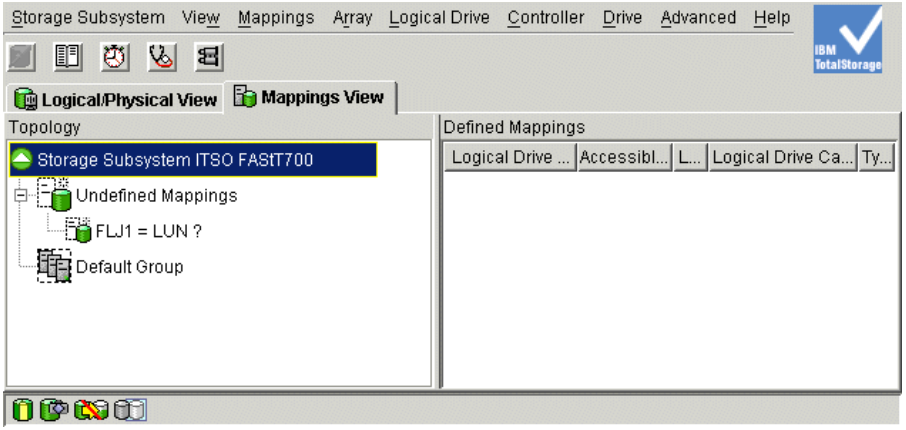


Figure 5-10 Mappings view

In the **Mappings view** window select the **Default Groups** option as shown in Figure 5-11, right-click the **Default Groups** and select **Define Host Group**.

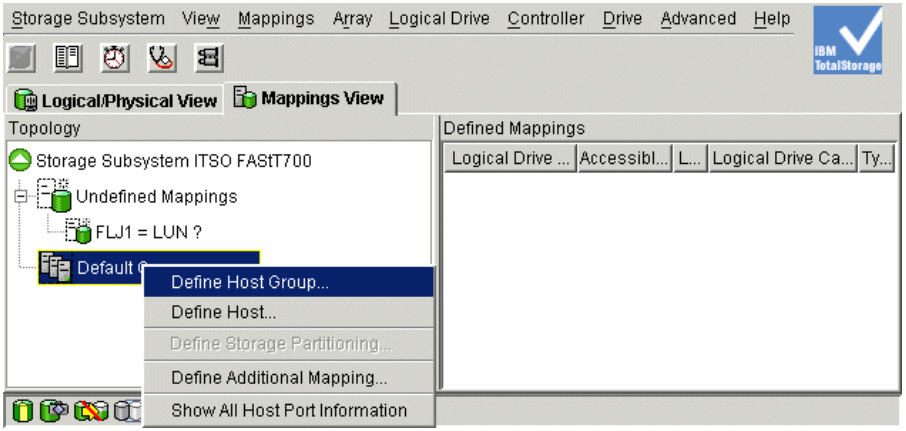


Figure 5-11 Host Group configuration

Type the group name in that will be associated with the NAS Gateway 500 as shown in Figure 5-12, and click **Add**.

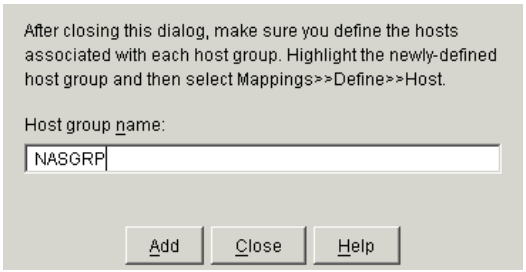


Figure 5-12 Host Group name

The host group will be added. You can add another group if required, or you can close the host group by selecting **Close**.

The host group will be added and shown in Figure 5-13. Right-click the newly created Host Group and select Define Host.

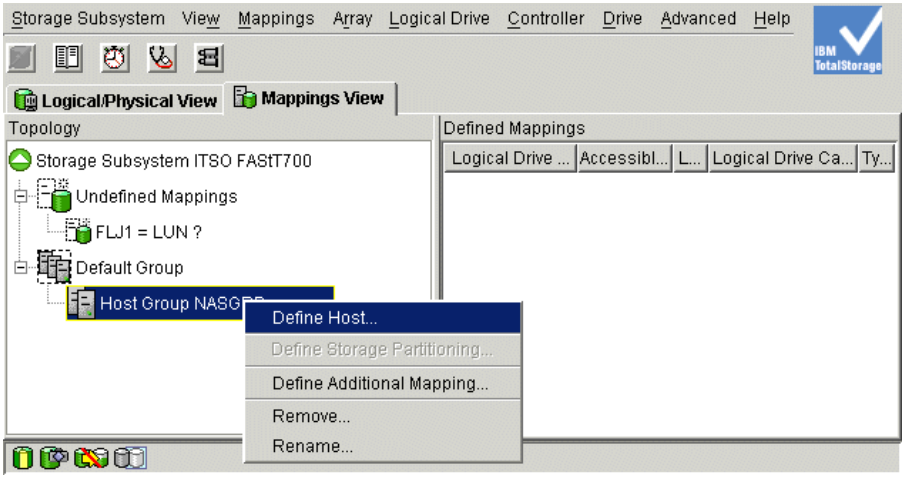


Figure 5-13 Host configuration

Type in the name that you want associated with the Host for the NAS Gateway 500 as shown in Figure 5-14, and select **Add**. Configure additional hosts, or close the window by selecting **Close**.

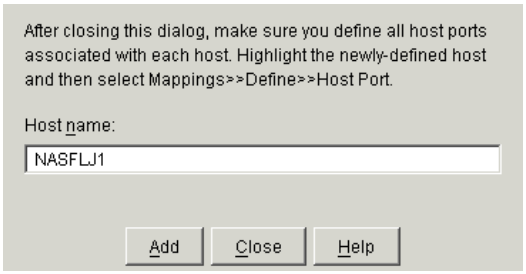


Figure 5-14 Define Host

The newly created host will now be available as shown in Figure 5-15, right-click the host and select **Define Host Port**.

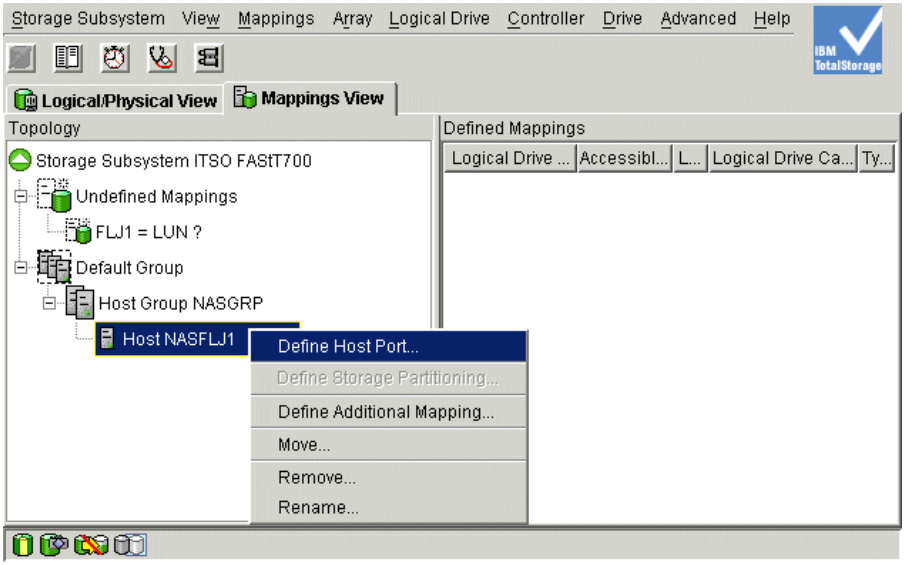


Figure 5-15 Define Host port

Select the WWN for the NAS Gateway 500 in the drop-down list under Host port identifier. Select **AIX** under Host type, then type in the name that will be associated with the Host port name as shown in Figure 5-16. Click **Add**.

Note: The WWNs of NAS Gateway 500 can be obtained as described in 3.2.1, “Finding the World Wide Name” on page 48.

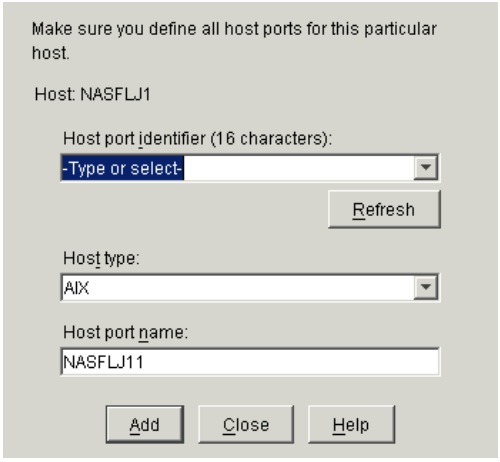


Figure 5-16 Host Port configuration

Configure additional host ports as required or select **Close** to finish.

5.3 Mapping logical drives

If you want to share the storage, right-click the **Group**. If you do not want to share the storage in the group, right-click the **Host** and select **Define Storage Partitioning** as shown in Figure 5-17.

Important: Remember that if you are configuring a cluster and using shared disks, you need to configure the second node in the same Host group but as a separate host with shared disk space between the group by adding the Storage partition to the Group and not the host port.

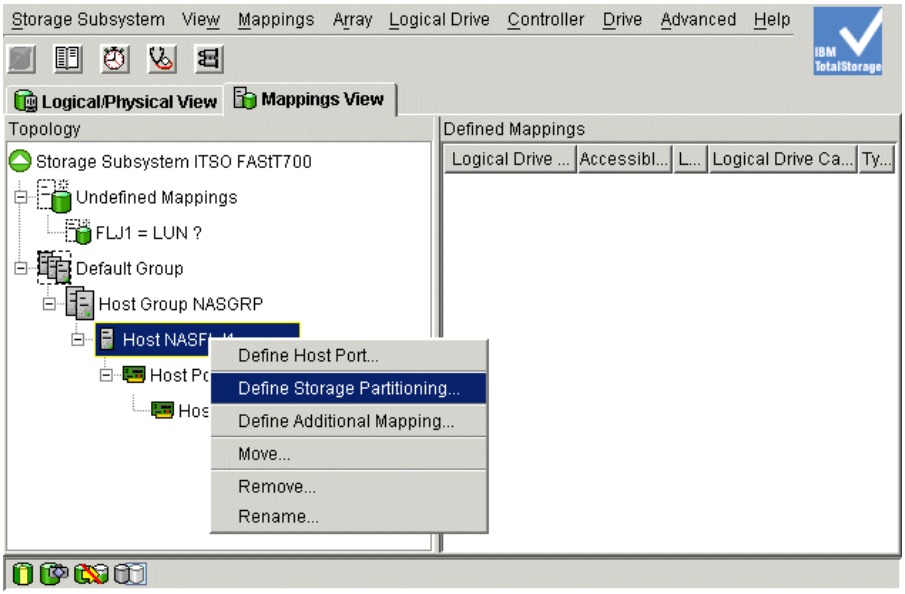


Figure 5-17 Storage partition

The partitioning wizard will now be opened as shown in Figure 5-18, select **Next**.

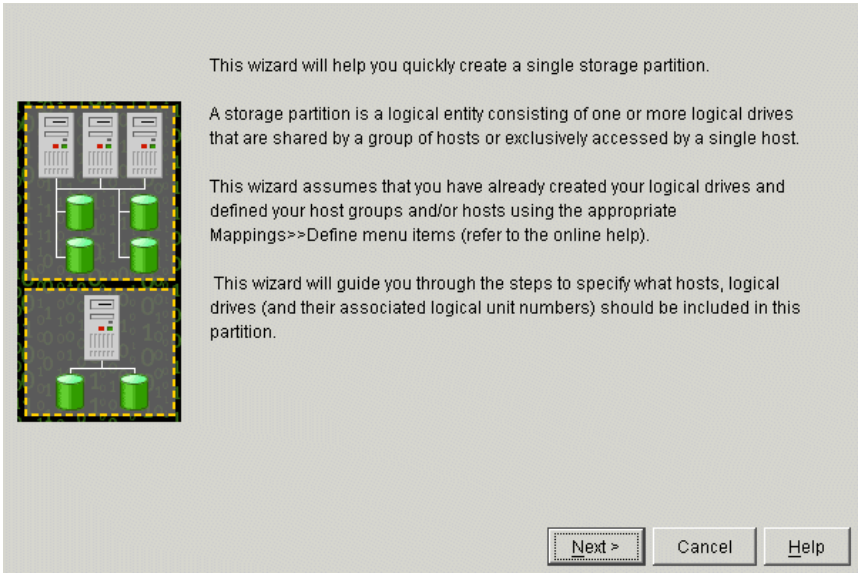


Figure 5-18 Partitioning wizard

The host group or host option will now be available, select **Host** and select the configured host for the NAS Gateway 500 as shown in Figure 5-19; select **Next**.

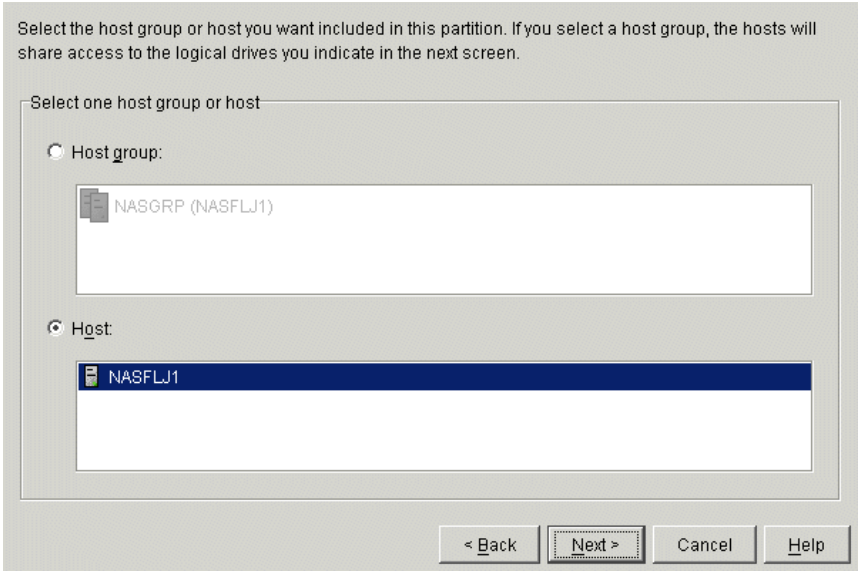


Figure 5-19 Assign host or host group

Select the configured storage partition on the left-hand side as shown in Figure 5-20 and click **Add**.

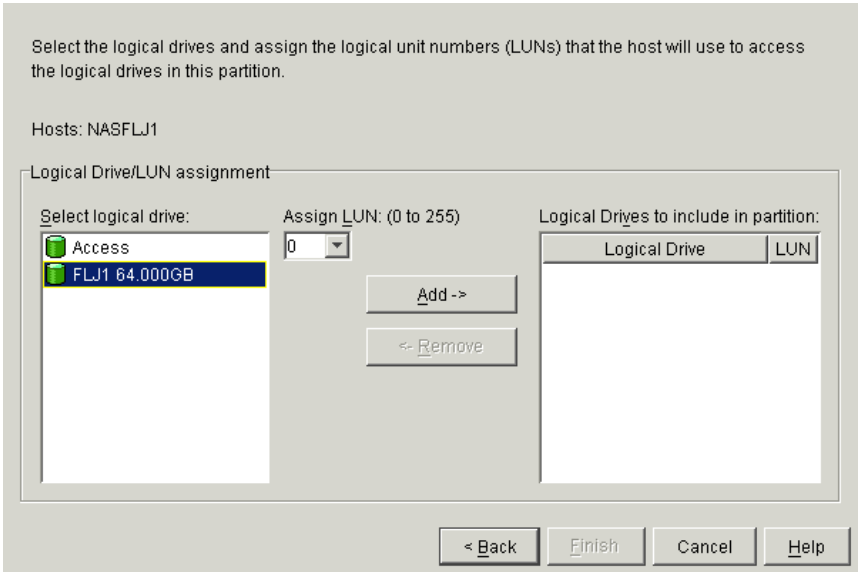


Figure 5-20 Logical Drive and LUN assignment

The logical drive will be moved to the right hand side as shown in Figure 5-21, select **Finish**.

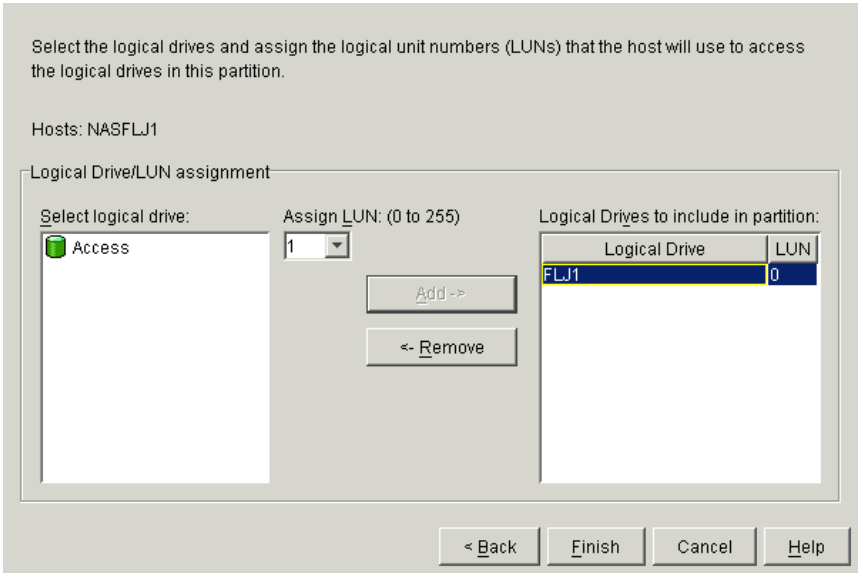


Figure 5-21 Configured logical drives and LUNs

The storage partitioning completion window will now be displayed as shown in Figure 5-22; select **OK**.

Figure 5-22 Completion

The configured storage on the FastT is now available as shown in Figure 5-23.

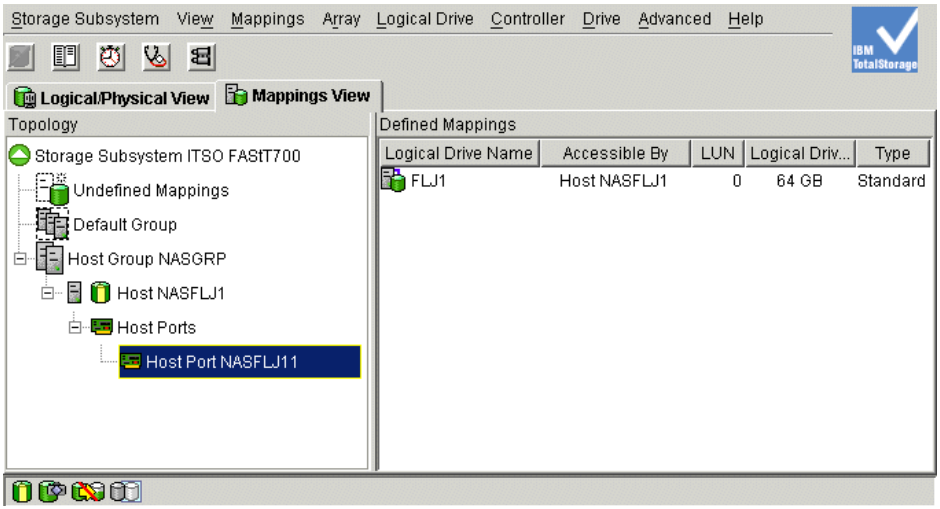


Figure 5-23 Configured FastT

The FAStT is now ready for use with the NAS Gateway 500. Next you need to configure the NAS Gateway 500 and assign the storage.

6

ESS storage configuration

If you are working in a production environment, there are many planning steps you should go through before proceeding with setup. This section does not cover all of them. If you need comprehensive background information on this subject, before proceeding, we recommend that you review either of the redbooks, *The IBM Enterprise Storage Server*, SG24-5645, or *ESS Solutions for Open Systems Storage: Compaq AlphaServer, HP, and SUN*, SG24-6119.

6.1 Regarding SAN zoning

With the ESS, we do not have to worry about setting failover modes like we do with the FAStT. Multiple failover modes are not required in the ESS, as the RAID controllers are separated from the connected hosts by a layer of management. The RAID controllers in the ESS are within the pSeries nodes inside the enclosure and, as these two nodes are in a clustered configuration, failure of a controller or entire node is handled internally.

Because failover is handled internally to the cluster, hosts connected to the ESS do not need to be aware of the internal workings of the disk subsystem — this is all provided by the cluster. If a failure occurs, although many changes take place within the cluster, the connected hosts see no differences, as their LUNs maintain their device and path identifiers on the alternate node — this is one of the features of the ESS solution.

Note: This description does not account for adapter or link failure in the connected hosts.

Figure 6-1 shows a logical view of the internals of the ESS. Connectivity to the disk is through the “intelligent” pSeries controllers (Nodes A and B).

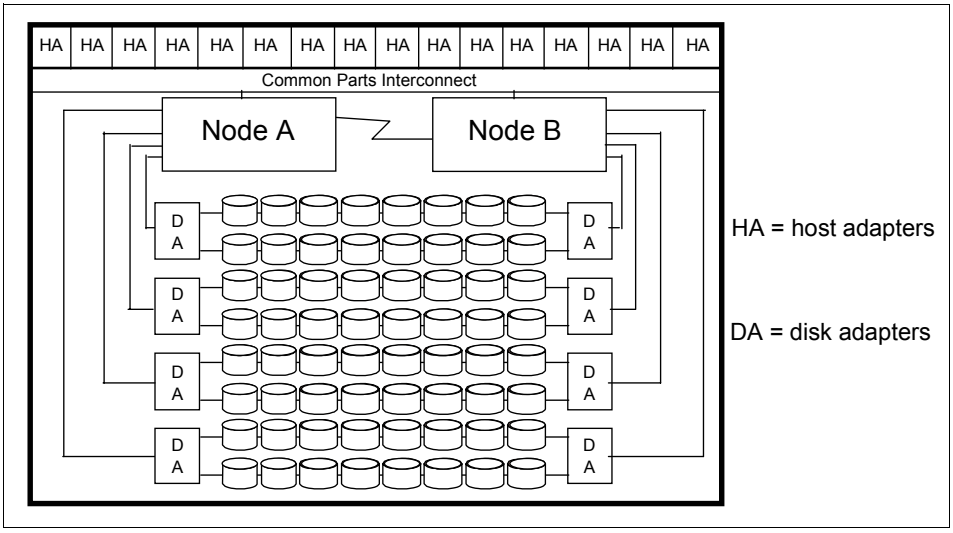


Figure 6-1 ESS internals

For more information on zoning and the switch products available from IBM, please see the redbook, the *IBM SAN Survival Guide*, SG24-6143.

6.2 Setting up the ESS

In this section, we document the steps involved in setting up the ESS for access by the NAS Gateway 500. A high-level view of the process is shown in Figure 6-2.

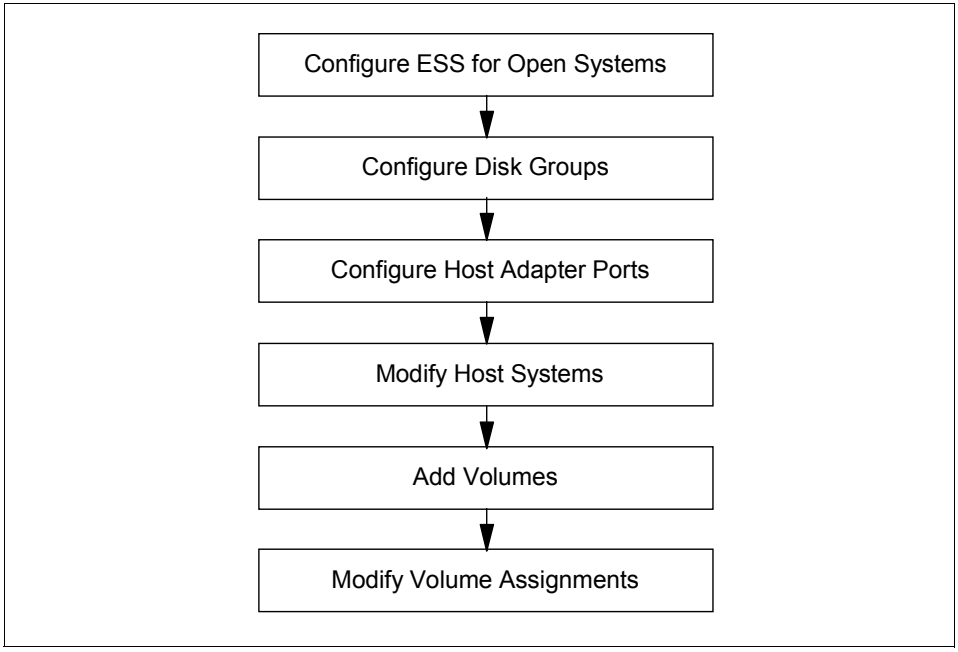


Figure 6-2 ESS preparation for the NAS Gateway 500

For the purpose of configuring the ESS, we will be using the IBM StorWatch ESS Specialist. It is a simple yet powerful administration tool that comes with the ESS at no additional cost, and it is the only supported way in which to manage the allocation of storage within the ESS storage subsystem.

More information on the IBM StorWatch ESS Specialist can be found in the redbook, *Implementing the Enterprise Storage Server in Your Environment*, SG24-5420.

6.2.1 Configure ESS for open systems storage

To configure our ESS, we must first launch the IBM ESS Specialist by entering the hostname or IP address for either of the ESS clusters in the location or URL window of the browser. Doing so will bring us to the ESS home page, as shown in Figure 6-3.

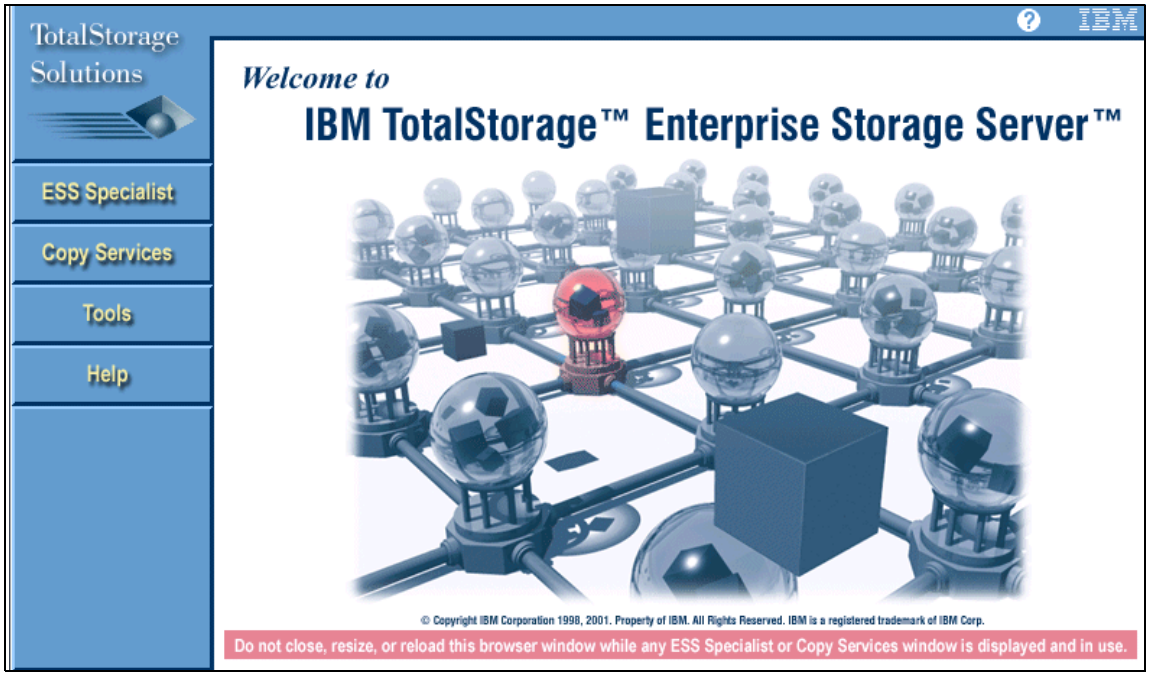


Figure 6-3 IBM ESS home page

Next we select the **ESS Specialist** option that will launch the IBM ESS Specialist home page as shown in Figure 6-4.

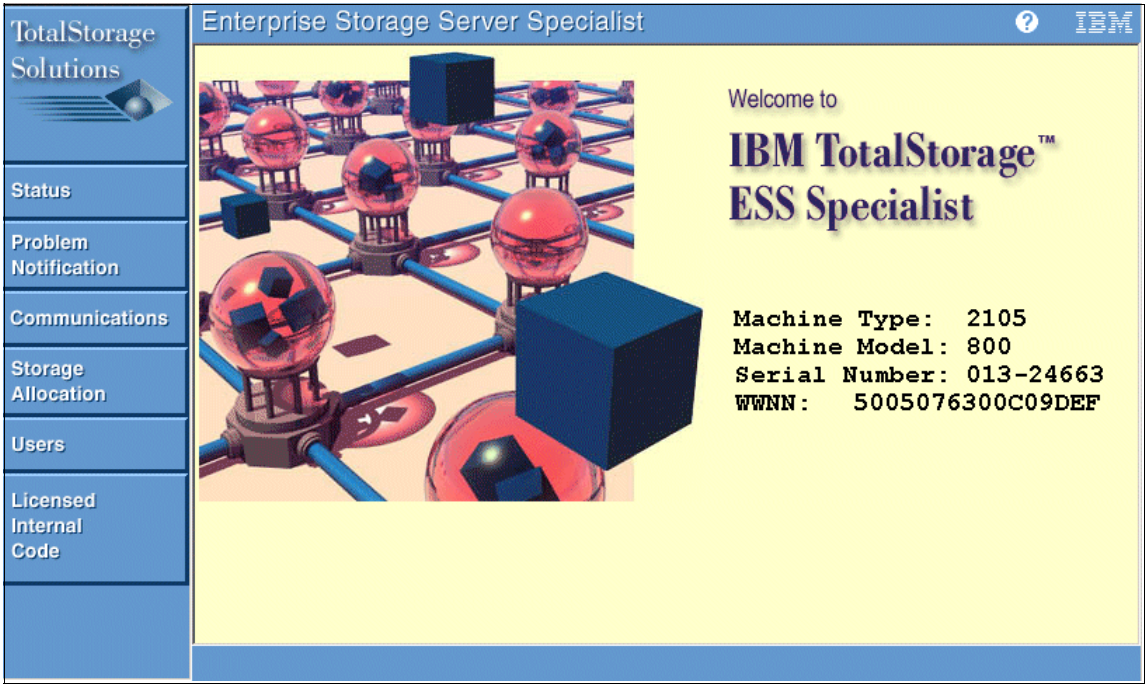


Figure 6-4 IBM TotalStorage ESS Specialist home page

Selecting the **Storage Allocation** button on the left of the home page will present the administrator with a number of security certificates and a login pop-up window. After successfully entering a valid login and password, the administrator will see the **Storage Allocation - Graphical View** window as shown in Figure 6-5.

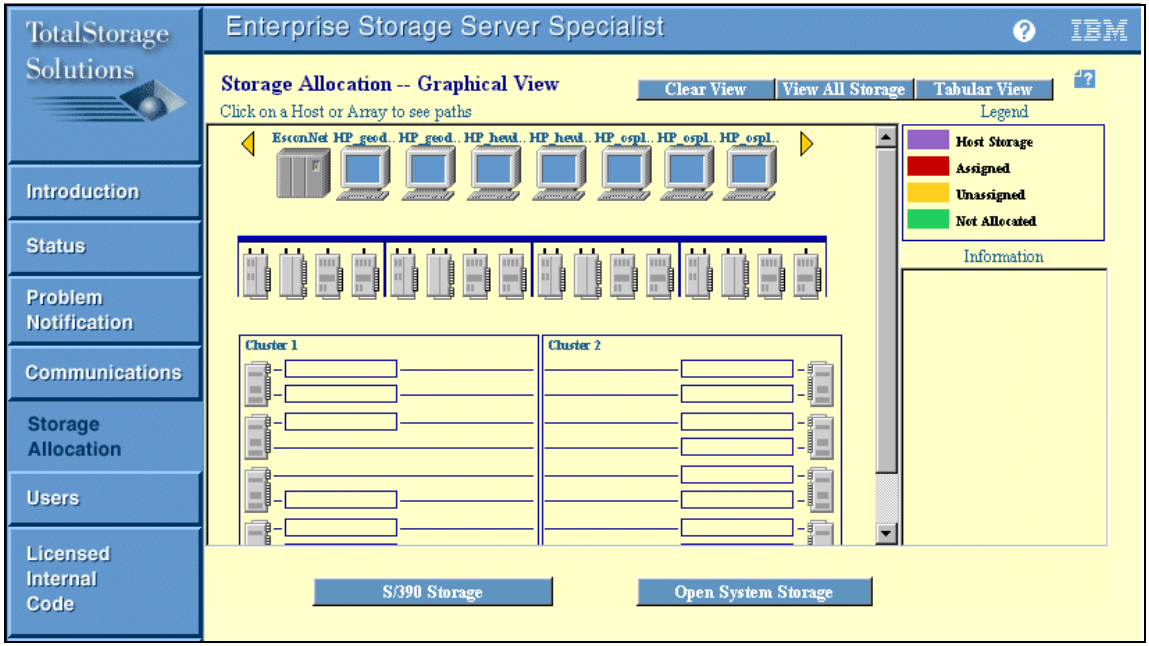


Figure 6-5 Storage Allocation panel

The **Storage Allocation** panel is the most important and detailed of the ESS Specialist panels. It provides an authorized user with a graphical representation of the hosts, host adapters (ESCON, SCSI, Fibre Channel and FICON), Device adapters (SSA Adapters), Clusters, and Arrays on the ESS machine.

From the Storage Allocation panel (seen in Figure 6-5), we can choose to create either **S/390 Storage** or **Open System Storage.** As we are creating a storage partition for the NAS Gateway 500, we should click the **Open System Storage** button in the bottom right of the panel.

Clicking the **Open System Storage** button will produce a screen similar to the one depicted in Figure 6-6. From this view, it is possible to add and remove hosts, configure HAs, setup disk groups, add and remove volumes, and modify how existing volumes are assigned.

The basic setup procedure is to click the buttons on the bottom of the screen in the order shown in the following pages.

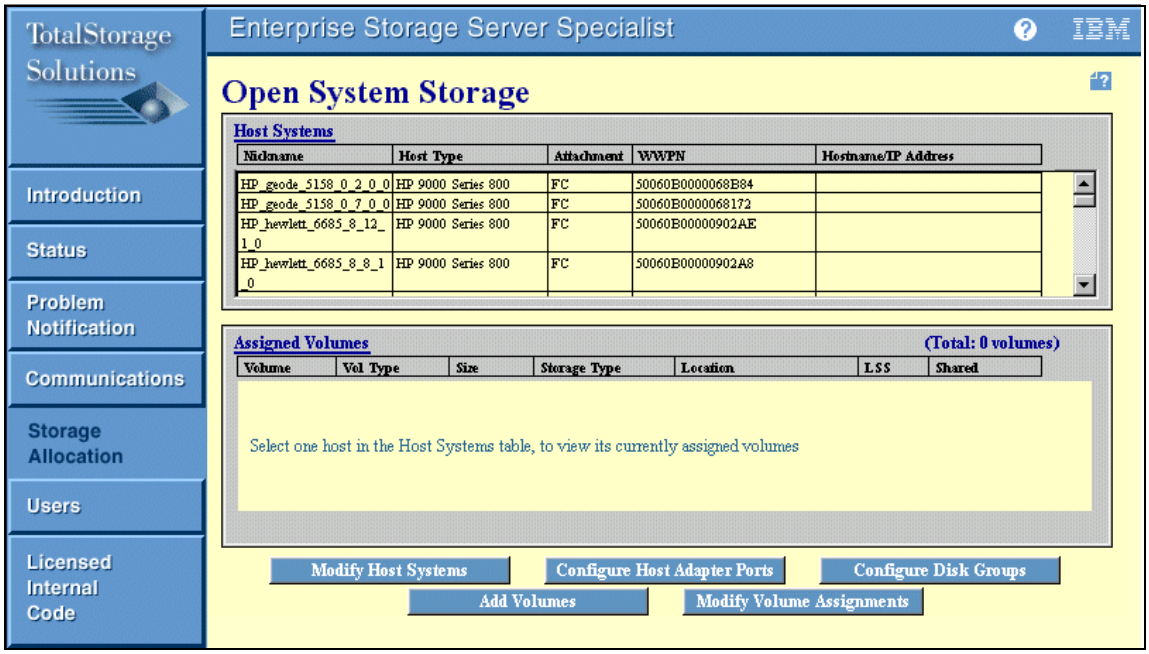


Figure 6-6 Open Systems Storage panel

6.2.2 Configure disk groups

We start here and click the **Configure Disk Groups** button. This brings up the window shown in Figure 6-7.

Note: This step is only necessary if no disk groups exist, or if there is insufficient space on the currently available disk groups.

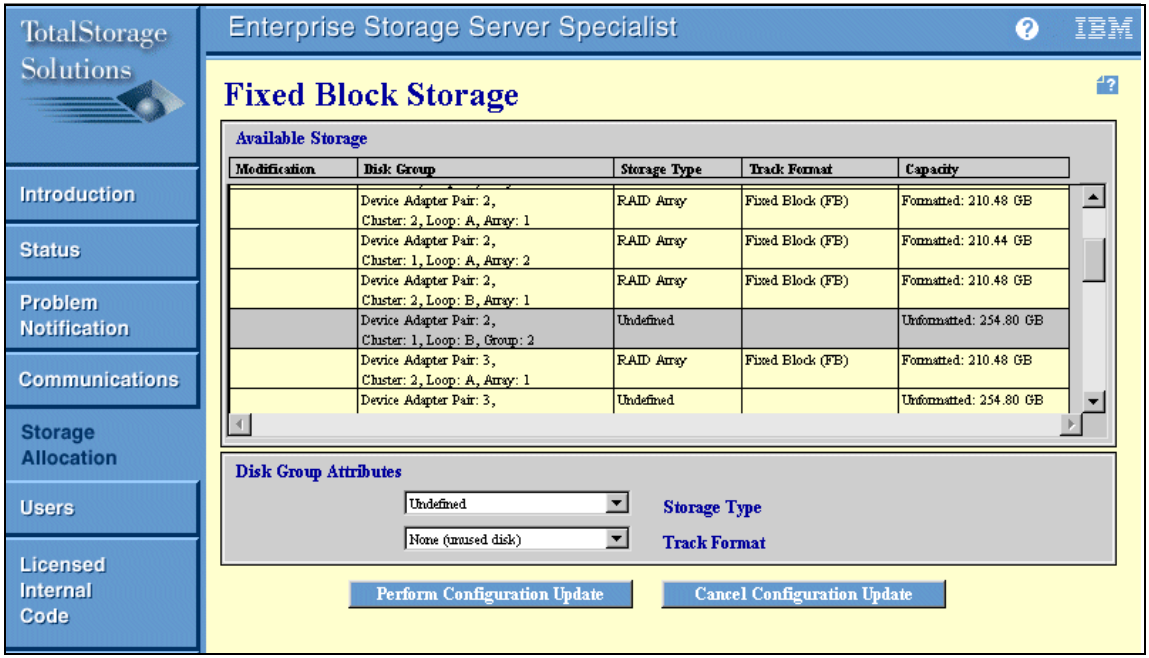


Figure 6-7 Fixed block storage groups

Scrolling through the table, we select an undefined disk group, select a Storage Type from the drop-down list (we chose **RAID ARRAY**) and **Fixed Block** as our Track Format as shown in Figure 6-8.

Attention: Changing disk group configuration will delete data on the disks. Ask your storage administrator if other systems are connected to the specific disk group.

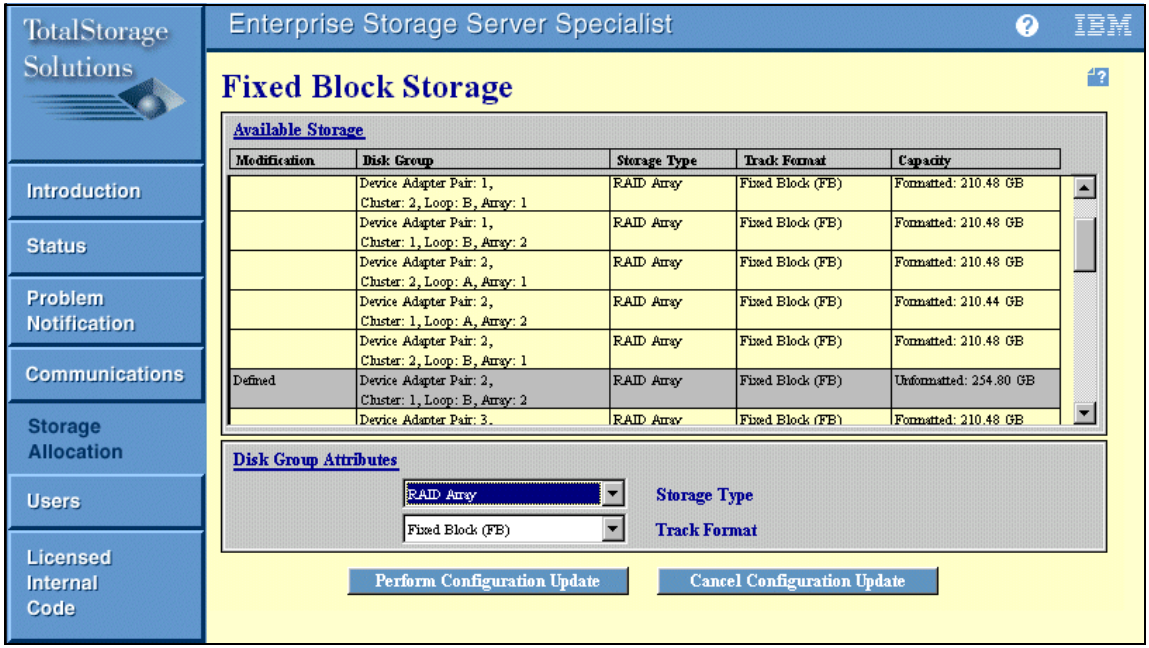


Figure 6-8 Define fixed block storage (RAID array)

Clicking the **Perform Configuration Update** button will reveal a warning message. This configuration update initializes the disk group ready for volumes to be created on it as shown in Figure 6-9.

Figure 6-9 Time intensive action warning

Clicking **Yes** will begin the process. (We recommend either taking a lunch break now or saving this action until just before going home and then picking up again the following day, because, depending on how busy the subsystem is, this process can take a couple of hours.)

6.2.3 Configure host adapter ports

Now we have configured our disk groups, we need to configure the host adapter ports in the ESS, as follows.

Select the **Configure Host Adapter Ports** button. This will bring up a display similar to the one in Figure 6-10. The HAs are graphically represented beneath the Configure Host Adapter Ports title. ESCON and SCSI HAs are identified by two ports located on the top of each HA in the view while Fibre Channel HAs have only a single port. ESCON and SCSI can be differentiated by the detail on the HA representation. Also, by clicking the HAs icon or by selecting the bay-adapter-port in the Host Adapter Port pull-down, different attributes will be displayed below the row of HAs.

Attention: Changing adapter definitions may cause connection problems. Please ask you storage administrator if you want to change HBA settings.

Finally, only those adapter slots that are occupied will be visible. Empty adapter slots will not be visible.

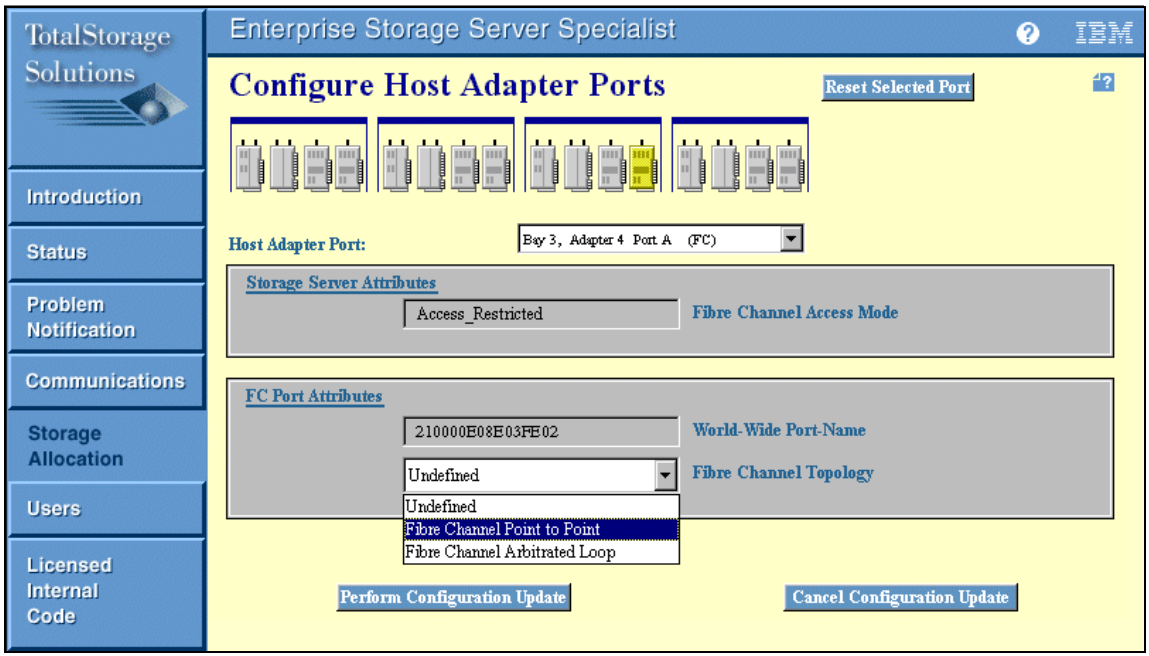


Figure 6-10 Configure host adapter ports

Unlike SCSI, Fibre Channel allows all hosts in a FC-SW or FC-AL environment to view all storage available within the environment (assuming no zoning has been established within a switch or restrictions put in place elsewhere). In order to get around the “see everything” issue, the Fibre Channel HAs within the ESS can be configured with **Access Restricted** attributes.

Using **Access Restricted** mode, the ESS limits the visibility of the LUNs to only those WWNs associated with each LUN. In effect, the ESS performs LUN masking to prevent other hosts from gaining access to LUNs that are not defined as available to those hosts.

Select a Fibre Channel host adapter card at the top of screen and we see whether it is configured as **Undefined**, **Fibre Channel Point to Point**, or **Fibre Channel Arbitrated Loop**. We can either use a predefined adapter or define our own by finding an adapter that is **Undefined** and selecting the appropriate Fibre Channel topology. When connecting direct from the host to the ESS or via a hub, we must select **Fibre Channel Arbitrated Loop**. If connecting via a switch, we must select **Fibre Channel Point to Point**.

At this point we can click **Perform Configuration Update**.

6.2.4 Modify host systems

To add, remove, or modify an existing host, select the **Modify Host Systems** button from the bottom left of the Open Systems Storage panel. The display in will appear as shown in Figure 6-11.

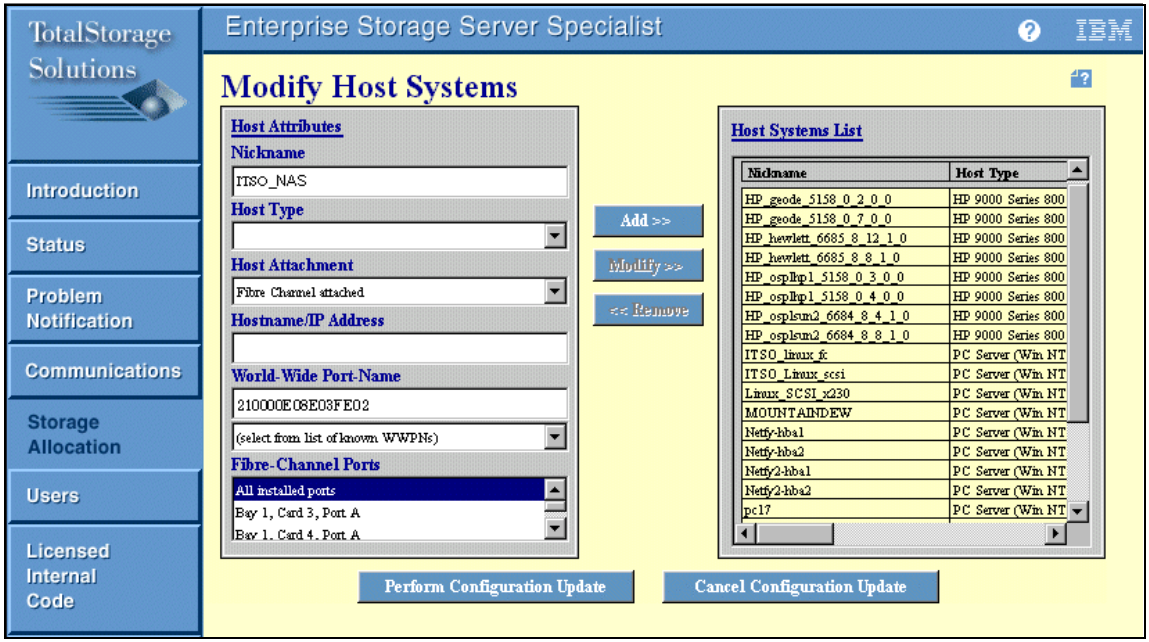


Figure 6-11 Modify Host Systems panel

To add a new host, fill in the fields within the Host Attributes table on the left. The Host Type configured is extremely important, as the ESS determines drive geometry, labels, targets, and LUNs available, and so on, based on the `Host Type` field.

The Hostname/IP Address field is optional in all cases. However, when configuring a Fibre Channel host, we must enter the WWN of the host adapter. Be careful, as mistakes in typing this number will lead to hard-to-trace connectivity failure.

Once you are satisfied with the settings, click the **Add** button and the newly created host will be displayed within the Host Systems List table on the right, as shown in Figure 6-12.

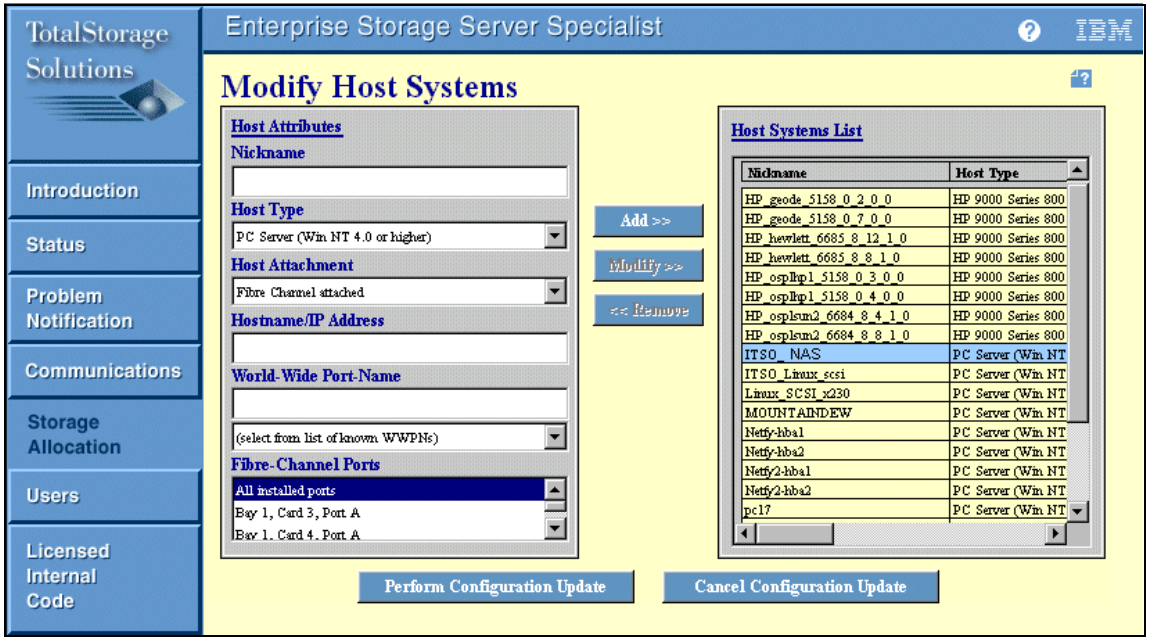


Figure 6-12 Added host systems

None of the changes we have made to this point will take effect until the **Perform Configuration Update** button at the bottom of the screen is selected. Once we select this button, we see a progress window as shown in Figure 6-13.

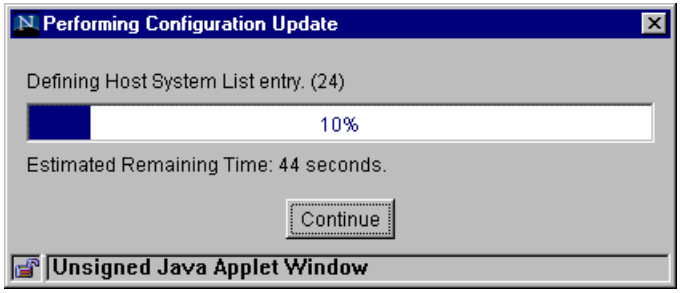


Figure 6-13 Host modification in progress

6.2.5 Add volumes

Now that we have a defined Open System disk groups, configured the host adapter ports, and modified host systems we are ready to add volumes to it and assign them to our hosts. From the Open Systems Storage panel, click the **Add Volumes** button on the bottom left of the screen. Doing so will reveal the Add Volumes (1 of 2) panel, as shown in Figure 6-14.

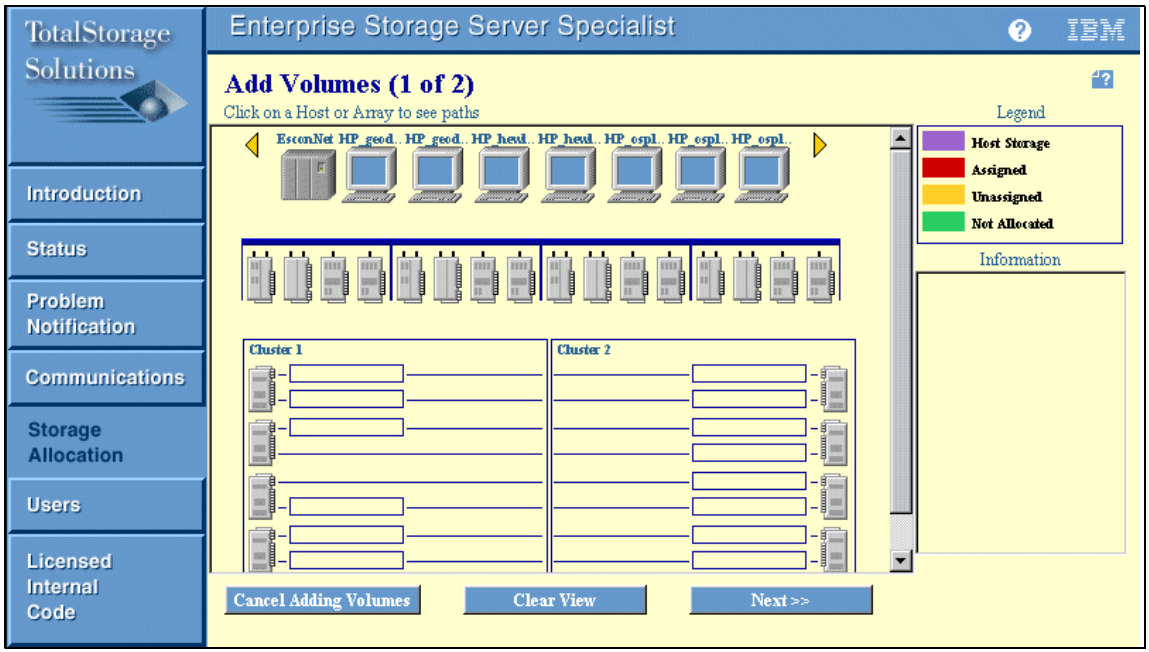


Figure 6-14 Add volumes panel

Scroll through the list of hosts at the top of the screen and select the Fibre Channel host we defined earlier. Once selected, lines will be drawn to all host adapters through which that host can access LUNs, as shown in Figure 6-15. Select the appropriate host adapter.

Note: After selecting a fibre-attached host, all Fibre Channel host adapters in the ESS will be highlighted as being valid access paths to LUNs. This indicates *possible* connections rather than actual connections as, in the case when we are direct connected, we can actually only see LUNs through the host adapter we are physically connected to. Be sure to select a Fibre Channel adapter we are *actually* able to connect through, as dictated by direct connection or SAN zoning.

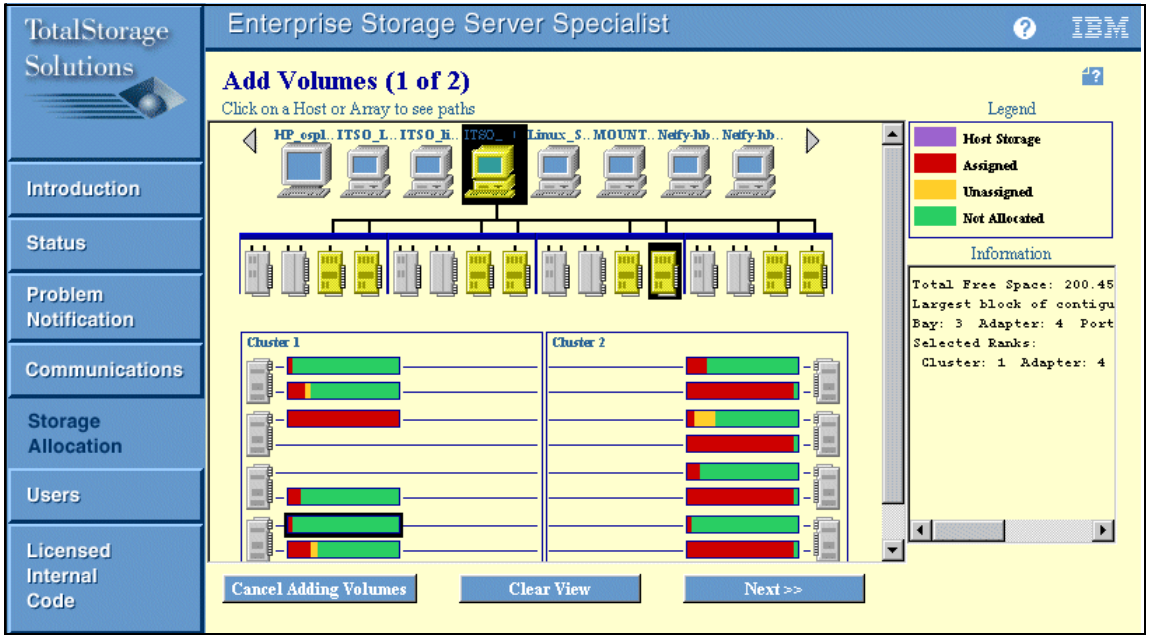


Figure 6-15 Add volumes to selected host

After selecting a valid Fibre Channel host adapter, we highlight the disk group (or groups) on which we wish to create LUNs. Then, click the **Next** button to reveal the second configuration page, as shown in Figure 6-16.

Note: We are showing the process of setting up LUNs on disk groups, but this should not be done in isolation from, or prior to, an end-to-end storage plan for the subsystem.

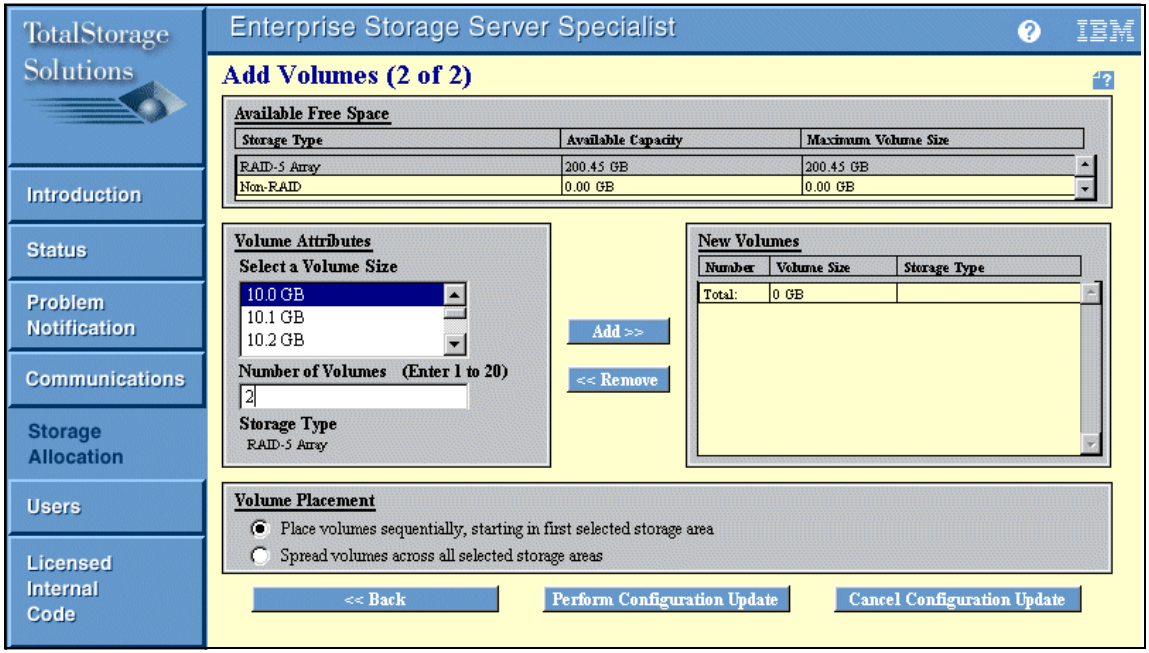


Figure 6-16 Select number and size of LUNs

On this panel we select an item from the list of available free space in the top window (typically RAID-5 Array), then select the size of the volume(s) we wish to create in the Volume Attributes window and the number of volumes of that size we wish to create. We have selected to create two 10 GB LUNs. If we had selected more than one disk group in the step before this, we could also select to have our LUNs distributed evenly across those groups. As we did not do so, we will leave the default Volume Placement selection as is.

We click the **Add** button, and the new LUNs appear in the New Volumes window on the right of the screen as shown in Figure 6-17.

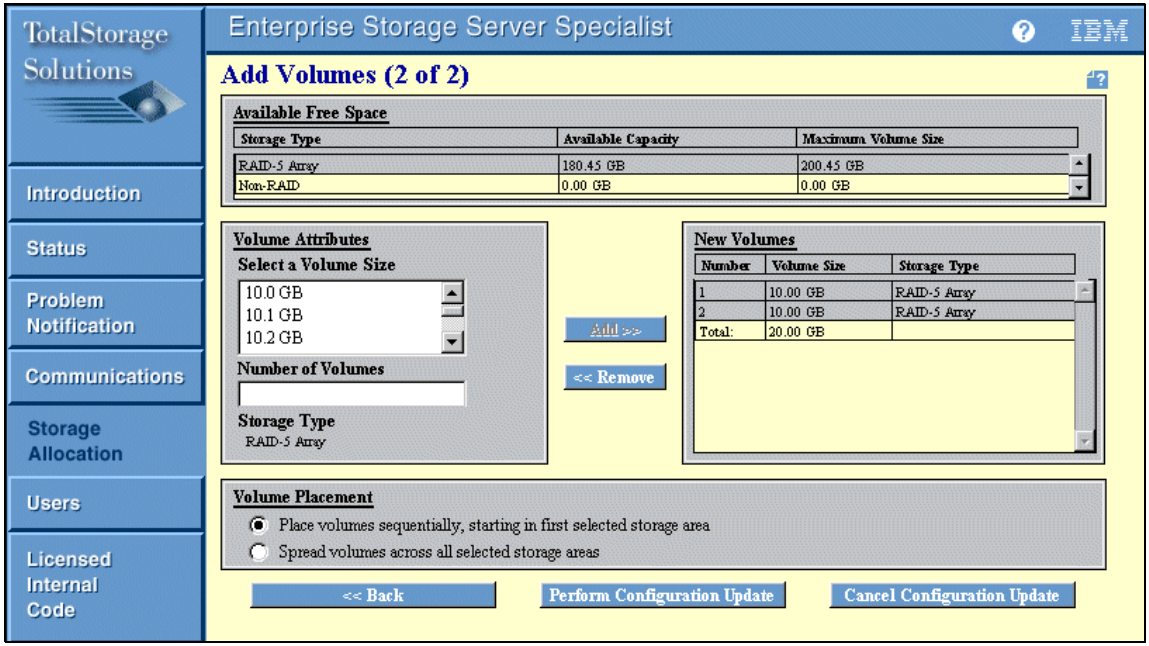


Figure 6-17 New volumes created

Create additional LUNs as desired. When finished, click **Perform Configuration Update**. Once again, we see a “time intensive activity” warning window followed by the progress indicator and, finally, the “Volumes Successfully Added” message box.

When this is done, we are returned to the Add Volumes panel.

6.2.6 Modify volume assignments

From time-to-time, it may become necessary to modify the assignment of volumes. For example, if we wish to assign a LUN to the second host in a cluster or assign a LUN to a second adapter in an existing host (which must have multi-path support in host operating system). We are going to assign LUNs to a second adapter in our host.

First we need to define our new host and the host adapter port in the ESS. Then we are ready to assign our LUN using the Modify Volume Assignments display.

From the Open System Storage window, select the **Modify Volume Assignments** button as shown in Figure 6-18.

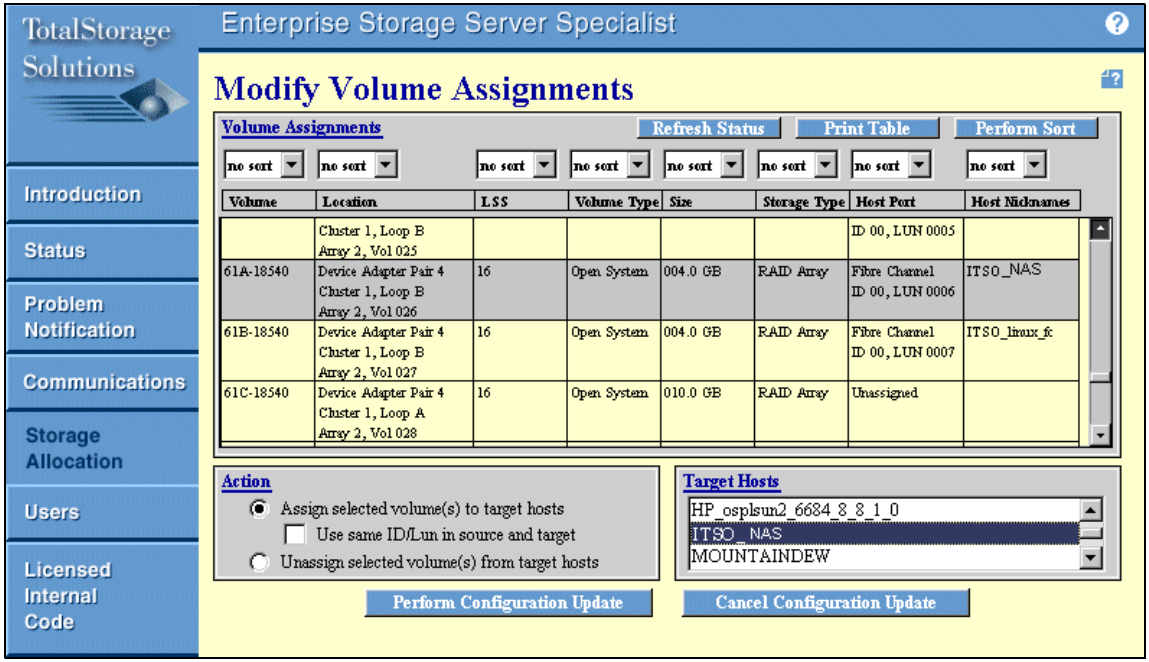


Figure 6-18 Modify volume assignments

We select the volume(s) that we wish to modify from the table. When we select the `Action` radio button (either assign or unassign) notice the list of hosts in the Target Host window on the bottom right of screen changes. Select the host or hosts to perform the action on, and select **Perform Configuration Update**.

Note: The check box, Use same ID/Lun in source and target, is optionally selected to allow some control over the ID and LUN used for the new assignment.

We should now see the progress indicator followed by the “volume assignment successful” message box. If we now scroll back through the Modify Volume Assignments table (easier if we sort first), we see that the LUNs are now assigned to our host as shown in Figure 6-19.

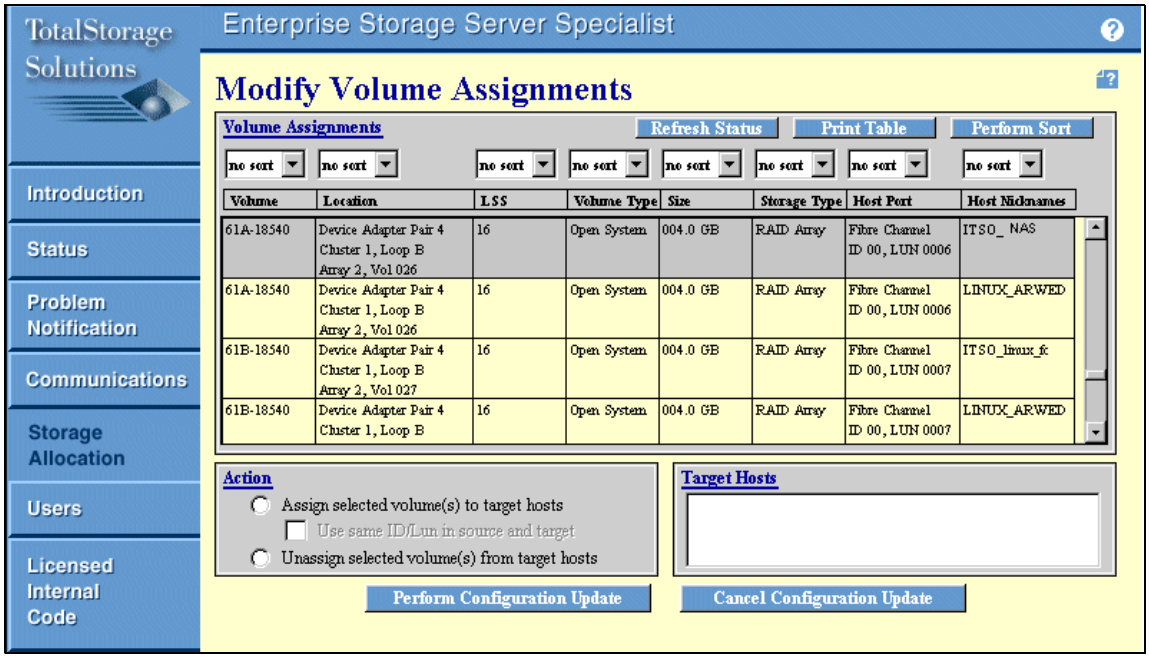


Figure 6-19 Validate volume assignment modification

We have now completed all the tasks required on the ESS side of things; we have allocated storage to our NAS Gateway 500.

Part 3

Implementation

In this part of the book, we introduce how to implement the NAS Gateway 500 system in your network.

7

Single node setup

This chapter describes initial configuration procedures which have to be done after unpacking the NAS Gateway 500.

The following topics are covered:

- Description of our lab environment
- Planning for the setup
- NAS Gateway 500 communication and signalization
- Installing the Web-based System Manager client program
- Initial configuration of a single node
- Feature selection
- General wizard
- Network configuration
- CIFS configuration
- NAS volume wizard
- Starting the Feature wizard again

Important: Before you set up the NAS Gateway 500, make sure you have SAN storage available, otherwise you will not be able to create any CIFS or NFS shares.

7.1 Our environment

Here is the description of the lab environment we were using for this book (Figure 7-1).

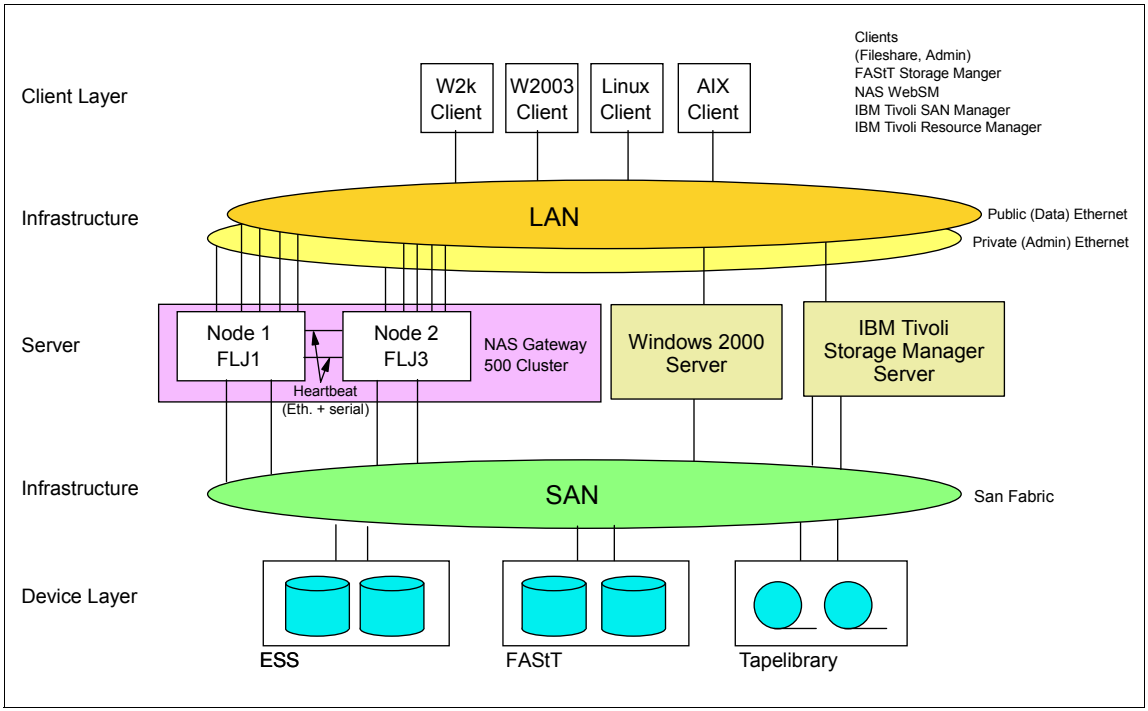


Figure 7-1 Our lab environment

Dependent on the section of the book, single NAS Gateway 500 node or both nodes are used. On the client side, the NAS Gateway 500 is connected to the public LAN, where the following servers and clients have access to it:

- Windows 2000 server
- Windows 2003 server
- Red Hat Linux 9.0
- SuSE Enterprise Server
- Apple 10.x client
- AIX 5.2 client

Through fabric connection on the storage side, the NAS Gateway 500 has access to ESS, FAStT, and a tape library. Additionally, a Tivoli Storage Manager server is used to do LAN-free backup of the NAS Gateway 500 device.

Disclaimer: At the time this book was written, the final release of the NAS Gateway 500 code was not available yet. Because we were working with the prerelease code, it is possible there are some differences to the final product.

7.2 Planning for the setup

Before starting the setup of the IBM TotalStorage NAS Gateway 500, it is a useful practice to create a plan. Basically, you need to write down the important data about the NAS Gateway 500, such as the following items:

- Name of the machine (or machines if used in a clustered configuration)
- Type and number (maximum 4) of network adapters installed in the machines
- Type and number of Fibre Channel adapters (maximum 6 per machine)
- IP address to be used for each ethernet adapter
- WWN of each used Fibre Channel adapter
- Administrator, user names, and passwords to be used on NAS Gateway 500
- Cluster name
- Cluster host names
- IP addresses, subnet, and gateway address for the cluster
- Method of cluster failback

You will find the *IBM TotalStorage NAS Gateway 500 Planning Guide* on the shipped Publications CD-ROM (included with the NAS Gateway 500 shipment) in softcopy. A download is also available on the IBM TotalStorage NAS Web page.

`http://www-1.ibm.com/servers/storage/support/nas/index.html`

In addition to describing the device, it also provides basic steps of the setup and configuration worksheets, where you can write the above-mentioned information. Look in Appendix D for these two worksheets:

- Network adapters worksheet
- Clustering worksheet

7.3 Service/management connections and indicators

NAS Gateway 500 is a file serving device, designed to be used in a headless mode. This means it uses no keyboard and mouse and has no internal video adapter to connect to a monitor. There are two preferred ways of connecting to the NAS Gateway 500 for setup and configuration purposes:

- Via ethernet port from a network connected management workstation
- Via a serial port using an ASCII terminal

Important: The initial configuration must be done via WebSM on Ethernet port 1.

The NAS Gateway 500 has an additional way of communicating its status — an LCD operator panel in the upper left front side of the box, as visible in the photograph in Figure 7-2.

Figure 7-2 NAS Gateway 500 LCD operator panel

There are several buttons and indicators located on the LCD operator panel (Figure 7-3). Following this is the description.

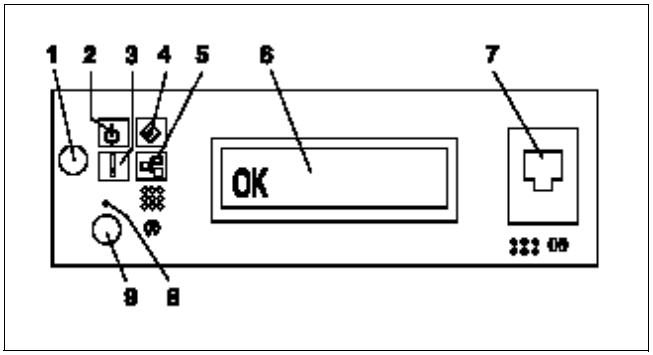


Figure 7-3 LCD operator panel

1. Power-on button
2. Power-on LED (blinks when the NAS Gateway 500 is not powered on)
3. System Attention LED
4. SCSI port activity LED
5. Ethernet port activity LED
6. LCD operator panel display

7. Serial port 1 (RJ-48 connector)
8. Service processor reset button (pinhole)
9. System reset button.

Serial port 1 is also connected to a DB-9 connector on the back side of the NAS Gateway 500. It should be used for connecting the ASCII terminal for configuring the NAS Gateway 500 device (Figure 7-4).

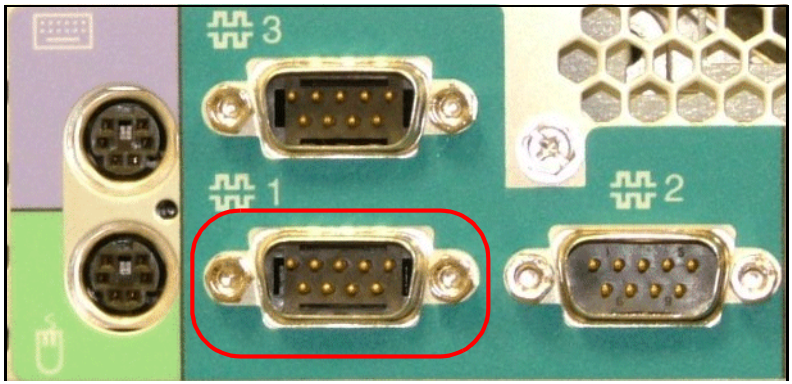


Figure 7-4 Serial port 1 for ASCII terminal

7.4 Basic setup of a single node NAS Gateway 500

The IBM TotalStorage NAS Gateway 500 is designed as a headless system, so setup and management has to be done from a network management workstation. The first steps include positioning the NAS Gateway 500 in a secure environment, and connecting it to the power, network connection, and external storage. After initial configuration you can also use a console, attached to the serial port 1 for service and management.

7.4.1 Connecting and powering on the NAS Gateway 500

For initial configuration, the integrated ethernet port 1 (bottom of the two) on the back of the NAS Gateway 500 must be used (Figure 7-5).

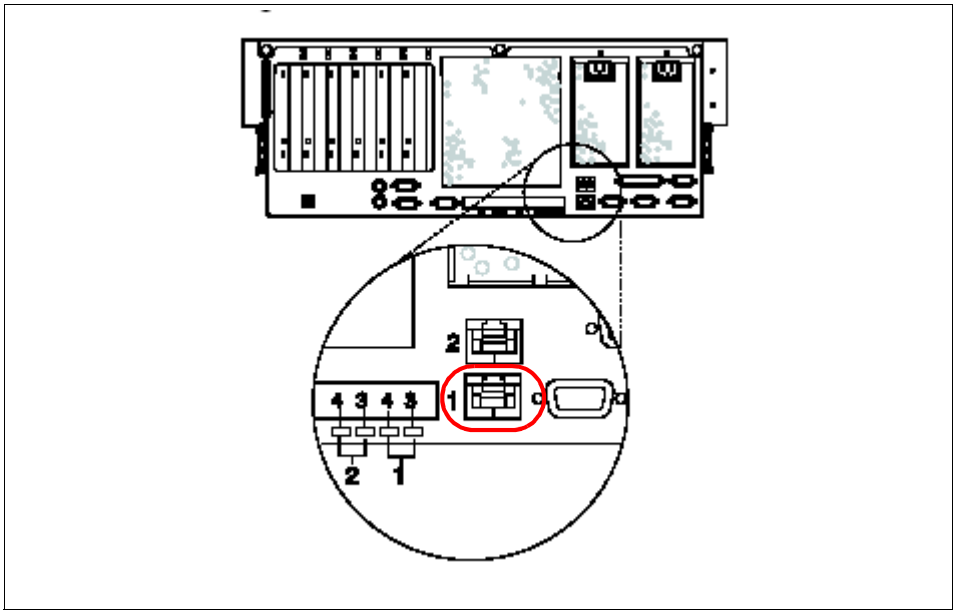


Figure 7-5 Connecting to the integrated ethernet port 1

Power on the NAS Gateway 500 by pressing the power-on button. Wait for the operating system to load. If there is a DHCP server in the network, the NAS Gateway 500 will accept a dynamic IP address. If there are no available dynamic addresses, the NAS Gateway 500 will use a predefined IP address.

Important: The IP address and the ethernet interface used during the configuration will be displayed on the IBM NAS Gateway 500 LCD operator panel, as shown in Figure 7-6. Write down the IP address and interface number for future reference.

Figure 7-6 IP address and ethernet port

7.4.2 Web-based System Manager Remote Client installation

To be able to set up and manage the NAS Gateway 500 using a graphical user interface, Web-based System Manager (WebSM) Remote Client has to be installed first for Windows or Linux client systems. The installation code is provided on the NAS Gateway 500 itself and will download to the managing workstation the first time you connect to it. Open a browser and type in the IP address, shown on the LCD operator panel.

Note: If the client operating system is AIX, the Remote Client is a part of AIX and no installation is necessary.

For our lab setup we will show how to download and install the WebSM Client on a Windows system.

Note: When you try to browse to the NAS Gateway 500 the next time after you accepted the license agreement, you have to append **`/NAS500Index.html`** to the IP address.

After selecting the default language, move on by clicking the **Continue** button (Figure 7-7).

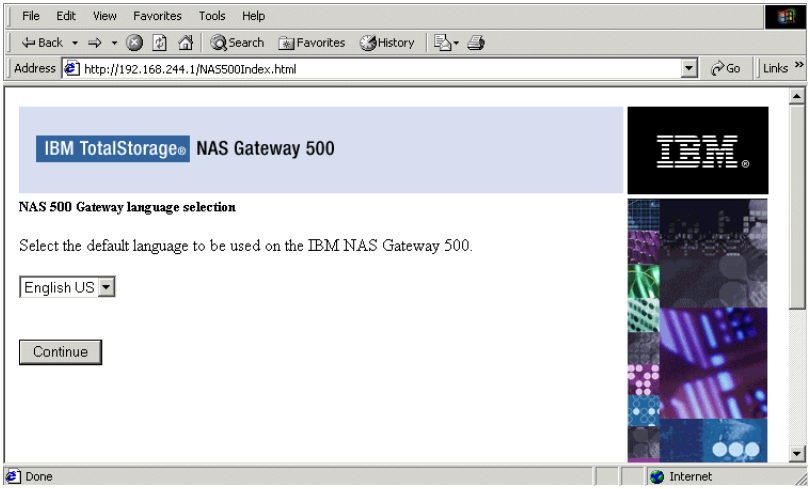


Figure 7-7 Connecting to the NAS Gateway 500

Read the licensing terms and continue by clicking **Accept** (Figure 7-8).

Important: You have to accept the licensing terms, otherwise you will not be able to connect to the NAS Gateway 500 with WebSM.

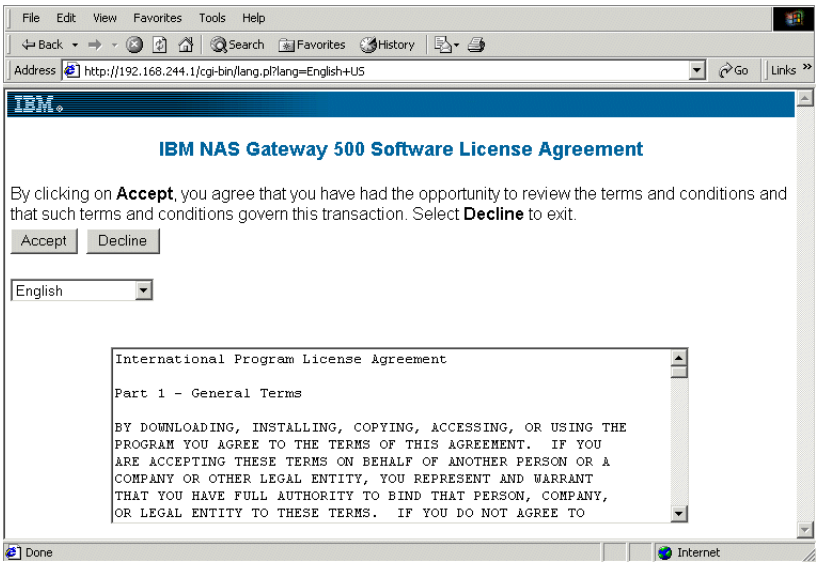


Figure 7-8 Software License Agreement

Select the correct version of the Remote Client based on the workstation operating system you are using for this configuration by clicking the corresponding link. Versions for Windows or Linux environments are available (Figure 7-9). AIX client systems do not require this installation.

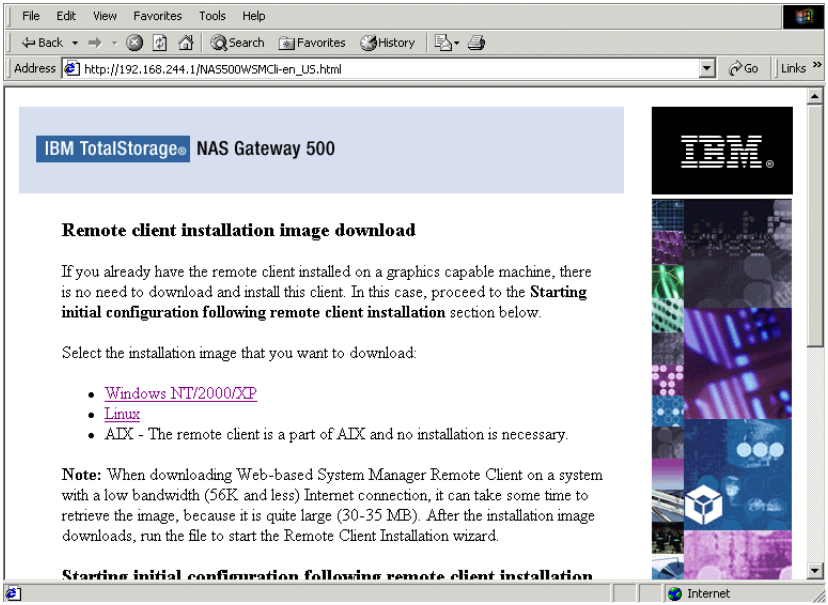


Figure 7-9 Selecting the client version

Download the installation program first. Select **Save this program to disk** and click **OK** to download it to your machine first (Figure 7-10).

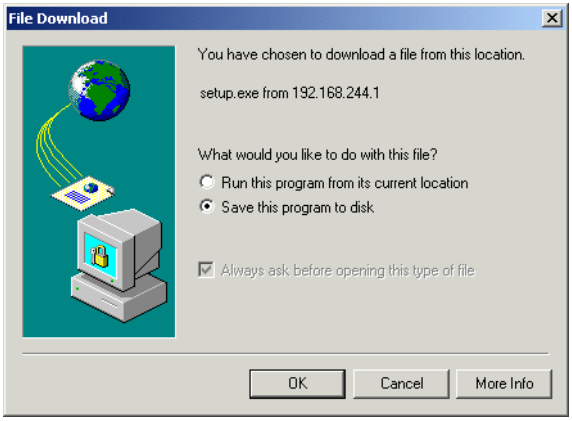


Figure 7-10 Downloading the installation program

When download is complete, double-click the file. The installation of the WebSM client will start (Figure 7-11).

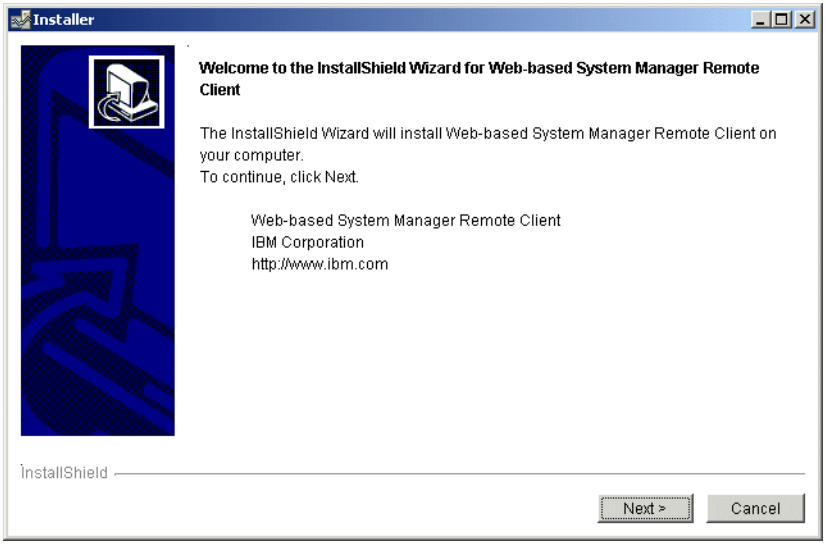


Figure 7-11 WebSM client installation start

Confirm the proposed installation folder or define another location (Figure 7-12).

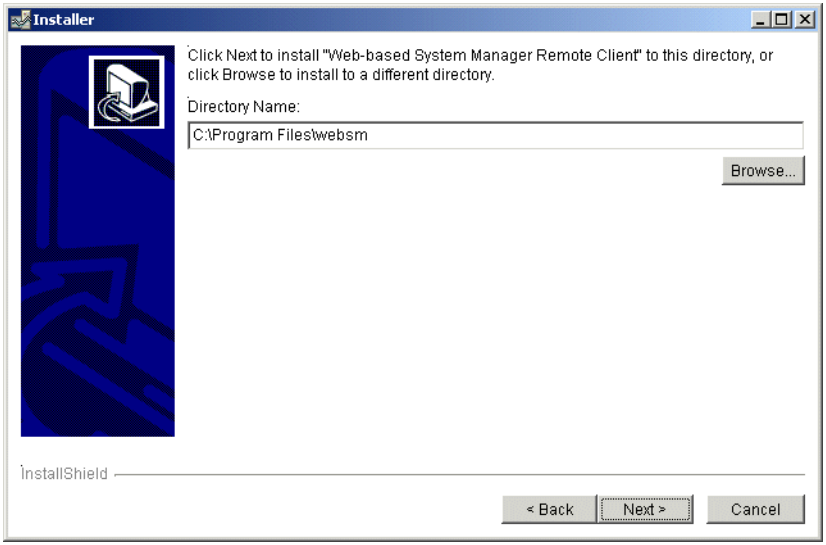


Figure 7-12 Installation folder

By clicking **Next**, the installation will start, as shown in Figure 7-13.

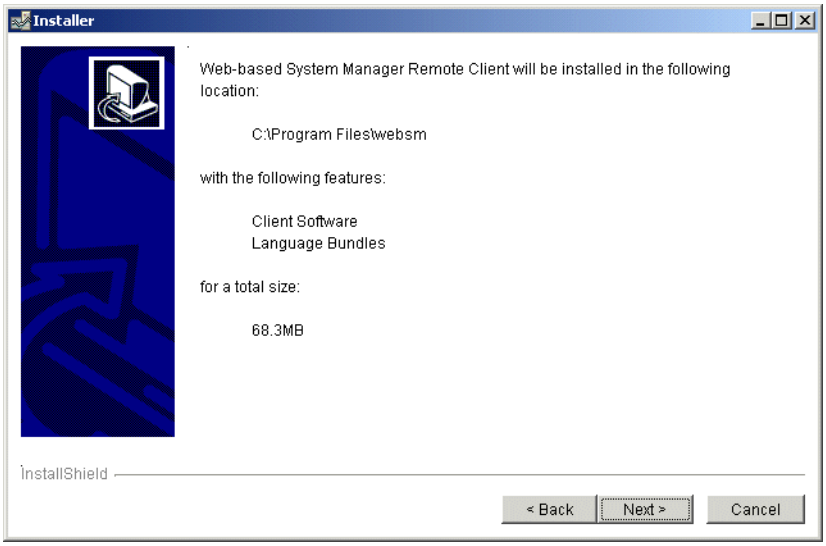


Figure 7-13 Confirming the installation features

During the installation the copied files will be shown on the progress indicator (Figure 7-14).

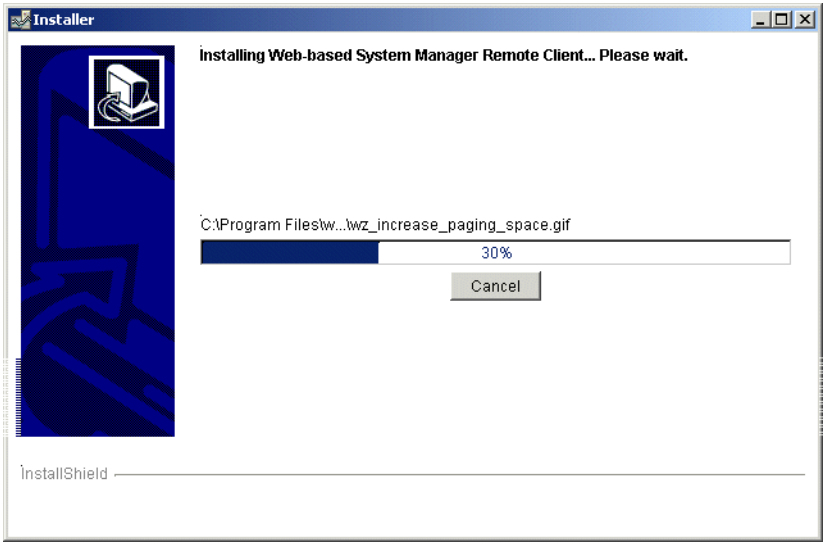


Figure 7-14 Installation progress

When the copying is done, click **Finish** to end the installation process of the WebSM client (Figure 7-15).

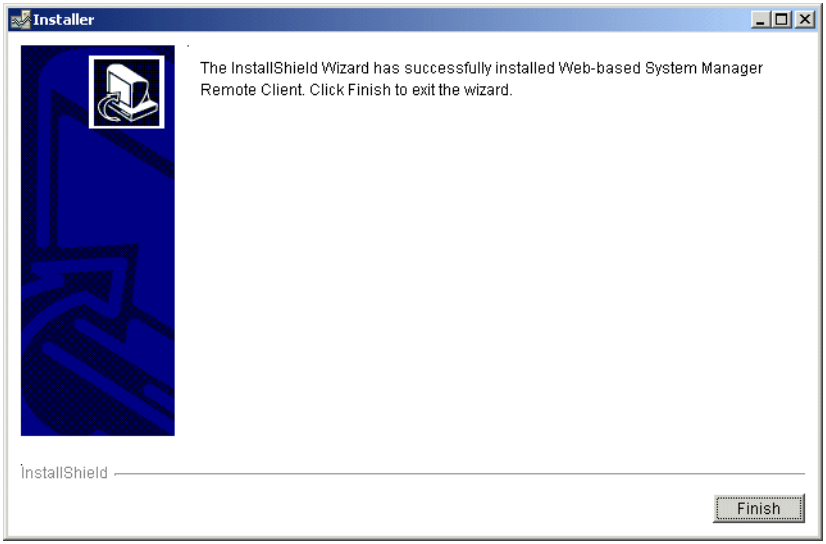


Figure 7-15 Installation completed

7.4.3 Basic setup using Web-based System Manager Remote Client

After completing installation, the Web-based System Manager Remote Client can be used to do the initial configuration of the NAS Gateway 500. Double-click its icon which was created on the desktop of your managing client. A Java™ information screen is displayed as shown in Figure 7-16.

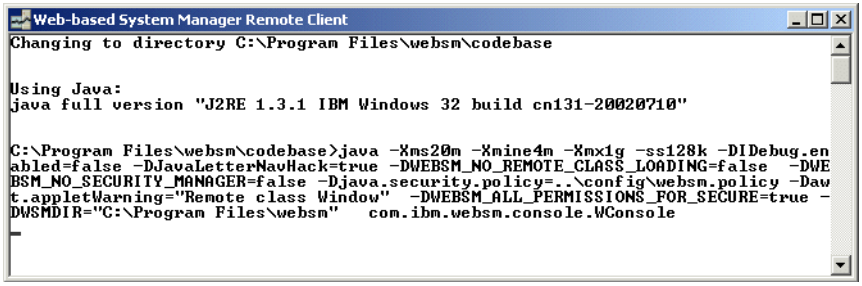


Figure 7-16 Java information screen

Shortly after that the Java console will be created. The progress is shown in Figure 7-17.

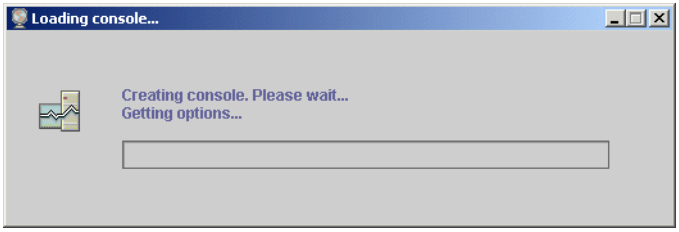


Figure 7-17 Console creation progress

When the console is created, you can logon to the NAS Gateway 500 by providing:

- Host name: type the IP address shown on the LCD operator panel
- User name: type `root`
- Password: type `password`

After you entered the needed information click **Log On** to get access to the NAS Gateway 500 (Figure 7-18).

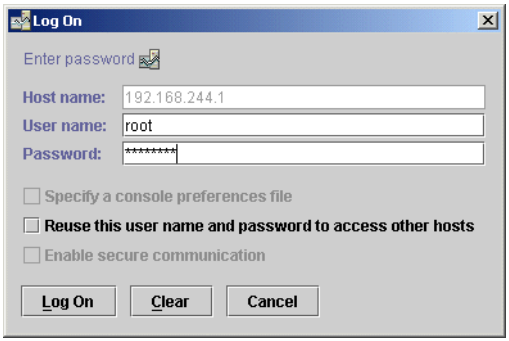


Figure 7-18 Logon panel

Now the WebSM main window is displayed. When it is run for the first time only the Welcome heading is available in the left pane of the main window, and the right pane is empty, as shown in Figure 7-19 on page 128.

Initial Configuration wizard

The initial Configuration wizard is a collection of individual wizards that are grouped together. They are listed here in the same order as they show when you execute the Initial Configuration wizard:

- Feature wizard.
- General System Configuration wizard.
- Network Configuration wizard — if clustering is not selected in the Feature wizard.
- Cluster Configuration wizard — if clustering is selected in the Feature wizard. For more information about configuring a clustered NAS Gateway 500 please refer to Chapter 9, “Cluster configuration” on page 173.
- CIFS Configuration wizard — if CIFS is selected in the Feature wizard.
- Volume Configuration wizard.

To enter basic details into the NAS Gateway 500, select the **Initial Configuration wizard** in the right pane (Figure 7-19):

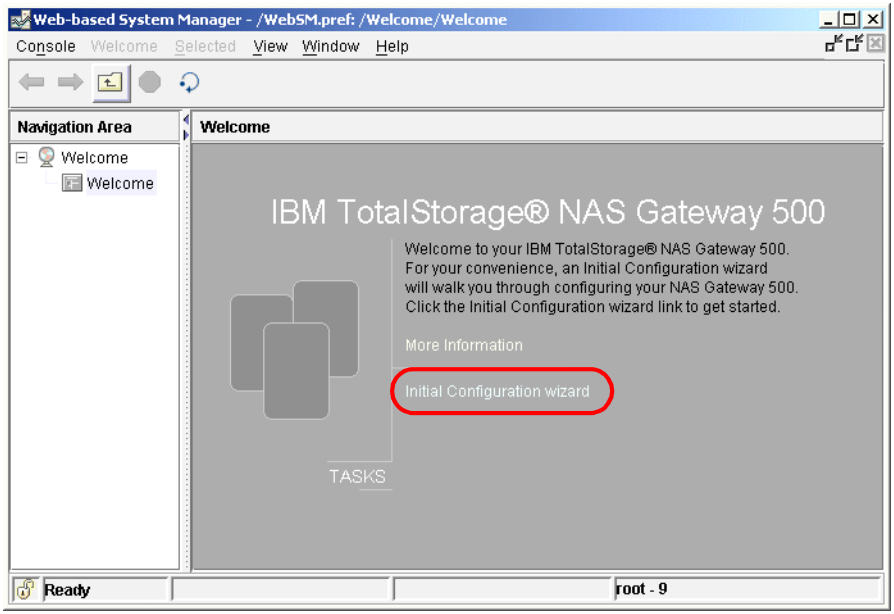


Figure 7-19 Welcome panel

Here, the basic tasks like selecting the optional features, setting date and time, managing users, configuring directory services, and setting host names and ethernet addresses can be done, as shown in Figure 7-20.

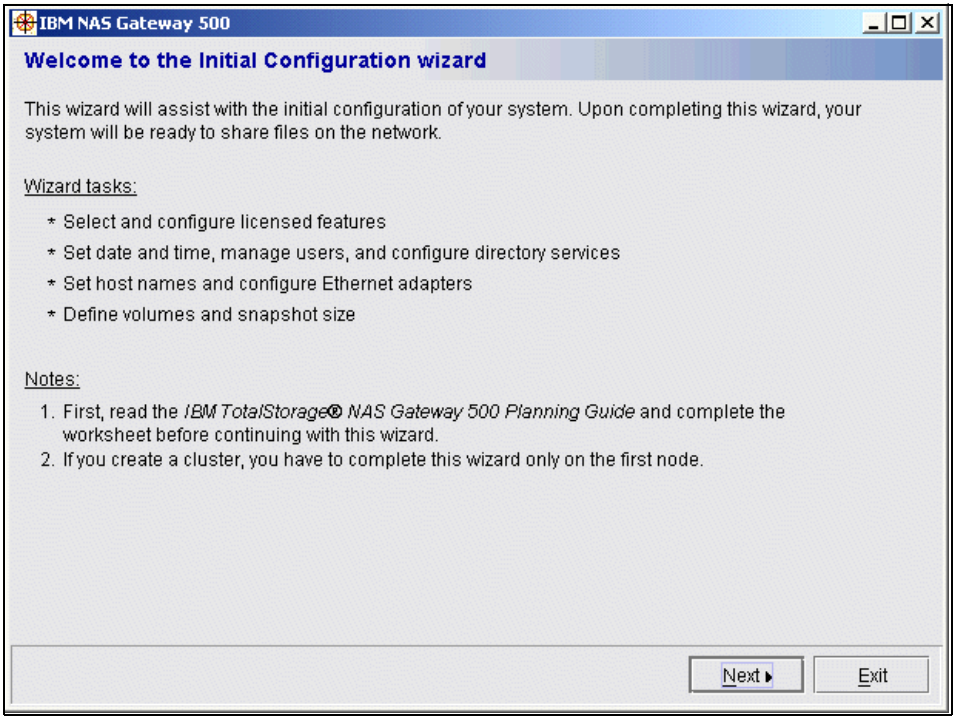


Figure 7-20 Initial Configuration wizard

Feature wizard

If you would like to enable optional features on the NAS Gateway 500, you can do it here. Please be aware that additional features must be purchased. If a two-node configuration has been purchased, the **Clustering** feature can be selected. In this case make sure that both nodes are powered on and positioned close enough to each other so the ethernet and the serial connections for the cluster heartbeat can be cabled between the nodes.

Important: Ethernet crossover cable for the cluster heartbeat should be connected to the integrated ethernet port 2 and the serial null-modem cable should be connected to the serial port 3 on the back side of the NAS Gateway 500.

Another option is to select the **CIFS File Serving** feature so that Windows-based clients can use shared storage (Figure 7-21).

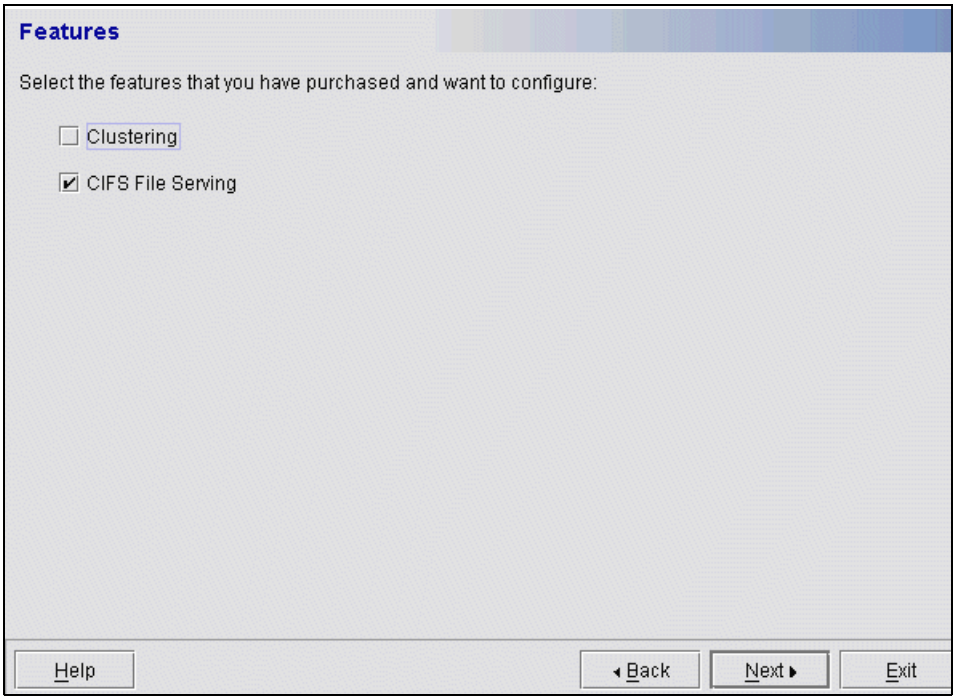


Figure 7-21 Optional features

Tip: It is also possible to start the Features Wizard after you have completed the initial configuration of the NAS Gateway 500 as described in “Starting the Feature wizard after initial configuration” on page 144.

General System Configuration wizard

To enter general information into the NAS Gateway 500, continue on with the General System Configuration wizard. On the following panel, the date, time and time zone settings can be entered. If Daylight saving time is used in your geography, click the **Time zone observes daylight saving time (DST)**, as shown in Figure 7-22. Also, regular synchronization of the NAS Gateway 500 device’s clock can be automated if the IP address of a time server is entered.

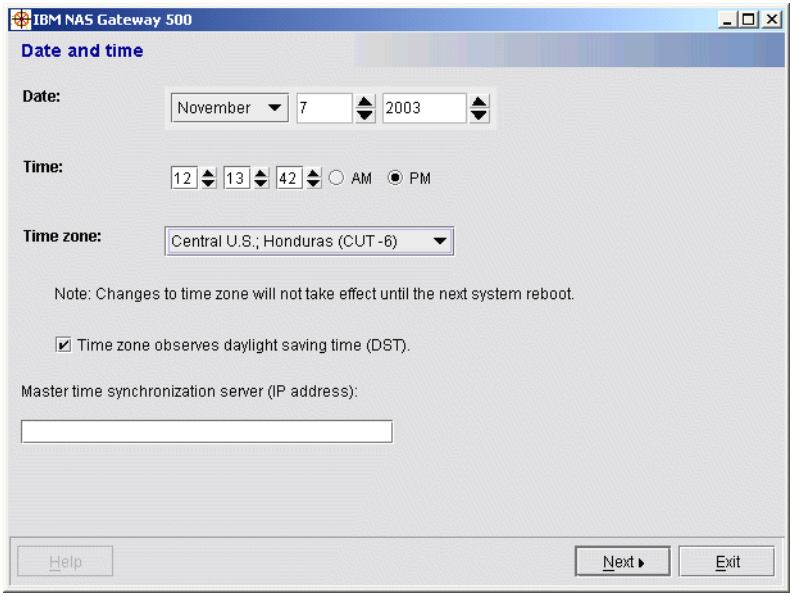


Figure 7-22 Date and time settings

For security reasons, the password for the root user should be changed (Figure 7-23).

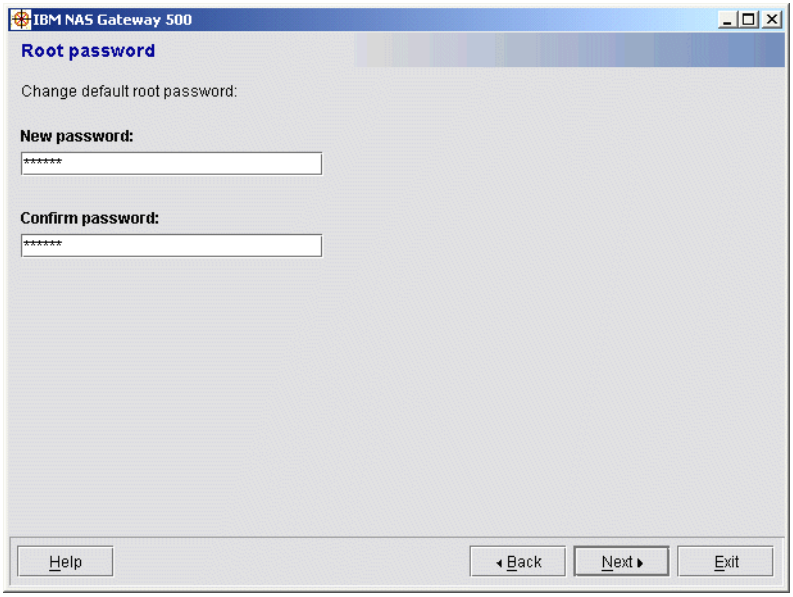


Figure 7-23 Root password

Root account should not be used for daily administration of the NAS Gateway 500. Administrator accounts can be created, edited or deleted on the next panel. NAS administrators have all the rights, for example configuring clustering, remote mirroring or Windows file serving. To create an account with administrator privileges, click the **Add** button, as shown in Figure 7-24.

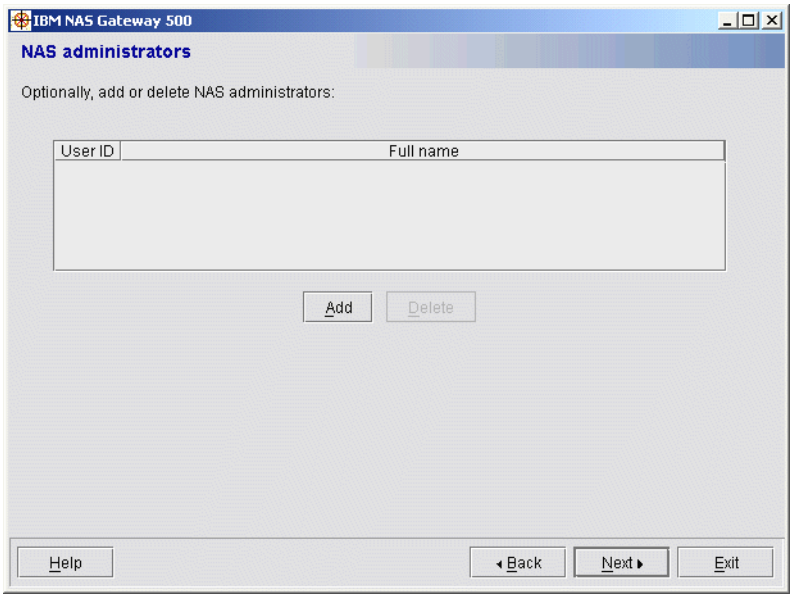


Figure 7-24 Administrator accounts

Enter the User ID, full name and password for the new administrator account and confirm the account creation by clicking **OK** (Figure 7-25).

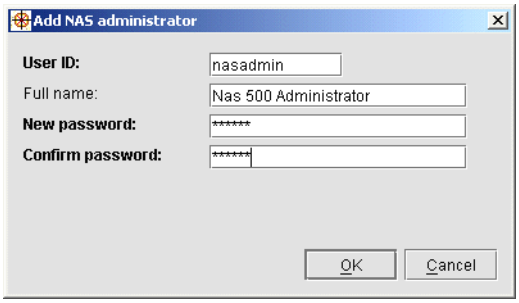


Figure 7-25 Creating the administrator account

The new account will be presented on the NAS administrators panel (Figure 7-26).

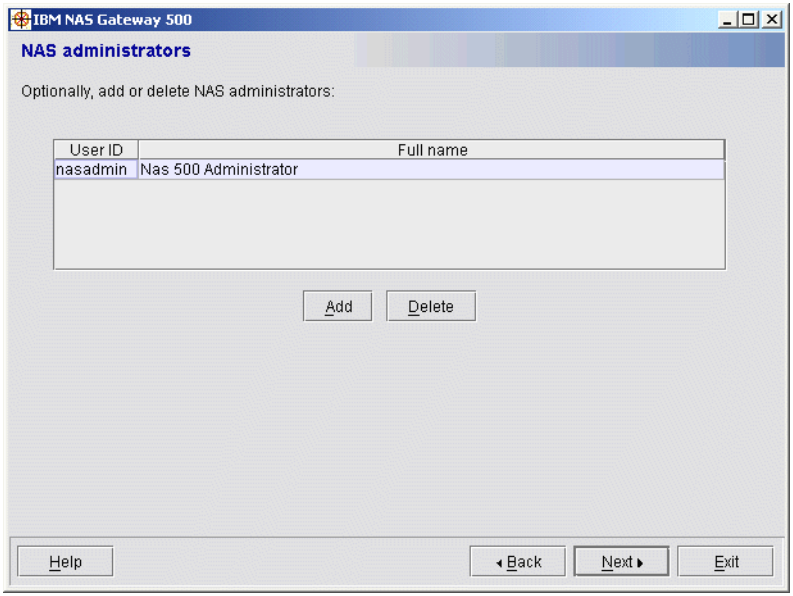


Figure 7-26 Newly added account

NAS Gateway 500 can be optionally integrated into existing directory services infrastructure for automated user authentication. Select NIS to enable this option.

For detailed information on how to integrate the NAS Gateway 500 into Windows environments, please refer to Chapter 10, “Windows systems integration” on page 211.

If directory integration is not needed, select **None** and continue by clicking **Next** (Figure 7-27).

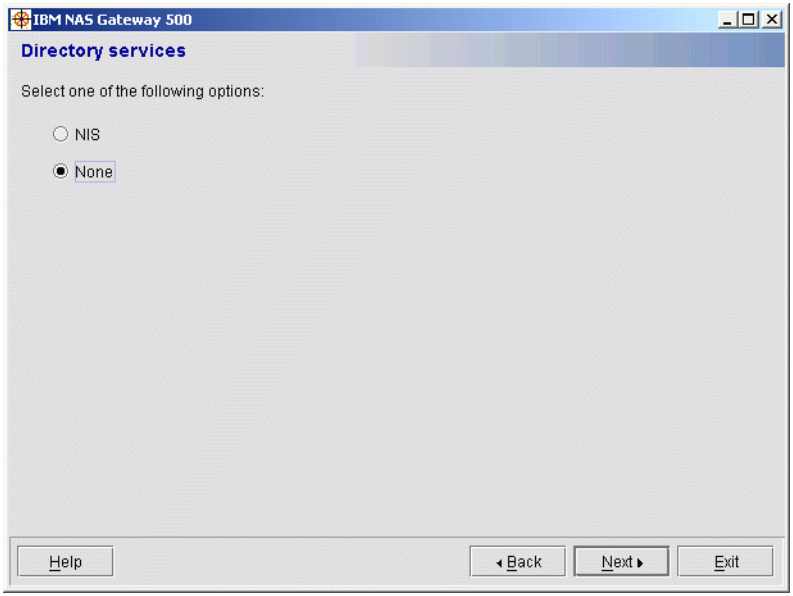


Figure 7-27 Directory services

File users accessing the storage will need to have user accounts created on the NAS Gateway 500 device. They can be managed on the File access users panel. To create a new user, click the **Add** button (Figure 7-28).

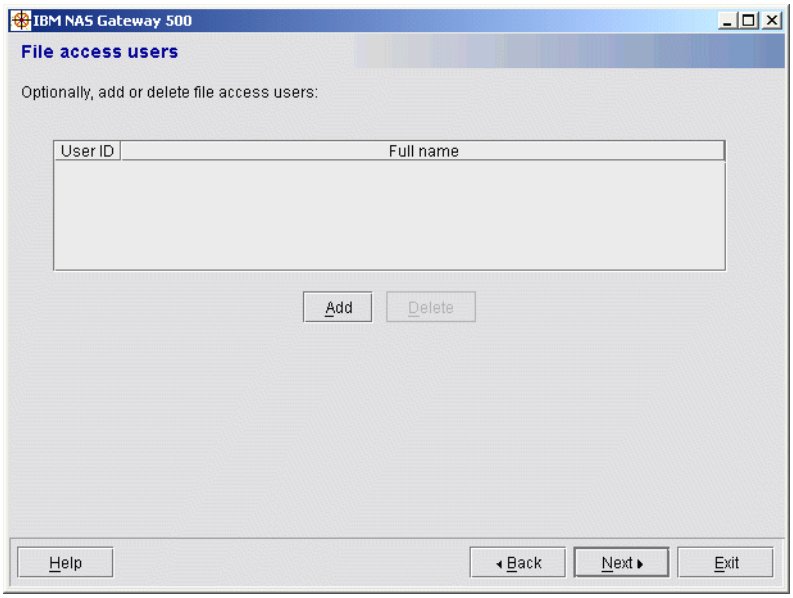


Figure 7-28 File access users

Provide the User ID, full name and password for the new user account and confirm the account creation by clicking **OK** (Figure 7-29).

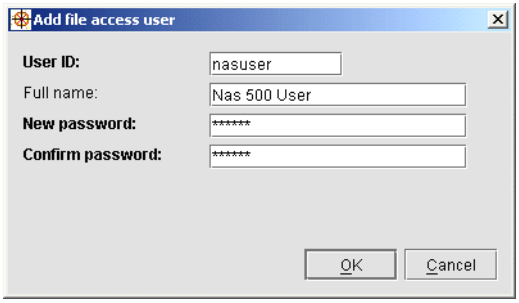


Figure 7-29 Adding a user

The newly created user account will be shown in the File access users panel (Figure 7-30).

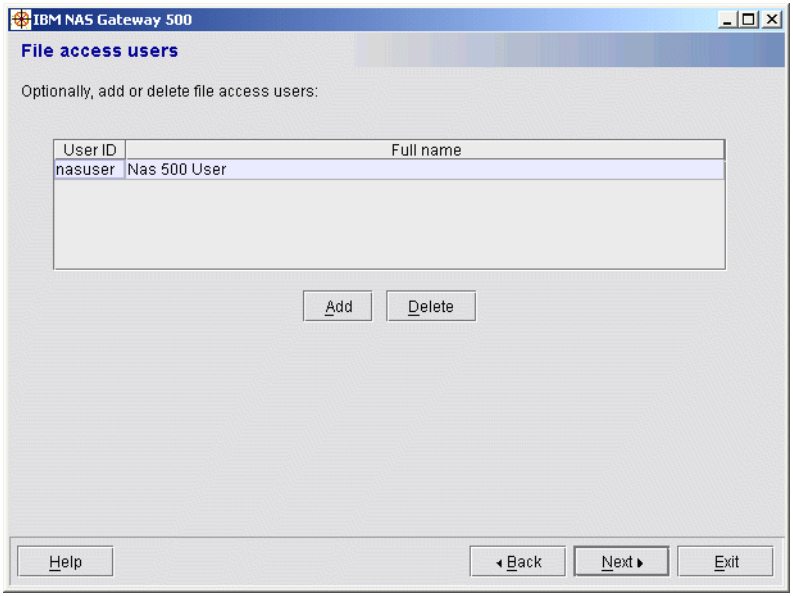


Figure 7-30 Newly added user

Network configuration wizard

If clustering feature was not selected in the Feature wizard, this wizard will be shown next. Here you can configure the network ports used for the client network (Gigabit adapters) of a single node NAS Gateway 500 device. The Host name, DNS domain name, DNS server addresses and default gateway address can be entered here. By selecting an ethernet adapter from the list and clicking the **Edit** button, you can configure its IP address and subnet mask (Figure 7-31).

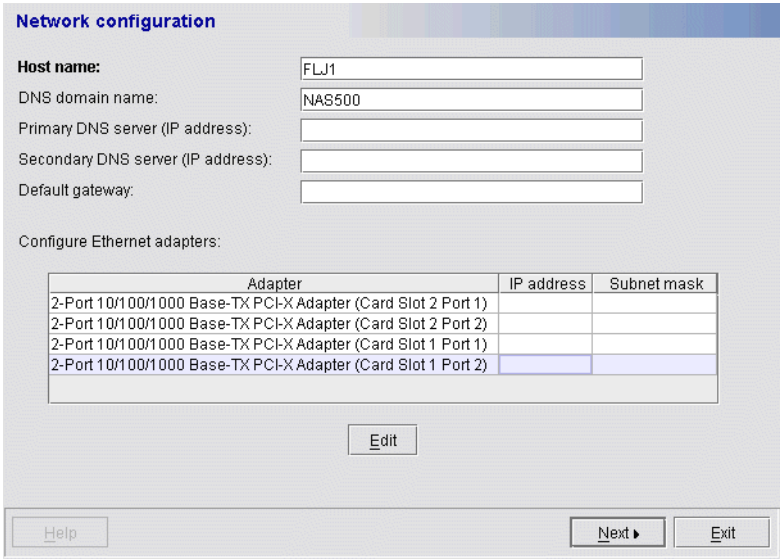


Figure 7-31 Network configuration

Note: In this step it is not possible to change the configuration of the service ethernet port. You can do that immediately after initial configuration has been done, as described in “TCP/IP configuration” on page 149.

CIFS wizard

If Windows based clients will be accessing the NAS Gateway 500, the CIFS file sharing feature has to be configured. If you selected **CIFS File Serving** check mark in the Feature wizard (as shown in Figure 7-21 on page 130), the CIFS configuration panel will be shown next.

First, enter the name for the NAS Gateway 500 under which the Windows users will connect to file shares. Additional server description can be entered that will be displayed next to the server name in the client’s Network Neighborhood (renamed to My Network Places in Windows 2000). Enter the domain or workgroup as you want it to appear in the Network Neighborhood. Click **Next** to proceed to the next panel (Figure 7-32).

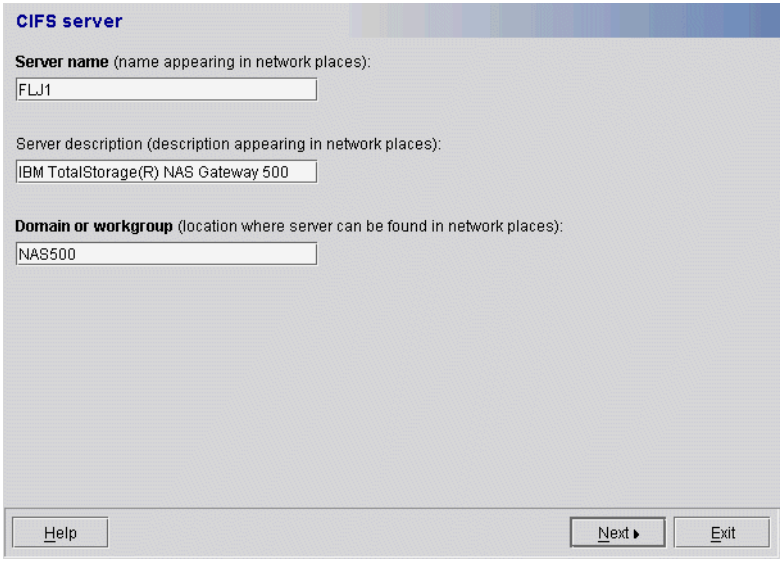


Figure 7-32 Server identification

If clients in your network are using WINS servers for name resolution you can enter the address of those servers in the next panel (Figure 7-33).

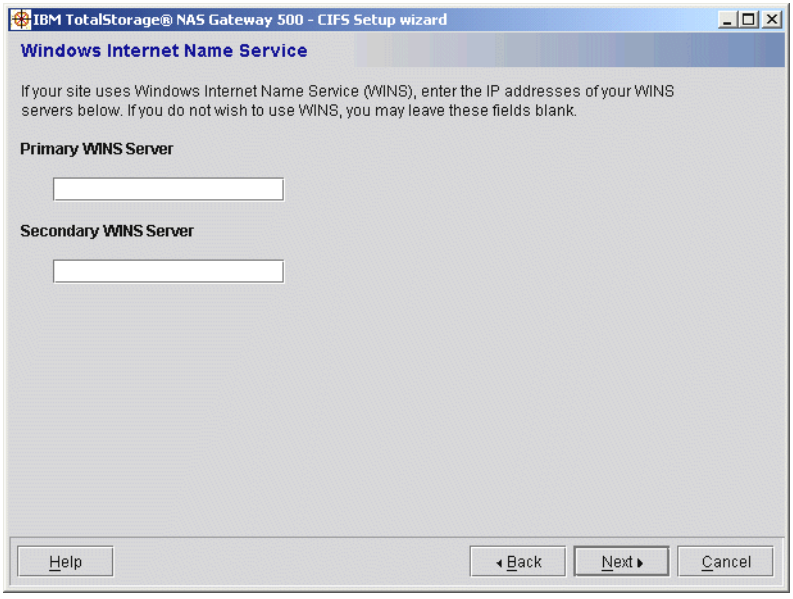


Figure 7-33 WINS servers

For CIFS users to access the file shares they have to be authenticated first. If your Windows environment is using Active Directory to authenticate clients, select **Active Directory/NT4 Domain**, and enter the IP address of up to two authentication servers (Active Directory Controllers in case you are using Windows 2000 or 2003 domain). Otherwise select **Locally on each machine**. In this case you have to select the type of password encryption as well. For higher security, user passwords can be encrypted during authentication by selecting **Yes, only allow encrypted passwords**, as shown in Figure 7-34. If there are clients accessing the NAS Gateway 500 that cannot use encrypted passwords choose one of the other two options and click **Next** to proceed.

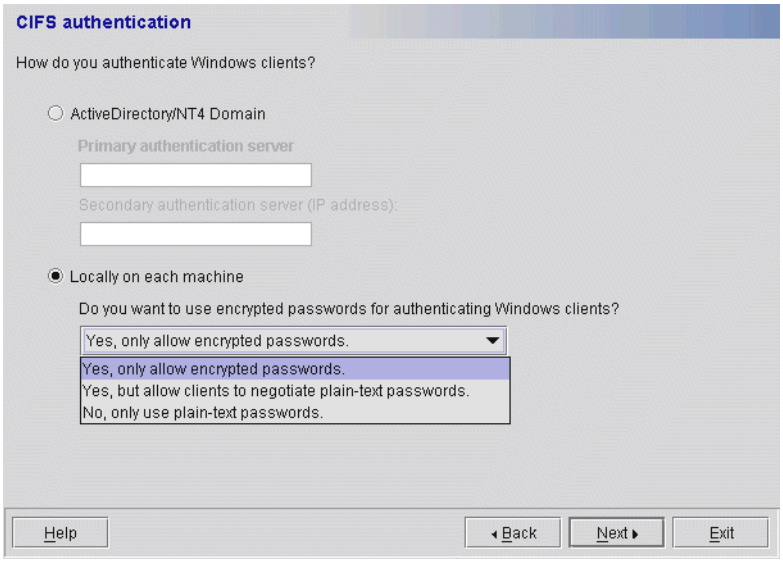


Figure 7-34 User authentication for CIFS

If you selected the **Active Directory/NT4 Domain** for CIFS user authentication in the previous panel, then the next panel asks you about user account association. Authenticated Windows users will need a local reader account on the NAS Gateway 500. This account will be created automatically if you select **Yes, use Dynamic User Creation**. Alternately, this account can be created manually (Figure 7-35).

Note: For more information about CIFS please refer to Appendix B, “Windows networking basic definitions” on page 381.

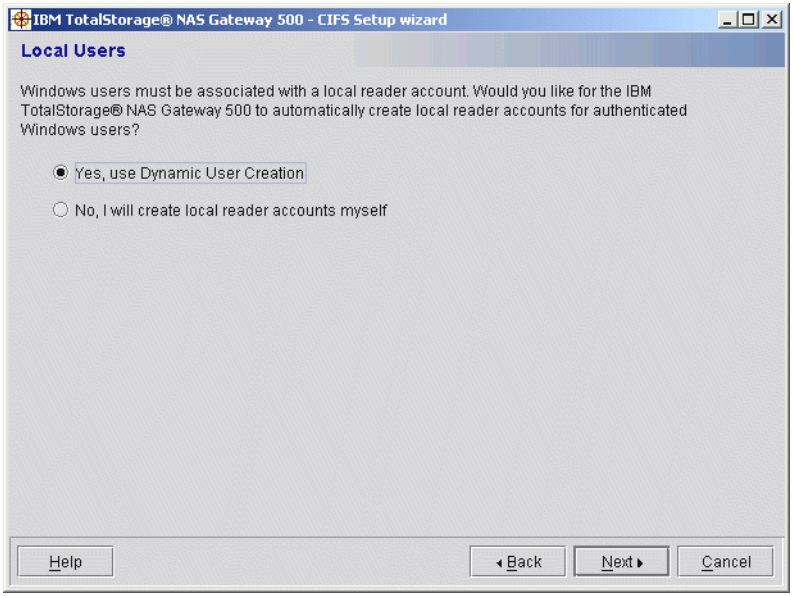


Figure 7-35 Local User association

A summary of selected settings is shown on the next panel. If they are correct, click **Next** to confirm them. To proceed, click **Next** (Figure 7-36).

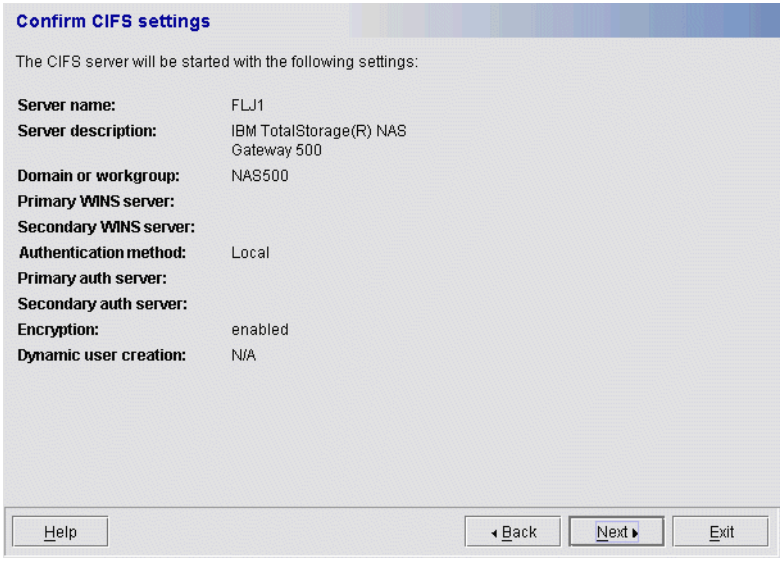


Figure 7-36 CIFS Settings confirmation

Volume wizard

If the storage has been configured on the storage device beforehand, it can be immediately mapped for users to be able to access it. After you completed the CIFS setup, you can continue with creating NAS volumes as part of the Initial Configuration wizard.

If you break out of the Initial Configuration wizard without creating the NAS Volumes, you can map the storage later as part of a device discovery procedure. For detailed instructions please refer to Advanced storage configuration topic discussed in 8.2, “Storage configuration” on page 154.

Supported external storage devices are:

- IBM FAStT family of storage servers
- IBM Enterprise Storage Server
- IBM TotalStorage SAN Volume Controller
- IBM TotalStorage SAN Integration Server

In this setup example we defined a 74 GB logical drive in a RAID-5 array made of four physical disk drives residing in a FAStT 700 storage server. We used the IBM FAStT Storage Manager version 8.4 running on a Windows 2000 server with the Fibre Channel adapter inserted to configure it.

If a disk were configured in advance it would show up on the next panel under the Logical Volumes heading. Select it and click **Add** to establish a NAS volume (Figure 7-37).

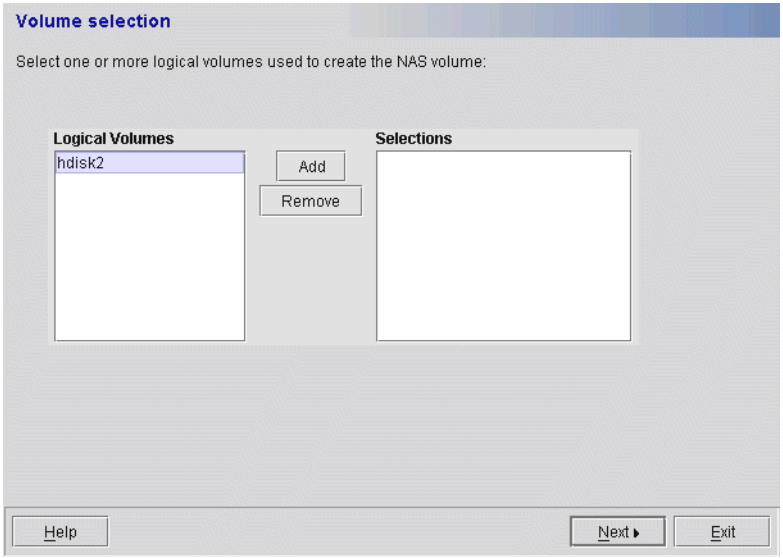


Figure 7-37 Volume selection

The selected volume will show in the right pane under Selections (Figure 7-38).

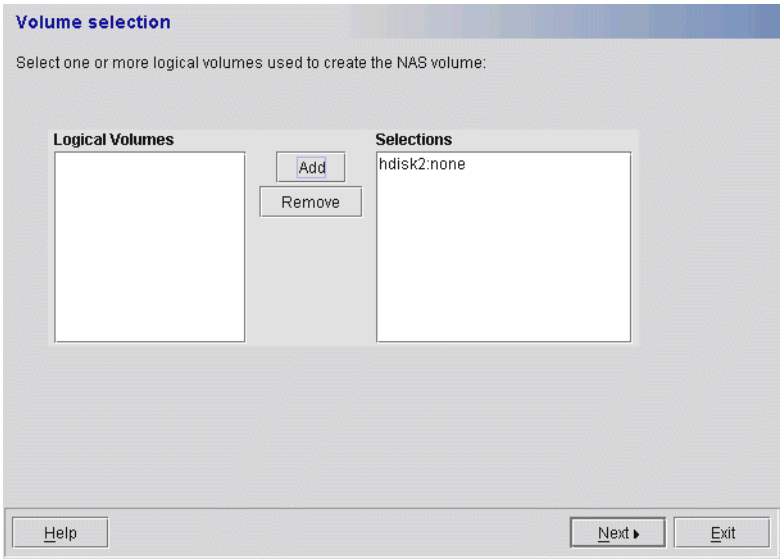


Figure 7-38 Volume selected

Note: All NAS Gateway 500 volumes are automatically formatted with the JFS2 file system.

Now enter the Volume name under which the users will be able to access it. If you enable the snapshot feature, you also have to provide the maximum number of snapshots and snapshot size. This way the NAS Gateway 500 device will know how much space it needs to reserve for the snapshot feature. Additionally, you can specify what kind of volume sharing (CIFS, NFS or both) will be enabled with this volume (Figure 7-39).

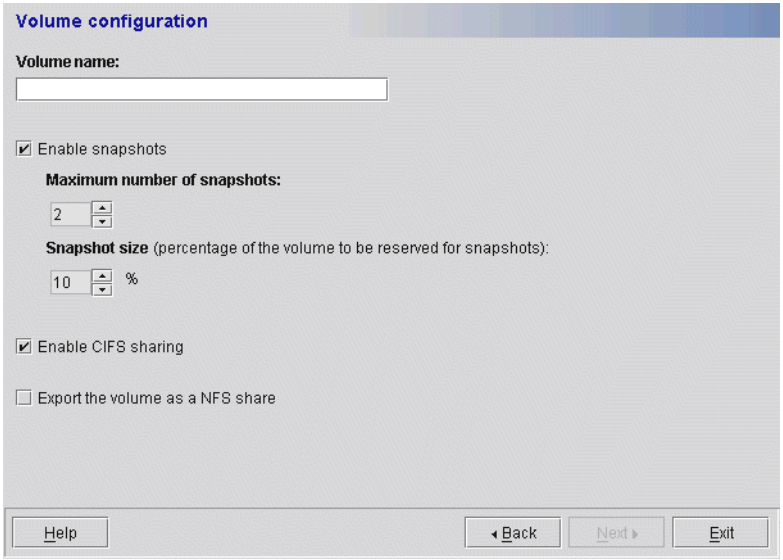


Figure 7-39 Volume configuration

After defining all options, the summary panel is presented (see Figure 7-40). You can still change them by clicking **Back** or confirm them by clicking **Next**.

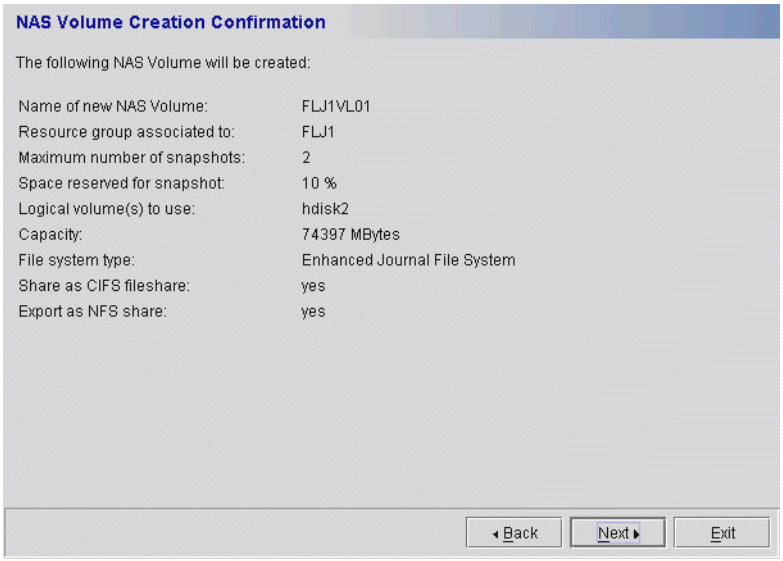


Figure 7-40 NAS Gateway 500 volume creation confirmation

The NAS volume is created. By clicking **Create Another Volume**, you can repeat the procedure to create another NAS volume (Figure 7-41).

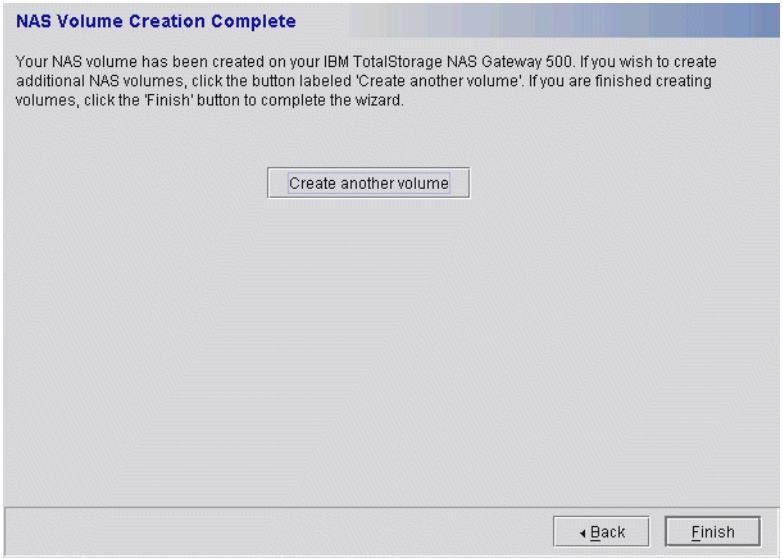


Figure 7-41 Completing the Volume creation

This concludes the initial configuration of the NAS Gateway 500 single node device. After you have done these basic steps, the Welcome heading is removed from the left pane of the WebSM main window.

Important: Although it is possible to use dynamic IP address for the service ethernet interface, it is advisable to change to static addressing immediately after initial configuration of the NAS Gateway 500 has been done. Please refer to “TCP/IP configuration” on page 149 for detailed guidance.

Starting the Feature wizard after initial configuration

The Welcome wizard can be run only during initial configuration of the NAS Gateway 500. If, however, you need to change some features of the NAS Gateway 500, it is possible to do so by using the Feature wizard. Start the WebSM and login as root. In the main panel open **NAS Management —> NAS System —> Feature Management** and click the **Feature wizard** in the right pane, as shown in Figure 7-42.

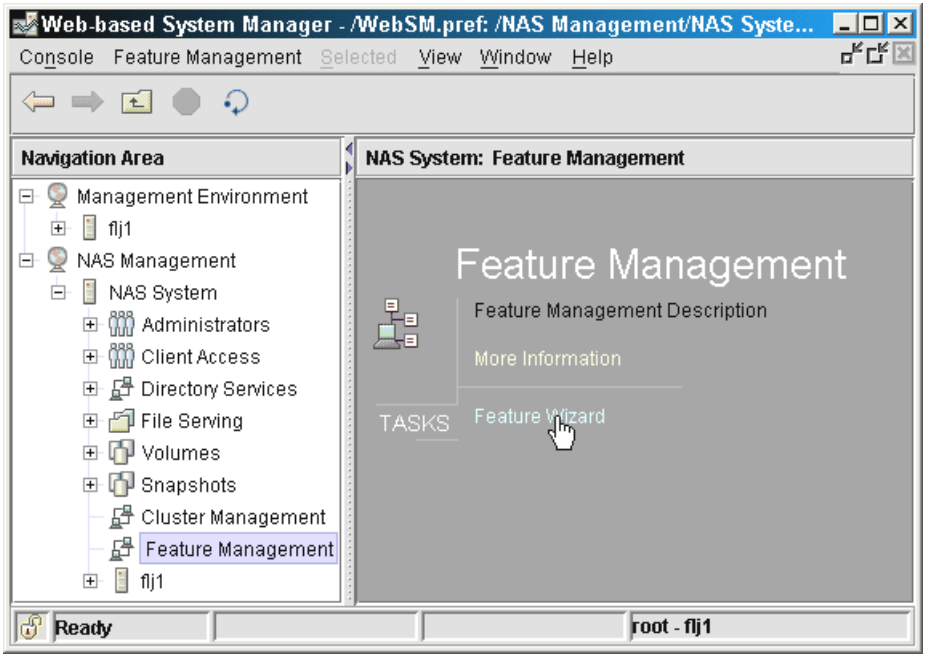


Figure 7-42 Starting the Feature wizard

The Feature Selection wizard window opens with a description of what it can be used for (Figure 7-43).

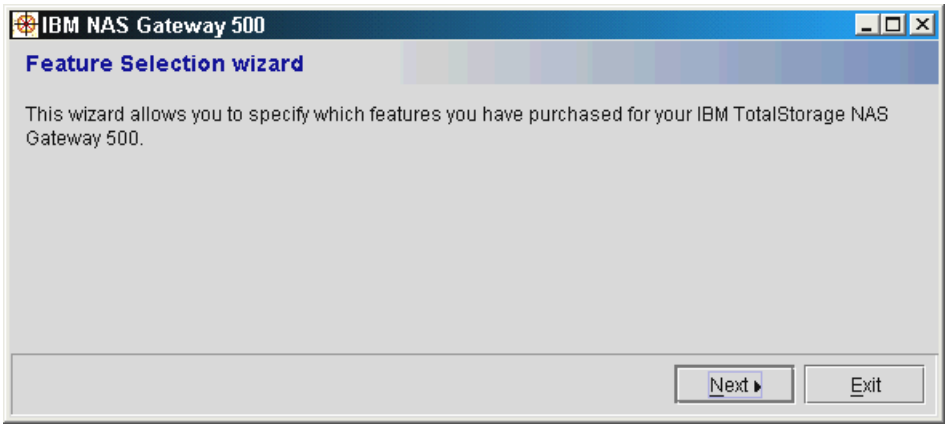


Figure 7-43 Feature selection wizard

After clicking **Next** on the previous screen, you get the feature selection window again to enable the option you left out at the initial configuration (Figure 7-44).

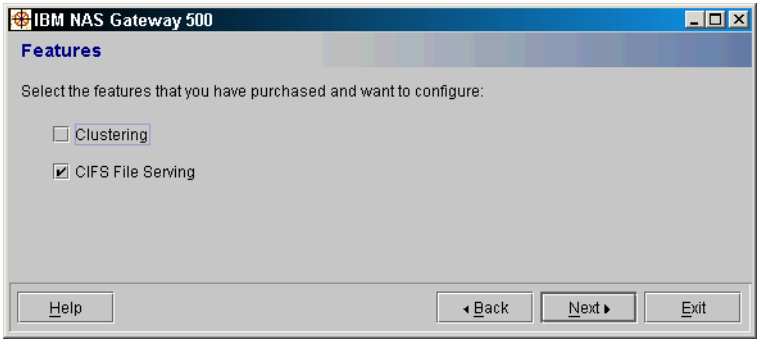


Figure 7-44 Selecting features: Clustering and CIFS

Clicking **Next** without selecting or deselecting features has the effect of exiting the window. Selecting a feature will start the wizard for that feature.

8

Subsequent configuration

This chapter discusses the subsequent and advanced configuration of the NAS Gateway 500. The following topics are covered:

- Network configuration
- Discovering new storage devices
- Creating a NAS volume
- Creating a mirror
- System errors and notification

8.1 Network configuration

Here we introduce how to configure networking on a NAS Gateway 500. You can use this method to configure the administrative network interface, which is not covered by the Initial Configuration wizard.

8.1.1 Network interface description

The NAS Gateway 500 system board contains two integrated 10/100 Mb ethernet ports, directly connected to the PCI bus. For connecting the network cables, there is a dual RJ-45 connector with activity LEDs on the back of the system, as shown in Figure 8-1. There is also an activity LED on the front panel. The top port, port 2, is reserved for cluster interconnect. The bottom port, port 1, is used for service purposes. Neither port can be used as a fileserving network adapter.

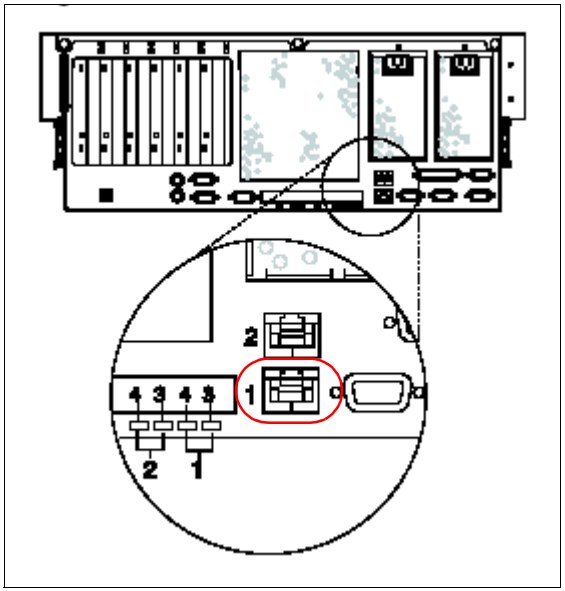


Figure 8-1 On-board ethernet ports

Important: Ethernet Port 1 (bottom port) should be used for all configuration tasks.

8.1.2 TCP/IP configuration

IP address of the NAS Gateway 500 can be changed in the Basic TCP/IP Configuration wizard. To start it, select **Protocol Configuration** under **NAS Management** and click the **Set up basic TCP/IP configuration** task in the right pane, as shown in Figure 8-3.

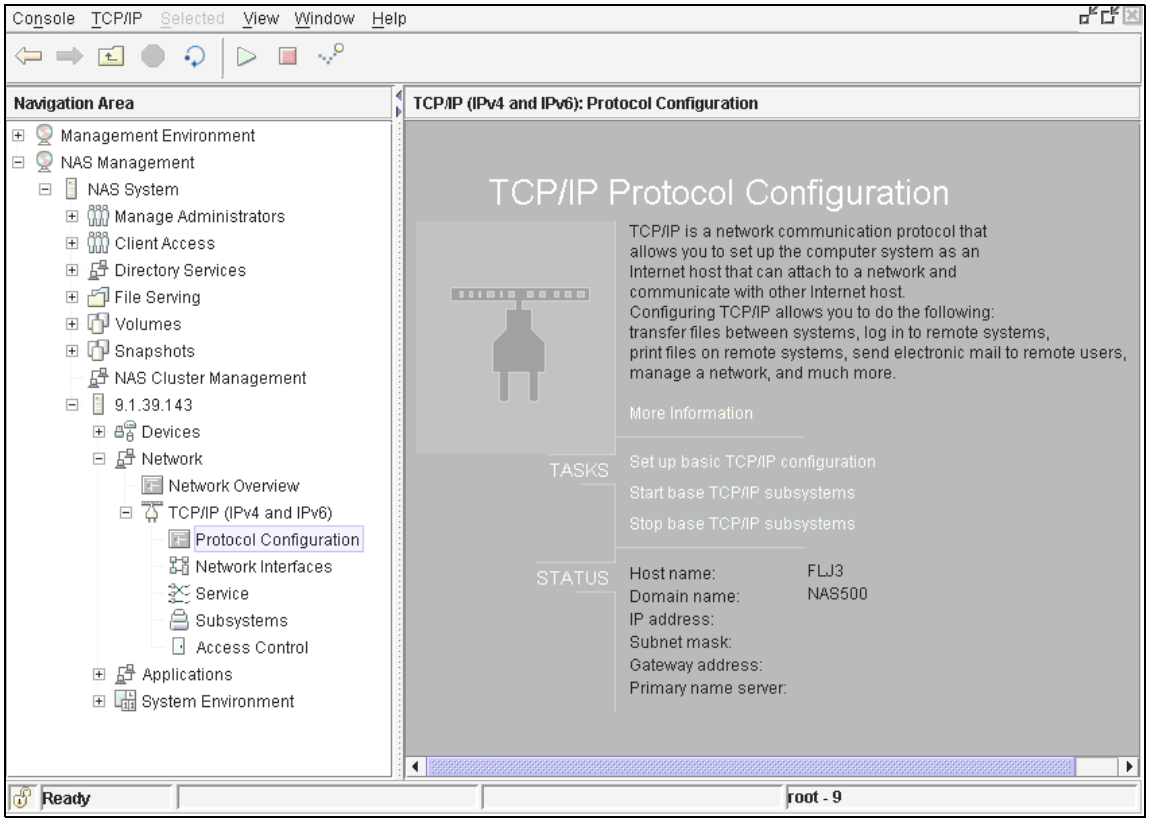


Figure 8-2 Basic TCP/IP configuration welcome screen

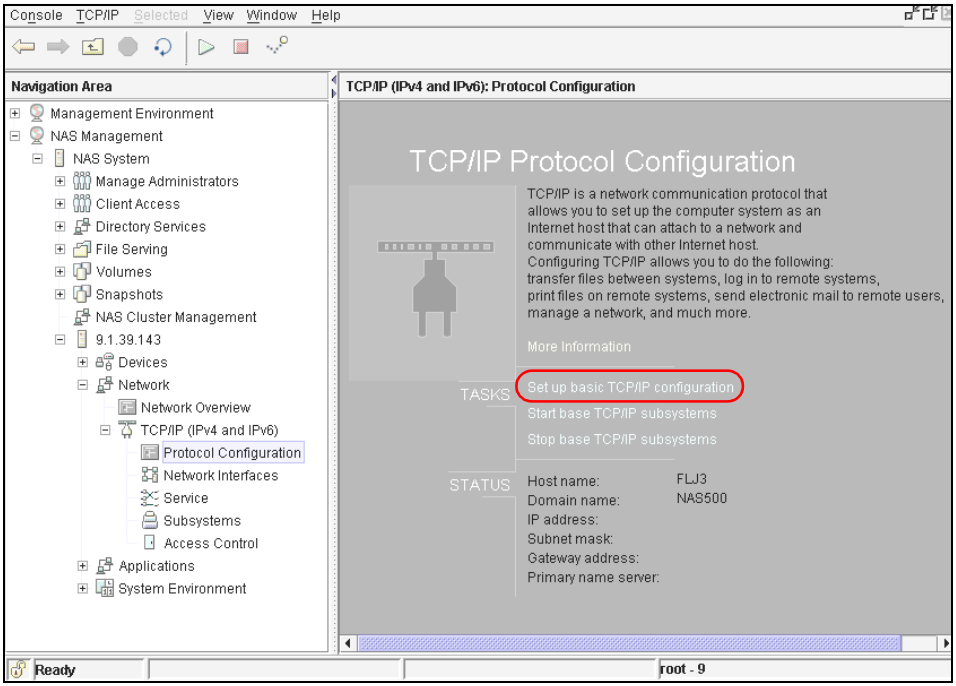


Figure 8-3 TCP/IP configuration

The wizard shown in Figure 8-4 starts and asks you whether you want to use a static IP address (select **Manually configure TCP/IP**) or have it assigned dynamically by a DHCP server in your network (**Automatically configure TPC/IP using DHCP**).

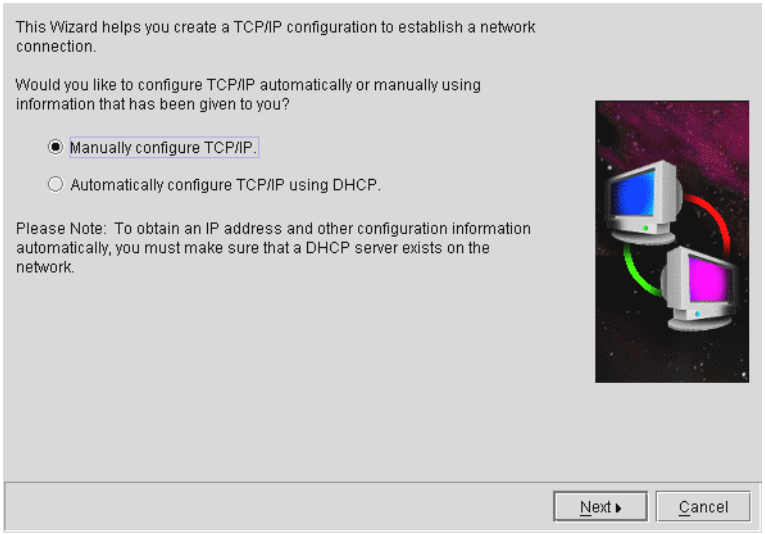


Figure 8-4 IP address allocation mode

If you select manual configuration, you have to enter the Host name, an available IP address, and a corresponding subnet mask for your NAS Gateway 500 (Figure 8-5).

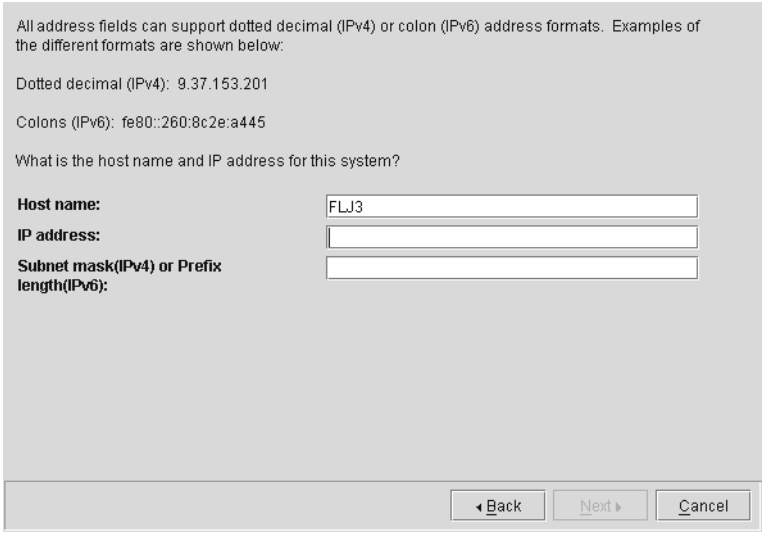


Figure 8-5 Host name, IP address and subnet information

Now select the ethernet adapter to be associated with the IP address entered in the previous step. The onboard Ethernet port 1 should be used for all configuration tasks. Use the number of the interface displayed on the LCD operator panel during the initial configuration of the NAS Gateway 500 (see “Connecting and powering on the NAS Gateway 500” on page 119). In our example, it is the **en5** network interface (Figure 8-6).

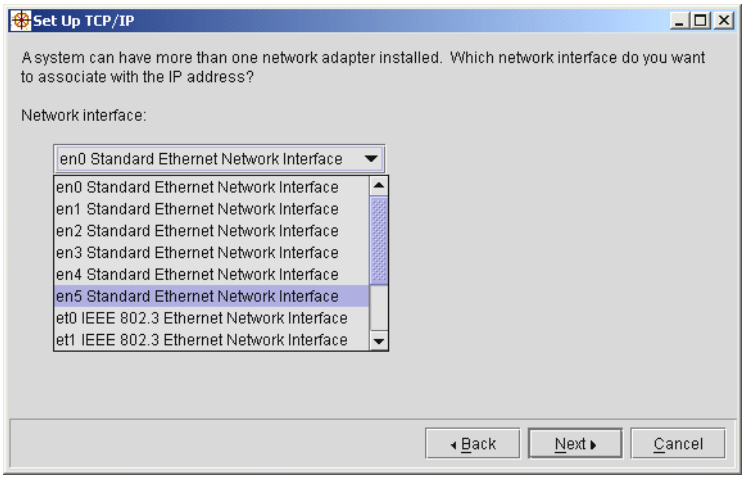


Figure 8-6 Selecting the network interface

Tip: You can also use the **lsent** command to find out which **ent** adapter is which port. Run **/opt/nas/lib/lsent ent***.

For communication outside of the native network segment, you need to enter the address of a default gateway. For name resolution, enter the DNS domain name and IP address of your DNS server (Figure 8-7).

Figure 8-7 Gateway and DNS information

After you have entered all needed information, the summary panel is displayed. Click **Back** if you want to change some of the information or select **Finish** to apply the changes. To exit this part of the configuration without any changes, you can click **Cancel** (Figure 8-8).

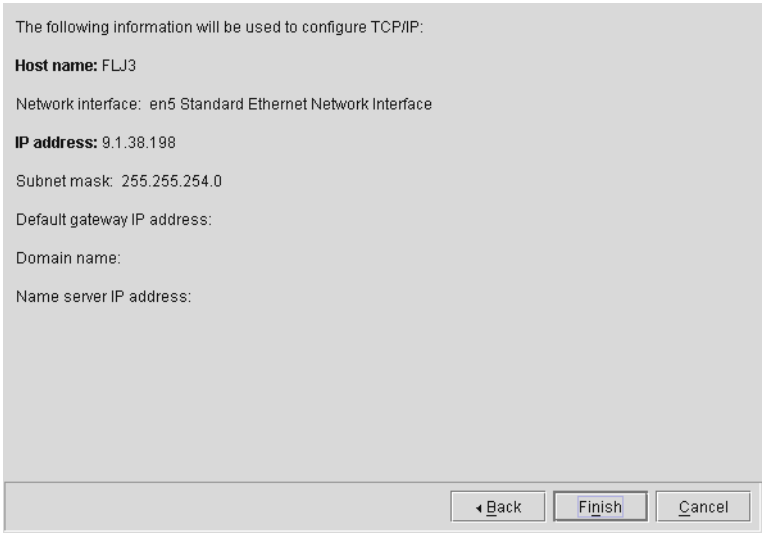


Figure 8-8 TCP/IP configuration summary

As the changes are being applied, a progress panel is displayed. By clicking the **Show Details** button you can see detailed information about this procedure. When it is finished, the Success or Failure (together with reasons for it) will be shown. Click **Close** to remove this panel (Figure 8-9).

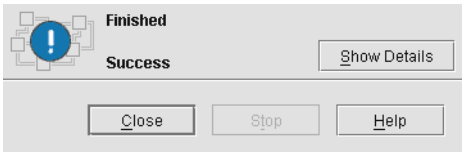


Figure 8-9 Configuration progress

If you try to start another task now, a warning panel is shown stating that the network connection to the NAS Gateway 500 is lost (see Figure 8-10). This is normal because the IP address was just changed. Restart the WebSM and enter the new IP address.

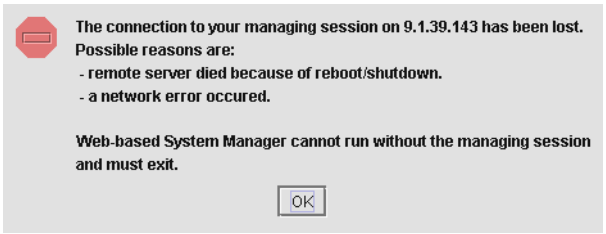


Figure 8-10 Connection lost message

8.2 Storage configuration

There are some storage configuration tasks that have to be done after the NAS Gateway 500 has been setup with the Initial configuration wizard. To help you understand them more easily, we first describe how AIX operating system handles storage.

The five basic logical storage concepts are: physical volumes, volume groups, physical partitions, logical volumes, and logical partitions. The relationships among these concepts are illustrated in Figure 8-11.

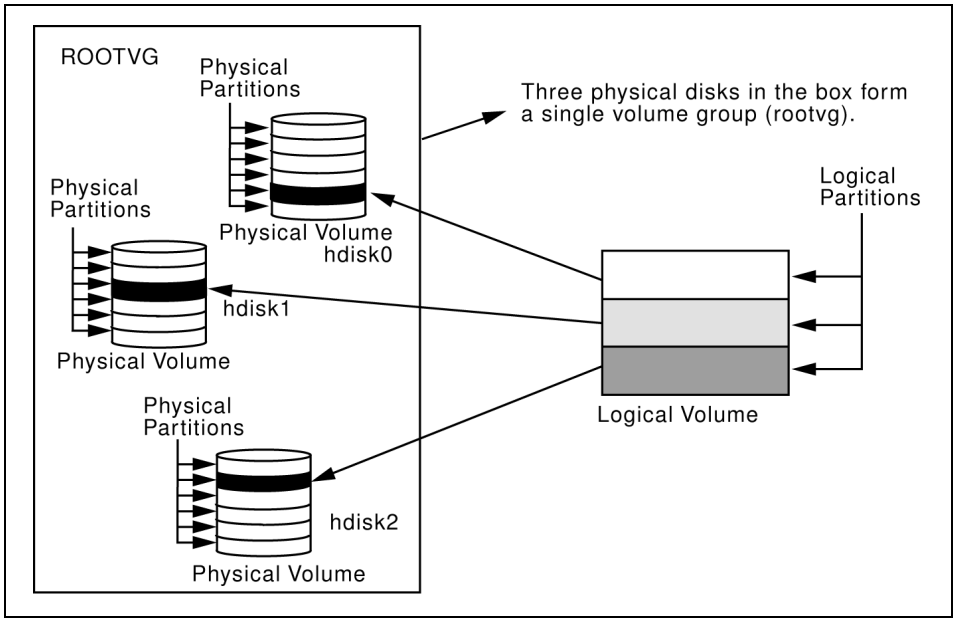


Figure 8-11 Relationship between logical storage components

The following statements can be made regarding Figure 8-11:

- Each individual hard disk drive is called a physical volume (PV) and has a name (for example: hdisk0, hdisk1, or vpath0).
- All physical volumes belong to one volume group (VG) named rootvg.
- All of the physical volumes in a volume group are divided into physical partitions (PPs) of the same size.
- Within each volume group, one or more logical volumes (LVs) are defined. Logical volumes are groups of information located on physical volumes. Data on logical volumes appear as contiguous to the user but can be discontiguous on the physical volume.
- Each logical volume consists of one or more logical partitions (LPs). Each logical partition corresponds to at least one physical partition. If mirroring is specified for the logical volume, additional physical partitions are allocated to store the additional copies of each logical partition.
- Logical volumes can serve a number of system purposes (paging, for example), but each logical volume that holds ordinary systems, user data, or programs, contains a single journaled file system (JFS). Each JFS consists of a pool of page-size (4 KB) blocks. In AIX Version 4.1 and later, a given file system can be defined as having a fragment size of less than 4 KB (512 bytes, 1 KB, 2 KB).

After installation, the system has one volume group (the rootvg volume group), consisting of a base set of logical volumes required to start the system.

NAS volumes are file systems on disk space on external storage that serve files to client machines. During the NAS volume setup, the NAS management software automatically creates underlying volume groups and logical volumes.

8.2.1 Discovering storage devices

After the Initial Configuration wizard has been used to create the NAS volume, the volume is ready to be used. However, if you exited out of the wizard without creating the NAS volume, there are additional tasks to be done before volumes can be used. The procedure is somewhat different than when using the Initial Configuration wizard. First, storage devices need to be discovered. In the WebSM main panel, select **Devices —> Overview and Tasks** under NAS Management in the left pane. In the right pane you will see status of the Device Manager. Selecting **Discover devices that were powered on after the last system restart** task will start the discovery procedure (Figure 8-12).

Figure 8-12 Starting the discovery task

Tip: The discovery procedure is done automatically in the background and thus it is seamless for the administrator if the volume was set up as part of the Initial Configuration wizard (see “Volume wizard” on page 141).

The Discovery task is displayed on the progress indicator panel, as shown in Figure 8-13. By clicking **Show Details**, you can get a description of the procedure.

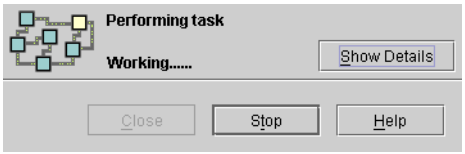


Figure 8-13 Discovery task progress

The new hard disk will be included in the total Available Hard Drives count in the right pane, as shown in Figure 8-14.

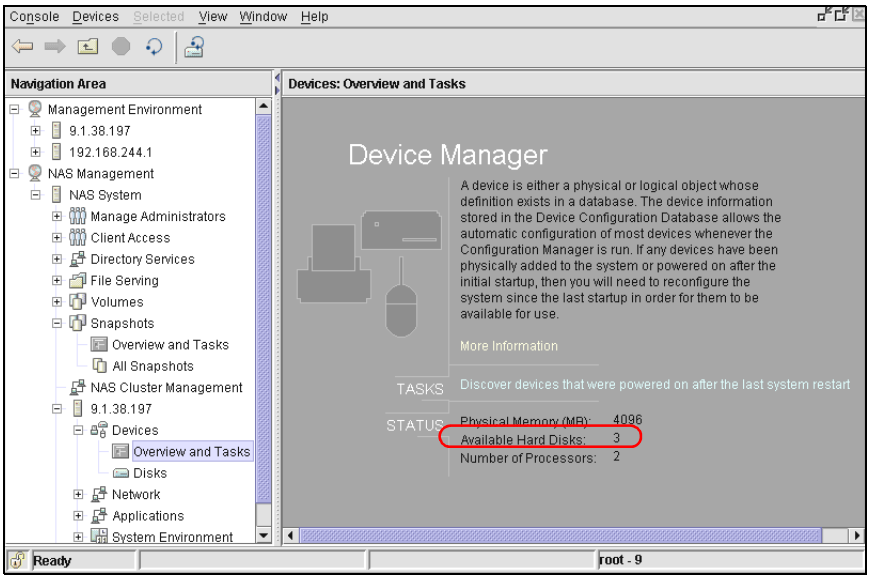


Figure 8-14 New storage device

8.2.2 Creating a NAS volume

Before users can connect to the new hard disk, it has to be mapped as a NAS volume. Under **NAS Management**, select **NAS System —> Volumes —>Overview and Tasks** and click the **Create a NAS Volume** task in the right pane (Figure 8-15).

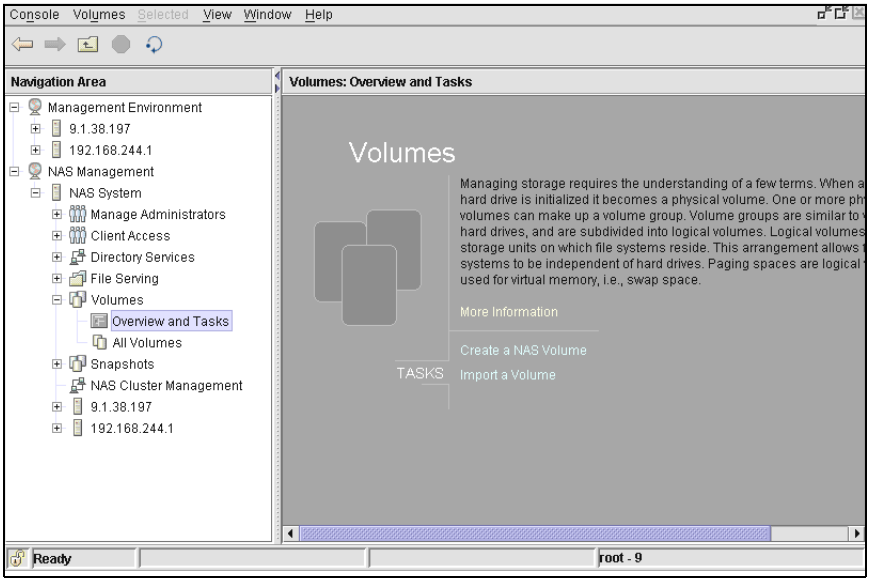


Figure 8-15 Creating new NAS Gateway 500 volumes

The NAS Volume wizard will start (Figure 8-16).

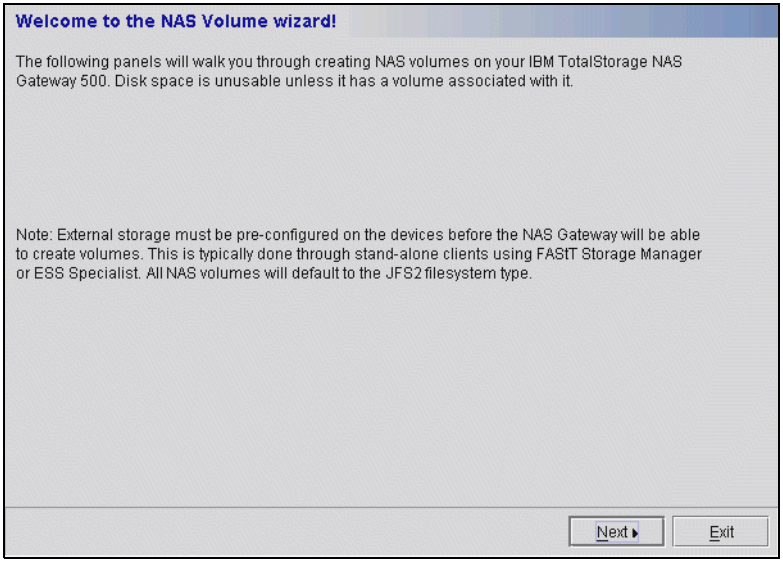


Figure 8-16 NAS Gateway 500 Volume wizard

The newly discovered disks will be presented under Logical volumes in the left pane (Figure 8-17).

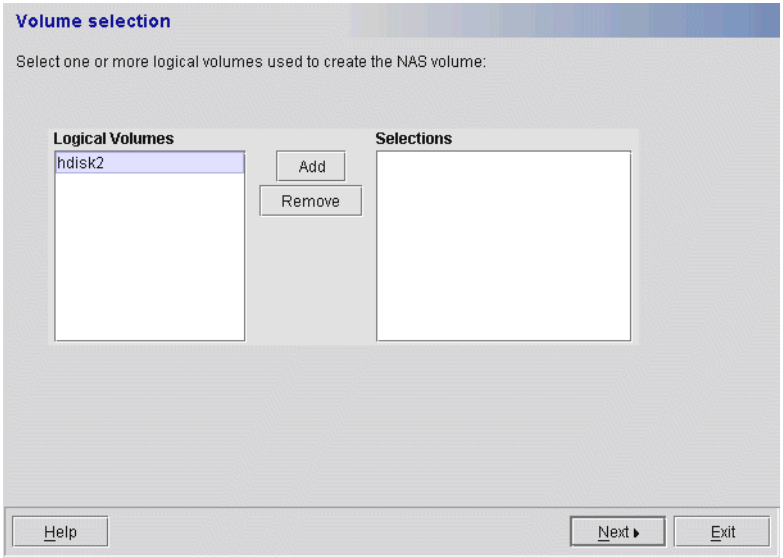


Figure 8-17 Volume selection

Select the new disk and click **Add** to move it under Selected pane on the right (Figure 8-18).

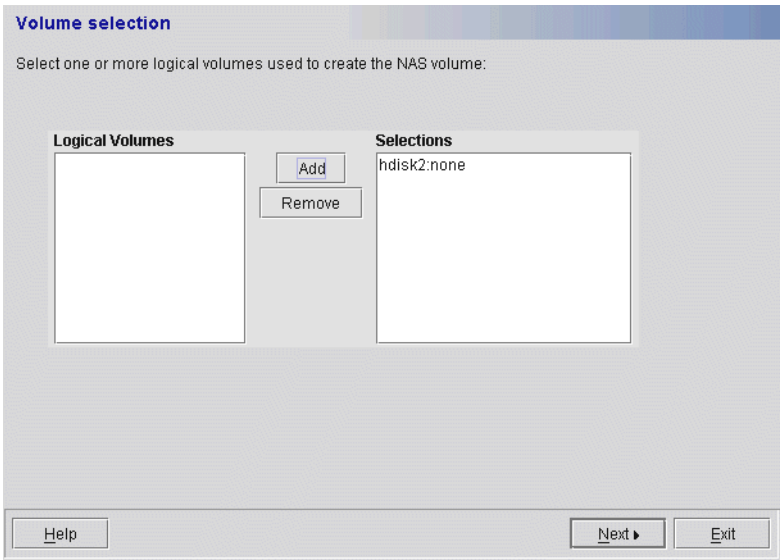


Figure 8-18 Volume selected

Now enter the Volume name under which the users will be able to access it. If you enable the snapshot feature, you also have to provide the maximum number of snapshots and snapshot size. This way the NAS Gateway 500 device will know how much space it needs to reserve for the snapshot feature. Additionally, you can specify what kind of volume sharing (CIFS, NFS or both) will be enabled with this volume (Figure 8-19).

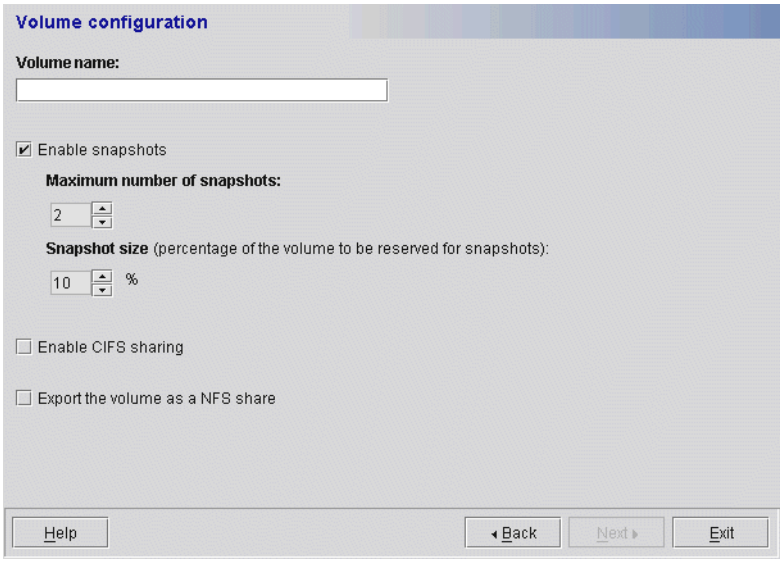


Figure 8-19 Volume configuration

After defining all options, the summary panel is presented (see Figure 8-20). You can still change them by clicking **Back** or confirm them by clicking **Next**.

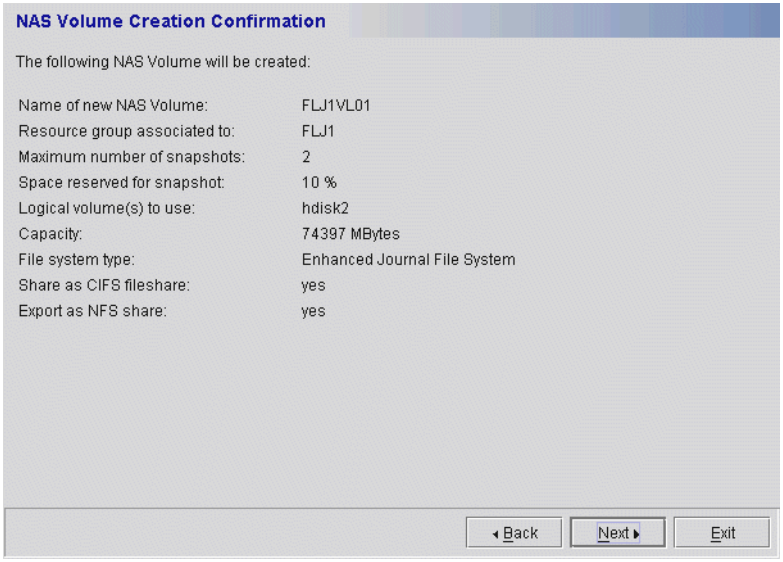


Figure 8-20 NAS Gateway 500 volume creation confirmation

The NAS volume is created. By clicking **Create Another Volume** you can repeat the procedure to create another NAS volume. Exit the wizard by clicking **Finish** (Figure 8-21).

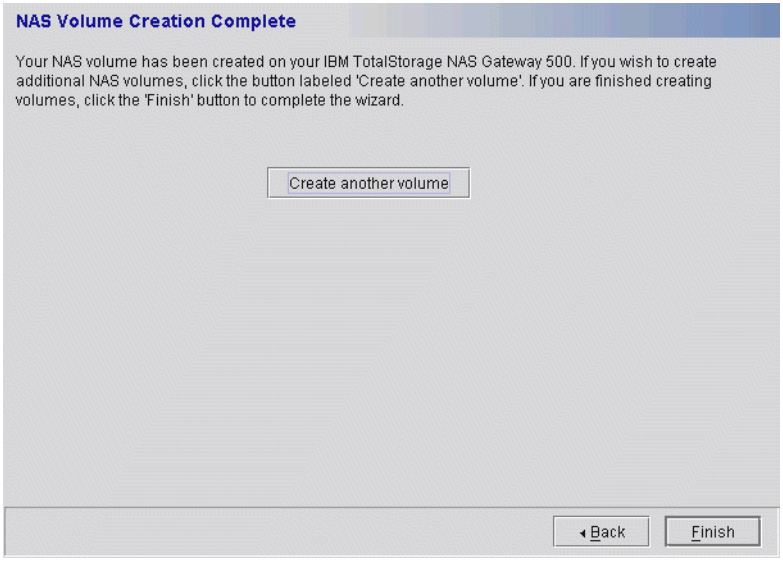


Figure 8-21 Completing the volume creation

8.2.3 Creating a mirror

The NAS Gateway 500 comes with four hot-swap hard drive bays. With the standard configuration, the first drive bay is populated with a 36 GB hard disk. If your initial NAS Gateway 500 order includes the mirroring feature, the second drive bay is populated with a 36 GB hard disk, and factory personnel have employed the AIX Logical Volume Manager mirroring function to protect the operating system against the possible failure of the first disk. IBM does not support the population of the remaining hard drive bays in the NAS Gateway 500.

If you order the mirroring feature after you have already ordered the NAS Gateway 500, see the section titled "Mirroring Option" in the IBM TotalStorage NAS Gateway 500 Hardware Installation Guide. It tells you how to install the hard drive that comes with the feature, and how to invoke the AIX Logical Volume Manager mirroring function using the SMIT interface.

The following pages tell you how to invoke the AIX Logical Volume Manager mirroring function using the WebSM interface. Remember, you don't need to do this if your NAS Gateway 500 came from the factory with two hard drives, because the mirroring function was installed at the factory.

Note: While the NAS Gateway 500 administrator account can be used for the majority of everyday tasks on the NAS Gateway 500, for this specific task you have to use the root account.

To create a mirror of the volume select **Volumes —> Volume Groups** under **Management Environment** in the left pane. The root volume group is displayed in the right pane, as shown in Figure 8-22.

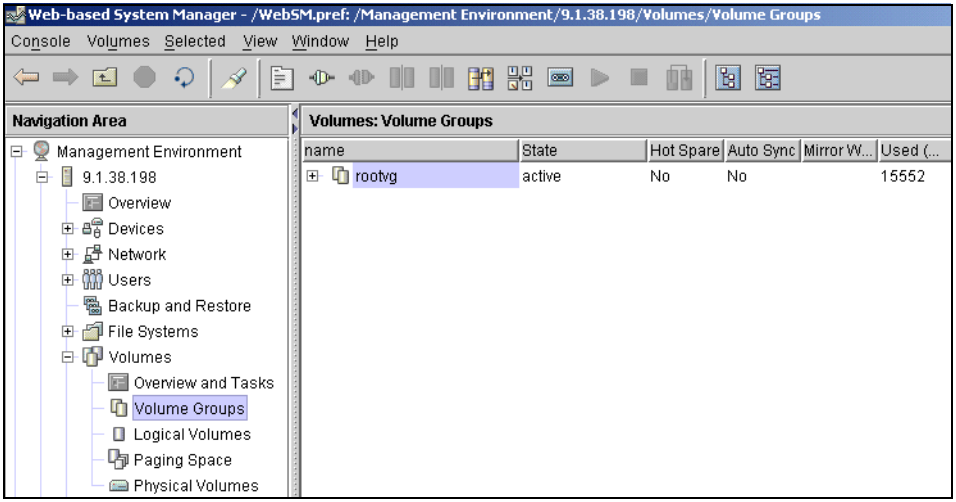


Figure 8-22 Volume groups

Our NAS Gateway 500 has two hard disks installed, seen by the operating system as physical volumes hdisk0 and hdisk1. The operating system is installed on the hdisk0, which is part of the root volume group. The hdisk1 has to be added to the rootvg and then the mirror can be established.

You can determine the hard disk number by “location code”. The location code can be obtained by the command **`lsdev -Cc disk`**. The output looks like Example 8-1.

Example 8-1 Determine hard disk number

```
[localhost_52]/>lsdev -Cc disk
hdisk0 Available 10-60-00-8,0 16 Bit LVD SCSI Disk Drive
hdisk1 Available 10-60-00-9,0 16 Bit LVD SCSI Disk Drive
```

The last digit before “,” is the SCSI ID of the hard disk. The SCSI IDs are also marked on the hot-plug disk slots. The SCSI IDs of the four slots are (from left to right): 8, 9, 10, 11.

Right-click the rootvg and select **Properties**, as shown in Figure 8-23.

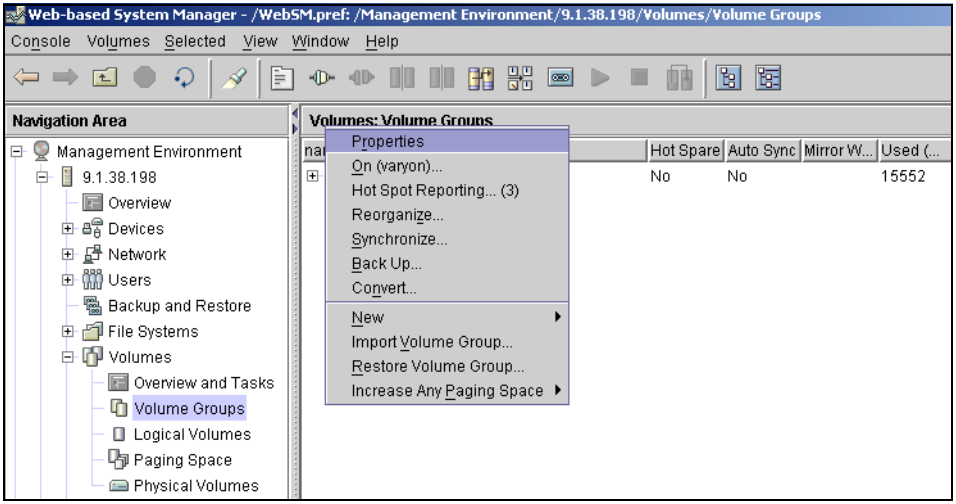


Figure 8-23 Rootvg properties

Open the **Physical Volumes** tab of the rootvg properties. Add hdisk1 from Available Physical Volumes to the rootvg by selecting it and clicking the **<** icon (Figure 8-24).

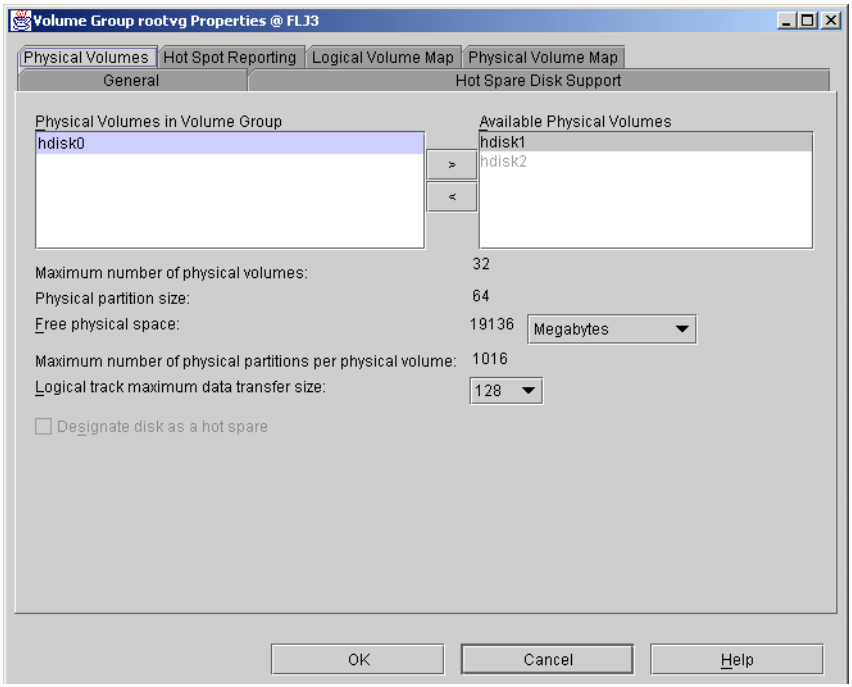


Figure 8-24 Adding physical volumes to rootvg

The new drive is now displayed under the Physical Volumes in the Volume Group pane. Select **OK** to initiate the procedure (Figure 8-25).

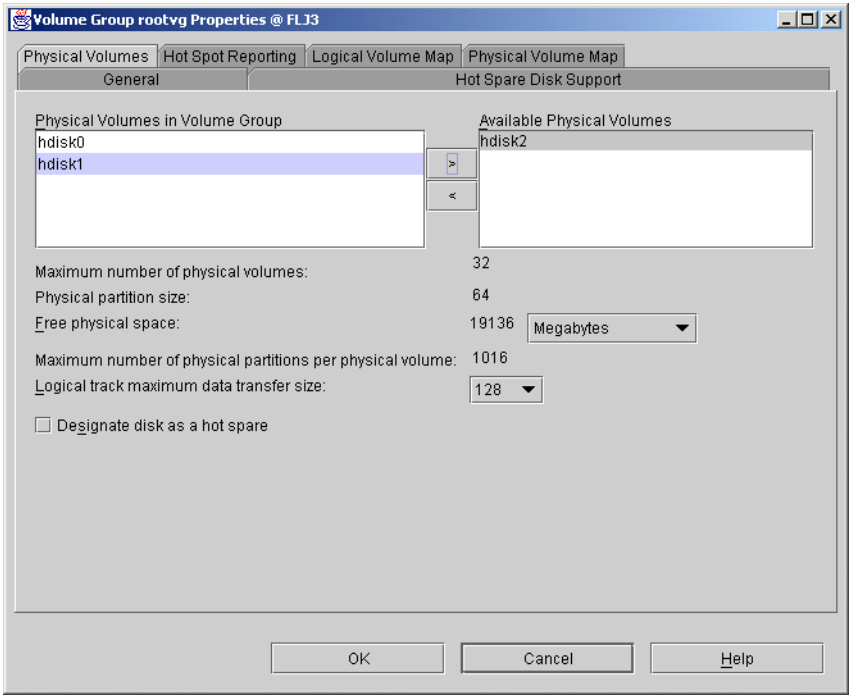


Figure 8-25 New physical volume added to rootvg

When the procedure is done, the progress panel displays Success. If there happened to be some error, you could click **Show Details** to get an explanation of the problem (Figure 8-26).

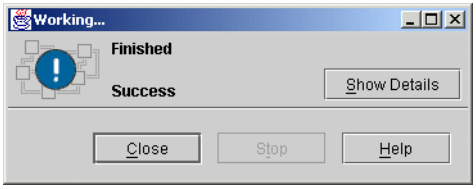


Figure 8-26 Progress panel

The next step is to establish a mirror. Back in the main WebSM window, right-click the rootvg again and select **Mirror**, as shown in Figure 8-27.

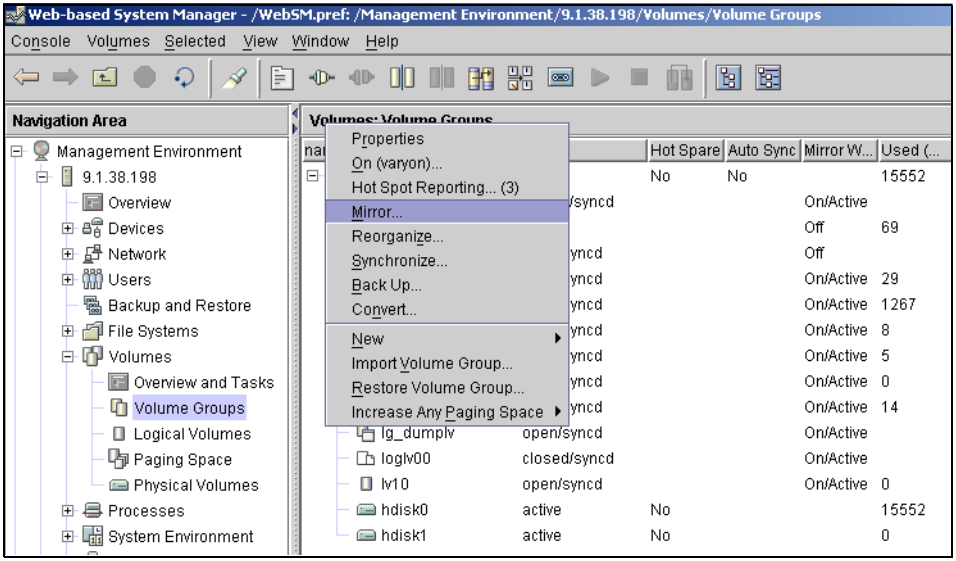


Figure 8-27 Establishing a mirror

The Mirror Volume Group window is displayed. Leave the default option **Default to any physical volume in volume group** selected. The bottom two options (Keep quorum checking on, and Create an exact logical volume mapping) should not be selected (Figure 8-28).

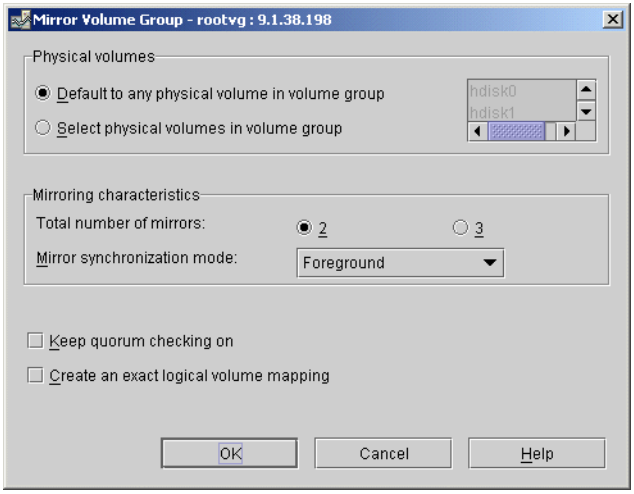


Figure 8-28 Configuring the mirror

After clicking **OK**, the mirror will be initiated. By clicking **Show Details**, the progress and possible messages will be displayed in the progress window (Figure 8-29).

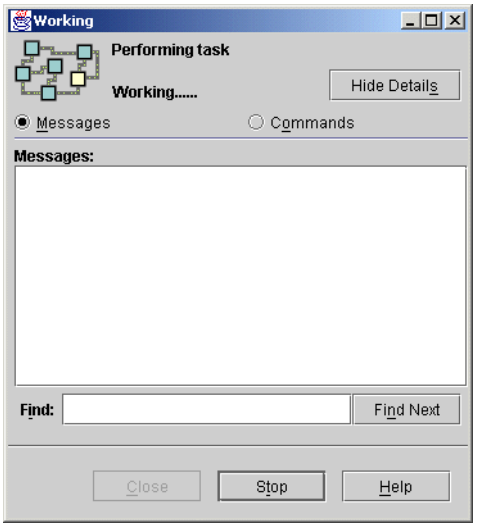


Figure 8-29 Progress window

When the mirror is created, the Success window is displayed (Figure 8-30).

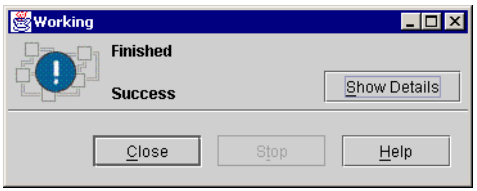


Figure 8-30 Mirror created

After the “Mirror” step is completed, use WebSM (see Figure 8-27 on page 166) and execute the “Synchronize” step for your newly created mirror.

You can find additional information on how to mirror the rootvg in NAS Gateway 500 Hardware Installation Guide. Please take a look at Section 7.2, “Planning for the setup” on page 117 to find out how to obtain a copy of the guide. The final steps for mirroring rootvg using the command line interface are to enter the commands **`bosboot -a`** and **`bootlist -m normal hdisk0 hdisk#`**, where `#` is the number of the new disk.

If the primary hard disk fails in such a configuration, the operating system continues to run from the second hard disk until the failed drive is replaced. If a reboot has to be done in this degraded state, the operator needs to select the second disk as the booting device in the boot list.

8.3 System errors and notification

There are several layers of error capture and notification implemented in the NAS Gateway 500. In this section we offer a short overview and point out the basic tasks that the system user is able to do before calling support personnel.

8.3.1 Service Processor

The Service Processor is an autonomous part of the machine used to monitor the NAS Gateway 500, its hardware parts, and the operating system. It writes the monitoring results into system logs. The Service Processor runs its own firmware code and is independent of the operating system. If the operating system hangs or is not in an operational state, the Service Processor offers the possibility to communicate with the machine or restart the operating system. Additionally, the Service Processor is able to start automatic corrective actions, like sending out error notification to IBM Service. As this is beyond the scope of this book, please refer to *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide* for more information about the Service Processor.

8.3.2 Operating system error logging

Another level of error logging is done inside the operating system. If an operating system module detects an error, it sends the error information to the errlog kernel service, which adds the timestamp and writes it to the error log file.

8.3.3 System error log

When an error or potential problem is detected by the operating system or service processor, the System Attention LED on the operator panel is turned on. Information about the error or potential problem is stored in error logs. The error logs can be accessed from the console that is used to manage the system.

Viewing the system error log

If you want to view the system error log, connect to the NAS Gateway 500 and login as root (Figure 8-31).

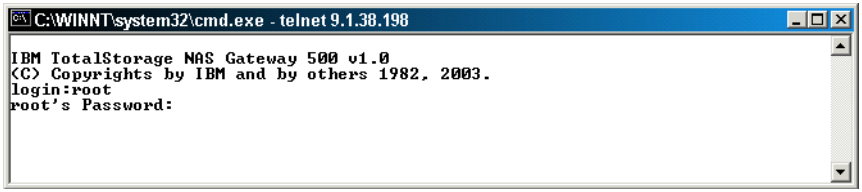


Figure 8-31 Telnet login

Once inside the NAS Gateway 500 command prompt, execute the **errpt -dH** command. This will display all hardware errors (Figure 8-32).

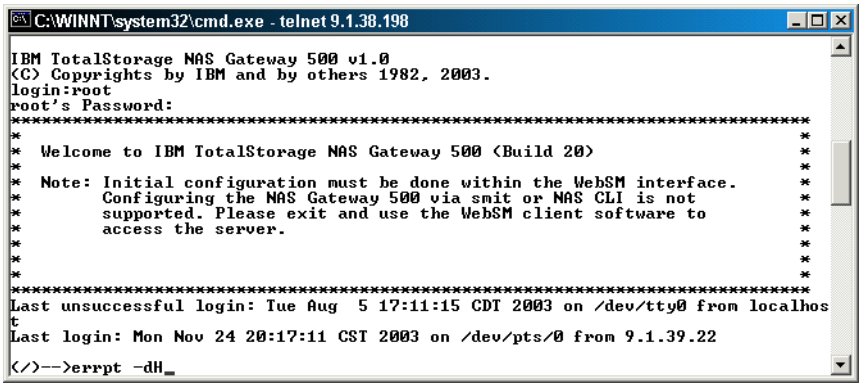


Figure 8-32 Viewing error log

If the list (see Figure 8-33) is not empty and there are relevant error entries, you should contact support personnel.

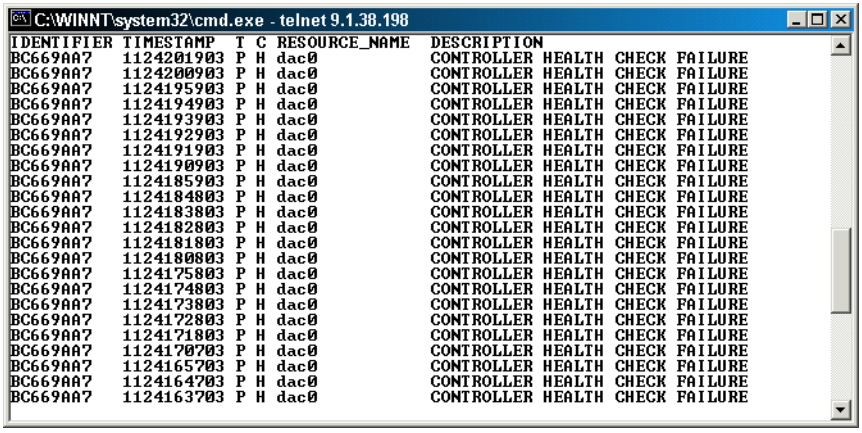


Figure 8-33 List of errors

For more information on the system error log, see Appendix A, “Error log information” on page 373.

8.3.4 System Attention LED

The System Attention LED on the operator panel turns on if specific failures have happened. This is how the NAS Gateway 500 signals the fact to the operator (Figure 8-34).

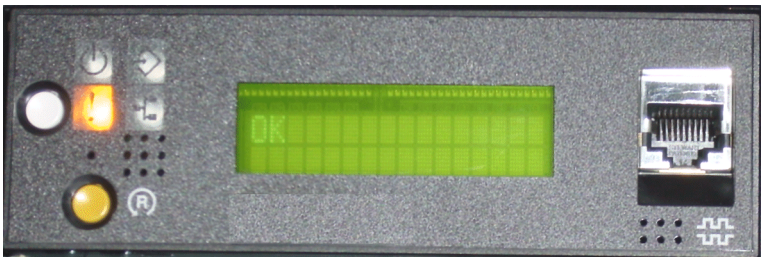


Figure 8-34 System Attention LED

Important: Before clearing the System Attention LED, the system error log should be diagnosed to find out if a corrective action is needed.

Resetting the System Attention LED

To reset the System Attention LED, proceed with the following steps. If the NAS Gateway 500 is powered on, run the following commands:

As a user with root authority, type **`diag`** on the command line, and do the following steps:

1. Select **Task Selection**.
2. On the Task Selection Menu, select the **Identify and Attention Indicators**.
3. When the list of LEDs is displayed, use the cursor to highlight **Set System Attention Indicator to Normal**.
4. Press Enter, and then press F7 to commit. This action turns off the LED.

If the system is shutdown and in Standby (with OK on the display), access the service processor menus. From the service processor main menu, do the following:

1. Select **System Information Menu** (see Figure 8-35).
2. Select **LED Control Menu** (see Figure 8-36).
3. Select **Clear System Attention Indicator**. This action turns off the LED (see Figure 8-37).

As an alternative, if powered on and logged in, you can also follow this process, which causes a system restart:

```
shutdown -F
```

If the NAS Gateway 500 is powered off, apply power on and wait for the Main Menu to display on the terminal, as shown in Figure 8-35. Press **3** to enter the System Information Menu.

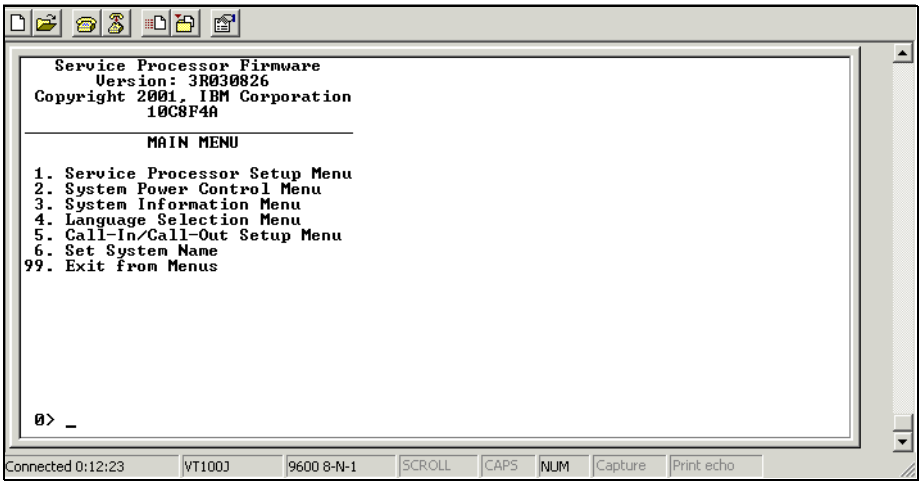


Figure 8-35 Main menu

Enter **10** to access the menu for controlling the LEDs on the front panel (Figure 8-36).

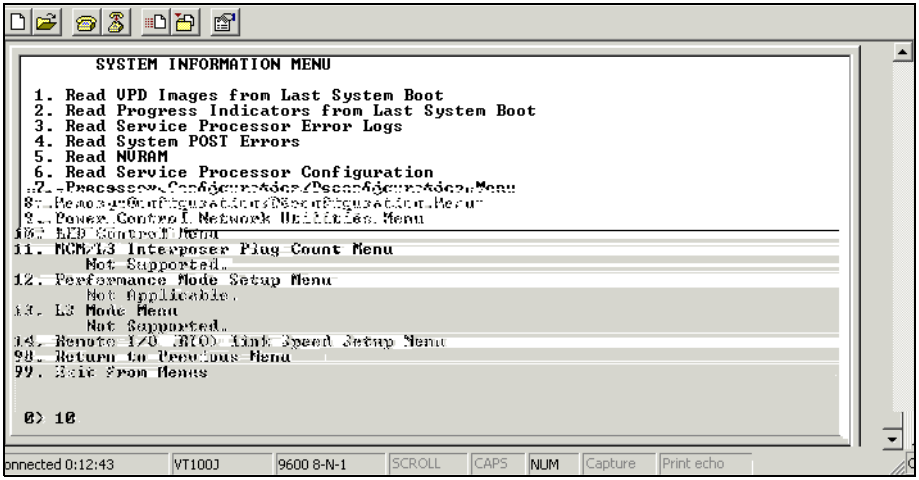


Figure 8-36 System Information menu

When the LED Control menu opens, enter **2** to clear the System Attention LED (Figure 8-37).

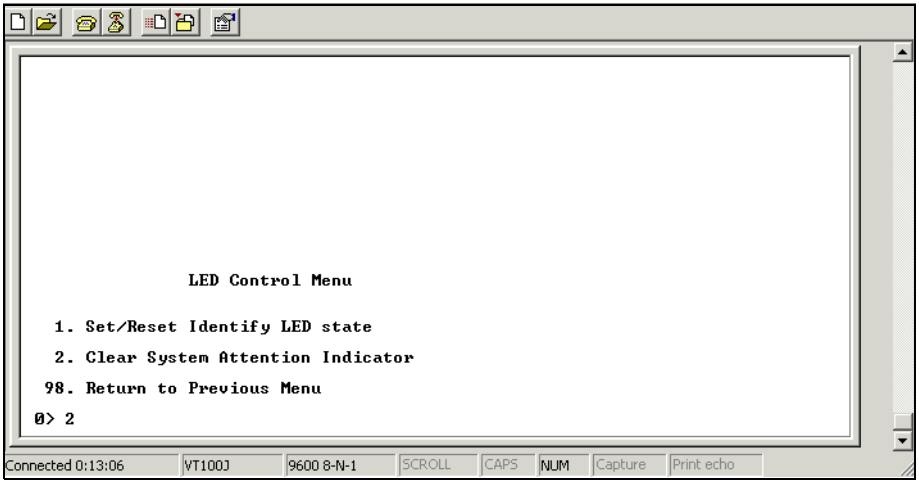


Figure 8-37 LED Control menu

The System Attention LED will be cleared and you can continue to boot the NAS Gateway 500.

9

Cluster configuration

This chapter discusses the cluster configuration of NAS Gateway 500. We go through a sample cluster configuration, covering the following topics:

- Cluster concepts
- Cluster planning
- Our cluster configuration
- Cluster setup
- Additional setup tasks
- Testing the cluster
- Cluster management

9.1 Cluster concepts

In this section we introduce some concepts of HACMP, the underlying clustering software used by NAS Gateway 500. Those terms may not appear in the NAS Gateway 500 cluster configuration menus, but understanding these concepts can be very helpful for the cluster planning, configuration, and management.

9.1.1 High availability

A NAS Gateway 500 cluster is a high availability cluster. High availability is:

- The masking or elimination of both planned and unplanned downtime
- The elimination of single points of failure (SPOFs)
- Fault resilience, but not fault tolerance

High availability systems are an excellent solution for applications that can withstand a short interruption should a failure occur, but which must be restored quickly.

Here is the difference between fault tolerance and high availability: A fault tolerant environment has no service interruption, while a highly available environment has a minimal service interruption. Many sites are willing to absorb a small amount of downtime with high availability rather than pay the much higher cost of providing fault tolerance. Additionally, in most highly available configurations, the backup servers are available for use during normal operation.

9.1.2 Cluster topology

The cluster topology consists of cluster nodes, cluster networks, communication interfaces, and communication devices. In this section we introduce the definition of these terms and their corresponding components in a NAS Gateway 500 cluster.

Cluster nodes

A node is a computer that runs the clustering software. Nodes may share a set of resources — disks, volume groups, filesystems, networks, network IP addresses, and applications.

In a NAS Gateway 500 cluster, both NAS Gateway 500 boxes are cluster nodes. They share external disks, volume groups, filesystems, networks, and network IP addresses; they also run the same file serving applications to provide services to clients.

Cluster networks

A cluster network connects two or more physical network interfaces. For example, all Ethernet adapters connected to the same HUB or VLAN are in the same cluster network, and two serial ports connected via null modem cable are in another cluster network.

There are many types of networks. HACMP differentiates between two major types of networks: TCP/IP networks and non-TCP/IP networks.

HACMP utilizes both of them for exchanging heartbeats. HACMP uses these heartbeats to detect failures in the cluster. Non-TCP/IP networks are used to distinguish an actual hardware failure from the failure of the TCP/IP software. If there were only TCP/IP networks being used, and the TCP/IP software failed, causing heartbeats to stop, HACMP could falsely detect a node failure when the node was really still functioning. Since a non-TCP/IP network would continue working in this event, the correct diagnosis could be made by HACMP. In general, all networks are also used for verification, synchronization, communication, and triggering events between nodes. Of course, TCP/IP networks are used for communication with client machines as well.

In a typical NAS Gateway 500 cluster, TCP/IP networks include the Ethernet connection used for providing file services to client systems as well as the Ethernet connection used for heartbeating. Non-TCP/IP network includes the serial connection between the two NAS Gateway 500 boxes.

Communication interfaces

An HACMP communication interface is a grouping of a logical network interfaces, file serving IP addresses and file serving IP labels that you defined to HACMP. HACMP communication interfaces combine to create IP-based networks.

An HACMP communication interface is a combination of:

- A logical network interface is the name of a physical network interface card.
- A file serving IP address is an IP address over which services, such as an application, are provided, and over which client nodes communicate.
- A file serving IP label is a label that maps to the file serving IP address.

Communication interfaces in HACMP are used in the following ways:

- A communication interface refers to IP-based networks and NICs. The NICs that are connected to a common physical network are combined into logical networks that are used by HACMP.

- Each NIC is capable of hosting several TCP/IP addresses. When configuring a cluster, you define to HACMP the IP addresses that HACMP will monitor (base or boot IP addresses), and the IP addresses that HACMP will keep highly available (the IP service addresses).
- Heartbeating in HACMP occurs over communication interfaces.

In a NAS Gateway 500 cluster, the Ethernet ports connected to client network and the Ethernet ports dedicated for heartbeating, their logical devices are used as communication interface.

Another type of communication interfaces in a NAS Gateway 500 cluster are file serving IP addresses. NAS Gateway 500 cluster use IP address takeover through IP aliasing for file serving IP addresses handling. Before the cluster software is started, each Ethernet interface has their boot-time IP address, called boot IP address; after the cluster software is started, the file serving IP address will be bound to one of those interfaces as an IP alias.

Note: On a NAS Gateway 500 cluster node, each boot IP address must be on different IP subnets.

Communication devices

HACMP also monitors network devices which are not capable of IP communications. Device-based networks are point-to-point connections that are free of IP-related considerations such as subnets and routing—each device on a node communicates with only one other device on a remote node.

In a NAS Gateway 500 cluster, such communication devices are serial ports. They connect two NAS Gateway 500s through a null modem cable assembly.

9.1.3 Cluster resources

HACMP considers the following as resource types:

- Volume groups
- Disks
- File systems
- File systems to be NFS mounted
- File systems to be NFS exported
- File serving IP addresses
- Applications, include the CIFS file server

Each resource in a cluster is defined as part of a resource group. This allows you to combine related resources that need to be operating together to provide a particular service. A resource group also includes the list of nodes that can acquire those resources and serve them to clients.

A resource group is defined as one of three types: cascading, rotating, or concurrent.

We only discuss the cascading resource group here, because it is the only resource group type used by the NAS Gateway 500 cluster.

All nodes in a cascading resource group are assigned priorities for that resource group. These nodes are said to be part of that group's resource chain. In a cascading resource group, the set of resources cascades up or down to the highest priority node active in the cluster. When a node that is serving the resources fails, the surviving node with the highest priority takes over the resources.

A parameter called Cascading Without Fallback (CWOF) is an attribute of cascading resource groups that defines its fallback behavior. When this flag is set to TRUE, a cascading resource group will not fallback to a higher priority node as the node joins or reintegrates into the cluster. A cascading group with CWOF set to FALSE will exhibit fallback behavior. The fallback behavior of a NAS Gateway 500 resource group can be set through the cluster configuration wizard.

9.2 Cluster planning

Here we explain how to plan a highly available NAS Gateway 500 cluster.

9.2.1 Eliminate the single point of failure

Our goal of building a cluster is to eliminate the single point of failure. Table 9-1 summarizes potential single points of failure within a NAS Gateway 500 cluster and describes how to eliminate them.

Table 9-1 Eliminating cluster objects as single points of failure

Cluster object	Eliminate a single point of failure by
Node	Using 2 nodes
Power source	Using multiple circuits or uninterruptable power supplies
Network adapter	Using multiple Ethernet adapters
Network	Using a separated, dedicated heartbeating network
TCP/IP subsystem	Using serial connection between nodes
Disk adapter	Using multiple Fibre Channel adapters

Cluster object	Eliminate a single point of failure by
Disk controllers	Using redundant disk controllers provided by storage device
Disk	Using RAID functions provided by storage device
Application	Assigning nodes for file serving takeover

9.2.2 Planning cluster networks

The NAS Gateway 500 system comes with up to 10 Ethernet ports, depending on the ordered feature codes. The onboard port 1 is used for administration purposes, and the onboard port 2 is used to build a dedicated cluster heartbeating network.

With clustering, there must be at least two and no more than four PCI-X Gigabit Ethernet adapters per cluster node. The adapters are not required to be the same feature code. Teaming is not supported when clustering.

The NAS Gateway 500 cluster uses IP address takeover with cascading resource group. This feature requires that each boot IP addresses on a node must be on separate IP subnets, and the file serving IP addresses must be on a subnet that is different from all boot IP address subnets. Your IP address assignment plan must meet these requirements.

The NAS Gateway 500 cluster uses the same subnet mask for all cluster subnets, include the file serving IP subnet and the boot IP subnets.

Important: The Ethernet ports connected to client network must be on the same VLAN.

Note: The network switch on the client network could be a single point of failure. You should also plan the high availability solution for network devices. However, this is out of the scope of this book.

9.2.3 Planning cluster disks

Before you perform the cluster configuration steps, you must attach the shared disk storage to both NAS Gateway 500 boxes. The shared storage must be configured to allow access from both nodes. The concurrent access feature is not required by a NAS Gateway 500 cluster.

9.2.4 Planning cluster resources

The resources used by a NAS Gateway 500 cluster include:

- Volume groups
- Disks
- File systems
- File systems to be NFS exported
- File serving IP addresses
- Applications, including the CIFS file server

You should group them logically by dependencies before configuring the cluster.

Here are the dependencies between these resources:

- NFS exports depends on file serving IP addresses and shared file systems.
- The CIFS file server depends on file serving IP addresses and shared file systems.
- Shared file systems depend on shared volumes. Volume groups and file systems configuration are simplified by NAS Gateway 500 management tools, generally there is a one-to-one correspondence between shared volume groups and shared filesystems.
- Shared volumes depends on shared disks.

Based on your requirements, you can decide which node should host which resource group for file serving, and which node should be the backup.

9.3 Our cluster configuration

We introduce our sample cluster configuration here. The cluster diagram is shown in Figure 9-1 on page 181.

9.3.1 Our cluster topology

We have two nodes. The hostname of node 1 is flj1, and the hostname of node 2 is flj3.

We connect serial port 3 of both NAS Gateway 500 boxes together through a null modem cable, which is provided with NAS Gateway 500 cluster.

We connect the onboard Ethernet port 2 of both NAS Gateway 500 boxes together through a crossover Ethernet cable, which is provided with a NAS Gateway 500 cluster.

We connect the Ethernet port 1 of each Gigabit Ethernet adapter to the client network switch. The cluster subnet mask is 255.255.254.0. The boot IP addresses assigned to them are listed in Table 9-2.

Table 9-2 Boot IP address assignment of our cluster

Ethernet port	Boot IP address
Node 1, Ethernet adapter 1, port 1	192.168.30.1
Node 1, Ethernet adapter 2, port 1	192.168.40.1
Node 2, Ethernet adapter 1, port 1	192.168.30.3
Node 2, Ethernet adapter 2, port 1	192.168.40.3

We use two file serving IP addresses:

- 9.1.38.198 for CIFS file sharing
- 9.1.38.197 for NFS file sharing

9.3.2 Our shared disks

We have two logical drives from a FastT storage server, connected to both nodes.

9.3.3 Our resources

We use two shared filesystems, one on each shared disk.

The resource groups in our cluster are as follows:

- Resource group 1 (node 1)
  - Disks: shared disk 1
  - Volume groups & file systems: /Vols/volnfs on the shared volume group 1
  - File systems to be NFS exported: /Vols/volnfs
  - File serving IP addresses: 9.1.38.197
  - Preferred owner: flj1 (node 1)
  - Backup node: flj3 (node 2)
- Resource group 2 (node 2)
  - Disks: shared disk 2
  - Volume groups & file systems: /Vols/volcifs on the shared volume group 2
  - File systems to be NFS exported: none
  - File serving IP addresses: 9.1.38.198
  - CIFS file server: sharing /Vols/volcifs
  - Preferred owner: flj3 (node 2)
  - Backup node: flj1 (node 1)

Our cluster diagram is shown in Figure 9-1.

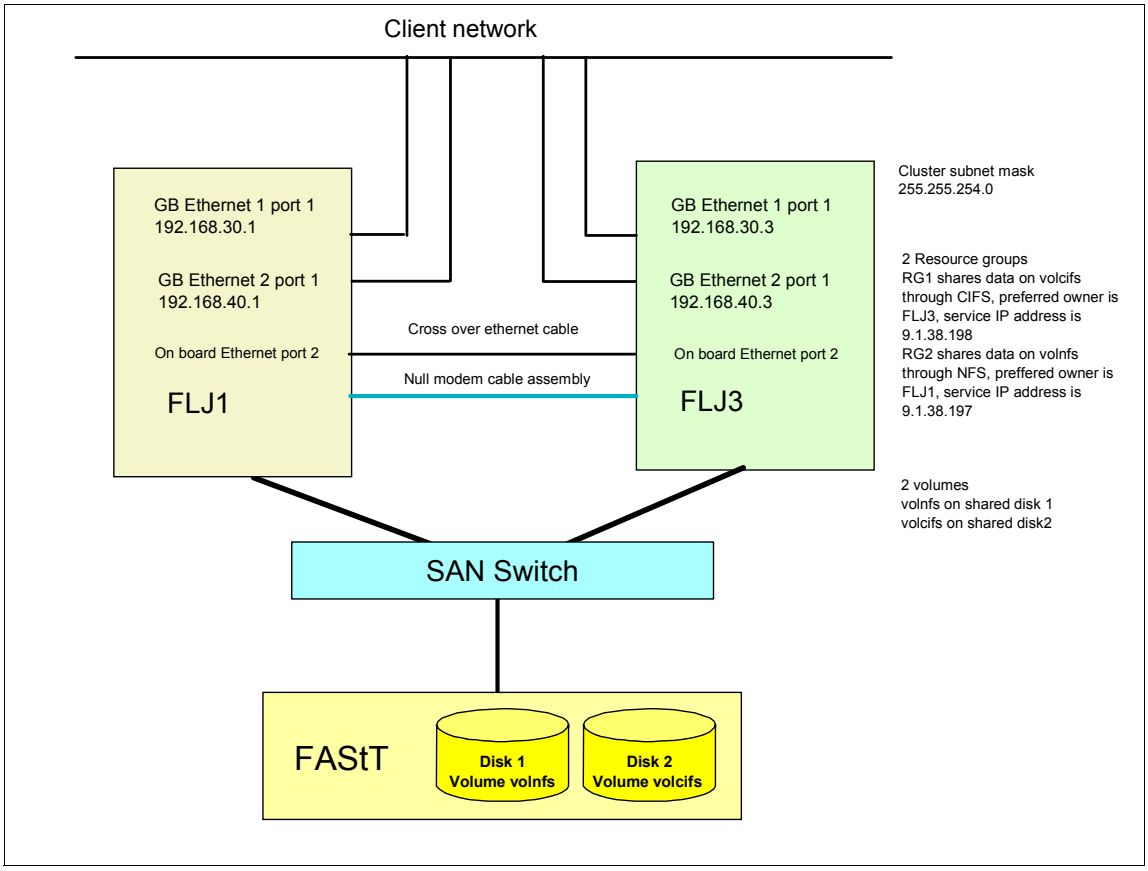


Figure 9-1 Our cluster configuration

Important: While setting up the cluster you must connect the NAS systems to your disk storage subsystem using a SAN switch. This will provide correct failover functionality.

9.4 Cluster setup

In this section we go through our sample cluster setup.

Disclaimer: At the time this book was written, the final release of the NAS Gateway 500 code was not available yet. Because we were working with the prerelease code, it is possible there are some differences as compared to the final product.

Connect the cables as described in 9.3.1, “Our cluster topology” on page 179.

Important: The four Ethernet ports connecting to the client network must be on the same VLAN.

Connect the integrated Ethernet port 1 of node 1 to the network in which your PC resides.

Important: You should not connect the node 2 integrated Ethernet port 1 to the client network unless you have a DHCP server on the network. If there is no DHCP server, both nodes will be assigned the same IP address on port 1, which will result in an IP address conflict if both nodes are connected.

Make sure that the Initial Configuration wizard on both nodes has not been run before.

Power on both nodes, and wait until both nodes have their IP addresses displayed on the LCD operator panel.

If the WebSM Remote Client is not installed on your PC, follow the steps described in 7.4.2, “Web-based System Manager Remote Client installation” on page 121 to install it. Use the IP address displayed on the LCD operator panel of node 1.

Start the WebSM Remote Client. In the Host name field, fill in the IP address displayed on the LCD operator panel of node 1. Fill in the root in the User name field. Fill in the password in the Password field. After that, press Enter or Tab and wait for connection to be established.

Start the Initial Configuration wizard as described in “Initial Configuration wizard” on page 128. Click **Next** to continue.

As shown in Figure 9-2, select **Clustering**. If the CIFS feature has been purchased, select **CIFS File Serving.** Click **Next** to continue.

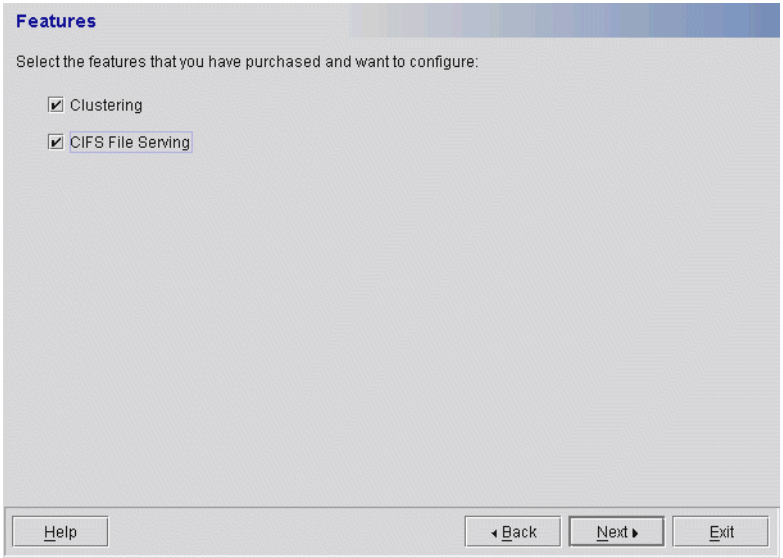


Figure 9-2 Select the clustering feature

The date and time settings screen will appear, as shown in Figure 7-22 on page 131. Enter the proper date and time settings, then click **Next** to continue.

The root password screen will appear, as shown in Figure 7-23 on page 131. Enter the new root password twice and click **Next** to continue.

The NAS Administrators screen will appear, as shown in Figure 7-24 on page 132. We add user nasadmin here as a NAS administrator account. This administrator account will be added to both nodes. Click **Next** to continue.

The directory service screen will appear, as shown in Figure 7-27 on page 134. Click **Next** to continue.

The file access users screen will appear, as shown in Figure 9-3. File Access Users are cluster aware, and if they exist, they should be added here.

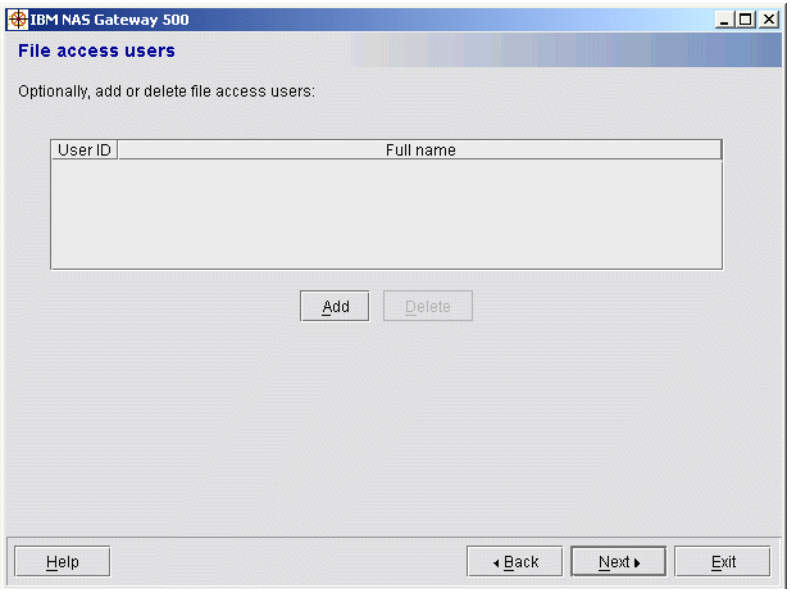


Figure 9-3 Cluster aware File Access User

Click **Next** to continue.

The Cluster wizard starts here, as shown in Figure 9-4. Fill in the Cluster name, Node 1 host name, and Node 2 host name field. Click **Next** to continue.

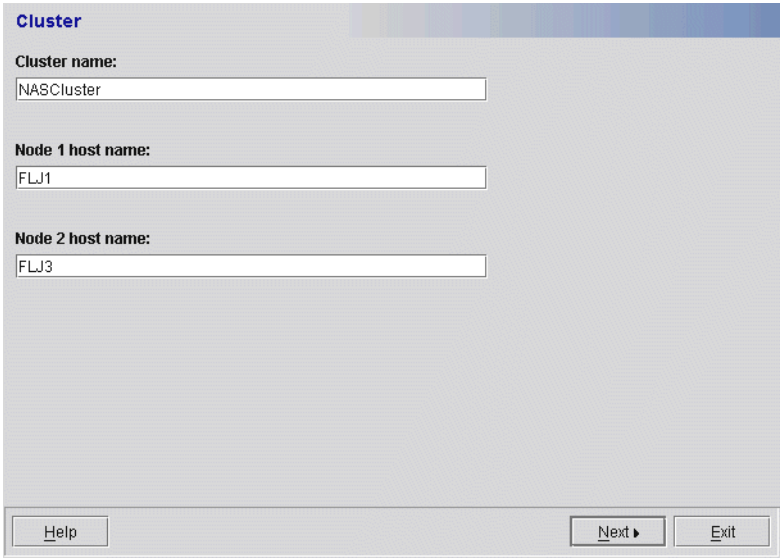


Figure 9-4 Setting cluster and node names

The cluster for node 1 screen will appear, as shown in Figure 9-5. We make the following configurations:

- In the Subnet mask field, we input 255.255.254.0.

Important: Here is where you would specify your default gateway if needed. If you have problems setting the default gateway, refer to Section 9.5.2, “Handling the default gateway” on page 197. Our default gateway is on the file serving IP address subnet, which is a different subnet from boot IP addresses.

- In the file serving IP addresses field, we input 9.1.38.197.
- We recommend that you leave the “Enable fallback” check box checked. Fallback means that after takeover has happened, if the preferred owner comes online again, the resource group will move back to the preferred owner. Fallback can cause service interruption for a short time, but it can balance the workload between the two nodes.
- From the Adapter pull down list, select card at slot 2 port 1. Fill 192.168.40.1 in the IP address field. Click **Add**.
- From the Adapter pull down list, select card at slot 1port 1. Fill 192.168.30.1 in the IP address field. Click **Add**.

Click **Next** to continue.

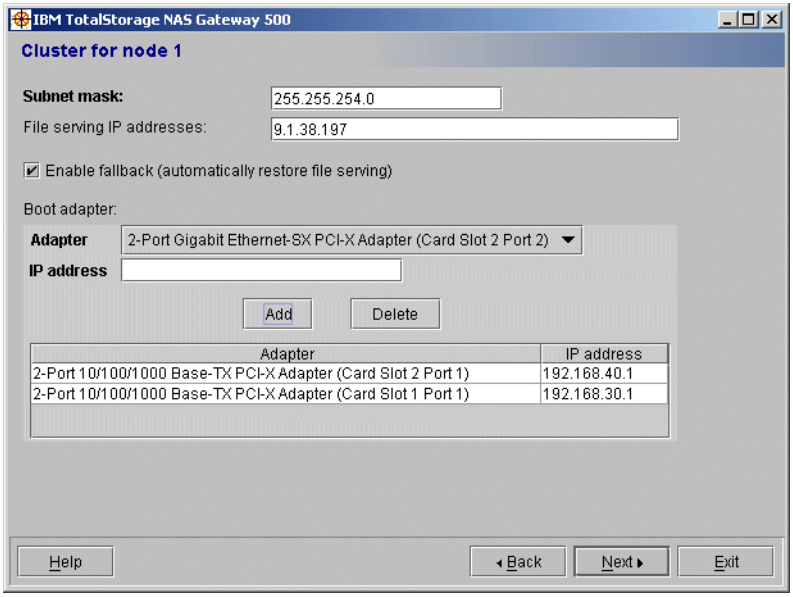


Figure 9-5 Cluster settings for node 1

The cluster for node 2 screen will appear, as shown in Figure 9-6. We make the following configurations:

- In the File serving IP addresses field, we input 9.1.38.198.
- Leave the “Enable fallback” check box checked.
- From the Adapter pull down list, select card at slot 2 port 1. Fill 192.168.40.3 in the IP address field. Click **Add**.
- From the Adapter pull down list, select card at slot 1port 1. Fill 192.168.30.3 in the IP address field. Click **Add**.

Click **Next** to continue.

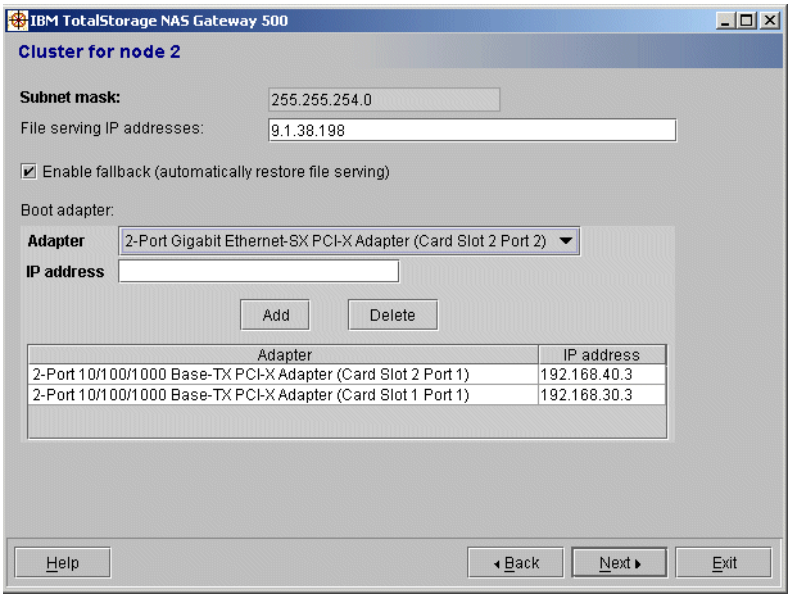


Figure 9-6 Cluster settings for node 2

The Synchronize Cluster screen appears, as shown in Figure 9-7. Click **Synchronize** to synchronize the cluster.

Note: The Cluster synchronization can take several minutes to complete. Don't make any change on any node during the synchronization period.

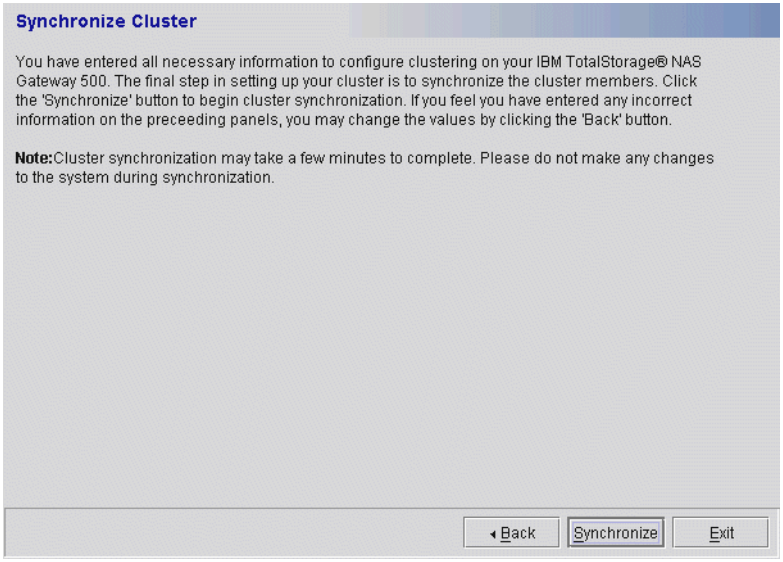


Figure 9-7 Synchronize cluster

The node 1 network configuration screen will appear. Because we don't have any more network interface to configure on node 1, just click **Next** to continue.

The node 2 network configuration screen will appear. Because we don't have any more network interface to configure on node 2, just click **Next** to continue.

Note: If you did not purchase the CIFS feature, please skip ahead to the volume selection screen description.

The CIFS server screen will appear, as shown in Figure 9-8. Set the NETBIOS server names, server description, and NETBIOS domain name here.

Click **Next** to continue.

Note: The two nodes must have different NETBIOS server names, and they must belong to the same NETBIOS domain or workgroup.

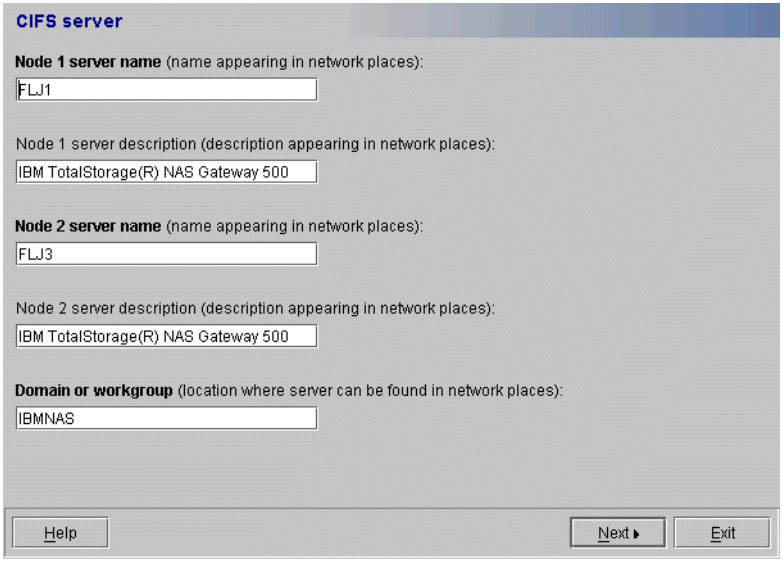


Figure 9-8 CIFS server settings

The WINS configuration screen will appear. Because we don't use WINS in our lab, we just click **Next** to continue.

Note: If you use WINS with your NAS Gateway 500 cluster, make sure the WINS server settings are always identical on both nodes.

The CIFS authentication screen will appear, as shown in Figure 7-34 on page 139. We select local authentication and click **Next** to continue.

Note: All authentication settings on both nodes must be identical in a NAS Gateway 500 cluster.

The Local Users screen will appear. We select **No, I will create local reader accounts myself**. Click **Next** to continue.

Important: Do not select dynamic user creation here. The dynamic user creation on NAS Gateway 500 is not cluster aware. It only creates local user accounts on the node which is providing CIFS file service. After failover has happened, the same user accounts may be recreated on the backup node. In this situation, the local user accounts for the same CIFS user will be likely to have different user IDs, which can cause serious file permission problems. For example, users can't access the files created by themselves, but can write to files owned by other users instead.

The confirm CIFS settings screen will appear, as shown in Figure 9-9. Review the settings and click **Next** to continue.

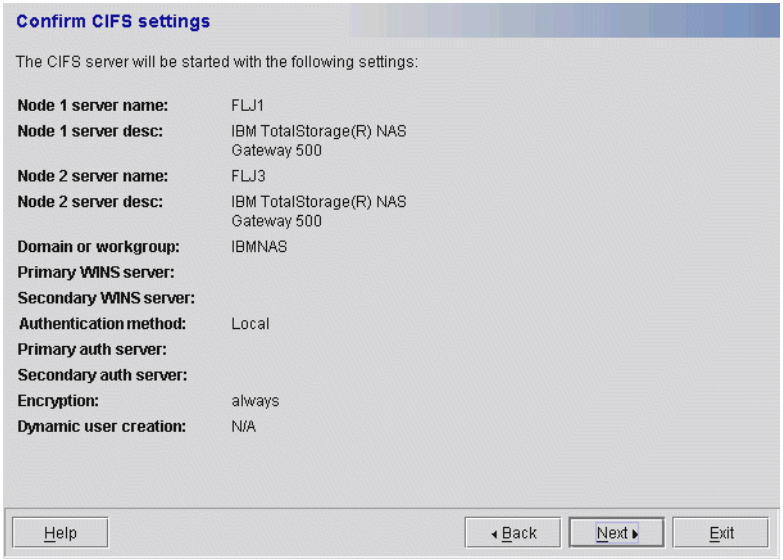


Figure 9-9 Confirm CIFS settings

The volume selection screen will appear, as shown in Figure 9-10. The disks listed here are physical volumes found on the shared storage.

We select hdisk2 and click **Add**. Click **Next** to continue.

Important: If you have created non-shared logical drives for the NAS Gateway 500 nodes on the external storage system, the logical drives may also be listed as hdisk devices in the Logical Volumes pane. With the Initial Configuration wizard, you have no way to find out which one is a shared logical drive and which one is not. If you select a non-shared logical drive to create a NAS volume in a cluster configuration, the Initial Configuration wizard will report an error.

To avoid this problem, you may need to login to the NAS Gateway 500 nodes through a serial terminal with the root account, and use storage system specified tools to identify which hdisk device is a shared logical disk.

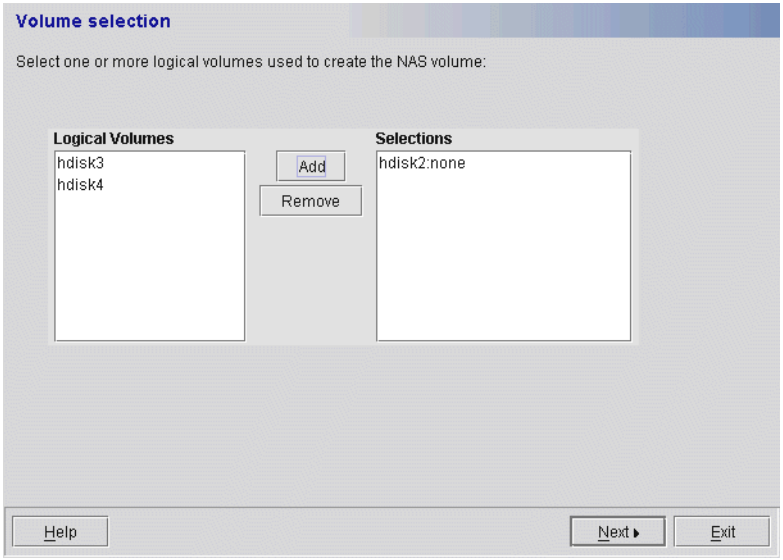


Figure 9-10 Volume selection

The volume configuration screen will appear, as shown in Figure 9-11.

Keep in mind that a NAS volume is a filesystem on the shared storage. NAS management tools automatically create and manage the volume group and other underlying structures for these filesystems.

We type in `volnfs` as the volume name. In the Hostname pull down list, we select FLJ1 as the preferred owner of this volume. Select the “Export the volume as an NFS share” check box.

Click **Next** to continue.

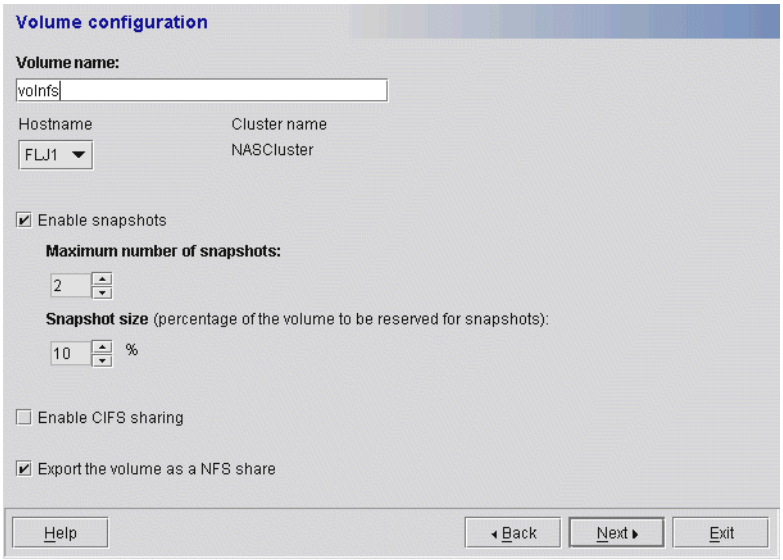


Figure 9-11 Volume configuration

The NAS volume creation confirmation screen will appear, as shown in Figure 9-12.

Click **Next** to create the NAS volume.

Note: The volume creation can take several minutes to complete. Don’t change any settings on the attached storage systems during this period.

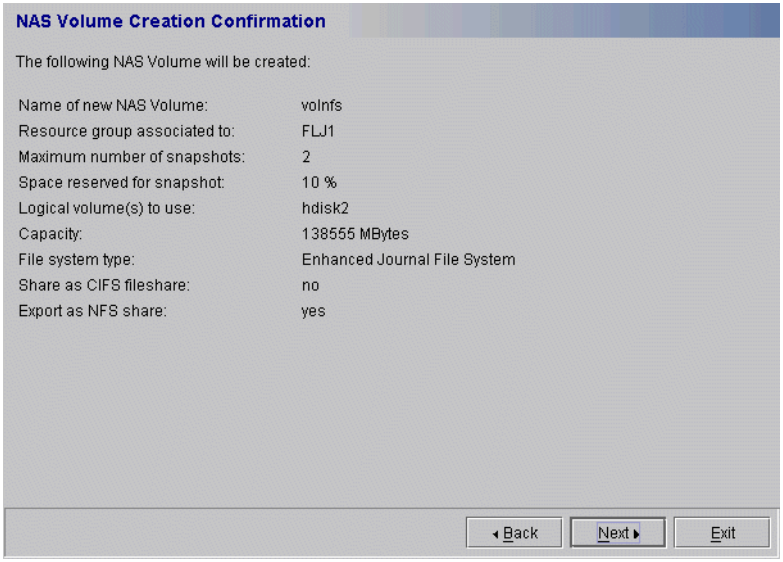


Figure 9-12 Volume creation confirmation

Next we create one more NAS volume.

Select hdisk3 from logical volumes and click **Add**, as shown in Figure 9-13. Click **Next** to continue.

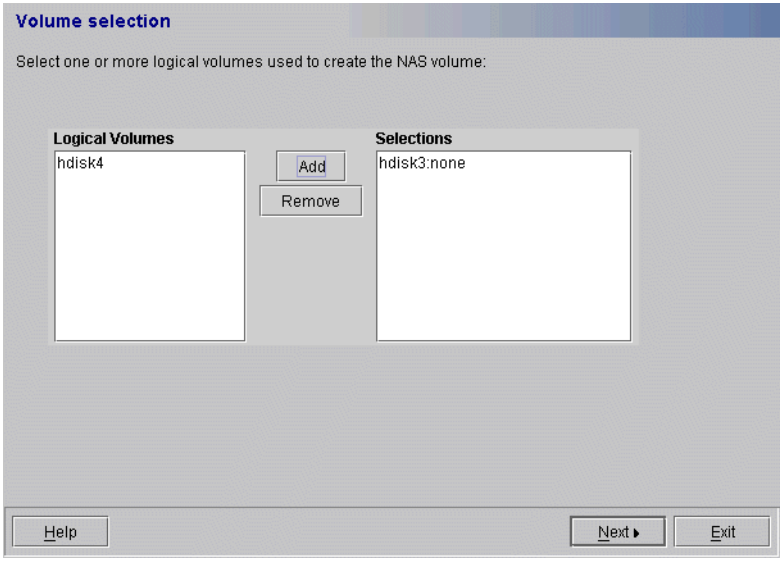


Figure 9-13 Volume selection for the second NAS volume

Name the volume volcifs, select flj3 as the preferred owner, and select the **Enable CIFS sharing** check box (Figure 9-14).

Click **Next** to continue.

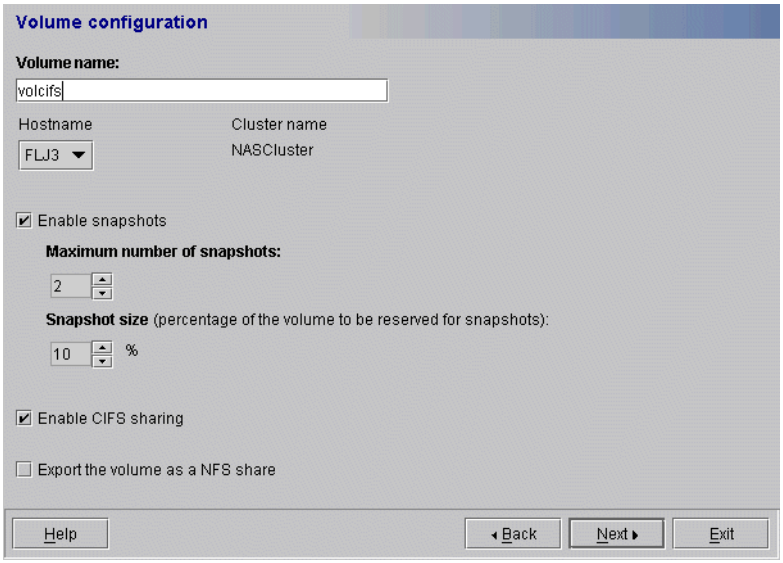


Figure 9-14 Volume configuration for the second NAS volume

Review volume settings on the NAS volume configuration confirmation screen, and click **Next** to create the second NAS volume (Figure 9-15).

Wait until the volume creation is completed.

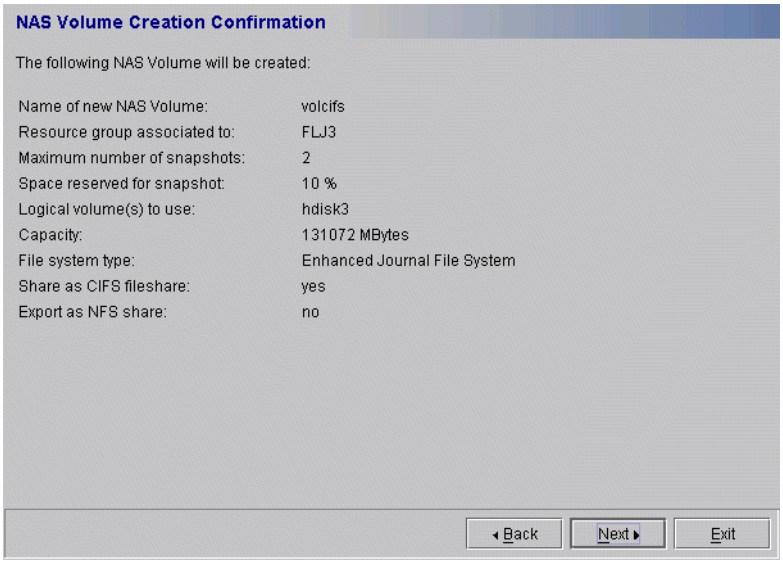


Figure 9-15 NAS volume creation confirmation for the second NAS volume

Select **Finish** to exit the Initial Configuration wizard. Now we have finished the basic cluster setup.

9.5 Additional setup tasks

With the Initial Configuration wizard, we built a very basic cluster. In order to make the cluster serve client machines properly, some additional configuration is required.

9.5.1 Checking the cluster status

Prior to performing more configuration tasks, you must make sure your cluster is running in a stable state.

In this section, we explain how to check the cluster status.

Use WebSM to connect to node 1. Login with the NAS administrator account.

Select **Cluster management** in the left pane, then select **Show Cluster Server State** in the right pane. The dialogue shown in Figure 9-16 will appear.

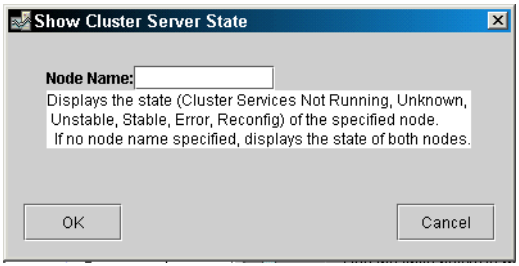


Figure 9-16 Show Cluster Server State

Just click **OK** to continue. Click **Yes** on the next prompt. Wait for the success message and click **Show Details** for cluster state, as shown in Figure 9-17.

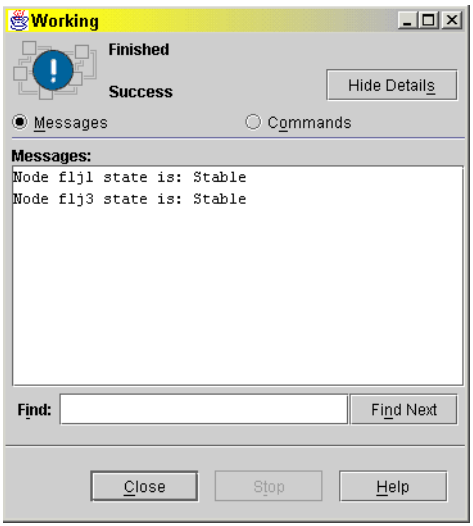


Figure 9-17 The cluster server state

The state of both nodes should be stable. If the state of a node is idle, that means cluster service is not started on that node, use **Enable Server in Cluster** in the right pane to start cluster service on that node. If the state of a node is unstable, wait until it becomes stable.

Don't continue the cluster configuration unless the states of both nodes are stable.

9.5.2 Handling the default gateway

With the NAS Gateway 500 cluster created by the Initial Configuration wizard, the two NAS Gateway 500 nodes will boot up with the boot IP address. After the cluster service is started, the file serving IP addresses are configured, and client machines can access file shares through the file serving IP address. In a production environment, the client machines may reside on different IP subnets than the file serving IP addresses. A default gateway on the file serving IP addresses subnet is required to enable access from these clients.

You can set a default gateway on NAS Gateway 500, and it will be added to the route table at system startup. The problem is that during system startup, only boot IP addresses, heartbeat network IP addresses, and the administrative IP address are available. If none of them are in the same IP subnet as the file serving IP addresses (and they should not be), the default gateway will not be added to the route table because it is not reachable.

We can use persistent IP addresses to solve this problem.

A persistent IP address is an IP alias that can be assigned to a specific node on a cluster network and that:

- Always stays on the same node (is node-bound)
- Co-exists on a network interface card that already has a file serving IP label defined
- Does not require installing an additional physical network interface card on that node
- Is not part of any resource group.
- Is configured at boot time.

If we have persistent IP addresses in our cluster, and they are in the file serving IP subnet, the default gateway will be reachable at system start.

Here we show you how to configure it in a NAS Gateway 500 cluster.

We need two more IP addresses in the file serving IP subnet. We use 9.1.38.191 and 9.1.38.155 in our lab.

Preparing the /etc/hosts file on both nodes

Login to node 1 as root, via a serial terminal. Run command **`smitty mkhostent`**.

In the INTERNET ADDRESS field, fill in the persistent IP address for node 1. We enter 9.1.38.191 here.

In the HOST NAME field, enter a name for the persistent IP address of node 1. We enter flj1_pers here. Press Enter to process.

Press Esc+0 to exit to the command line prompt.

Run command **smitty mkhostent**.

In the INTERNET ADDRESS field, fill in the persistent IP address for node 2. We enter 9.1.38.155 here.

In the HOST NAME field, enter a name for the persistent IP address of node 2. We enter flj3_pers here. Press Enter to process.

Press Esc+0 to exit to the command line prompt.

Login to node 2 as root, via a serial terminal. Run command **smitty mkhostent**.

In the INTERNET ADDRESS field, fill in the persistent IP address for node 1. We enter 9.1.38.191 here.

In the HOST NAME field, enter a name for the persistent IP address of node 1. We enter flj1_pers here. Press Enter to process.

Press Esc+0 to exit to the command line prompt.

Run command **smitty mkhostent**.

In the INTERNET ADDRESS field, fill in the persistent IP address for node 2. We enter 9.1.38.155 here.

In the HOST NAME field, enter a name for the persistent IP address of node 2. We enter flj3_pers here. Press Enter to process.

Press Esc+0 to exit to the command line prompt.

Now we have the /etc/hosts file on both nodes ready.

Adding persistent IP addresses to cluster

Login to node 1 as root, via a serial terminal. Run command **smitty hacmp**.

Select **Extended Configuration** -> **Extended Topology Configuration** -> **Configure HACMP Persistent Node IP Label/Addresses** -> **Add a Persistent Node IP Label/Address**. Then select node 1, for us it is flj1. The SMIT screen shown in Figure 9-18 will appear.

In the Network Name field, select the network that contains your file serving IP subnet. The name is ended with “pubnn1”.

In the Node IP Label/Address field, select the persistent IP address name of node 1. For us, it is flj1_pers. Press Enter to process. Press Esc+0 to exit to the command prompt.

```
                    Add a Persistent Node IP Label/Address

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* Node Name                                           flj1
* Network Name                                       [nasclusterpubnn1] +
* Node IP Label/Address                              [] +

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 9-18 Add a persistent IP address to cluster

Run command **`smitty hacmp`**.

Select **Extended Configuration** -> **Extended Topology Configuration** -> **Configure HACMP Persistent Node IP Label/Addresses** -> **Add a Persistent Node IP Label/Address**. Then select node 2, for us it is flj3.

In the Network Name field, select the network contains your file serving IP subnet. The name is ended with “pubnn1”.

In the Node IP Label/Address field, select the persistent IP address name of node 2. For us, it is flj3_pers. Press Enter to process. Press Esc+0 to exit to the command prompt.

Run command **smitty hacmp**.

Select **Initialization and Standard Configuration** -> **Verify and Synchronize HACMP Configuration**. Wait until the synchronization is completed.

Now we configured the persistent IP addresses in the cluster.

Configuring default gateway

Now we configure default gateway on the NAS Gateway 500 nodes.

Login to node 1 as root, via a serial terminal. Run command **smitty route**. Select **Add a Static Route**. The SMIT screen shown in Figure 9-19 will appear.

```
                                Add Static Route

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
  Destination TYPE                                     net +
* DESTINATION Address                                  [] (dotted decimal or
symbolic name)
* Default GATEWAY Address                              []
  (dotted decimal or symbolic name)
  COST                                                 [0] #
  Network MASK (hexadecimal or dotted decimal)         []
  Network Interface                                    [] +
  (interface to associate route with)
  Enable Active Dead Gateway Detection?                 no +
  Is this a Local (Interface) Route?                    no +



F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 9-19 Add a static route

Fill number 0 in the DESTINATION Address field. Fill the default gateway IP address in the Default GATEWAY Address field. Press Enter to process.

Login to node 2 as root, via a serial terminal. Run command **`smitty route`**. Select **Add a Static Route**.

Fill number 0 in the DESTINATION Address field. Fill the default gateway IP address in the Default GATEWAY Address field. Press Enter to process.

Now we have done the default gateway configuration for the NAS Gateway 500 cluster.

9.5.3 Creating file access users

Here we explain how to create file access users in a NAS Gateway 500 cluster.

In the NAS Gateway 500, file access is controlled by user ID. In order to make file shares highly available to users, each user must have identical user IDs on both nodes of a NAS Gateway 500 cluster.

At the time this IBM Redbook went to print, the WebSM method of file access user creation was the easiest and safest. File access user creation on WebSM is cluster-aware, meaning that when you create a file access user on one node, the user definition is propagated to the other cluster node. This guarantees that both cluster nodes have the same user names and user IDs.

If you use SMIT or the command line to create file access users, you must do it in the same way on each cluster node, being careful to specify the same user name-user ID number combination on each node. If you make a mistake and supply a user name with a certain user ID number on one node, and on the other node you supply the same user name but a different user ID number, the file access user will lose contact with the file shares if there is a cluster failover. So, the WebSM method is the recommended way to do it, because WebSM ensures that each user name will have the same user ID number across all cluster nodes.

To create a file access user with the WebSM Remote Client, go to **NAS Management --> NAS System --> Client Access --> Overview and Tasks --> Create a new user**. This will take you to the **Add NAS user** panel, where you will click the **Add** button. When you see the popup box, add the user name (not the user ID number) and the password, and click **OK**. Repeat this process for each new file access user.

9.5.4 Creating CIFS users

After the file access users are created, we can create CIFS users for CIFS access.

The CIFS user creation tool in WebSM is cluster aware, so just use the same steps as in the single node configuration.

See 10.3, “User creation on the NAS Gateway 500” on page 220 for the detailed steps about CIFS user creation.

We create CIFS user nasuser here.

9.6 Testing the cluster

In this section we discuss how to test the cluster, including the file serving testing, cluster verification, and error simulations.

9.6.1 File serving testing

After we finished the cluster setup, we should test if the resources managed by the NAS Gateway 500 cluster can be accessed by client machines.

NFS testing

On a client machine running UNIX, perform following operations:

1. Run command **`showmount -e 9.1.38.197`**, /Vols/volnfs should be listed in the exports list.
2. Try mount 9.1.38.197:/Vols/volnfs to a local directory. The **`mount`** command should complete successfully.

   Note: You may experience error with **`mount`** command if the NAS Gateway 500 nodes can’t resolve the client machine’s IP address to hostname. See Chapter , “The reverse lookup problem on AIX” on page 266 for details.

3. Run command **`df -k`** to verify the free space on the mounted NFS filesystem in kilobytes. The free space should be equal to the capacity displayed on the volume creation confirmation screen.
4. Try to copy some files to and from the mounted NFS filesystem. The copy actions should complete successfully.

CIFS testing

On a client machine running Windows, perform the following operations:

1. Open a command prompt.
2. Run command **`net use x: \\9.1.38.198\volcifs /USER:nasuser`**. Supply the CIFS password of nasuser. This command should complete without problems.
3. Run command **`dir x:`**, the free space displayed should be equal to the capacity displayed on the volume creation confirmation screen.
4. Try to copy some files to and from x:. The copy actions should complete successfully.

9.6.2 Cluster verification

The purpose of cluster verification is to make sure cluster topology and cluster resources are configured properly for high availability. Follow these steps to perform a cluster verification:

1. First, use **`telnet`** or serial terminal to connect to node 1, and login with the NAS administrator account you created in the Initial Configuration wizard. In our configuration, that is nasadmin.
2. Then run command **smitty**. The SMIT screen shown in Figure 9-20 will appear. Select **Manage Cluster** to continue.

Tip: In a SMIT screen, use cursor keys to move cursor up and down. Press Enter to select.

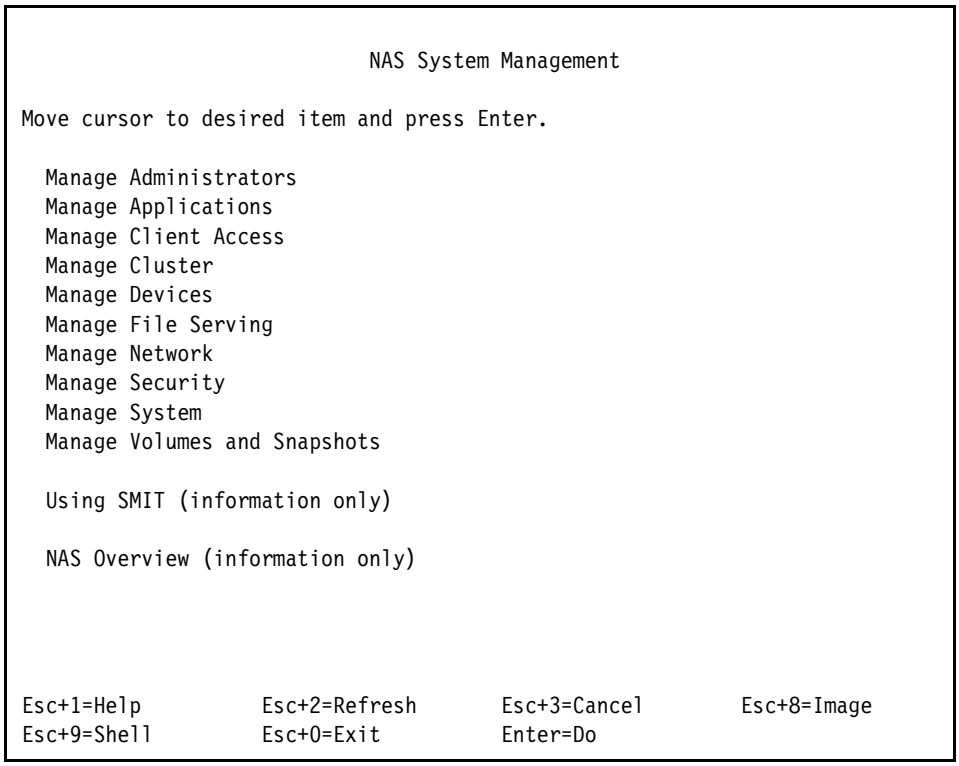


Figure 9-20 Verify the cluster: the root menu of smitty

3. Select **Verify Cluster** in the Manage Cluster screen, as shown in Figure 9-21.

```
                                Manage Cluster

Move cursor to desired item and press Enter.

  Enable Cluster
  Disable Cluster
  Verify Cluster
  Synchronize Cluster
  Delete Cluster

  Show Cluster Server State
  Enable Server in Cluster
  Disable Server in Cluster
  Move Service to Another Adapter

  Show Volumes Being Served
  Relocate Volumes
  Enable a Volume in the Cluster
  Disable a Volume in the Cluster

  View Cluster Log

Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel        Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 9-21 Verify the cluster: the Manage Cluster SMIT menu

4. Wait until the cluster verification is completed. If the verification is failed, read the detailed message presented in the SMIT screen, and review your cluster planning and configuration.

9.6.3 Simulating errors

The next step of cluster testing is to simulate errors to verify the high availability. Here, we explain how to test the cluster behavior on network adapter/cable failure and node failure. You should also test the high availability of the following devices:

- Storage system, such as disk adapter, disk controller, cables, disks
- Power source
- Network devices, such as Ethernet switch and router

However, the setup and testing procedure of high availability on these devices is beyond the scope of this book.

Simulate the network adapter/cable failure

Follow these steps to simulate a network adapter/cable failure:

On node 1 and 2:

1. Connect a serial terminal to the node. Login as root.
2. Use **`netstat -in`** command to determine which port is bound with the file serving IP address.

   Tip: We know the corresponding boot IP address of each Ethernet port. So we can use the boot IP address on the interface where the file serving IP address is located to determine which Ethernet port it is.

3. Run this command on the NAS node: **`tail -f /logs/cluster/hacmp.out`**.
4. Unplug the cable from the port which the file serving IP address is bound. Look at the terminal screen, make sure the swap adapter event is processed.
5. Try to access file share from client machines. Make sure the share still can be accessed.
6. Plug the cable. Make sure the join standby event is processed.
7. Unplug another cable. Look at the terminal screen, make sure the swap adapter event is processed.
8. Try to access file share from client machines. Make sure the share still can be accessed.
9. Plug in the cable. Make sure the join standby event is processed.

Simulate the node failure

Follow these steps to simulate a node failure:

1. Connect a serial terminal to node 2. Login as root.
2. Run this command on node 2: **`tail -f /logs/cluster/hacmp.out`**.
3. Power down node 1 by pressing the power button.
4. Look at the terminal screen. Make sure the node down event is processed.
5. Try to access file shares from client machines. Make sure the share of node 1 still can be accessed.
6. Power on node 1. Look at the terminal screen. Wait until the node up event is processed.
7. Connect a serial terminal to node 1. Login as root.
8. Use **netstat -in** command to verify the file serving IP address is back on node 1.

9. Try to access file shares from client machines. Make sure the share of node 1 still can be accessed.
10. Run this command on node 1: **`tail -f /logs/cluster/hacmp.out`**.
11. Power down node 2 by pressing the power button.
12. Look at the terminal screen of node 1. Make sure the node down event is processed.
13. Try to access file shares from client machines. Make sure the share of node 2 still can be accessed.
14. Power on node 2. Look at the terminal screen of node 1. Wait until the node up event is processed.
15. Login as root from the terminal connected to node 2.
16. Use **`netstat -in`** command to verify the file serving IP address is back on node 2.
17. Try to access file shares from client machines. Make sure the share of node 2 still can be accessed.

9.7 Cluster management

You can use both SMIT menu and WebSM GUI for cluster management. The functions provided by both tools are all very straightforward, and also have contextual help messages (see Figure 9-22 and Figure 9-23).

With these tools, you should have no problems in cluster management.

Tip: Press **F1** in the SMIT interface can bring up contextual help messages for the highlighted item.

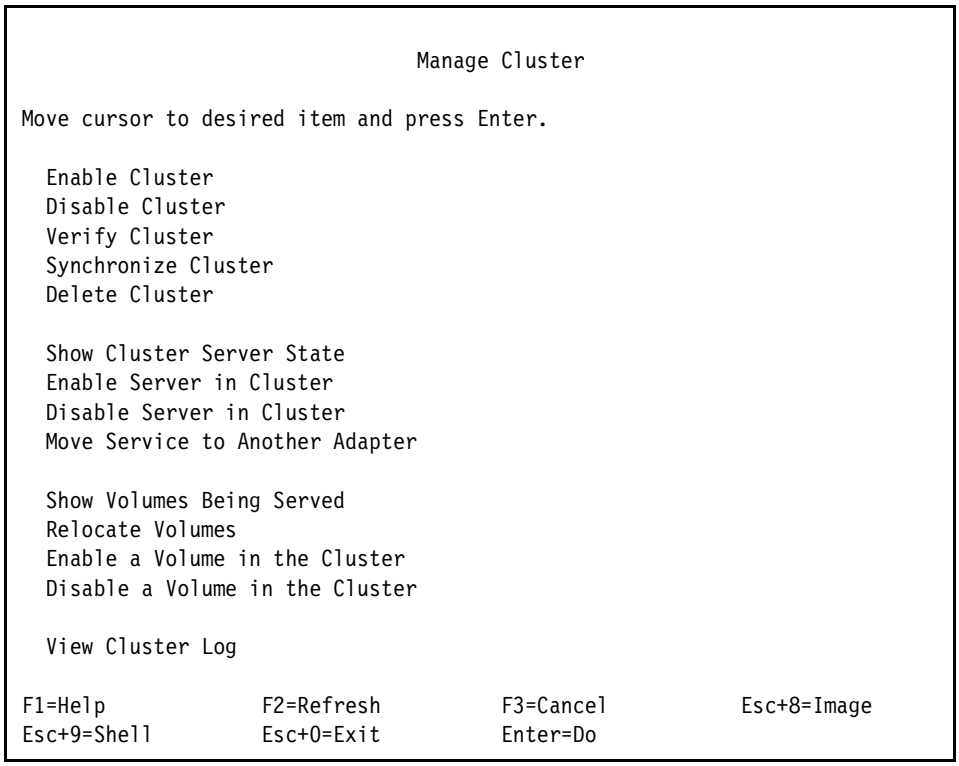


Figure 9-22 The Manage Cluster SMIT menu

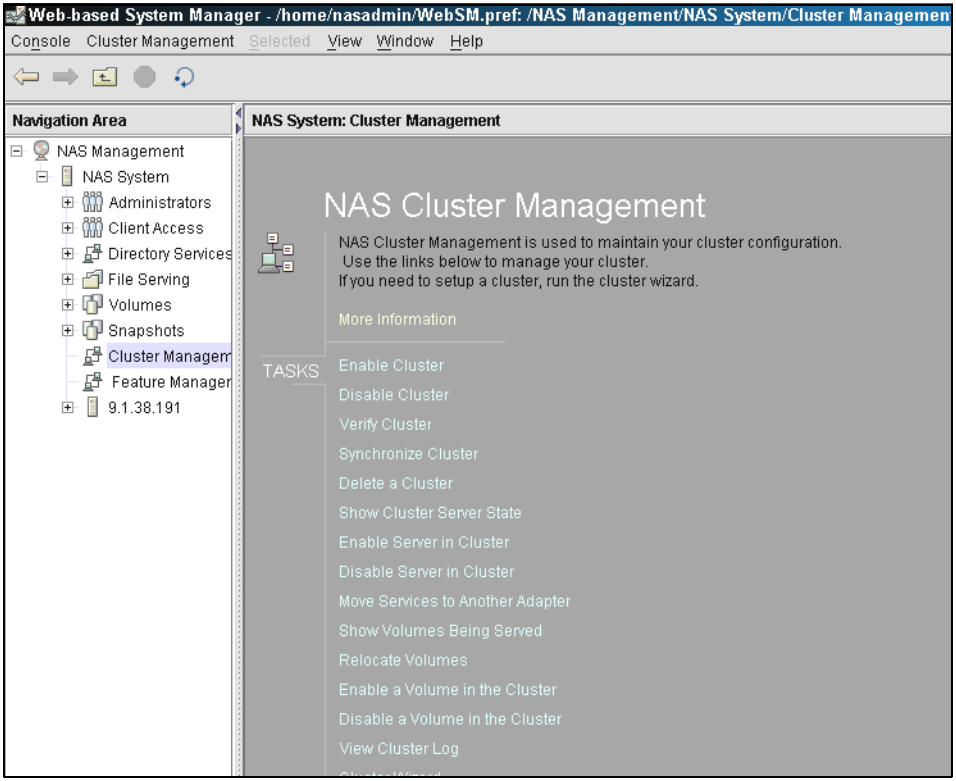


Figure 9-23 The cluster management screen in WebSM

10

Windows systems integration

In this chapter we describe how to integrate the NAS Gateway 500 into the Windows environment. The NAS Gateway 500 will work with all types of Windows systems.

We discuss the following topics:

- CIFS concepts
- Authentication
- Creating a CIFS share
- User creation on the NAS Gateway 500
- Advanced CIFS features
- Connecting Windows 2000 and 2003
- Setting up startup scripts for Windows
- Disabling auto disconnect
- Publishing shares to Active Directory

10.1 CIFS concepts

There are two parts to granting a Windows user access to a CIFS share:

- Map the user to a NAS file access user. This allows the NAS Gateway 500 to handle file permissions and access rights.
- Authenticate the user to prove that the user is allowed access.

Windows users accessing CIFS shares on the NAS Gateway 500 must be mapped to a NAS file access user. If the Windows and NAS file access user names are identical, the user is mapped automatically. When the user names do not match, a NAS administrator must define a user mapping so that the NAS Gateway 500 can authenticate and handle the Windows user.

10.1.1 Authentication

To access shares on the CIFS server, a Windows user must be authenticated. The CIFS server can handle authentication in two ways, pass through and local. The authentication method is selected during initial configuration in the CIFS wizard.

Pass through authentication is commonly used in Microsoft Active Directory or Windows NT Domain environments. The authentication request is passed off to an Active Directory Server (ADS) or Primary/Backup Domain Controller (PDC/BDC), which checks the password.

Local authentication is used if an ADS or PDC/BDC is not available. All password authentication is handled by the NAS Gateway 500. Passwords may be encrypted or plain text:

- Plain text passwords are insecure, but require little administrative overhead. CIFS requests are authenticated against the standard system user registry. The password is compared against the associated NAS file access user's password.
- Encrypted passwords are more secure, but require the NAS administrator to define a CIFS user for each NAS file access user account that is used to access CIFS files. The CIFS user essentially stores an encrypted CIFS password for a NAS file access user.

10.2 Creating a CIFS share

Under **NAS Management**, select **File Serving —> Overview and Task** and click the **CIFS wizard**. The CIFS wizard configures the NAS Gateway 500 to provide CIFS file sharing services to your Windows-based clients. This wizard configures the CIFS server name and workgroup, specifies WINS (optional), and configures CIFS share users, as shown in Figure 10-1.

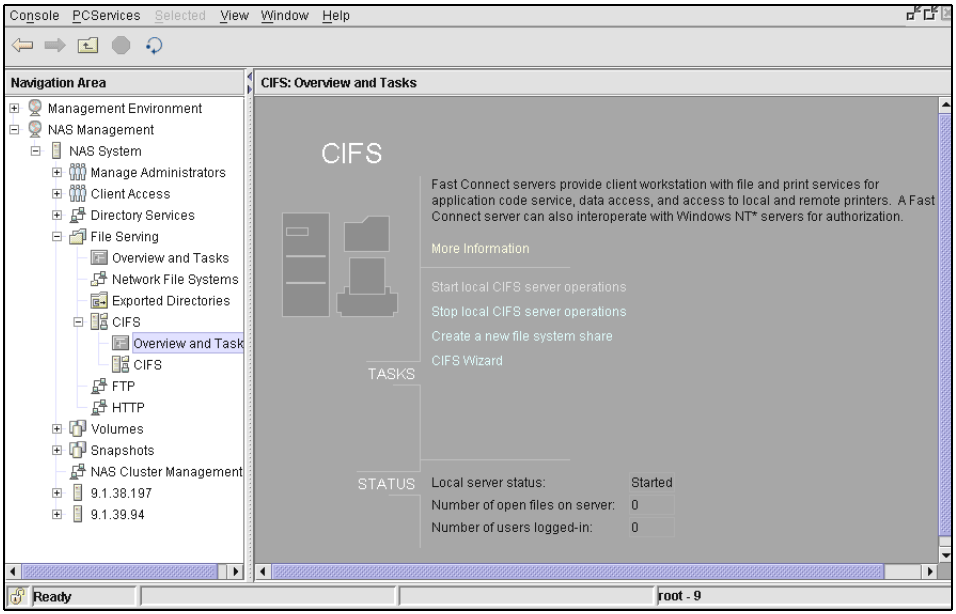


Figure 10-1 CIFS overview and tasks

The Welcome to the CIFS Setup wizard screen will be launched. The wizard will guide you to set up the NAS Gateway 500. Select **Next** as shown in Figure 10-2.

Figure 10-2 Welcome to the CIFS wizard

Now start configuring the CIFS server by typing in the name that will be used for the Windows clients to connect to. This name will appear in the network places. Type in the server description, which will be displayed as the description in network places. Type in the Domain or workgroup where the server will be found in network places and select **Next** as shown in Figure 10-3.

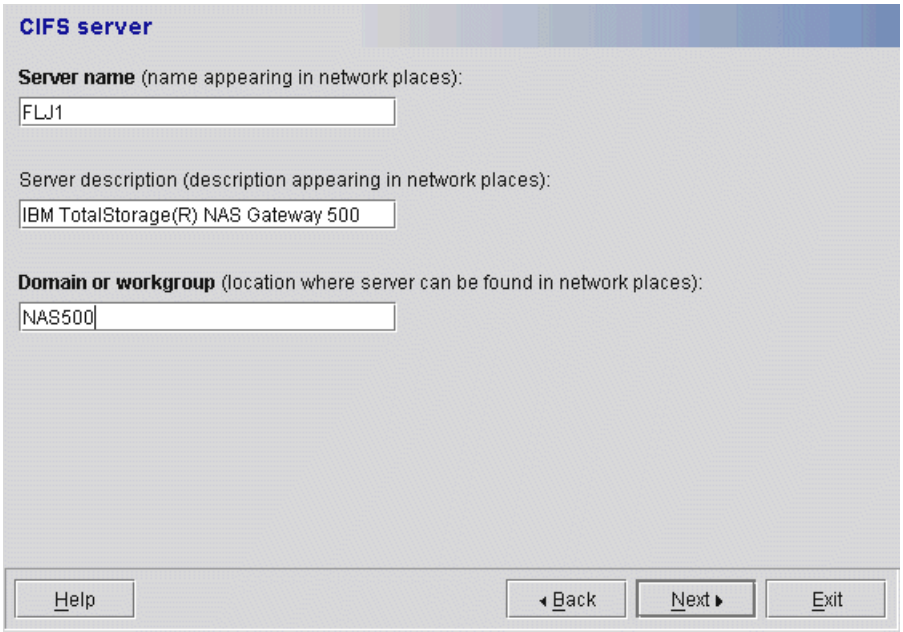


Figure 10-3 CIFS network configuration

The Windows Internet Name Service (WINS) is an advanced NetBIOS name server. It is used to map IP addresses to more human-readable hostnames. The CIFS Setup wizard allows you to specify WINS servers by entering the IP addresses of the servers into the fields provided:

- If you do not want to use WINS, leave the fields blank and click **Next**.
- If you want to use WINS, enter the server IP addresses and select **Next** as shown in Figure 10-4.

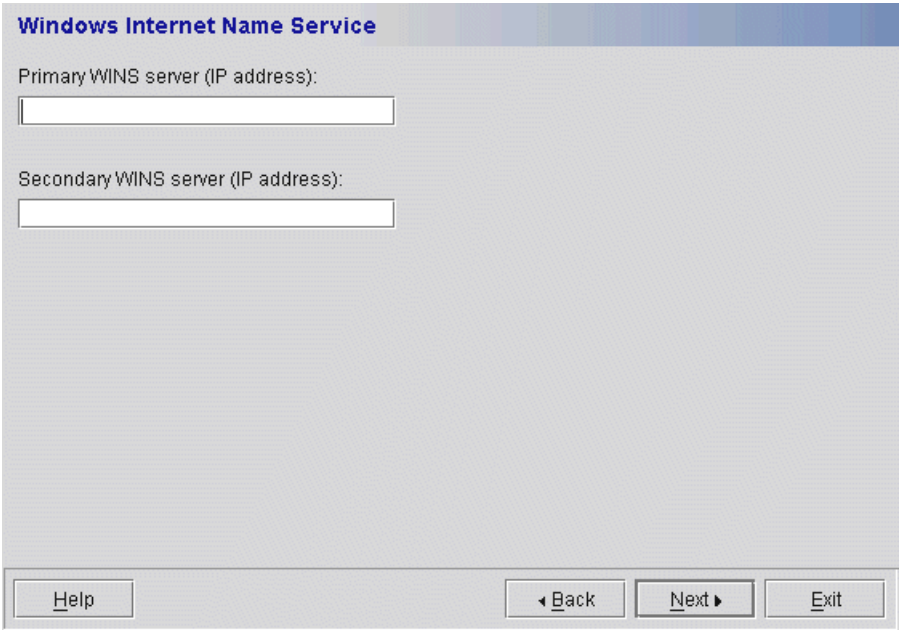


Figure 10-4 Windows Internet Name Service panel

The CIFS authentication panel is used to specify how you want the NAS Gateway 500 to authenticate Windows users that have access to defined shares. Windows users can be authenticated in two ways:

1. Through an Active Directory or NT4 Domain. This means that when a user enters their username and password into a Windows computer, they are passed-through to a domain controller, which authenticates the user.
2. Locally on each machine. This means each machine keeps track of the users that log into it. When a person types their username and password, it is verified on the machine on which it was entered.

Password encryption can be handled in three ways:

1. No Encryption: Only plain text passwords are accepted.
2. Only Encryption: Only encrypted passwords are accepted.
3. Negotiate Encryption: Clients can negotiate either plain text or encrypted passwords.

Use the pull-down list to specify the desired encryption. Select **Next** after the options are selected, as shown in Figure 10-5.

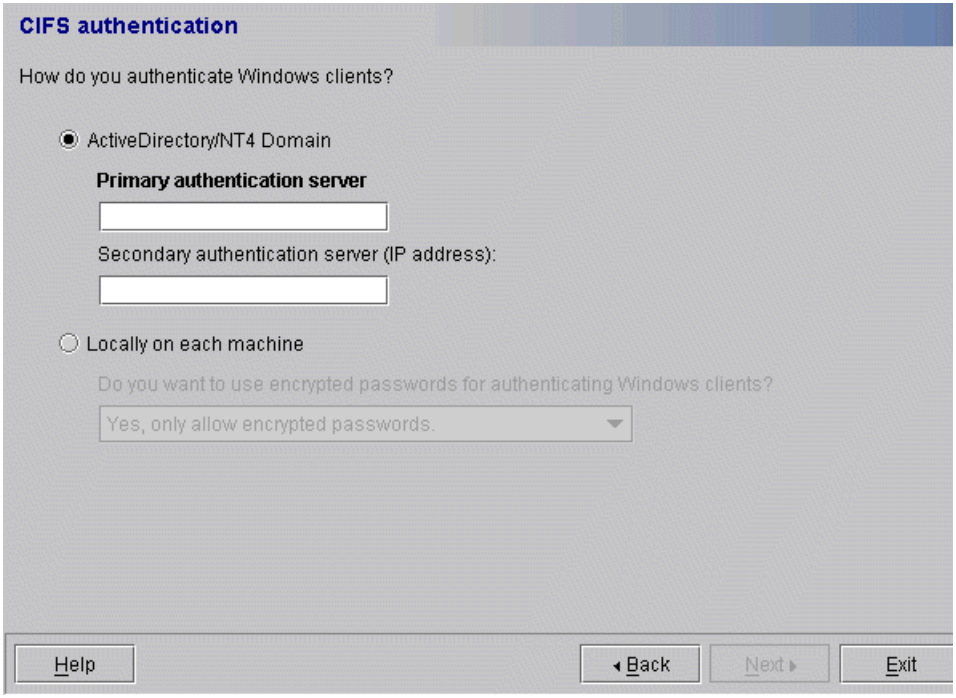


Figure 10-5 CIFS authentication

The Local users option window will be displayed if the Active Directory or Windows NT4 option is selected. Choose between dynamic user creation or local user creation, and click **Next** as shown in Figure 10-6.

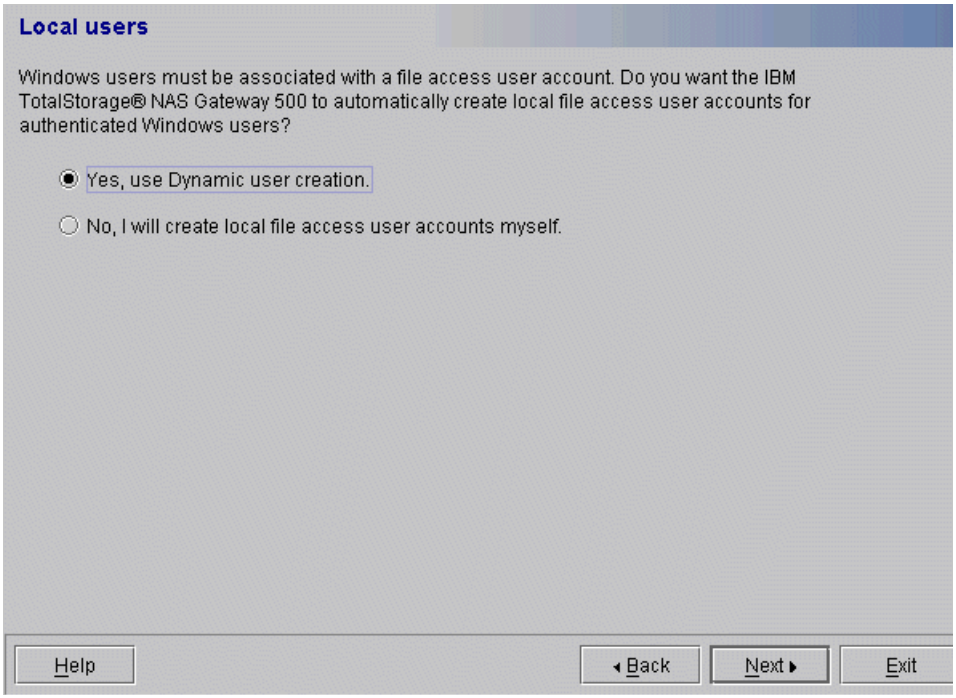


Figure 10-6 Local user selection

The Confirmation window of the CIFS configuration settings will appear where the selected settings can be verified; click **Next** as shown in Figure 10-7.

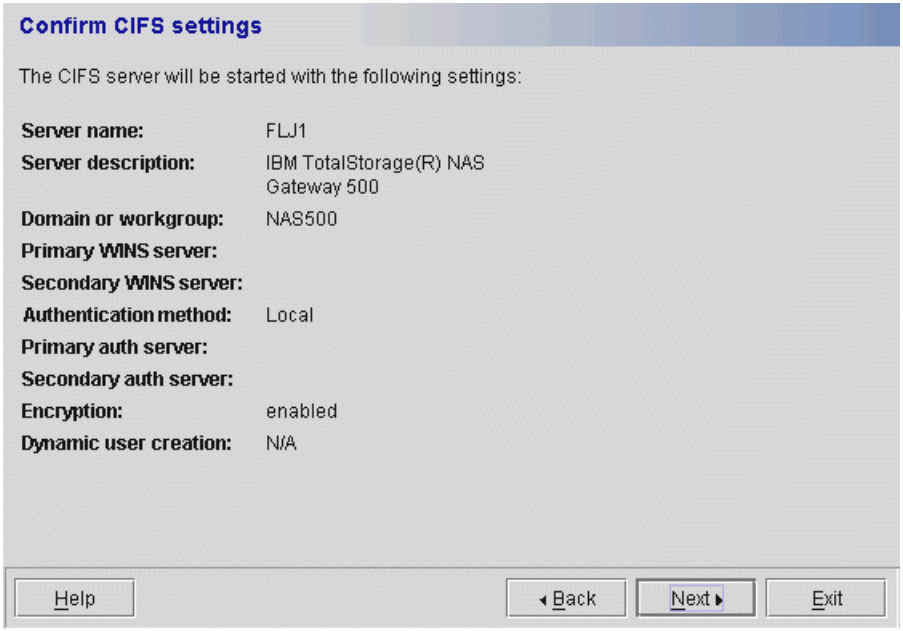


Figure 10-7 CIFS confirmation

10.3 User creation on the NAS Gateway 500

This section describes how to create and manage users on the NAS Gateway 500.

10.3.1 User creation

The CIFS server can be started and stopped from the Overview and Task option under CIFS. Start the CIFS server if it is not started by right-clicking **CIFS Server** and selecting **Start Server Operations**. Right-click the file share and select **User Administration**, as shown in Figure 10-8.

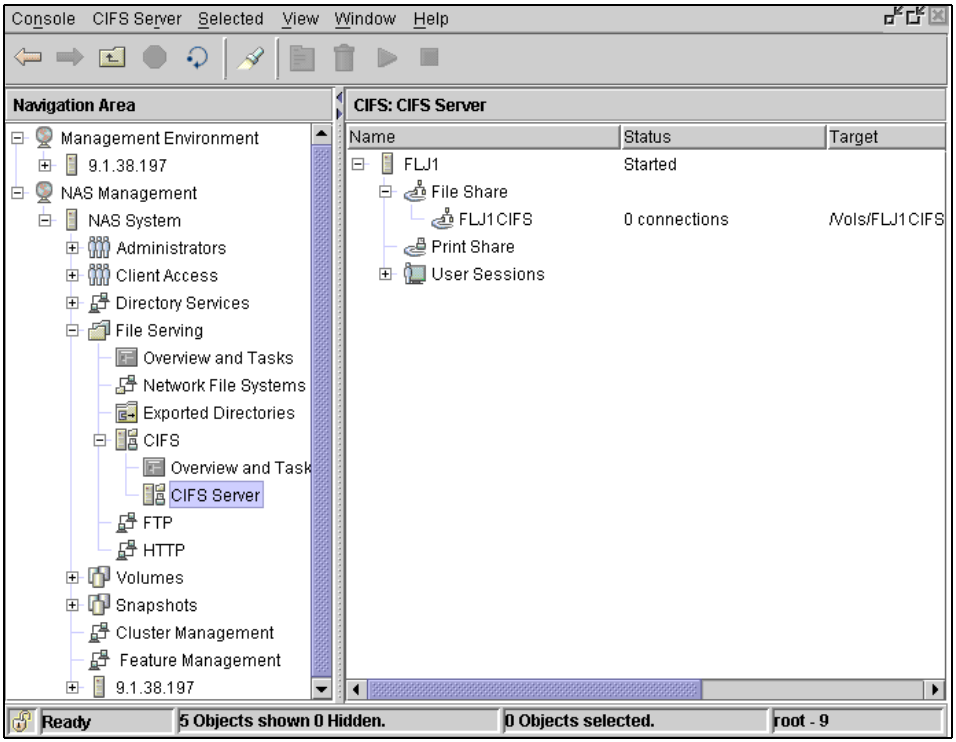


Figure 10-8 CIFS file and print share

Add a user by selecting **Create User**, as shown in Figure 10-9.

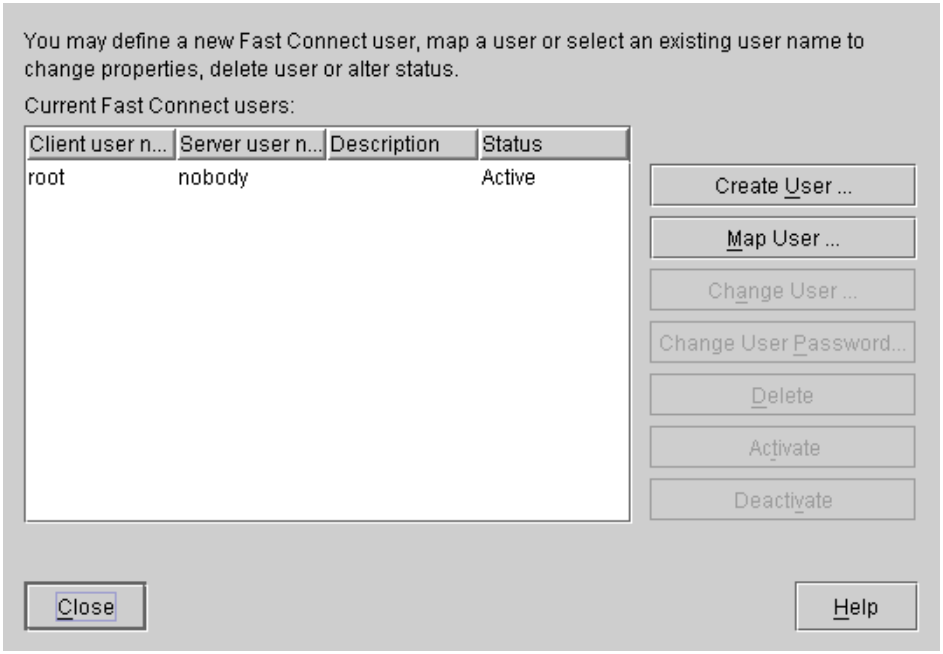


Figure 10-9 User administration

From the drop-down list, select the user that will have access to the CIFS server; this user must have been created in the **Client Access** panel in order to be added. Type in and confirm the user password. Select **OK**, as shown in Figure 10-10.

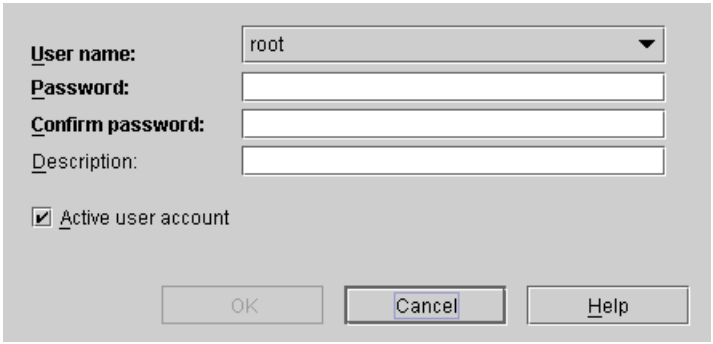


Figure 10-10 User creation

The success screen will be displayed when a user is created successfully. Select **Close**, as shown in Figure 10-11.

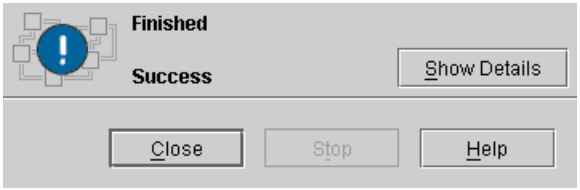


Figure 10-11 Successful user creation

The user administration window will be updated with the newly created user.

Select **Close** as shown in Figure 10-12.

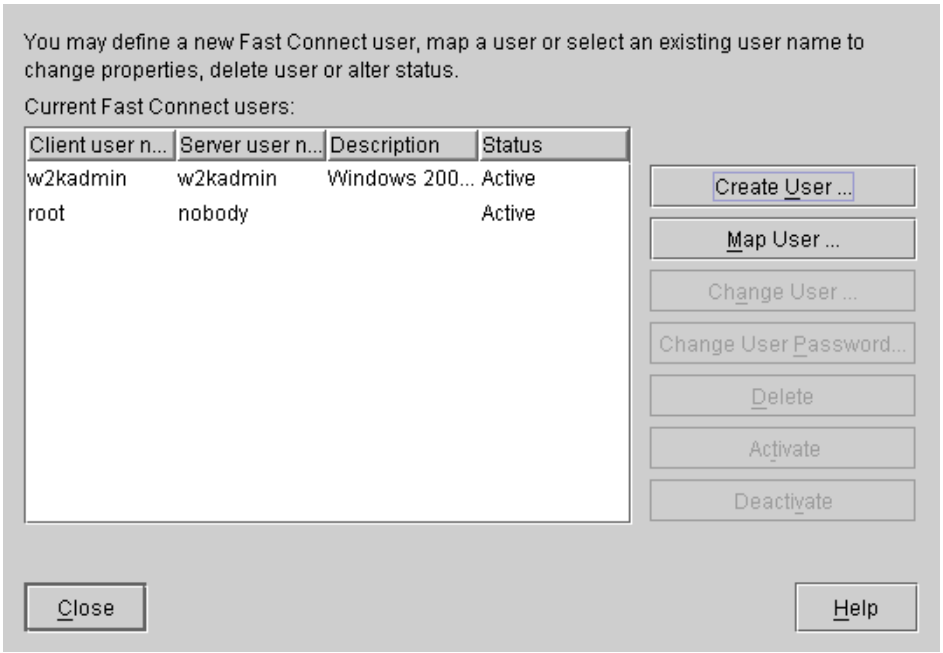


Figure 10-12 User Administration

10.3.2 Dynamic user creation

This feature allows the CIFS server to automatically create and map local users and groups for authenticated Windows users and groups. This allows Windows users seamless access to CIFS file shares on the NAS Gateway 500 without having a file access user account.

Note: NT Passthrough Authentication must be enabled to use this feature.

Dynamic user creation is most useful in an environment where Windows users and UNIX users do not share files, or in a solely Windows-based network. Complications may result in environments where UNIX and Windows users both log on. Keep the following considerations in mind when maintaining an environment that includes both Windows and UNIX users:

- If a UNIX user account with the same name as a Windows user account already exists on the CIFS server, then the Windows user will be mapped to the existing UNIX user (instead of creating the name userXYZ). In this case, the group information for the UNIX user is modified when synchronization with the passthrough authentication server occurs.
- If a Windows user (for example, nasuser) has successfully logged into the CIFS server and is mapped to the CIFS user usrXYZ, it is possible that a UNIX user named nasuser could later be added manually. This could cause confusion because the Windows user nasuser would be mapped to usrXYZ.

Dynamic user creation is disabled by default:

- To enable dynamic user creation: net config /dynuser:1
- To disable dynamic user creation: net config /dynuser:0
- To change the user prefix: net config /dynuser_prefix: xxx
- To change the group prefix: net config /dyngroup_prefix: xxx

Note: Users created by this feature are always created in the local user registry. Therefore, when using a directory service (such as NIS, NIS+ or LDAP) for management of your UNIX users, disabling this feature is strongly recommended.

10.4 Creating file system shares

Under **NAS Management**, select **File Serving —> CIFS,** right-click **file sharing**, select **New File system share**. This will launch the new file system share window, as shown in Figure 10-13.

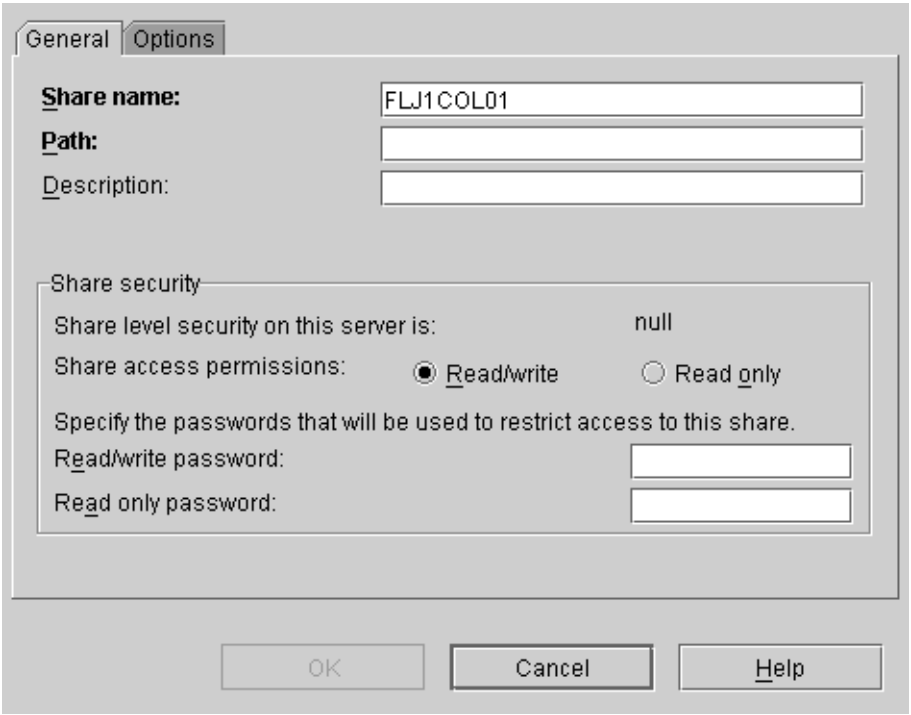


Figure 10-13 New file system share with permissions

Type in the share name that will be shown to the Windows users in the CIFS server that was created. Type in the destination path of the source volume, this is case sensitive. Type in the description and the read / write password.

The volume information can be shown by going to **NAS Management —> Volumes —> All Volumes.** Right-click the selected volume and select **Properties**, as shown in Figure 10-14.

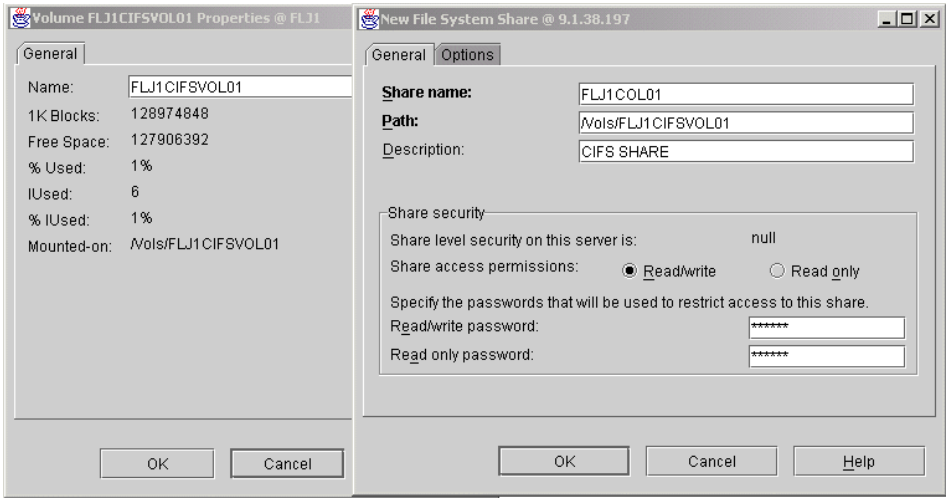


Figure 10-14 Volume and File system information

Select **OK**, as shown in Figure 10-15.

Figure 10-15 File system share information

Select **Close** as shown in Figure 10-16.

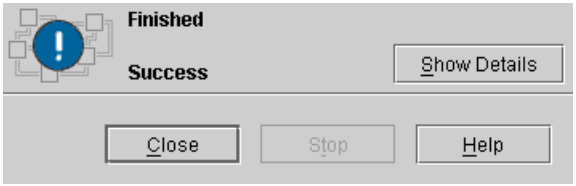


Figure 10-16 Successful creation

The NAS Gateway 500 CIFS server is ready for use by Windows based clients.

10.5 Advanced CIFS features

In this section we give a brief overview of advanced features available with the CIFS Server function.

From **NAS Management —> NAS System —> File Serving —> CIFS —> CIFS Server** in the Web based management tool, right-click the CIFS server and select **Properties** as shown in Figure 10-17 and Figure 10-18.

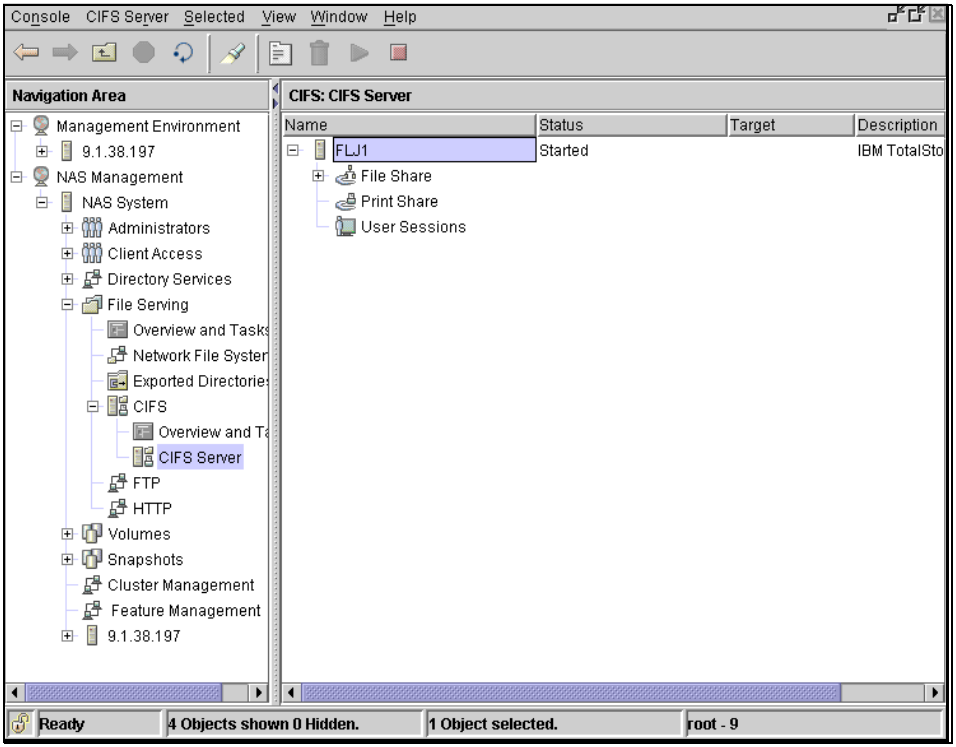


Figure 10-17 CIFS Server

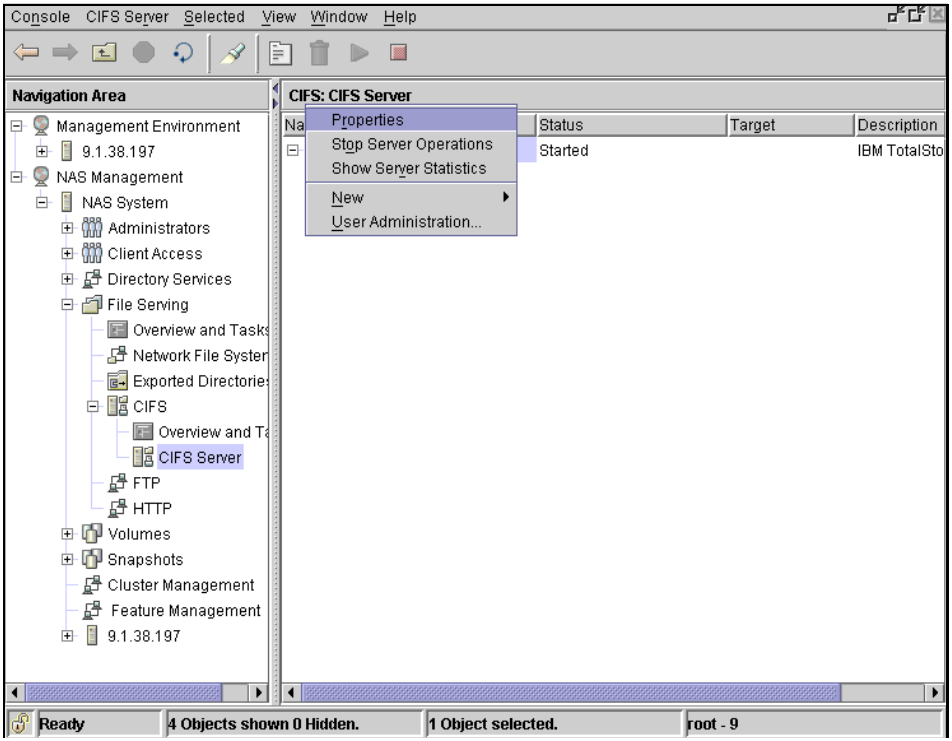


Figure 10-18 CIFS Server properties

The Fast Connect CIFS server properties window will be opened as shown in Figure 10-19. When the Basic setup tab is selected, the following settings are available for change:

- Server name
- Domain name
- Description
- WINS address:
  - Server acts as proxy WINS server
  - Server acts as NetBIOS name server
  - Enable NetBIOS datagram service
  - Enable Master Browser support

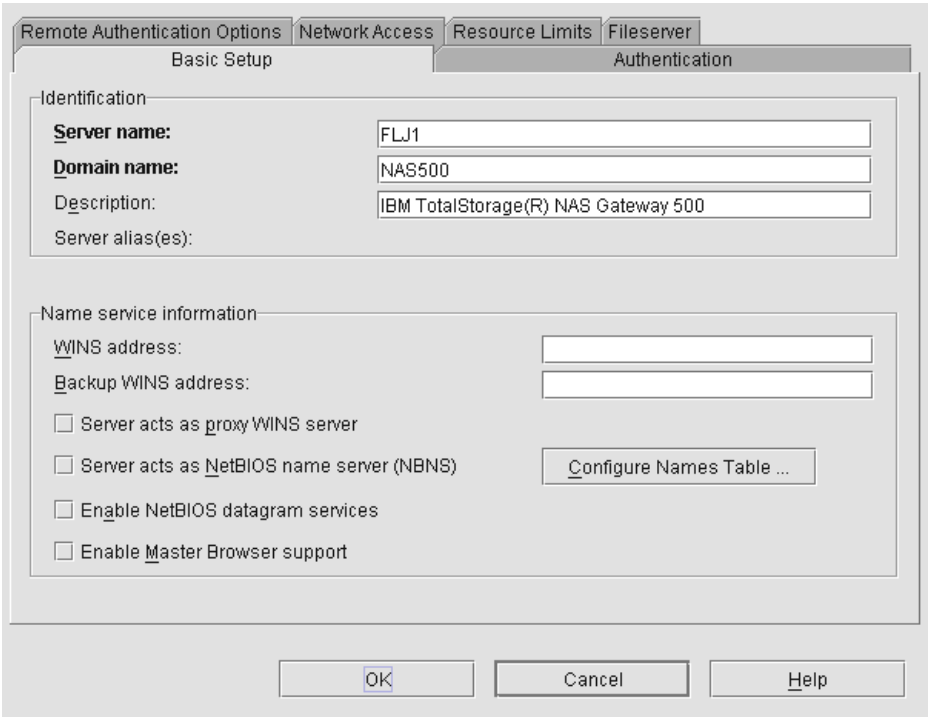


Figure 10-19 Fast Connect CIFS server properties

By clicking the **Remote Authentication Options** tab as shown in Figure 10-20, the following settings are available for change:

- Allow DCE/DFS™ access:
  - Passthrough authentication server address
- Enable Kerberos 5 authentication:
  - Kerberos server name
- Enable LDAP based authentication:
  - Server name
  - User context (DN)
  - Administrator account
  - Keytab file

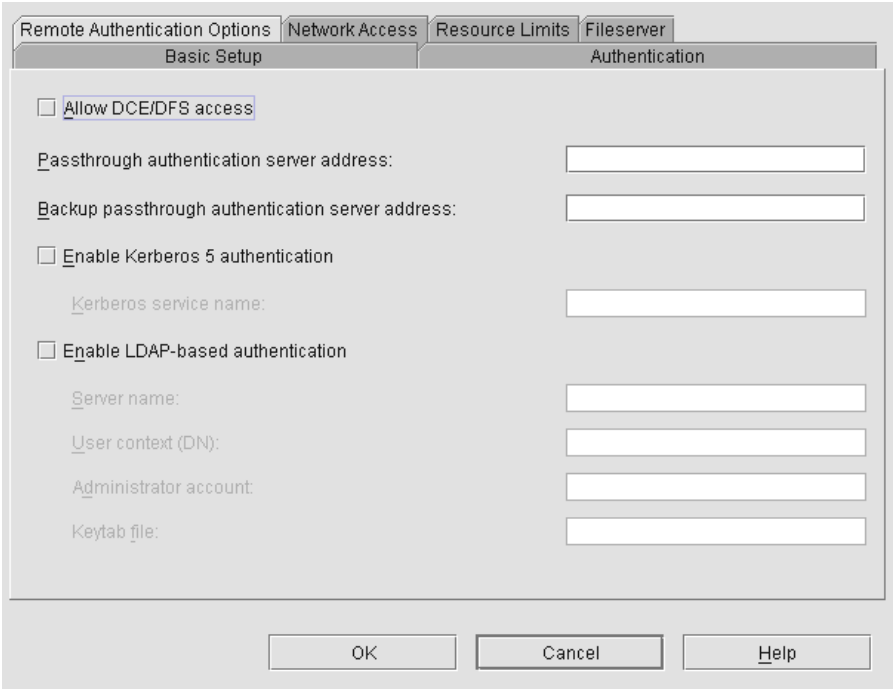


Figure 10-20 Remote authentication options

By clicking the **Network Access** tab as shown in Figure 10-21, the following settings are available for change:

- Enable Network Logon server for cliet PCs:
  - Profile path type
  - Profile path
  - Network logon path
  - Client startup script file name
  - Allow remote password change
  - Synchronize AIX passwords

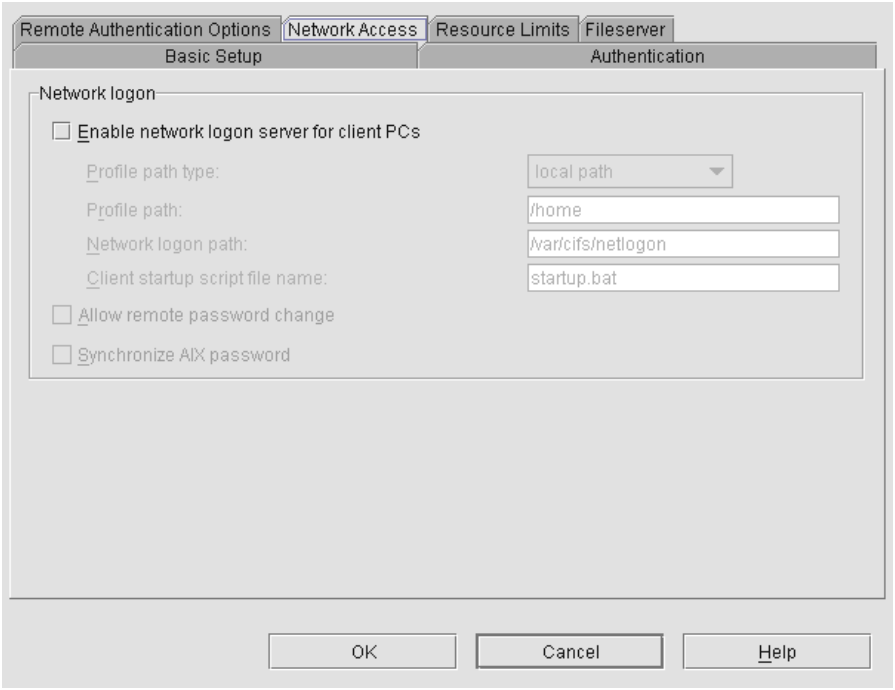


Figure 10-21 Network access options

By clicking the **Resource Limits** tab as shown in Figure 10-22, the following settings are available for change:

- Time-out for inactive, unused session
- Maximum number of:
  - Users allowed to be logged on
  - Connections allowed to server resources
  - Open files on the server
  - Directory searches on the server
  - Shares

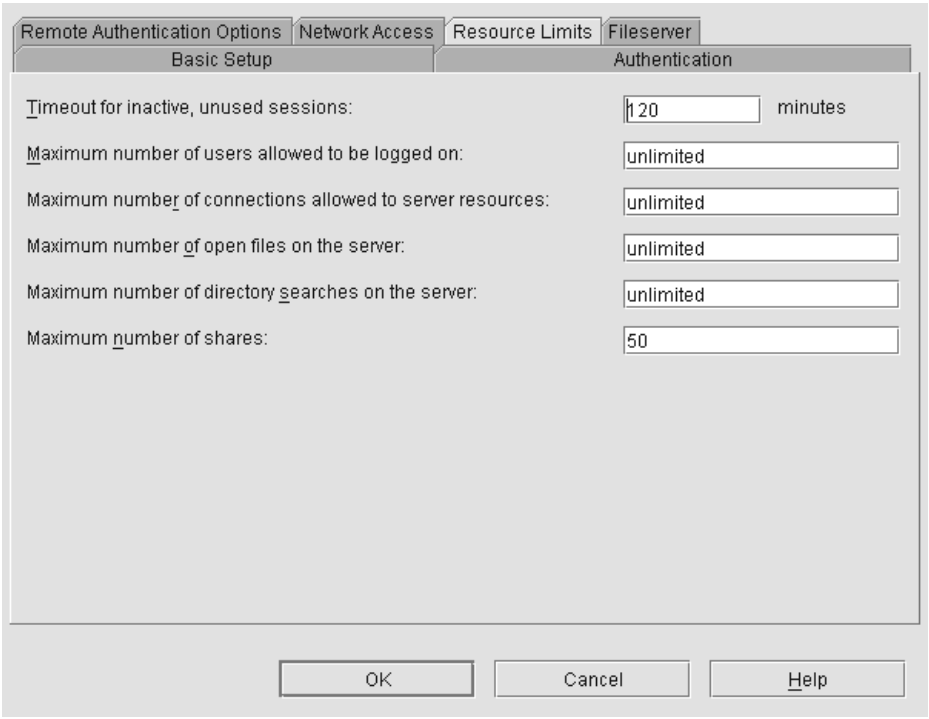


Figure 10-22 Resource limits

By clicking the **Fileserver** tab as shown in Figure 10-23, the following settings are available for change:

- Enable opportunistic locking
- Enable search caching
- Enable send file API support
- Umask:
  - Preserve ACL inheritance
  - JFS ACL inheritance
  - DOS file attributes support
  - Map long filenames to DOS 8.3 filenames
- Mapping character:
  - Enable memory mapped files
- Double byte character mapping:
  - Enable MSDFS support
  - MSDFS load levelling

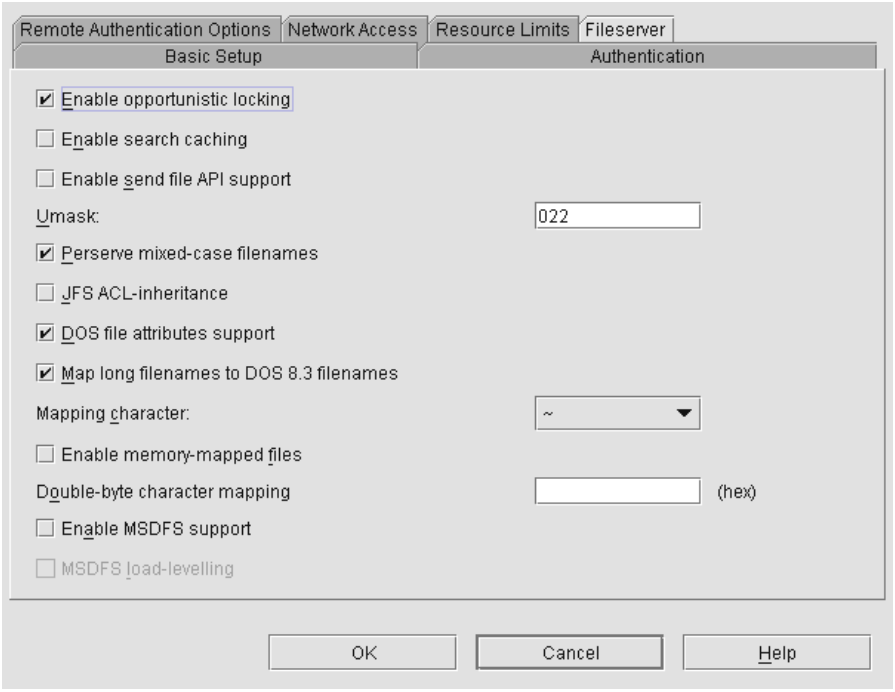


Figure 10-23 File server

After all the required changes are made, select **OK** to finish and save the settings. See the NAS Gateway 500 product documentation for details about these settings.

10.6 Connecting Windows 2000 and 2003

In this section we will describe how to set up a connection from a Windows 2000/2003 platform.

Connecting a Windows 2003 system

You may have compatibility problems when integrating NAS Gateway 500 with Windows 2003 server systems.

With default settings, a Windows 2003 server system uses NTLM v2 messages only for CIFS shares access. A NAS Gateway 500 system uses NTLM v1 messages only to handle CIFS requests from clients. So they cannot talk to each other for a successful CIFS session.

The symptom of this compatibility problem is that you always get an incorrect password error on Windows 2003 when accessing CIFS shares on NAS Gateway 500.

You must change the security settings on Windows 2003 to make it work with NAS Gateway 500. Here is an example of how to locate and change the setting related to NAS Gateway 500 integration.

Important: The purpose of the following steps is to tell you how to locate and change the NTLM settings on Windows 2003. Other settings may also be changed with the same set of tools. If you do not check all settings carefully as suggested, some unexpected changes may be made on your system. You should verify the security settings with your security needs before applying them to your computer.

First, click **Start**, click **Run**, type **mmc** (Microsoft Management Console), then click **OK**.

An MMC console window will appear. Select **Add/Remove Snap-in** from the menu, as shown in Figure 10-24.

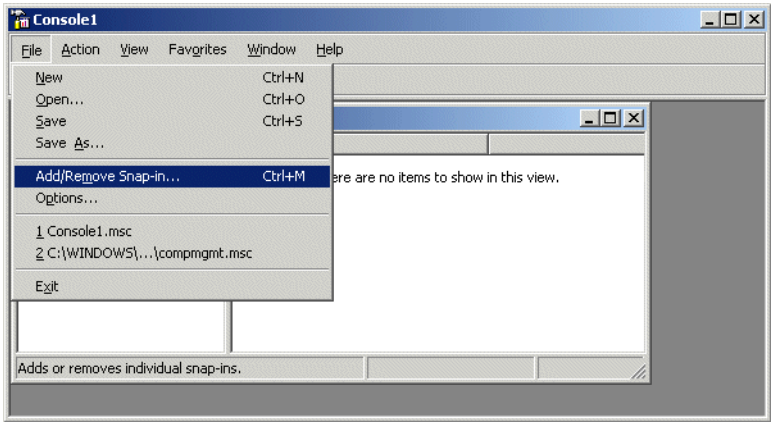


Figure 10-24 The Add/Remove Snap-in menu

Click **Add** on the following screen, as shown in Figure 10-25.

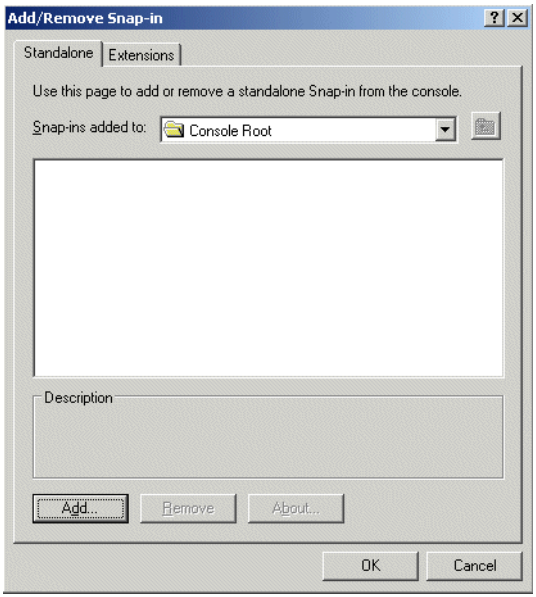


Figure 10-25 Add a Snap-in

Select **Security Configuration and Analysis** on the following screen and click **Add**. Click **Close** then **OK** to return to the main MMC window, as shown in Figure 10-26.

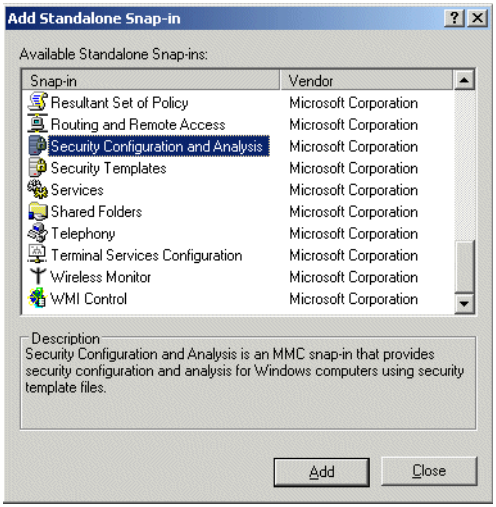


Figure 10-26 Select the Security Configuration and Analysis Snap-in

Select **Open Database** from the menu, as shown in Figure 10-27.

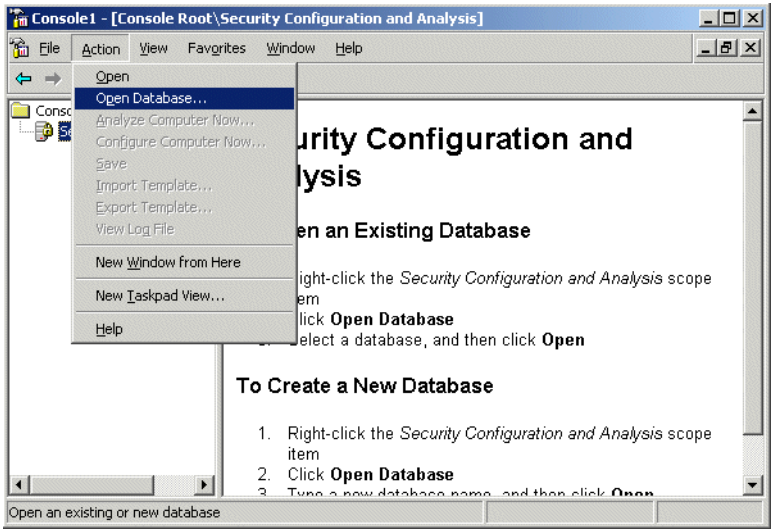


Figure 10-27 Select Open Database from the menu

Type in a name for the database, as shown in Figure 10-28.

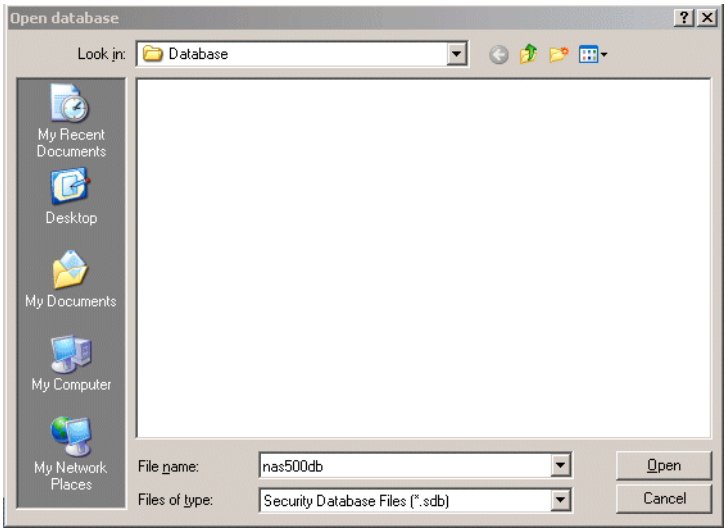


Figure 10-28 Naming the database

Select **setup security.inf** in the Import Template window, as shown in Figure 10-29. This is the security template created by Windows 2003 setup.

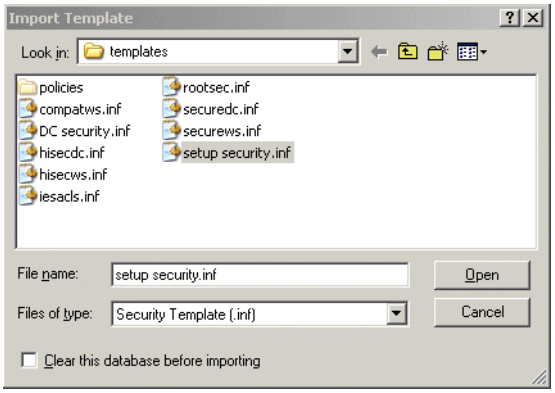


Figure 10-29 Select template to import

Select **Analyze Computer Now** from the menu, as shown in Figure 10-30. Wait until the action is completed.

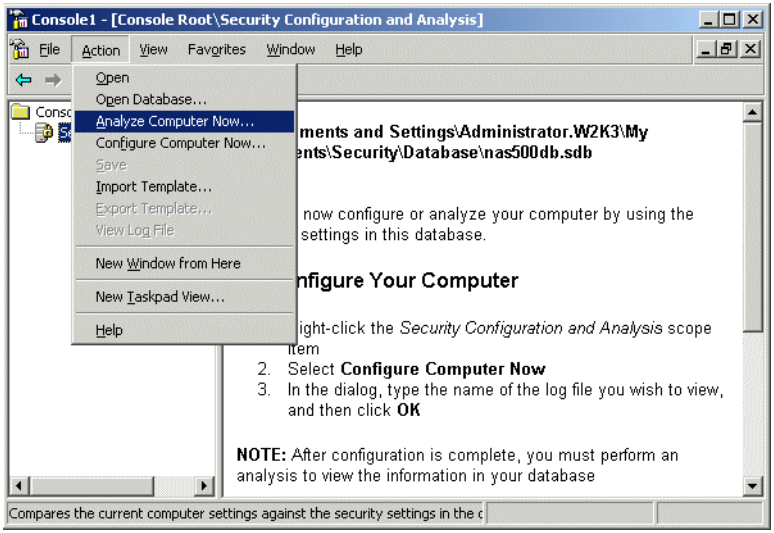


Figure 10-30 Analyze computer

Navigate to **Local Policies** -> **Security Options**, find the network security option about the LAN manager, as shown in Figure 10-31.

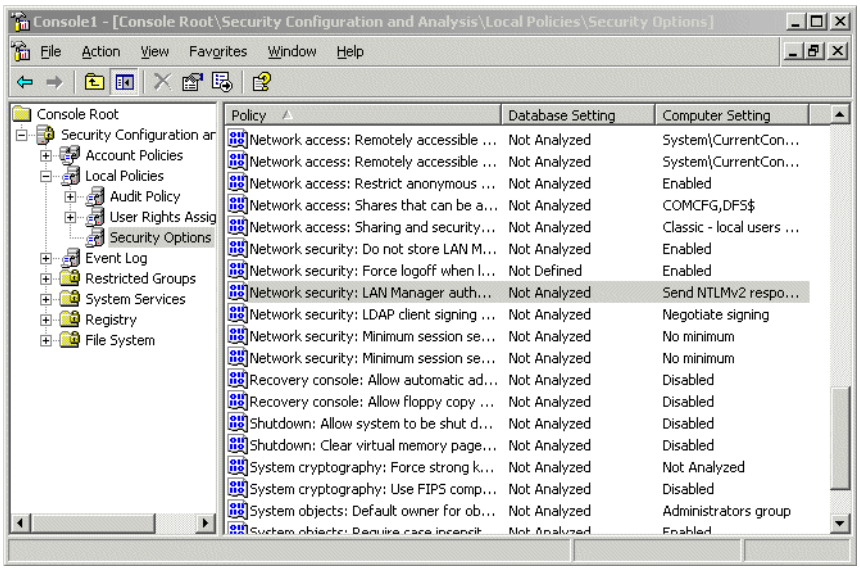


Figure 10-31 Find LAN manager security settings

Change the setting in the database to **Send LM&NTLM responses**. Click **OK**, as shown in Figure 10-32.

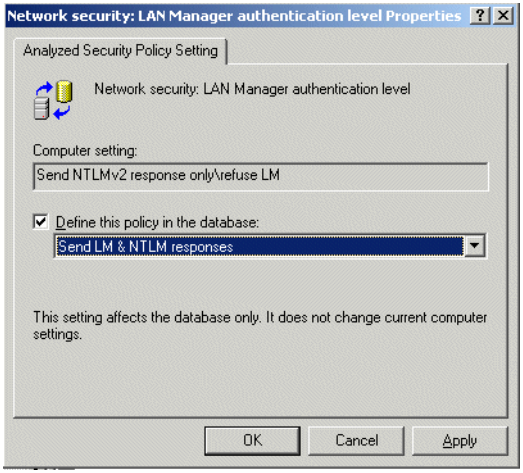


Figure 10-32 Change the LAN Manager settings

Important: Now you should expand all nodes on the left pane, and click each node on the left pane. Look at the right pane as you click nodes in the left pane. For every entry marked with a red X and exclamation mark on the right pane, you should check the setting of that entry and make sure the setting in the database is what you want.

Select **Configure Computer Now** from the menu, as shown in Figure 10-33. This will apply the settings in database to your computer.

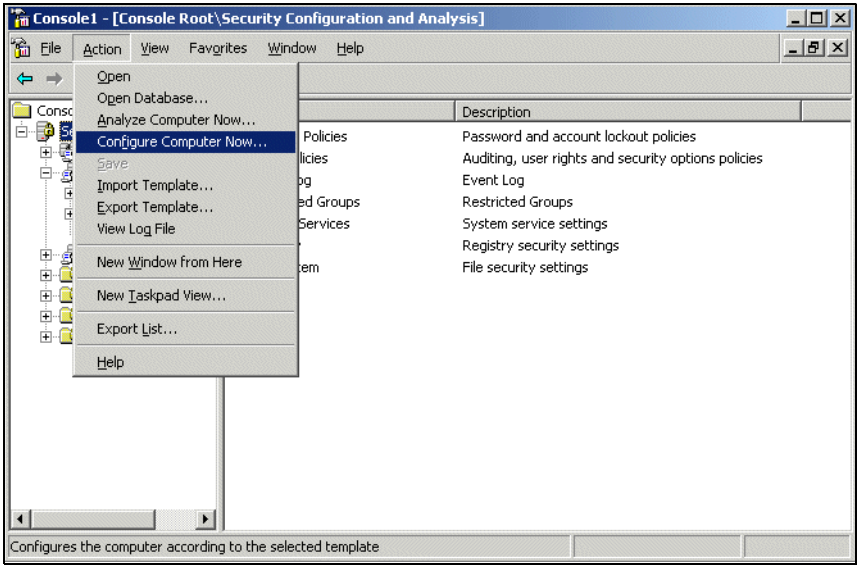


Figure 10-33 Save settings to computer

Log off and logon again. Now the Windows 2003 system is compatible with the NAS Gateway 500 gateway.

10.6.1 Connecting and mapping a Windows client

Browse to the NAS Gateway 500 CIFS server by using the Windows network browser. Select the required NAS Gateway 500 CIFS server, as shown in Figure 10-34.

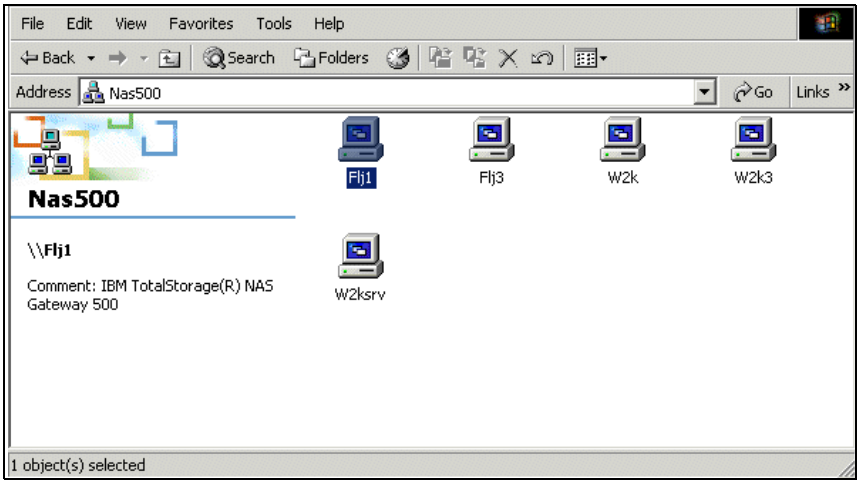


Figure 10-34 Network browser

Double-click the NAS Gateway 500 CIFS server. If the user is logged on as a user that was created in the NAS Gateway 500 administrator / user account for the NAS Gateway 500 CIFS server, the CIFS server will be opened. If the user is not logged on as a known user, the **`logon as`** window will appear if browsing with a Windows 2000/2003 system, as shown in Figure 10-35 and Figure 10-36.

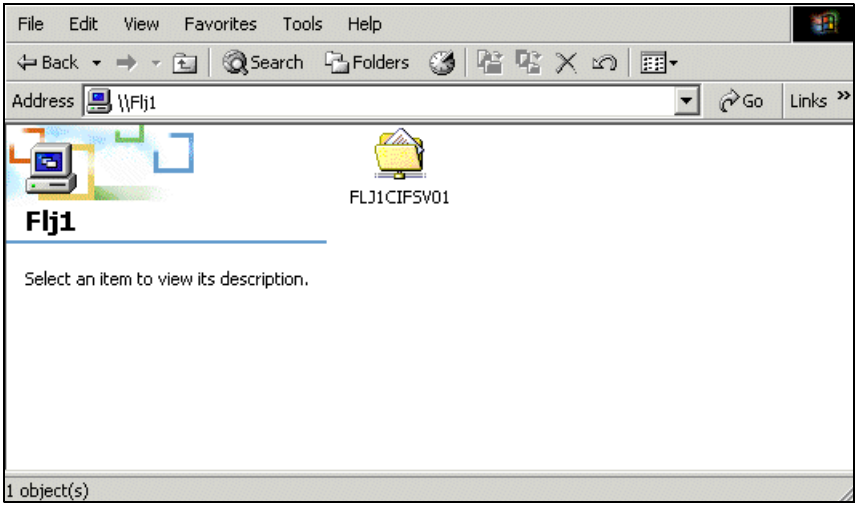


Figure 10-35 CIFS server file share

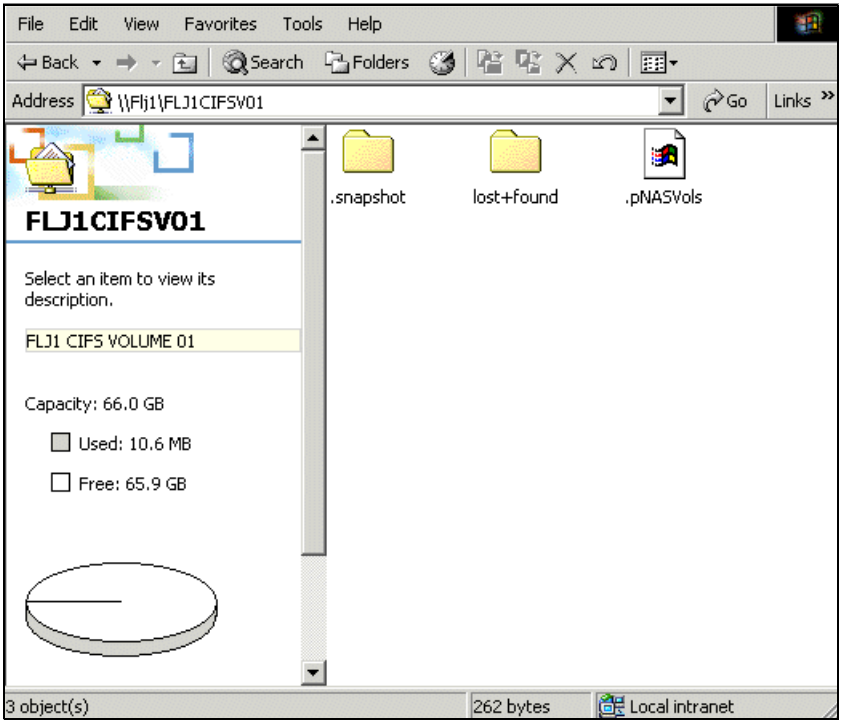


Figure 10-36 CIFS server shared file

A Windows base client can now browse or map the shared file.

10.7 Setting up startup scripts for Windows

A common issue with the Windows client is that certain automatic services, such as those associated with popular database programs or the LanmanServer service, can start before the network drives are available. If these services depend on being able to access files on the network drive, and the drive is not available when these services start, then the services generate errors, and manual user intervention is required.

The solution for this is to use a Microsoft tool called AutoExNT, that is provided in the Windows 2000 resource kit. The following files should be loaded into the C:\WINNT\SYSTEM32 directory for Windows 2000, or the C:\Windows\system32 directory for Windows 2003:

- autoexnt.bat
- instexnt.exe
- autoexnt.exe
- Sleep.exe
- Servmess.dll

AutoExNT is a service which starts automatically each time the machine starts. As a service, it can do anything that an administrator of the machine can do. It can start and stop services or applications. It will work on both Windows NT and Windows 2000.

Note: Microsoft does not support the tools from the Resource Kit. They are provided on an “as-is” basis.

The LanmanServer service is responsible for restoring network shares on your computer. It can happen that the share is not restored before the application specific services start. The solution is to use the AutoExNt service to start and stop the required LanmanServer service and restart the LanmanServer service, guaranteeing that any network disks will be restored. The following steps will assist in performing this.

Installing the AutoExNT service

To install the service, follow these steps:

1. Copy the files instexnt.exe, autoexnt.exe, Servmess.dll and sleep.exe to the system 32 directory

   From a command prompt, change to the system32 directory and type:

   ```
   instexnt.exe install / interactive
   ```

Note: The interactive switch will make the autoexnt.bat run on a visible command line, and a user can interact and stop the autoexnt.bat from running.

2. Create a blank text file named AutoExNt.bat in the system32 directory. This file will tell the AutoExNt service what you want it to do.
3. From the ‘Services’ control panel window, select:

   Control Panel -> Administrative Tools -> Services

   Change the startup type setting from automatic to manual for the following services:

   – Server
   – Computer browser

Change the Startup type setting from automatic to manual for any application specific services that are affected. For information on affected services, refer to the event viewer.

4. Edit the AutoExNT.bat file that was created in step 2. Here is where you start and stop services manually, as needed, and in the order that you specify, as shown in Example 10-1 and Example 10-2.

The **net use** command can be used to restore a network drive connection. In this example we stop the **Server** and **Computer browser** services if the network drive is not present. This is to prevent the Windows unit from going online; user intervention is required to reconnect the network drive and start the services if the drive fails to connect. Stopping these services is not required.

Stopping the services will prevent the server from sharing files and browsing the network.

A shortcut can be placed on the desktop to the file autoexnt.bat if you want to run the autoexnt.bat file manually.

Note: We did not describe the authentication of user name and password in this section. It is the administrator's function to set the **logon as** function in the properties function of AutoExNT service. Alternatively, type the user name and password in the **net use** portion of the command line. A third option is to create a computer account on the destination address, as this service starts before the user logs on. Thus the logon information cannot be used to reconnect the mapped network drive in this situation. It is recommended that you log on to the system with the same account that was set in the **logon as** function or the user name and password that was set in the **net use** command!

Example 10-1 Single drive startup script

```
net start "server"
net start "computer browser"
sleep 5

NET USE g: \\computername\sharename

if exist g:\ goto netdrive_online

goto Drive_offline

:netdrive_online

net start "The required services 1"
net start "The required services 2"
```

```
Goto end

:Drive_offline

net stop “computer browser” /yes
net stop “server” /yes

:end
```

For checking multiple network drives, the script in Example 10-2 can be used.

Example 10-2 Dual drive startup scrip

```
net start “server”
net start “computer browser”
sleep 5

NET USE g: \\computername\sharename

if exist g:\ goto second_drive

goto Drive_offline

:second_drive

NET USE h: \\computername\sharename

if exist h:\ goto drive_online

goto Drive_offline

:drive_online

net start “The required services 1”
net start “The required services 2”

goto end

:Drive_offline

net stop “computer browser” /yes
net stop “server” /yes

:end
```

Note: The ‘sleep xx’ command above specifies a waiting period in seconds to do nothing, which ensures that the service has enough time to find and log into the target. It is also used between the net stop and net start, because sometimes the server service will crash if you stop it and then immediately restart it. The Browser service is also involved in this case, because it is dependent on the server service.

Tip: The drive does not have to be specified. A file on a specific drive can also be selected to prevent the services from starting in the case where a new drive was added and a wrong drive letter was allocated; add the file name to the command line:

if exist h:\file.txt goto....

This can be any file, even an executable or database file, because this part of the script just checks for the availability of the file, it does not open or launch the file.

5. Reboot the computer. If everything was set up correctly, the AutoExNt.bat file will be executed automatically by the Service Control Manager when the computer boots. There is no need to log into the computer for the AutoExNt.bat file to execute, because it runs as a system service.

10.8 Disabling auto disconnect

The auto disconnect feature disconnects a network drive after a time period of inactivity on the network drive. This is not a favorable environment to have a drive disconnect after a time period of inactivity if a data base or application server is running in the back ground.

Tip: For more information the article is available in the Microsoft Knowledge Base Article 138365.

The LAN Auto disconnect parameter is in the registry under the subtree:

HKEY_LOCAL_MACHINE under the subkey:
\System\CurrentControlSet\Services\LanmanServer\Parameters

Note that in the registry, you cannot disable the Auto disconnect parameter. This can only be done at a command line.

To set the parameter to not disconnect, type the following command on a command line:

```
net config server /autodisconnect:-1
```

Note: Setting the value to zero will disconnect the drive after a few seconds of inactivity!

The range is from -1 to 65535 minutes at the command line.

10.9 Publishing shares to Active Directory

You can publish CIFS shares on NAS Gateway 500 to Active Directory with the Active Directory management tools that are included in Windows. And there is also a command on NAS Gateway 500, which can add or remove all CIFS shares on NAS Gateway 500 in Active Directory. Here is the Command Reference description of the **cifsLdap** command:

Purpose:

Allows AIX Fast Connect to register and unregister its file share and print share names.

Syntax:

cifsLdap -h host -u adminDN {-a treeDN | -r treeDN | -f filename}

Description:

The cifsLdap command allows AIX Fast Connect to register and unregister its file share and print share names into the Windows 2000 active directory.

Flags:

-h host — Host name of the Windows 2000 Active Directory Server (ADS)

-u adminDN — Distinguished Name (DN) of ADS administrator account used for binding to the directory

-a treeDN — Adds all the current AIX Fast Connect shares to treeDN in the active directory

-r treeDN — Removes all the current AIX Fast Connect shares for treeDN in the active directory

-f filename — Sends filename to the Active Directory Server, where filename is an LDF-format data file containing LDAP commands for the Active Directory Server

In all cases, the user is prompted for the bindDN password associated with the adminDN account supplied on the command line, which must have the proper administrative access for the Active Directory Server given as -h host.

We also have examples here. We publish all CIFS shares on our NAS Gateway 500 to the test OU of the Active Directory of the domain nas500.local, as shown in Example 10-3.

Example 10-3 Publishing shares with the cifsLdap command

```
(/etc)-->cifsLdap -h 9.1.38.199 -u nas500.local/users/w2kadmin\
> -a ou=test,dc=nas500,dc=local
Enter bindDN password:
adding new entry cn=FLJ1CIFS,ou=test,dc=nas500,dc=local
```

Here we remove all published CIFS shares on our NAS Gateway 500 from the test OU of the Active Directory of the domain nas500.local, as shown in Example 10-4.

Example 10-4 Removing shares with the cifsLdap command

```
(/)-->cifsLdap -h 9.1.38.199 -u nas500.local/users/w2kadmin\
> -r ou=test,dc=nas500,dc=local
Enter bindDN password:
deleting entry cn=FLJ1CIFS,ou=test,dc=nas500,dc=local
delete complete
```

Note: The cifsLdap command in our example is typed in two lines, separated by "\". This is because the command line is too long to fit in our terminal window, and we want to show you the whole command. You don't have to type "\" when you use this command. You can enter the command in a whole line like this:

cifsLdap -h 9.1.38.199 -u USERNAME -a ou=OU,dc=DOMAIN,dc=DOMAIN

11

UNIX systems integration

In this chapter we describe how to integrate NAS Gateway 500 with UNIX systems, including AIX, Solaris, and HP-UX.

We discuss the following topics:

- Configuring NFS shares on the NAS Gateway 500
- Accessing the NAS Gateway 500 file service from:
  - AIX
  - HP-UX
  - Solaris

11.1 NFS protocol on NAS Gateway 500

NAS Gateway 500 supports the latest NFS protocol update, NFS Version 3. NAS Gateway 500 also provides an NFS Version 2 client and server and is therefore providing backward compatibility with existing install bases of NFS clients and servers. Negotiation will occur to check what is the highest version of NFS supported by both involved systems.

On the NFS transport layer, TCP and UDP are both supported in the NAS Gateway 500.

11.2 Configuring NFS shares on NAS Gateway 500

As soon as you have finished the initial configuration of NAS Gateway 500, you can start configuring NFS file shares for UNIX systems. In this section we discuss creating and modifying NFS shares with WebSM and SMIT interface.

11.2.1 Configuring NFS shares through WebSM

You can login as the NAS administrator user or root user to configure the NFS shares with WebSM.

There are two entries in the WebSM management interface of NAS Gateway 500 if you login as the root user, from where you can configure NFS shares. They are the standard NFS management tool for AIX and the NAS Gateway 500 specified NFS management tool. We highly recommend that you use the **File Serving** entry under the **NAS Management** section, as shown in Figure 11-1, because it is especially designed for NAS Gateway 500 and it is cluster aware in a clustered environment.

If you login as the NAS administrator user, only the entry under the **NAS management** section is available.

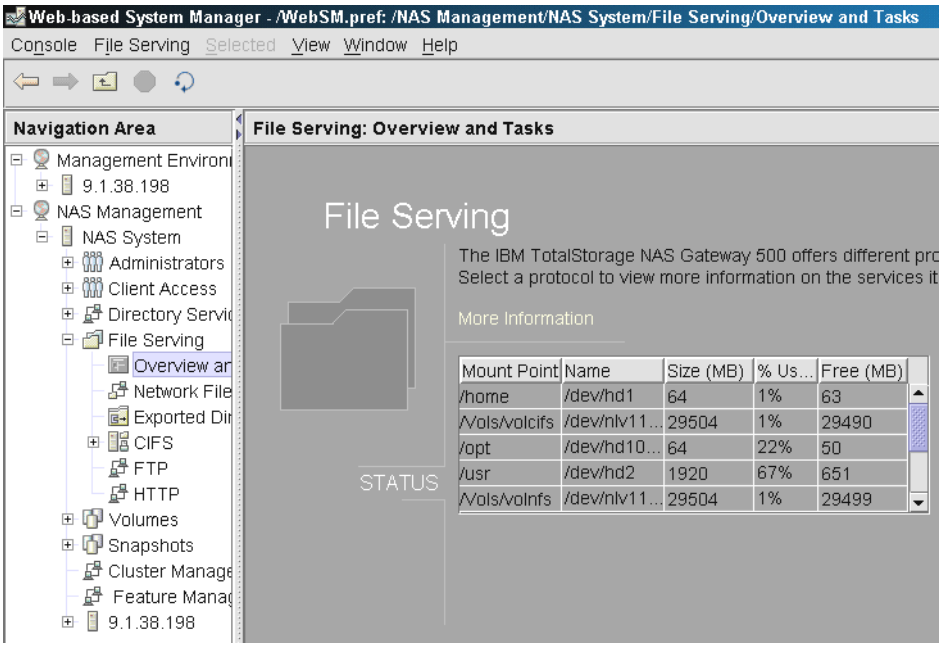


Figure 11-1 The File Serving section under NAS Management

Creating NFS shares via WebSM: single node configuration

Important: If you are running a NAS Gateway 500 cluster, always use the NAS volume creation tool to create NFS shares. Add a volume and mark the **Export the volume as an NFS share** check box.

Go to **NAS Management**->**NAS System**->**File Serving**, click **Exported Directories,** and then select **Directories** -> **New** -> **Export** from the menu, as shown in Figure 11-2. The screen as Figure 11-3 will pop up.

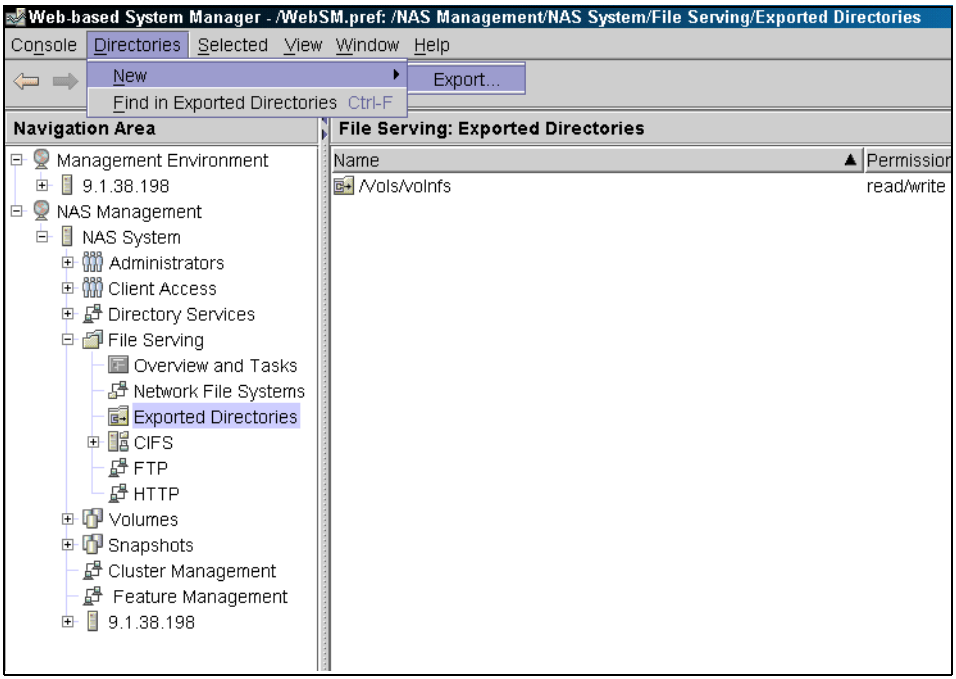


Figure 11-2 The Export menu

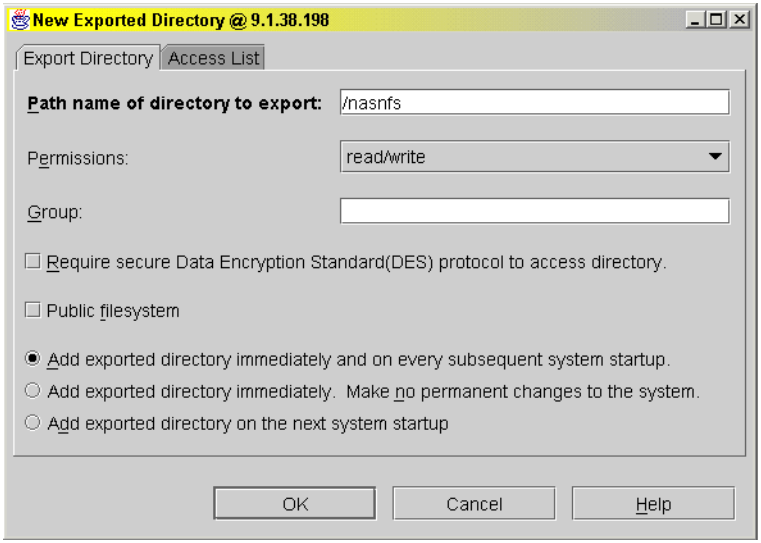


Figure 11-3 The NFS Export screen

Enter the directory you want to export in the Path name of directory to export field.

In the Permissions drop-down menu, you can define three kinds of permissions of the current NFS share:

- Read/write: Allow clients perform read and write operations on this share.
- Read only: Only allow read requests from clients.
- Read-mostly: Allow some clients perform read and write operations on this share, and allow read operations only to other clients.

Here we also have two more check boxes about DES encryption and public filesystem.

NFS server on NAS Gateway 500 support secure NFS sharing in a NIS or NIS+ environment, with the secure mode, in addition to the standard UNIX authentication system, the NFS server on NAS Gateway 500 provides a means to authenticate users and machines in networks on a message-by-message basis. This additional authentication system uses Data Encryption Standard (DES) encryption and public key cryptography. Secure NFS can improve security but requires the NIS or NIS+ environment and has some performance penalty on both server side and client side. The default setting is not to use secure NFS on shares.

The Public filesystem option is designed to work with WebNFS. WebNFS is a new protocol that allows client access to the NFS server through Web browsers. On supported Web browsers, you can access NFS shares on the NAS Gateway 500 with the URL:

```
nfs://www.nas500.YourCompany.com/nfsshare
```

If you choose one NFS share as the public filesystem, then any WebNFS URL referring to the root directory will be redirected to this share. For example, if we assign /nasnfs as the public filesystem, then the URL **nfs://nas500/** will gain access to /nasnfs directory on the server nas500.

WebNFS has not been widely supported on Web browsers until now. The default setting is not to set current NFS share as a public filesystem.

If you would like to learn more about the WebNFS Java pug-in, please refer to the following Web sites:

```
http://wwws.sun.com/software/webnfs/
http://www.sun.com/960710/feature2/webnfs.html
http://ntrg.cs.tcd.ie/undergrad/4ba2.01/group9/CommonFileSystems3.html
```

Then select the time scope of the new share. The export options are:

- Immediately and on every subsequent system startup. Export this directory now, and automatically export this directory at system restart.
- Immediately and make no permanent changes to the system. Export this directory now, and don't automatically export this directory at system restart.
- On the next system startup. Don't export this directory now, but automatically export this directory at system restart.

If you want to control the access to this NFS share, click the **Access List** tab. The screen shown in Figure 11-4 will appear.

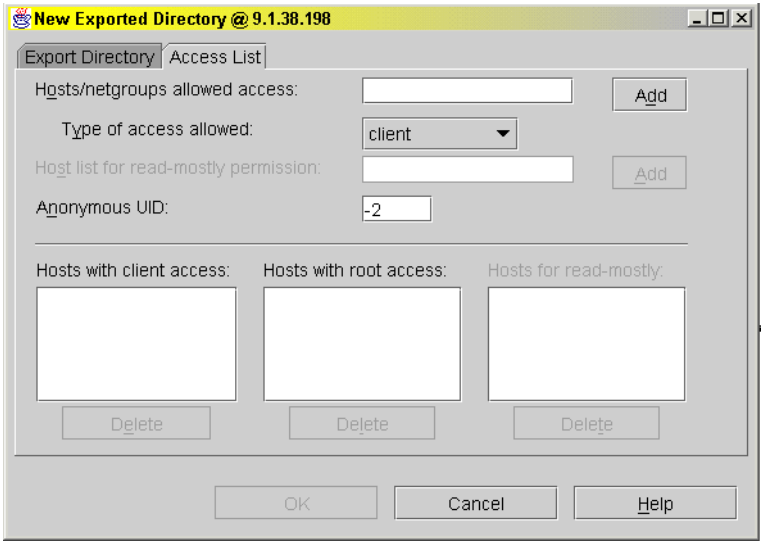


Figure 11-4 The NFS access list

You should set which client can access this NFS share here. For a storage system, control access by the host name or IP address is very handy.

Type in the IP address or host name of your NFS client in **Hosts/netgroups allowed access**, or netgroup name if you use NIS or NIS+. Then select **Type of access allowed**. Combine these two sections; you can add hosts to the Hosts with client access list and the Hosts with root access list.

The Hosts with client access list means that they give mount access to each client listed. If not specified, any client is allowed to mount the specified NFS share.

The Hosts with root access list means that they allow root access from the specified clients listed. Clients not in the list are not allowed root access. Root access means the root user on a client system has “super user” permission on mounted NFS files. On NAS Gateway 500, requests from the root user on a client machine without root access permission are treated as if received from an anonymous user.

Important: If you leave the Hosts with client access list empty, then all client systems connected to your network can access this NFS share.

If the permission of the current NFS share is read-mostly, you can grant clients read/write access to the share by add their IP address or host name to the Hosts for read-mostly list. Unlisted clients can’t write to this NFS share.

Make your choices and click **OK** to continue. The process takes several seconds to complete. Wait for the success message and click **Finish** to close the dialogue box.

Repeat the steps above until all desired NFS shares are created.

Creating NFS shares via WebSM: clustered configuration

NFS shares are handled by clustering software in a clustered environment. To ensure high availability, you should use the NAS volume creation tool to create new volumes and mark them as NFS shares. See Chapter 8.2.2, “Creating a NAS volume” on page 157 for details of creating new NAS volumes.

After creating the NAS volumes for NFS sharing, you can set their properties with either WebSM or SMIT.

Setting NFS shares properties via WebSM

In order to set properties of an NFS share, select the NFS share under **Exported Directories**, then from the **Selected** drop-down menu, select **Properties**, as shown in Figure 11-5.

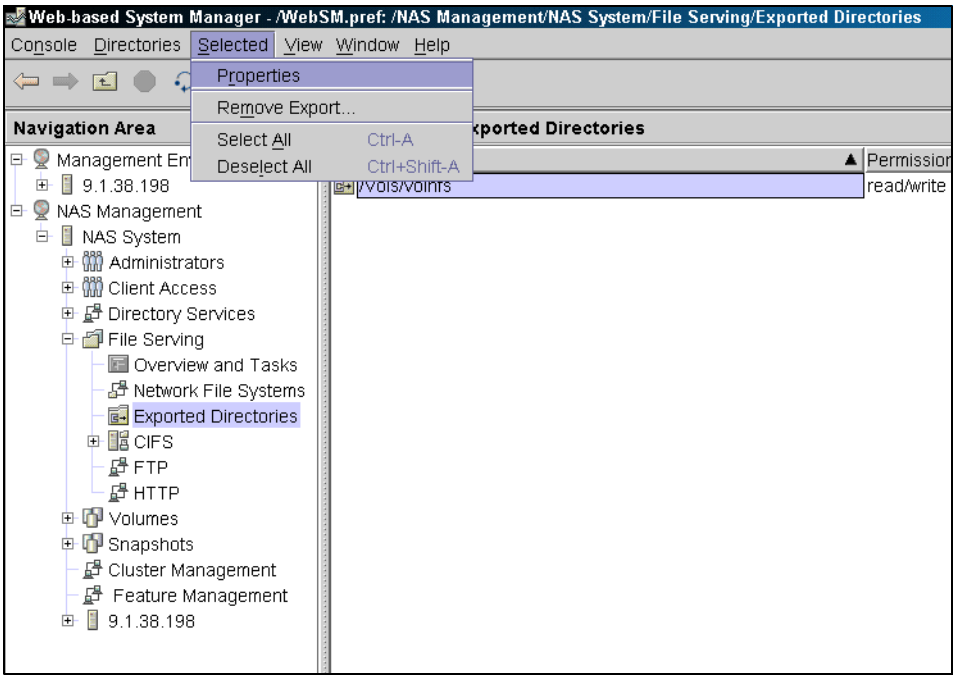


Figure 11-5 Access NFS share properties

The Exported Directory Properties screen shown in Figure 11-6 will appear.

In the Permissions drop-down menu, you can define permissions of the current NFS share.

We also have two more check boxes; one about DES encryption, and one about the public filesystem.

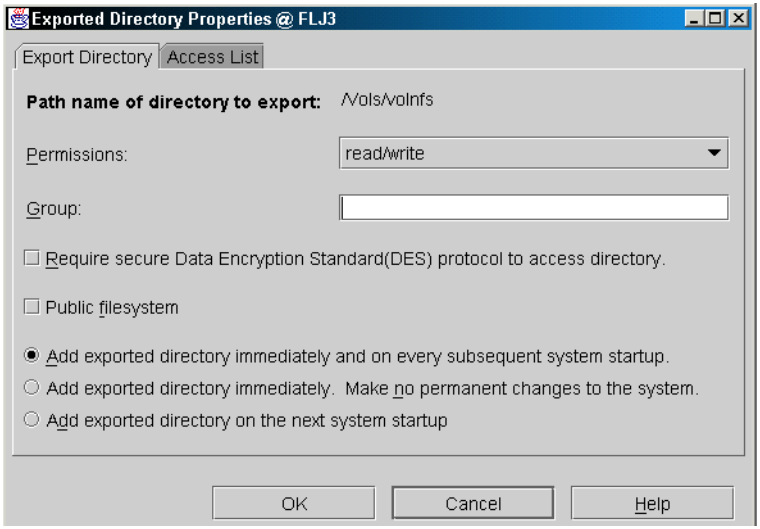


Figure 11-6 Exported Directory Properties

If you want to control the access to the NFS server of NAS Gateway 500, click the **Access List** tab. The dialogue shown in Figure 11-7 will be displayed.

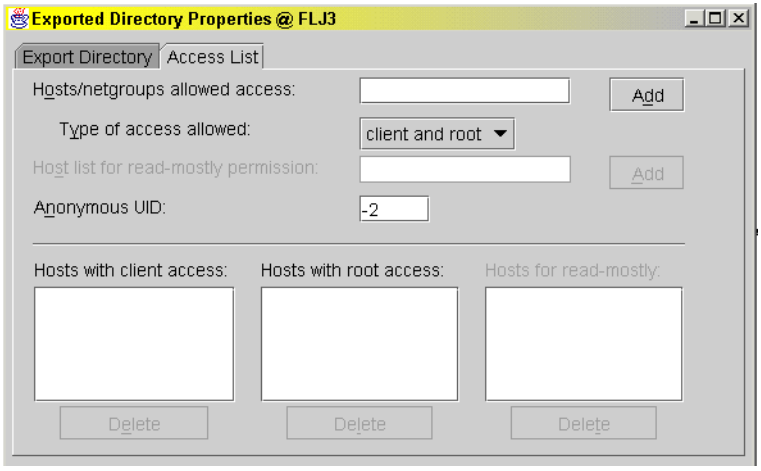


Figure 11-7 Access list to NFS shares

For detailed information on properties and access control settings, see “Creating NFS shares via WebSM: single node configuration” on page 251.

Important: If you leave the Hosts with client access list empty, then all client systems connected to your network can access this NFS share.

11.2.2 Configuring NFS shares with SMIT

In order to configure NFS shares via SMIT menus, you must login with the NAS administrator user account.

Important: Do not use SMIT to configure NFS shares if you login as root on NAS Gateway 500, especially in the clustered environment.

Creating NFS shares with SMIT: single node configuration

Important: If you are running a NAS Gateway 500 cluster, use the NAS volume creation tool to add a volume and mark the **Export the volume as an NFS share** check box.

First, enter the **smitty** command to bring up the root SMIT menu for NAS management, as shown in Figure 11-8.

```
                            NAS System Management

Move cursor to desired item and press Enter.

  Manage Administrators
  Manage Applications
  Manage Client Access
  Manage Cluster
  Manage Devices
  Manage File Serving
  Manage Network
  Manage Security
  Manage System
  Manage Volumes and Snapshots

  Using SMIT (information only)

  NAS Overview (information only)




F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 11-8 The SMIT root menu for NAS management

Then select **Manage File Serving**->**Manage NFS**->**Add a Volume to Export List**. The screen shown in Figure 11-9 appears.

Tip: Use cursor keys to move between SMIT menu items. Use the Enter key to select the highlighted item.

.

```
                          Add a Volume to Export List

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* PATHNAME of directory to export                     [] /
* MODE to export directory                             read-write +
  HOSTS & NETGROUPS allowed client access             []
  Anonymous UID                                       [-2]
  HOSTS allowed root access                           []
  HOSTNAME list. If exported read-mostly              []
  Use SECURE option?                                   no +
  Public filesystem?                                   no +
* EXPORT directory now, system restart or both         both +
  Node / Group                                        [] +




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 11-9 Add a volume to export list

Fill the directory you want to export into “PATHNAME of directory to export”.

In the “MODE to export directory” field you can select one of three modes for the NFS share:

- Read-write: Allow clients perform read and write operations on this share.
- Read-only: Only Allow read requests from clients.
- Read-mostly: Allow some clients perform read and write operations on this share, and allow read operations only to other clients.

In the “HOSTS & NETGROUPS allowed client access” field, enter the IP addresses or host names of clients allowed to access this share. If you leave this field blank, then all client systems connected to your network can access this NFS share.

In the “HOSTS allowed root access” field, enter the IP addresses or host names of clients allowed to make root access to this share. If you leave this field blank, then no client can make root access to this NFS share. Root access means the root user on a client system has “super user” permission on mounted NFS files. On NAS Gateway 500, requests from root user on a client without root access permission are treated as from anonymous user.

In the “HOSTNAME list. If exported read-mostly” field you can enter IP addresses or host names of clients allowed read-write access to this NFS share, if the mode of this share is defined as read-mostly.

The “Use SECURE option?” field allows for higher security settings. The NFS server on NAS Gateway 500 supports secure NFS sharing in a NIS or NIS+ environment, with the secure mode. In addition to the standard UNIX authentication system, the NFS server on NAS Gateway 500 provides a means to authenticate users and machines in networks on a message-by-message basis. This additional authentication system uses Data Encryption Standard (DES) encryption and public key cryptography. Secure NFS can improve security but requires a NIS or NIS+ environment and has some performance penalty on both server side and client side.

The “Public filesystem?” field is designed to work with WebNFS. WebNFS is a new protocol that allows client access NFS server through Web browsers. On supported Web browsers, you can access NFS shares on NAS Gateway 500 in this manner:

```
nfs://www.nas500.YourCompany.com/nfsshare
```

If you choose one NFS share as the public filesystem, then any WebNFS URL referring to the root directory will be redirected to this share. For example, if we assign /nasnfs as the public filesystem, then the URL **`nfs://nas500/`** will gain access to /nasnfs directory on the server nas500. WebNFS has not been widely supported on Web browsers until now.

You can also change the time scope of this NFS share. The default is to make the NFS share available to clients now, and automatically export this share after system restart.

Changing NFS shares with SMIT

In order to change NFS shares with SMIT, select **Manage File Serving**->**Manage NFS**->**Change / Show Characteristics of Currently Exported Volume** from the SMIT root menu for NAS management. Select the NFS share you want to change from the list, then the screen shown in Figure 11-10 appears.

```
                  Change Attributes of an Exported Directory

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* PATHNAME of Directory to Export                      /nasnfs
* MODE to export directory                             read-write +
  HOSTS & NETGROUPS allowed client access             []
  Anonymous UID                                       [-2]
  HOSTS allowed root access                           []
  HOSTNAME list. If exported read-mostly              []
  Use SECURE OPTION?                                   no +
  Public filesystem?                                   no +
* CHANGE export now, system restart or both            both +




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 11-10 Change attributes of an exported directory

Make the desired changes on this screen and press Enter to submit changes.

11.3 Access NAS Gateway 500 file service from AIX

In this section we discuss how to access NAS Gateway 500 NFS exports from an AIX system, as well as giving some troubleshooting and performance tuning information.

11.3.1 Mount an NFS file system on AIX

There are many ways to mount an NFS file system on AIX, we introduce two of them here: from the SMIT menu and from the command line.

Mount an NFS file system through the SMIT menu

In the AIX command line prompt, type **smitty mknfsmnt**. This command will open the screen shown in Figure 11-11.

```
                        Add a File System for Mounting

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                   [Entry Fields]
* PATHNAME of mount point                              []
* PATHNAME of remote directory                         []
* HOST where remote directory resides                  []
  Mount type NAME                                      []
* Use SECURE mount option?                             no
* MOUNT now, add entry to /etc/filesystems or both?    now
* /etc/filesystems entry will mount the directory      no
   on system RESTART.
* MODE for this NFS file system                        read-write
* ATTEMPT mount in foreground or background            background
  NUMBER of times to attempt mount                     []
  Buffer SIZE for read                                 []
  Buffer SIZE for writes                               []
[MORE...26]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 11-11 Screen of smitty: mounting an NFS filesystem

In order to mount an NFS share, three sections must be filled out, they are PATHNAME of mount point, PATHNAME of remote directory and HOST where remote directory resides:

- PATHNAME of mount point: This is a local empty directory you want to use to access the NFS export from NAS Gateway 500 after it is mounted. You can type in a new path name; SMIT will create the path for you if it doesn't exist.
- PATHNAME of remote directory: This is the exported directory path on NAS Gateway 500.
- HOST where remote directory resides: Enter the IP address or the resolvable host name of NAS Gateway 500.

If you want to make this NFS mount remembered by AIX system, you can change the setting of “MOUNT now, add entry to /etc/filesystems or both”. These are the options:

- Now: This means only mount the NFS share now, don’t change the system file /etc/filesystems, which contains a stanza for all “remembered” filesystems.
- Both: This means mount the NFS share now, and change /etc/filesystems to record this file system.
- Filesystems: This means record this file system to /etc/filesystems, but don’t mount it now.

Example 11-1 is a sample NFS entry in /etc/filesystems.

Example 11-1 NFS stanza in /etc/filesystems

```
/nas:
        dev             = "/nasnfs"
        vfs             = nfs
        nodename        = nas500
        mount           = false
        options         = bg,hard,intr
        account         = false
```

If you select **both** or **filesystems** for “MOUNT now, add entry to /etc/filesystems or both”, then within this SMIT screen you can also make this NFS share to be automatically mounted during AIX start up. Just select **yes** on “/etc/filesystems entry will mount the directory on system RESTART”.

There are also several other options when considering an NFS mount. The most common issue is whether to use a hard mount or a soft mount. A soft mount will try to re-transmit a number of times. This re-transmit value is defined by the **retrans** option. After the set number of retransmissions has been used, the soft mount gives up and returns an error. A hard mount retries a request until a server responds. The hard option is the default value. On hard mounts, the **intr** option should be used to allow a user to interrupt a system call that is waiting on a crashed server.

Both hard mounts and soft mounts use the **timeo** option, to calculate the time between re-transmits. The default value is 0.7 seconds for the first time out. After that, it increases the time out exponentially until a maximum of 30 seconds, where it stabilizes until a reply is received. Depending on the value set for the retrans option, the soft mount has probably given up already at this stage. You need to scroll down to set hard/soft mount in this SMIT screen.

Mount an NFS file system through the command line

Use the **mount** command to temporarily mount NFS file systems. For example, in order to mount the remote directory **/nasnfs** residing on host system **nas500** to local mount point **/nas**, you can type the following command:

```
#mount nas500:/nasnfs /nas
```

The **mount** command can be used with lots of options. The syntax of the mount command is:

```
mount [ -f ] [ -n Node ] [ -o Options ] [ -p ] [ -r ] [ -v VfsName ] [
-t Type| [ Device | Node:Directory ] Directory | all | -a ][-V
[generic_options] special_mount_points
```

In Table 11-1 we list the most useful options of the **mount** command.

Table 11-1 Useful mount options

Flags	Description
-[a | all]	Mounts all file systems in the /etc/filesystems file with stanzas that contain the true mount attribute.
-n <node>	Specifies the remote node that holds the directory to be mounted.
-o fg	Foreground mount attempt.
-o bg	Background mount attempts.
-oproto=[tcp|udp]	Protocol to use.
-o vers=[2|3]	NFS version to use.
-o soft	Returns an error if the server does not respond.
-o hard	Retries a request until the server responds.
-o timeo=n	Sets the Network File System (NFS) timeout period to n tenths of a second.
-o intr	Allows keyboard interrupts on hard mounts.
-o retrans=n	Sets the number of NFS transmissions to n.

11.3.2 AIX NFS mount problem determination

Here we show some common NFS mount problems on AIX and give you some ideas on how to solve them.

Check if the file system you try to mount is exported

When a mount request is sent to a server for an export that does not exist, the error message shown in Example 11-2 appears.

Example 11-2 AIX NFS mounting error 1

```
# mount nas500:/nasnfs /nas
mount: 1831-011 access denied for nas500:/nasnfs
mount: 1831-008 giving up on:
nas500:/nasnfs
The file access permissions do not allow the specified action.
```

Then you must check if the directory you want to mount is actually exported on the NAS Gateway 500. To check what file systems, directories, or files are exported from NAS Gateway 500, use the **showmount** command as follows:

```
showmount -e <IP address of NAS Gateway 500>
```

The output from the command shows you the directories exported, and to whom they are exported.

If NAS Gateway 500 doesn't respond to the **showmount** command, or the error shown in Example 11-3 is reported, you should check if the NFS server daemons are running at NAS Gateway 500.

Example 11-3 AIX RPC error

```
RPC: 1832-019 Program not registered
```

Use this command:

```
rpcinfo -p <IP address of NAS Gateway 500>
```

Example 11-4 shows the output you will get from this command.

Example 11-4 rpcinfo on AIX

```
# rpcinfo -p 9.1.38.198
   program vers proto   port  service
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100021    1   udp  32772  nlockmgr
    100021    2   udp  32772  nlockmgr
    100021    3   udp  32772  nlockmgr
    100021    4   udp  32772  nlockmgr
    100021    1   tcp  32773  nlockmgr
    100021    2   tcp  32773  nlockmgr
    100021    3   tcp  32773  nlockmgr
    100021    4   tcp  32773  nlockmgr
    100024    1   tcp  32789  status
    100024    1   udp  32798  status
    100133    1   tcp  32789
    100133    1   udp  32798
    200001    1   tcp  32789
    200001    1   udp  32798
    200001    2   tcp  32789
    200001    2   udp  32798
```

The output shows that the portmap (program 100000) is available, but statd (100024), lockd (100021), nfsd (100003), and mountd (100005) are not available. This means NFS server is not up and running. You must review the NFS exports configuration steps introduced in the beginning of this chapter. Make sure there is no error generated when you make or modify NFS exports.

The reverse lookup problem on AIX

Sometimes you mount an NFS share through SMIT menu or command line and get the error message shown in Example 11-5.

Example 11-5 AIX NFS mounting error 2

```
# mount nas500:/home /mnt
nfsmnthelp: 1831-019 nas500: System call error number -1.
mount: 1831-008 giving up on:
nas500:/home
System call error number -1.
```

This is usually caused by the reverse lookup problem, which means NAS Gateway 500 can't resolve AIX client's IP address to host name.

There are several ways for NAS Gateway 500 to make IP address to host name resolution. The most widely used methods in the TCP/IP world are DNS system and local file mapping. For availability reasons, we highly recommend that you use local file mapping, that is, store host to IP address mapping in the /etc/hosts file on NAS Gateway 500. We just don't want a DNS server outage to bring down the storage system.

Next we explain how to manage the local mapping on NAS Gateway 500.

First of all, you need to build an interactive session to the NAS Gateway 500, either through terminal or through telnet. Login as root user. Run the command **smitty hostent**.

You will get a screen as shown in Figure 11-12.

```
                          Hosts Table (/etc/hosts)

Move cursor to desired item and press Enter.

  List All Hosts
  Add a Host
  Change / Show Characteristics of a Host
  Remove a Host

F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 11-12 Smitty hostent

You can add, remove, and modify local IP address to host name mapping entries here. We take the add task as an example, shown in Figure 11-13; other functions of this menu are also very straightforward.

```
                                Add a Host Name

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* INTERNET ADDRESS (dotted decimal)                    [9.1.38.191]
* HOST NAME                                            [crete]
  ALIAS(ES) (if any - separated by blank space)        []
  COMMENT (if any - for the host entry)                []

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 11-13 Add a host name entry

After adding all mappings for your storage client, wait for a while and try the NFS mount again; the problem should be solved.

Check the syntax on the mount command

Try to use SMIT menus instead of long and complex command line entries, this can help you avoid a lot of errors.

Important: Always remember that only root can issue any **`mount`** command, and system group members can issue mounts, provided they have write access to the mount point.

11.3.3 Tuning AIX to improve NAS Gateway 500 NFS performance

An AIX NFS client performance discussion often concentrates on the number of biods used. Biod is the NFS client daemon on AIX. For biod daemons, there is a default number of biods (six for a V2 mount, four for a V3 mount) that may operate on any one remote mounted file system at one time. The idea behind this limitation is that allowing more than a set number of biods to operate against the server at one time may overload the server. Since this is configurable on a per-mount basis on the client, adjustments can be made to configure client mounts by the server capabilities.

If there are multiple users or multiple processes on the client that will need to perform NFS operations to the same NFS mounted file systems, you have to be aware that contention for biod services can occur with just two simultaneous read or write operations.

Since up to six biods can be working on reading a file in one NFS file system, if another read starts in another NFS mounted file system, both reads will be attempting to use all six biods. In this case, presuming that the NAS Gateway 500 are not already overloaded, performance will likely improve by increasing the biod number to 12. This can be done using the **chnfs** command (see Example 11-6).

Example 11-6 Changing biod number to 12

```
# chnfs -b 12
```

On the other hand, suppose both file systems are mounted from the same NAS Gateway 500 and the NAS Gateway 500 is already operating at peak capacity. Adding another six biods could actually decrease the response dramatically, due to the NAS Gateway 500 dropping packets, resulting in timeouts and transmits.

To change the number of biod daemons per mount, use the biod mount option.

Increasing the number of biod daemons on the client worsens NAS Gateway 500 performance because it allows the client to send more request at once, further loading the network and the NAS Gateway 500. In extreme cases of a client overrunning the NAS Gateway 500, it may be necessary to reduce the client to one biod daemon, as shown in Example 11-7.

Example 11-7 Stopping biod daemons

```
# stopsrc -s biod
```

This leaves the client with the kernel process biod still running.

11.4 Access NAS Gateway 500 file service from HP-UX

In this section we give some brief information about how to access NAS Gateway 500 through NFS from the HP-UX UNIX system.

11.4.1 Mounting a NAS Gateway 500 NFS filesystem on HP-UX

In order to mount an NFS filesystem on HP-UX, you must configure the HP-UX system as an NFS client first. The command for this task is **/sbin/init.d/nfs.client start**, as shown in Figure 11-14.

```
# /sbin/init.d/nfs.client start
    starting NFS CLIENT networking

killing nfsd
killing rpc.mountd
    starting up the rpcbind
        rpcbind already started, using pid: 553
    starting up the BIO daemons
        biod(s) already started, using pid(s): 578 579 580 577
    starting up the Status Monitor daemon
        rpc.statd already started, using pid: 588
    starting up the Lock Manager daemon
        rpc.lockd already started, using pid: 594
    starting up the Automount daemon
        automount already started, using pid: 605
    mounting remote NFS file systems ...
    starting NFS SERVER networking

    starting up the rpcbind daemon
        rpcbind already started, using pid: 553
    starting up the mount daemon
        /usr/sbin/rpc.mountd
    starting up the NFS daemons
        /usr/sbin/nfsd 4
    starting up the Status Monitor daemon
        rpc.statd already started, using pid: 588
    starting up the Lock Manager daemon
        rpc.lockd already started, using pid: 594
#
```

Figure 11-14 Start NFS client on HP-UX

You can also make NFS client processes start automatically at system start. Just edit the file /etc/rc.config.d/nfsconf, and change the NFS_CLIENT variable to 1.

To mount a NAS Gateway 500 NFS share on HP-UX, you can use a **mount** command such as this:

```
mount -F nfs nas500:/nasnfs /nas
```

You can also customize the mounting by appending other mount options to this command. Please see the HP-UX documentation for details.

To make the NAS Gateway 500 NFS share be mounted automatically during system start, you need to edit the /etc/fstab file. Create an entry like the one in Example 11-8.

Example 11-8 HP-UX: the NFS entry in /etc/fstab

```
nas500:/nasnfs /nas nfs defaults 0 0
```

You can also add mount options into this file. See the HP-UX documentation for details.

11.4.2 HP-UX NFS mount problem determination

Here we show some common NFS mount problems on HP-UX and give you some ideas on how to solve them.

Check if the file system you try to mount is exported

If you get the error shown in Example 11-9 on NFS mounting, you should check if you entered the correct NAS Gateway 500 host name and the shared directory.

Example 11-9 HP-UX NFS mounting error 1

```
# mount -F nfs nas500:/NASNFS /mnt
Permission denied
```

The process of checking exported directories on NAS Gateway 500 from HP-UX is almost identical to the process from AIX. Refer to “Check if the file system you try to mount is exported” on page 265 for details.

The reverse lookup problem on HP-UX

If you get error messages as shown in Example 11-10, then you should check the reverse lookup function on NAS Gateway 500. See “The reverse lookup problem on AIX” on page 266 for details.

Example 11-10 HPUX NFS mounting error 2

```
# mount -F nfs nas500:/NASNFS /mnt
Unknown error
```

11.5 Access NAS Gateway 500 file service from Solaris

In this section we give some brief information about how to access NAS Gateway 500 through NFS from a SUN Solaris system.

11.5.1 Mounting a NAS Gateway 500 NFS filesystem on Solaris

The command to mount an NFS filesystem on Solaris is:

```
mount -F nfs nas500:/NASNFS /MOUNTPOINT
```

In this command, NASNFS is the directory you exported on the NAS Gateway 500, and the MOUNTPOINT is the local directory on Solaris where you want to mount the filesystem. For more options of the **mount** command, please check the Solaris documentation.

If you want to mount a NAS Gateway 500 NFS filesystem automatically on Solaris startup, edit the /etc/vfstab file, add an entry for this NFS filesystem, and set the mount-at-boot field to **yes** (see Example 11-11).

Example 11-11 Solaris: the NFS entry in /etc/vfstab

```
nas500:/NASNFS - /MOUNTPOINT nfs - yes rw
```

In this command, NASNFS is the directory you exported on the NAS Gateway 500, and the MOUNTPOINT is the local directory on Solaris where you want to mount the filesystem. For the syntax of /etc/vfstab file, please check the Solaris documentation.

11.5.2 Solaris NFS mount problem determination

Here we show some common NFS mount problem on Solaris and give you some idea on how to solve them.

Check if the file system you try to mount is exported

If you get the error shown in Example 11-12 on NFS mounting, you should check if you entered the correct NAS Gateway 500 host name and the shared directory.

Example 11-12 Solaris NFS mounting error 1

```
# mount -F nfs nas500:/NASNFS /mnt
Permission denied
```

The process of checking exported directories on NAS Gateway 500 from SUN Solaris is almost identical to the process from AIX. Refer to “Check if the file system you try to mount is exported” on page 265 for details.

The reverse lookup problem on Solaris

The reverse lookup problem can cause the **mount** command on Solaris to crash on some Solaris releases, and can make it difficult to track the root cause, because no error message is generated by the **mount** command. So we highly recommend that you configure and test the name resolution on NAS Gateway 500 prior to integrating with SUN Solaris systems. For the details on how to configure local name resolution on NAS Gateway 500, check “The reverse lookup problem on AIX” on page 266.

12

Linux systems integration

In this chapter we describe how to integrate NAS Gateway 500 with Linux systems. We use Red Hat Linux 9 and SUSE Enterprise Server powered by United Linux in our environment.

In this chapter, the following topics are discussed:

- Accessing a NAS Gateway 500 NFS share from Red Hat Linux
- Accessing a NAS Gateway 500 NFS share from SUSE LINUX

12.1 Red Hat Linux: Access a NAS Gateway 500 share

Here we introduce how to access a NAS Gateway 500 NFS share from Red Hat Linux. We also provide some troubleshooting information for integrating NAS Gateway 500 with Red Hat Linux.

12.1.1 Mount a NAS Gateway 500 NFS share on Red Hat Linux

Here we discuss the **mount** command used to mount a NAS Gateway 500 NFS share on Red Hat Linux, and how to make the NFS share mounted automatically at system startup.

The mount command to use on Red Hat Linux

In order to mount a NAS Gateway 500 NFS share on Red Hat Linux, the **mount** command should be used as shown in Example 12-1.

Example 12-1 Red Hat: mount an NFS filesystem

```
[root@naslinux root]# mount -t nfs 9.1.38.198:/Vols/FJL3VOL01 /mnt/nfs
```

The -t option of the **mount** command on Red Hat Linux indicates the filesystem type to be mounted. It should always be nfs while mounting a NAS Gateway 500 NFS share.

You can also combine other mounting options with the mount command. See the Red Hat Linux documents for the detailed description of mounting options.

After the **mount** command is returned, you can run the **mount** command without parameters to verify the mount status (Example 12-2).

Example 12-2 The mount command output on Red Hat

```
parameters to verify the mount status:
[root@naslinux root]# mount
/dev/hda2 on / type ext3 (rw)
none on /proc type proc (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
/dev/hda1 on /boot type ext3 (rw)
none on /dev/pts type devpts (rw,gid=5,mode=620)
none on /dev/shm type tmpfs (rw)
9.1.38.198:/Vols/FJL3VOL01 on /mnt/nfs type nfs (rw,addr=9.1.38.198)
```

The NFS share, mount point, filesystem type, and mount options are displayed with this command.

Mount the NAS share automatically at system startup

In order to mount the NFS share automatically at Red Hat Linux startup, we edit /etc/fstab file on Red Hat Linux.

The /etc/fstab file on Red Hat Linux contains descriptive information about the filesystem. It is processed by the system scripts of Red Hat Linux during system startup. Our /etc/fstab is shown in Example 12-3. See the Red Hat Linux documentation for a detailed description of the /etc/fstab file.

Example 12-3 /etc/fstab on Red Hat Linux

```
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
9.1.38.198:/Vols/FJL3VOL01 /mnt/nfs             nfs     tcp,soft
0 0
none                    /dev/pts                devpts  gid=5,mode=620  0 0
none                    /proc                   proc    defaults        0 0
none                    /dev/shm                tmpfs   defaults        0 0
/dev/hda3               swap                    swap    defaults        0 0
/dev/cdrom              /mnt/cdrom              udf,iso9660
noauto,owner,kudzu,ro 0 0
/dev/fd0                /mnt/floppy             auto    noauto,owner,kudzu 0 0
```

12.1.2 Troubleshooting the NFS mount on Red Hat Linux

In this section we provide some troubleshooting tips.

The firewall issue

Some Red Hat Linux releases come with a firewall setting interface in the installation wizard. If you have chosen any options except “No firewall” in the installation phase, you may experience the error message shown in Example 12-4 when you try to mount a NAS Gateway 500 NFS share.

Example 12-4 Red Hat NFS mounting error 1

```
[root@naslinux root]# mount -t nfs 9.1.38.198:/Vols/FJL3VOL01 /mnt/nfs
mount: RPC: Timed out
```

This is caused by the firewall settings of Red Hat Linux. The firewall settings created by the Red Hat Linux tool can’t handle the NFS mount negotiations correctly when the UDP protocol is involved.

To overcome this problem, use the -o tcp option with the **mount** command (see Example 12-5).

Example 12-5 Mount with -o tcp

```
[root@naslinux root]# mount -t nfs -o tcp 9.1.38.198:/Vols/FJL3VOL01 /mnt/nfs
```

Check if the file system you try to mount is exported

Sometimes you get the error message shown in Example 12-6 while mounting a NAS Gateway 500 NFS share on Red Hat Linux.

Example 12-6 Red Hat NFS mounting error 2

```
[root@naslinux root]# mount -t nfs 9.1.38.198:/Vols/FJL3VOL1 /mnt/nfs
mount: 9.1.38.198:/Vols/FJL3VOL1 failed, reason given by server: Permission
denied
```

In this case, you should check if the NFS share on the NAS Gateway 500 is really shared for you. You can check this by using the **showmount** command (see Example 12-7).

Example 12-7 Red Hat: the showmount command

```
[root@naslinux root]# showmount -e 9.1.38.198
Export list for 9.1.38.198:
/Vols/FJL3VOL01 (everyone)
```

This command tells you which directories on NAS Gateway 500 are shared, and which hosts can access them. Check the NAS Gateway 500 configuration if the directory you want to access is not shared or your host is not in the access list.

If you got the error “RPC: Program not registered” while running the **showmount** command, you should check the NFS daemon status on the NAS Gateway 500. You can use the **rpcinfo** command on Linux (see Example 12-8).

Example 12-8 Red Hat: the rpcinfo command

```
[root@naslinux root]# rpcinfo -p 9.1.38.197
   program vers proto   port
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100021    1   udp  32772  nlockmgr
    100021    2   udp  32772  nlockmgr
    100021    3   udp  32772  nlockmgr
    100021    4   udp  32772  nlockmgr
    100021    1   tcp  32773  nlockmgr
    100021    2   tcp  32773  nlockmgr
```

```
100021    3   tcp  32773  nlockmgr
100021    4   tcp  32773  nlockmgr
100024    1   tcp  32774  status
100024    1   udp  32785  status
100133    1   tcp  32774
100133    1   udp  32785
200001    1   tcp  32774
200001    1   udp  32785
200001    2   tcp  32774
200001    2   udp  32785
```

In this example, the NFS server process is not listed in the registered programs on NAS Gateway 500. So we know the NFS server on NAS Gateway 500 is not up and running. If you get this problem, please review the NAS Gateway 500 setup process, and make sure there is no error reported during the NFS share configuration.

The reverse lookup problem on Red Hat Linux

Sometimes you get the error message shown in Example 12-9 while mounting a NAS Gateway 500 NFS share on Red Hat Linux.

Example 12-9 Red Hat NFS mounting error 3

```
[root@naslinux root]# mount -t nfs 9.1.38.198:/Vols/FJL3VOL01 /mnt/nfs
mount: 9.1.38.198:/Vols/FJL3VOL01 failed, reason given by server: unknown nfs
status return value: -1
```

This is usually caused by the reverse lookup problem, which means NAS Gateway 500 can't resolve the IP address of the Red Hat Linux client to host name.

You must configure name resolution on NAS Gateway 500 to fix this problem. See "The reverse lookup problem on AIX" on page 266 for the detailed steps.

12.2 SUSE LINUX: Access a NAS Gateway 500 share

Here we explain how to access a NAS Gateway 500 NFS share from SUSE LINUX. We also provide some troubleshooting information for integrating NAS Gateway 500 with SUSE LINUX.

12.2.1 Mount a NAS Gateway 500 NFS share on SUSE LINUX

Here we discuss the mount command used to mount a NAS Gateway 500 NFS share on SUSE LINUX, and how to make the NFS share mounted automatically at system startup.

The mount command to use on SUSE LINUX

In order to mount a NAS Gateway 500 NFS share on SUSE LINUX, the mount command should be used as shown in Example 12-10.

Example 12-10 NFS mount command on SUSE

```
naslinux:~ # mount -t nfs 9.1.38.198:/Vols/FJL3VOL01 /mnt/nfs
```

The -t option of the mount command on SUSE LINUX indicates the filesystem type to be mounted. It should always be nfs while mounting a NAS Gateway 500 NFS share. You can also combine other mounting options with the mount command. See the SUSE LINUX documents for a detailed description of mounting options.

After the mount command is returned, you can run the mount command without parameters to verify the mount status (Example 12-11).

Example 12-11 SUSE: the mount command output

```
naslinux:~ # mount
/dev/hda2 on / type reiserfs (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
9.1.38.198:/Vols/FJL3VOL01 on /mnt/nfs type nfs (rw,addr=9.1.38.198)
```

The NFS share, mount point, filesystem type, and mount options are displayed with this command.

Mount the NAS share automatically at system startup

In order to mount the NFS share automatically at SUSE LINUX startup, we can either configure the NFS client in yast2, or edit the /etc/fstab file on SUSE LINUX.

The configuration of the NFS client with yast2 is very straightforward, and yast2 accomplishes this task by modifying the /etc/fstab file. The /etc/fstab file on SUSE LINUX contains descriptive information about filesystem. It is processed by the system scripts of SUSE LINUX during system startup. Our /etc/fstab is shown in Example 12-12. See the SUSE LINUX documentation for a detailed description of the /etc/fstab file.

Example 12-12 /etc/fstab on SUSE LINUX

```
/dev/hda2       /       reiserfs        defaults 1 1
/dev/hda1       /data1  auto    noauto,user 0 0
/dev/hda3       swap    swap    pri=42 0 0
devpts  /dev/pts        devpts  mode=0620,gid=5 0 0
proc    /proc   proc    defaults 0 0
usbdevfs        /proc/bus/usb   usbdevfs        noauto 0 0
/dev/cdrecorder /media/cdrecorder       auto    ro,noauto,user,exec 0 0
/dev/fd0        /media/floppy   auto    noauto,user,sync 0 0
9.1.38.198:/Vols/FJL3VOL01      /mnt/nfs        nfs     defaults 0 0
```

12.2.2 Troubleshooting the NFS mount on SUSE LINUX

In this section we provide some troubleshooting tips.

Check if the file system you try to mount is exported

Sometimes you get the error message shown in Example 12-13 while mounting a NAS Gateway 500 NFS share on SUSE LINUX.

Example 12-13 SUSE NFS mounting error 1

```
naslinux:~ # mount -t nfs 9.1.38.198:/Vols/FJL3VOL1 /mnt/nfs
mount: 9.1.38.198:/Vols/FJL3VOL1 failed, reason given by server: Permission
denied
```

In this case, you should check if the NFS share on the NAS Gateway 500 is really shared for you. You can check this by using the **showmount** command (see Example 12-14).

Example 12-14 SUSE: the showmount command

```
naslinux:/mnt/nfs # showmount -e 9.1.38.198
Export list for 9.1.38.198:
/Vols/FJL3VOL01 (everyone)
```

This command tells you which directories on NAS Gateway 500 are shared, and which hosts can access them. Check the NAS Gateway 500 configuration if the directory you want to access is not shared or your host is not in the access list.

If you got the error “RPC: Program not registered” while running the **showmount** command, you should check the NFS server status on the NAS Gateway 500. You can use the **rpcinfo** command on Linux (see Example 12-15).

Example 12-15 SUSE: the rpcinfo command

```
naslinux:/mnt/nfs # rpcinfo -p 9.1.38.197
   program vers proto   port
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100021    1   udp  32772  nlockmgr
    100021    2   udp  32772  nlockmgr
    100021    3   udp  32772  nlockmgr
    100021    4   udp  32772  nlockmgr
    100021    1   tcp  32773  nlockmgr
    100021    2   tcp  32773  nlockmgr
    100021    3   tcp  32773  nlockmgr
    100021    4   tcp  32773  nlockmgr
    100024    1   tcp  32774  status
    100024    1   udp  32785  status
    100133    1   tcp  32774
    100133    1   udp  32785
    200001    1   tcp  32774
    200001    1   udp  32785
    200001    2   tcp  32774
    200001    2   udp  32785
```

In this example, the NFS server process is not listed in the registered programs on NAS Gateway 500. So we know the NFS server on NAS Gateway 500 is not up and running. If you get this problem, review the NAS Gateway 500 setup process. Be sure there is no error reported during the NFS share configuration.

The reverse lookup problem on SUSE LINUX

Sometimes you get the error message shown in Example 12-16 while mounting a NAS Gateway 500 NFS share on SUSE LINUX.

Example 12-16 SUSE NFS mounting error 2

```
naslinux:~ # mount -t nfs 9.1.38.198:/Vols/FJL3VOL01 /mnt/nfs
mount: 9.1.38.198:/Vols/FJL3VOL01 failed, reason given by server: unknown nfs
status return value: -1
```

This is usually caused by the reverse lookup problem, which means NAS Gateway 500 can't resolve the IP address of the SUSE LINUX client to host name. You must configure name resolution on NAS Gateway 500 to fix this problem. See "The reverse lookup problem on AIX" on page 266 for the detailed steps.

13

Apple systems integration

In this chapter we explain how to integrate NAS Gateway 500 with Apple Macintosh systems. We use a Power Mac G4 running Mac 10.2.8 Server. This connection process works for normal Mac systems as well.

The following topics are discussed:

- Accessing a NAS Gateway 500 NFS share from Apple Mac OS 10.x

13.1 Apple Mac OS 10.x accessing an NFS share

This section explains how to connect from an Apple Macintosh system to the NAS Gateway 500. Figure 13-1 shows the OS level we used. This procedure works for the normal Mac OS X version and for the Mac OS X Server version.

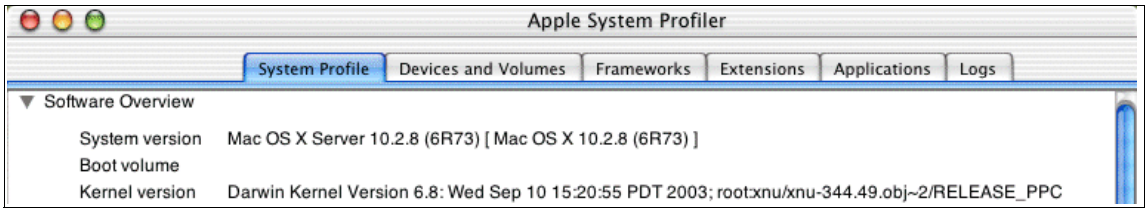


Figure 13-1 Mac OS level

First use the Finder application, select **Go** and scroll down to the **Connect to Server** entry as shown in Figure 13-2. Select that entry by clicking it.

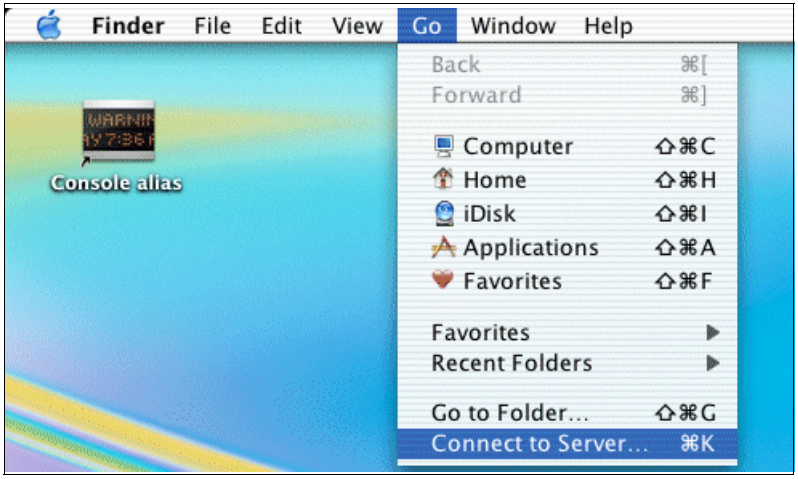


Figure 13-2 Using Finder

The Connect to Server dialog box will appear. Before you enter the NFS share, make sure to log on to the NAS Gateway 500 using telnet. When logged on, you can list the NFS shares using the commands **`exportfs`** or **`showmount -e`** to list your NFS shares. This is shown in Example 13-1.

Example 13-1 Display NFS shares on NAS Gateway 500

```
(/)-->exportfs
/Vols/FLJ1NFS -
(/)-->showmount -e
export list for FLJ1:
/Vols/FLJ1NFS (everyone)
(/)-->
```

Now type in exactly your NAS Gateway 500 NFS export:

```
nfs://<your_server_address>/<your_nfs_export>
```

An example is shown in Figure 13-3. Now click **Connect** to confirm your connection.

Figure 13-3 NFS connect dialog box

The system will connect to the NFS share exported on our NAS Gateway 500. Figure 13-4 shows our NFS share. This folder will appear on the desktop.

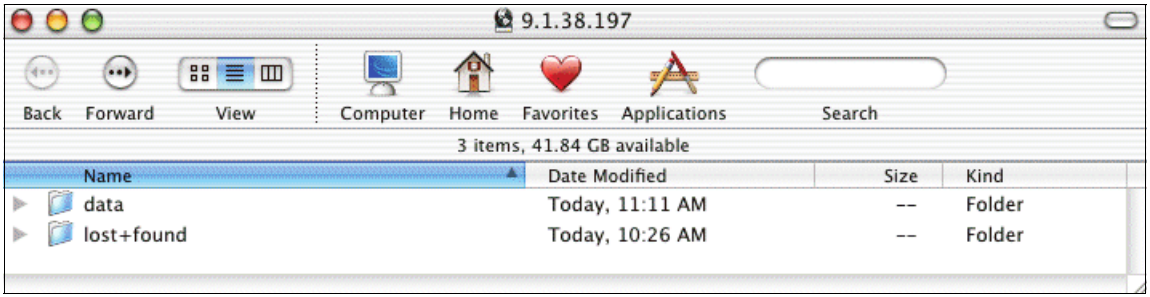


Figure 13-4 NFS share connected

In addition, the following icon will be added to the desktop (Figure 13-5), so after the initial connect, you can access the data by simply clicking that icon.

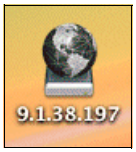


Figure 13-5 Desktop icon

Part 4

Backup and recovery

This part of the book describes how to back up and restore data and how to do disaster recovery of a NAS Gateway 500. Since this depends on which event has happened, an overall suggestion which fits for all cases cannot be offered. The range of failures that can affect your business can go from losing one file to losing the complete environment. The NAS Gateway 500 administrator must decide which action has to be taken. We show procedures that are necessary in the event of a failure.

14

Backup and restore basics and user interfaces

This chapter describes the basic tools, as well as how to back up and restore data, and how to do disaster recovery of a NAS Gateway 500.

The following topics are discussed:

- Interfaces to back up NAS Gateway 500
- Backup, restore, and disaster recovery basics

14.1 User interfaces for backup and restores

You can back up the NAS Gateway 500 in several ways. The way you should choose depends on which backup will be taken and which user interface the administrator prefers. The NAS Gateway 500 provides several user interfaces for backup and restore purposes:

- WebSM
- SMIT menu
- Command line

Basically, you can choose between WebSM, SMIT, and the command line. WebSM is a graphical user interface adjusted to specific NAS requirements. SMIT (**smitty**) is a menu driven character based interface, which enables the administrator to exploit almost all of the operating system commands AIX offers. The command line interface can be used to set up commands directly. The manual pages (**man** *command*, for example: **man mksysb**) are very useful to get a description of a command, its options and parameters . Be *careful* if you are working as the root user.

14.1.1 The WebSM interface

The backup and restore part of WebSM is divided into several areas. Launch WebSM, select the appropriate machine and the menu item **Backup and Restore**. On the right side of the window, you can see various backup and restore tasks:

- Back up the system (**mksysb**)
  See 15.2, “System backup manager (mksysb and mkcd)” on page 296.
- Incrementally back up the system (**backup**)
  See 16.1.2, “The backup and restore commands (full and incremental)” on page 334.
- System backup wizard (**mksysb** in conjunction with **mkcd** for optical media only).
- Restore file system backup
  See 15.2.2, “Restoring with the system backup manager” on page 304.
- Restore incremental backup files
  See “File system restore with the restore command” on page 337.
- View contents of full system backup
  See “View contents of a full system backup” on page 309.
- View content on incremental backup
  See “Verification of the file system backup” on page 343.

Figure 14-1 shows the WebSM Backup and Restore menu.

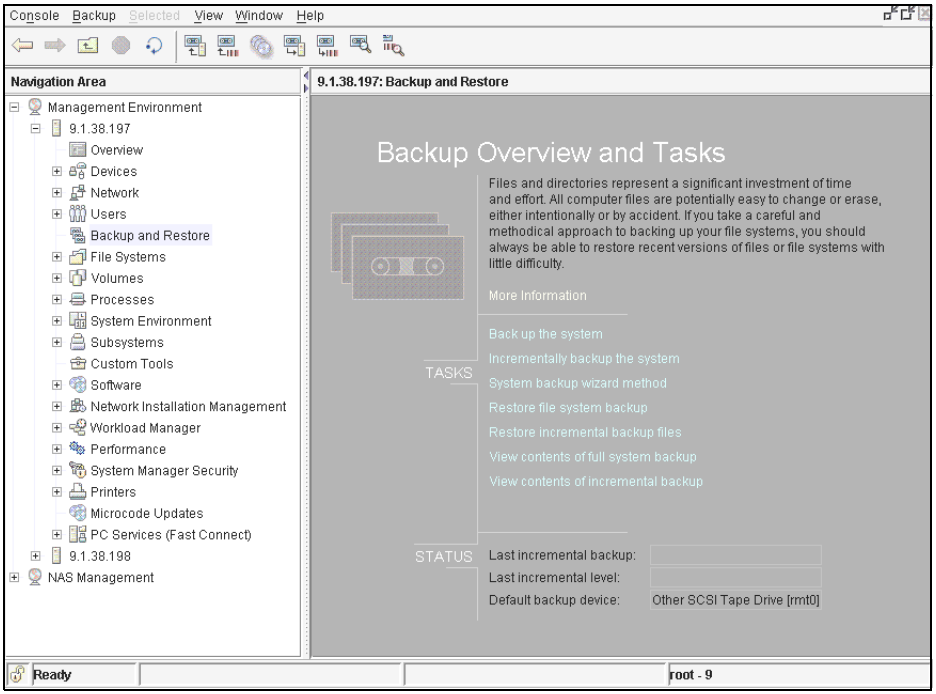


Figure 14-1 Using the WebSM for backup and restore

14.1.2 The SMIT menu

The administrator can use the SMIT menu as well to do backups. But be careful, because it depends on the user ID which interface has been provided by the system.

Using the SMIT interface and command line demands much more experience as compared to using WebSM. So please do not use the command line interface or SMIT interface if you are not familiar with the system and AIX.

The root user gets the interface shown in Figure 14-2.

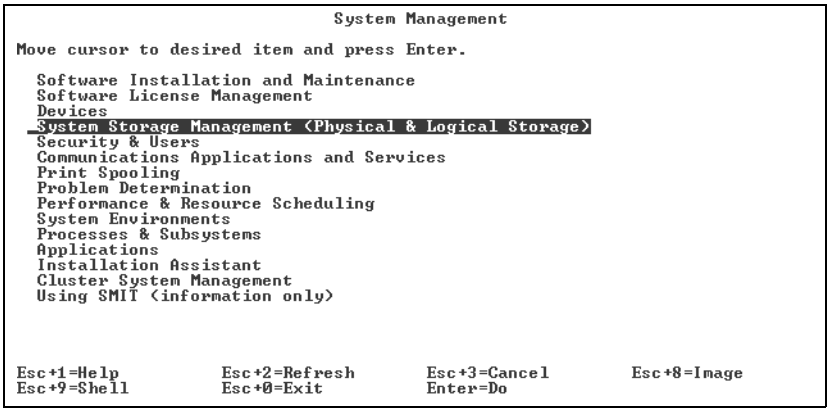


Figure 14-2 The SMIT menu entry user root

The NAS administrator is the user that was created during the initial setup (we used nasadmin). It gets a different SMIT screen (Figure 14-3).

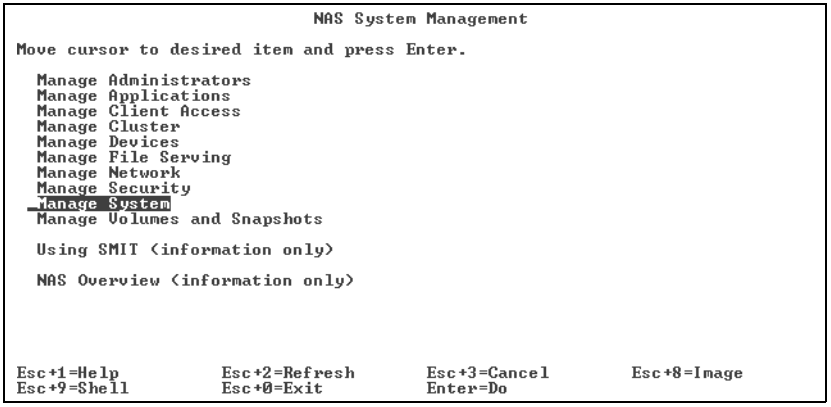


Figure 14-3 The SMIT menu of the NAS Administrator

14.1.3 The command line interface

The command line interface is the third interface to the NAS Gateway 500.

Restriction: It is not supported to do the initial configuration with the command line interface or SMIT. You have to use the WebSM interface.

Using the SMIT interface and command line interface demands much more experience as compared to the WebSM. So please do not use the command line interface or SMIT interface if you are not familiar with the system or AIX.

More information about how to use the particular interfaces is provided in the following sections by giving examples.

14.2 Fundamental backup and restore techniques

Before we start with our technical explanation, we present a summary of backup and restore types and their classification. We applied the following classifications to the NAS Gateway 500 in the next chapter.

There are three major backup categories:

- Bootable backups and restores:
  - System backup manager (root volume group)
  - Recovery CD images
  - NIM (Network Install Manager)
  - SysBack™ (IBM Tivoli Storage Manager for System Backup and Recovery)
- File, file system and volume backup and restore:
  - Operating system based backup tools:
    - **mknasb** / **restnasb** commands
    - **backup** / **restore** commands (full and incremental)
    - **restvg** / **savevg** (other volume groups)
    - Split mirror backup
    - **backsnap**, **snapback** (JFS2) commands
    - **dd**, **cpio**, **tar**, **pax**, and other operating system commands
  - IBM Tivoli Storage Manager Client backup and restore:
    - LAN based backup
    - LAN free backup
  - Disk subsystem based backups:
    - FlashCopy® (t0 copy, snapshot) (not covered in this redbook)
  - SANergy® (not covered in this redbook)
- Application backup and restore:
  - Backup agents used to back up applications (for example, IBM Tivoli Data Protection, Oracle RMAN, DB2 userexit, etc.) (not part of this redbook)

These three classes are described in the following sections in more detail.

15

Bootable backups and restores

A bootable backup allows you to restore a system from scratch by booting from the media where the image resides. This implies that the media has a section which can be read by the bootstrap loader. Therefore, a bootable image enables you to set up the NAS Gateway 500 as new, even if a new entire system or parts of the system, such as new disks, are provided.

This might occur, for example, during hard disk failure or human error, when the problem cannot be fixed with any other method (such as when there is an accidental delete of important system files from the system). The system administrator would then need to recover the operating system from scratch within the shortest time period, and restore the application data back to the system to resume normal operations.

15.1 Overview: bootable backup/restore

This step is one part of recreating the whole system (including the user data). The bootable restore creates a new image into the boot section followed by the rest of the system data. The NAS Gateway 500 uses hdisk0 for this purpose.

In most cases, when you restore a backup including the boot sector, you are not done with that. The image restore is just a part of the whole restore, because file, file system, and application restores may follow.

Bootable backups and restores can be:

- System backup manager (**`mksysb`** and **`mkcd`**)
- Bootable image (Recovery CD) provided by the NAS Gateway 500
- Network Install Image (NIM)
- Bare Machine Recovery Tools (BMR)
  (IBM Tivoli Storage Manager for System Backup and Recovery “SysBack”)

Important: Test the backup extensively before you start a production environment. Do not trust that you have done the backup by simply observing a return code of a command. You should restore the backup before going into production.

15.2 System backup manager (mksysb and mkcd)

In this section we discuss how to use the system backup manager for backup and restore.

15.2.1 Backup with the system backup manager (mksysb)

The system backup manager (command **mksysb**) creates a system backup image on a specified device. You may use a system backup image to restore your system to a previous state, including the creation of the boot image and/or to restore just files.

The **mksysb** backup image contains all details to rebuild the system volume group (*rootvg*). Other volume groups are *not* covered with this command and should be backed up through other commands (for example, **savevg, savevg4vp** and **restvg, restvg4vp**) or applications (IBM Tivoli Storage Manager, etc.)

The **mksysb** command creates an installable image of the root volume group either in a file or onto a bootable tape. The command is usually used to create a bootable tape or to create an image used in conjunction with NIM or **mkcd**. The **mksysb** command backs up mounted file systems in the rootvg volume group for subsequent reinstallation.

Tip: It is a good idea to do **mksysb** backups on a regular basis and after reconfiguring, adding new devices, etc. This keeps the restore and recovery process quicker and easier.

Depending on which option is used, the **mkszfile** command is run and creates the /image.data file which contains information on the root volume group. **mkszfile** records the size of mounted file systems in the rootvg volume group for reinstallation.

There are three ways to execute **mksysb**:

- WebSM interface
- SMIT interface
- Command line interface

Using WebSM to exploit mksysb

One way to use **mksysb** is provided by the WebSM interface. Use your WebSM client and logon to the NAS Gateway 500 as root.

In the WebSM screen, choose the appropriate NAS machine under **Management Environment** and select **Backup and Restore** in the Administration tree (Figure 15-1).

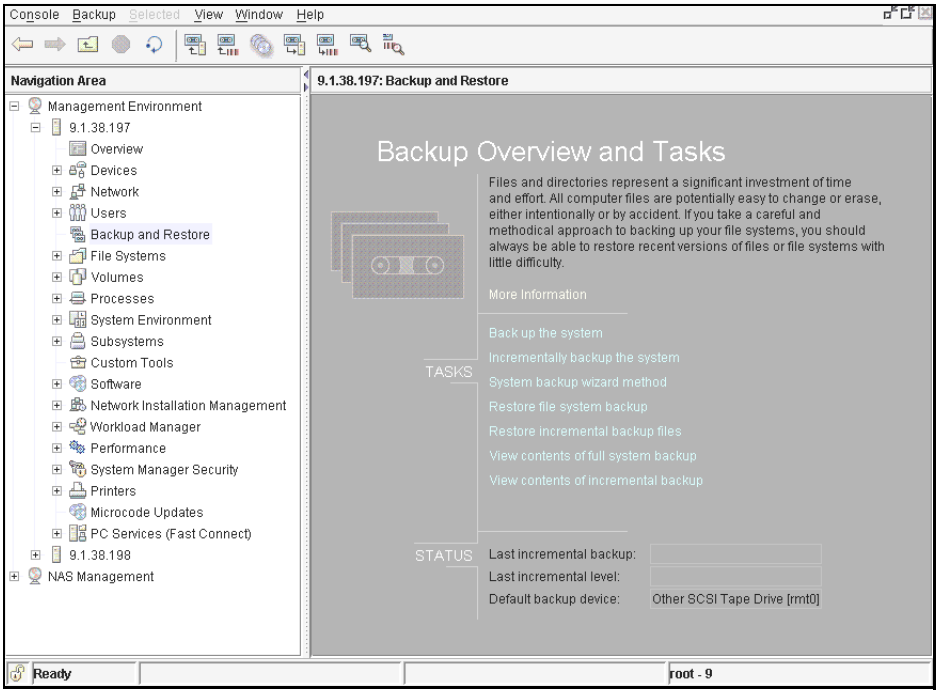


Figure 15-1 WebSM Backup the System via mksysb

Then click **Backup the system**. Now you can choose the appropriate options (Figure 15-2). Some options are listed here:

- Specify the correct device for the backup.
  We used: Other SCSI Tape Drive [rmt0]
- Create map files
  Creates map files, runs **`mkszfile`** command to create /image.data file
- Generate image.data file (default)
- Expand /tmp as needed
  The /tmp file system may need to be extended for the boot image if you are creating a bootable backup to tape.
- Exclude files from backup
  Can be selected to exclude files (option uses file /etc/exclude.rootvg).

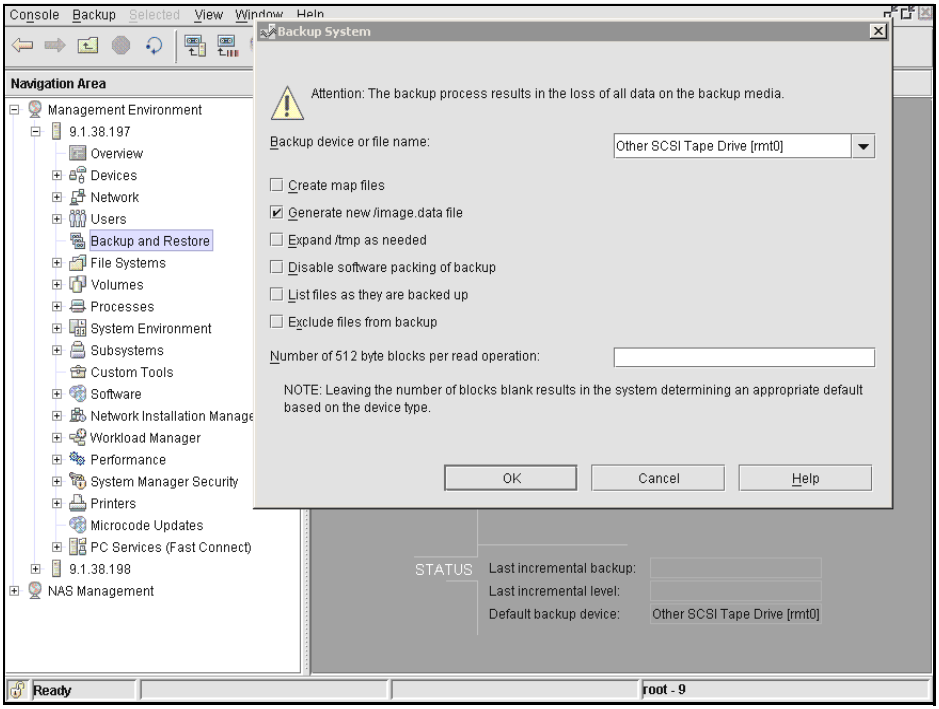


Figure 15-2 System backup options menu

After you choose **OK**, a new popup window tells you that the task is performing. Choose the **Show Details** button for more information (Figure 15-3).

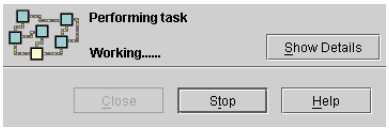


Figure 15-3 Performing task system backup

Finally, you should get a message that the task ended successfully. Before going into production, you should always test if the restore of a backup was successful (Figure 15-4).

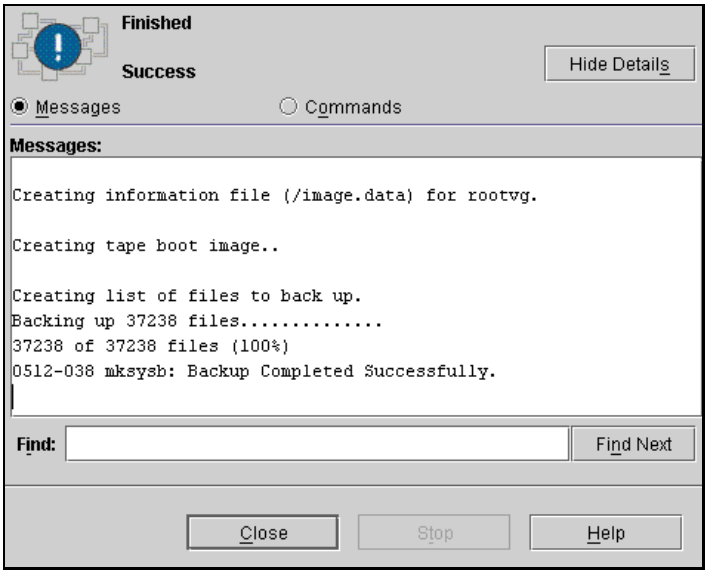


Figure 15-4 Details of system backup task

Using SMIT to exploit mksysb

As described in 14.1.2, “The SMIT menu” on page 291, you should be very careful using the SMIT interface as root. The following section shows how a bootable backup can be provided with the SMIT interface.

First log on to the system as the NAS administrator (at the initial configuration, we used **nasadmin**) and type **smit** and press Enter. Refer to the following screens to access the system backup task.

Choose **Manage System** and proceed as described in Figure 15-5.

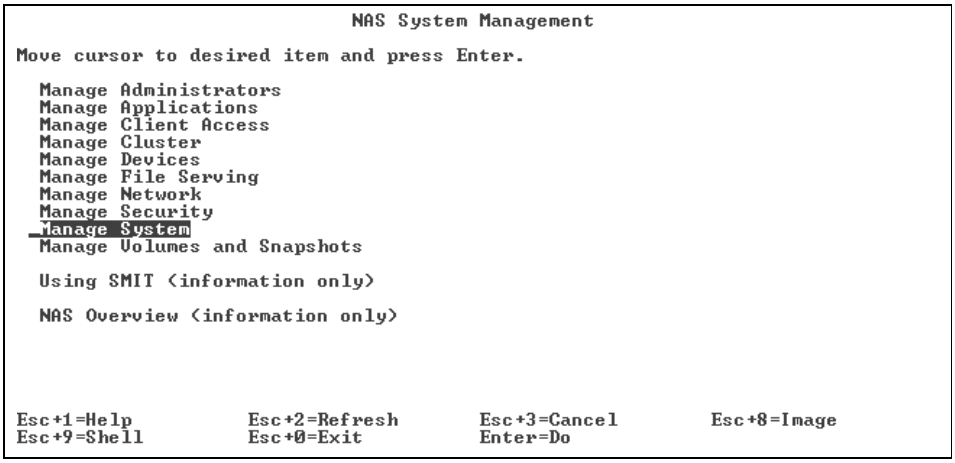


Figure 15-5 SMIT menu entry for bootable backups

The **Backup and Recovery** item will pass you to the next screen (Figure 15-6).

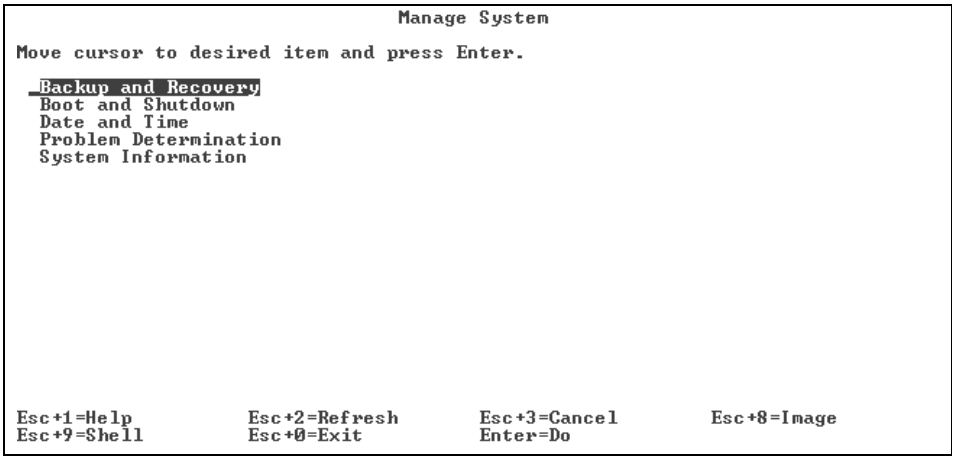


Figure 15-6 SMIT backup and recovery

Select **Backup and Recovery** and press Enter. The screen shown in Figure 15-7 will appear.

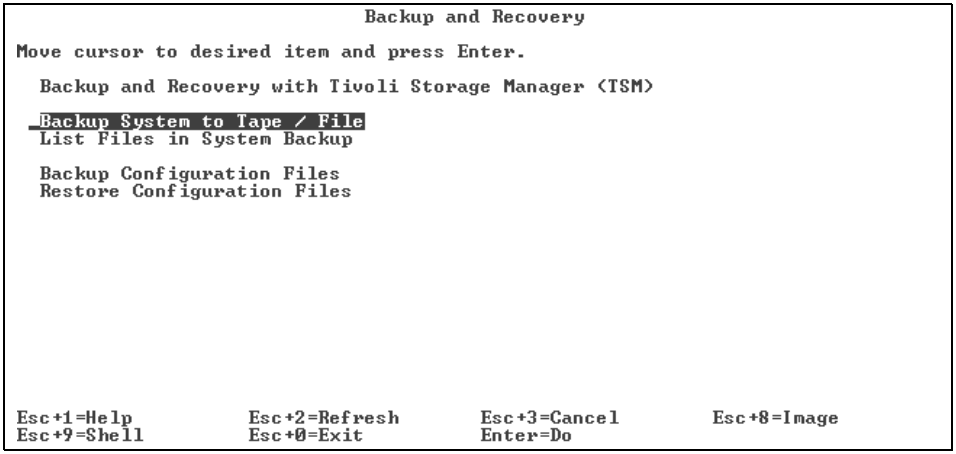


Figure 15-7 SMIT Backup the System to Tape / File

Select **Backup System to Tape / File** and proceed. This will take you to the **mksysb** screen (Figure 15-8). Press Enter to proceed. Wait for the backup to finish (Figure 15-9).

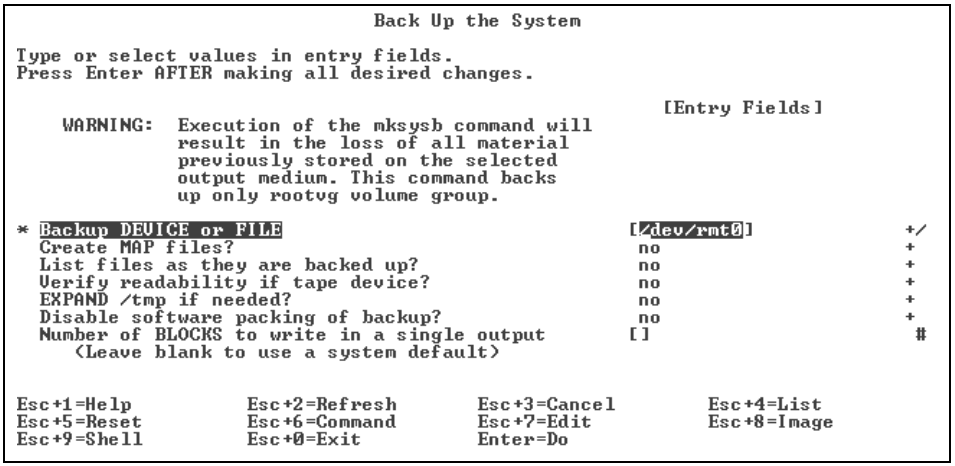


Figure 15-8 SMIT mksysb task

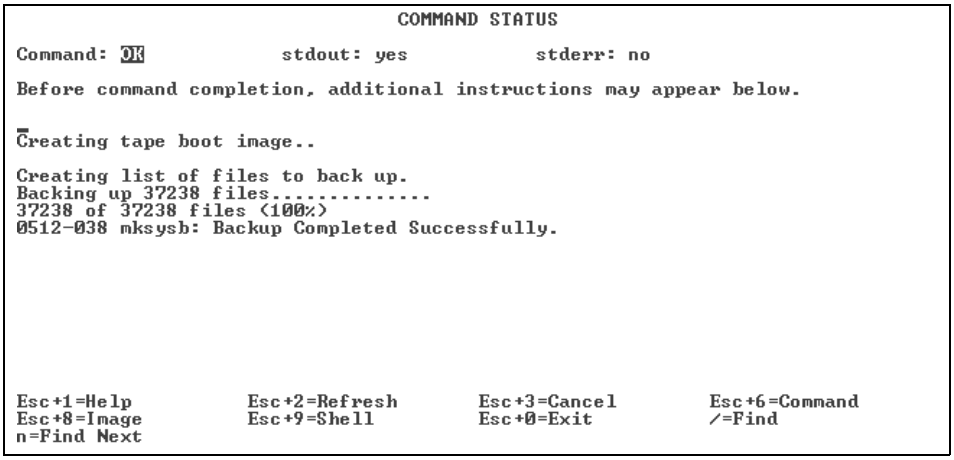


Figure 15-9 status of a completed mksysb backup with SMIT

Using the command line to exploit mksysb

The **mksysb** command can be run on the command line. You can use the NAS administrator user to exploit the **mksysb** command (Figure 15-10).

Tip: You may use the -e (expand) option if you have space problems in the /tmp directory during the backup regarding too little space.

Command syntax:

mksysb [-b Number] [-e] [-i] [-m] [-p] [-v] [-V] [-X] Device |File

-b block number of 512 byte blocks
-e excludes files
-i creates /image.data (runs mkszfile)
-m generates map files (will call mkszfile command as well)
-p packaging
-v verbose lists all backed up files
-V verification verifies the header (not the complete backup)
-X expands automatically /tmp file system
Device | File specifies the location either device or file

```
$ mksysb -i /dev/rmt0

Creating information file (/image.data) for rootvg.

Creating tape boot image..

Creating list of files to back up.
Backing up 37222 files.............
37222 of 37222 files (100%)
0512-038 mksysb: Backup Completed Successfully.
$
```

Figure 15-10 mksysb backup done on the command line

Example (backup to image file system - not bootable):

To generate a system backup file named /mksysb_images/nasnode01 and a new /image.data file for that image, type:

```
mksysb -i /mksysb_image_files/nasnode01
```

Note: This file will not be bootable and can only be installed using Network Installation Management (NIM).

Using the NAS administrator to back up (**mksysb**) to a file may abort, because of the restricted shell. Make sure that the path exists and enough space is available. If you have problems regarding the restricted shell, you may use root.

15.2.2 Restoring with the system backup manager

If a system has to be restored with a **mksysb** image, all data on the devices (hdisk0) will be lost.

mksysb on tape: whole system restore with new boot sector

You can easily restore a system with an image residing on a tape. The tape used for the restore must have a bootable image on the media. First mount the tape into a tape drive. (We used a tape drive attached to the on board SCSI Port on the back of the NAS node.)

Hook up with a serial port connection to the NAS Gateway 500, and power on the node. Use the procedure described in 15.3, “Recovery using the Recovery CDs” on page 311 to boot from tape and restore the system.

mksysb on tape: restore without creating boot image

Restoring a **mksysb** image means it is not mandatory to restore the boot sector. The administrator can even restore the system by files or file systems. The following two examples show how we did a restore of all files in a file system and a restore of a single file from the **mksysb** image.

Example 1: Restore of a complete file system

Attention: Restoring the root file system implies not restoring all other file systems. Be sure to choose the file systems that need to be restored.

The following screen captures show how we restored a complete file system (for example, restore of /home file system). The example shows how we did a restore of the /home file system. Actually we did not overwrite the existing /home file system, we restored the data in the /tmp directory.

In WebSM, we chose **Backup and Restore -> Restore file system backup** (Figure 15-11).

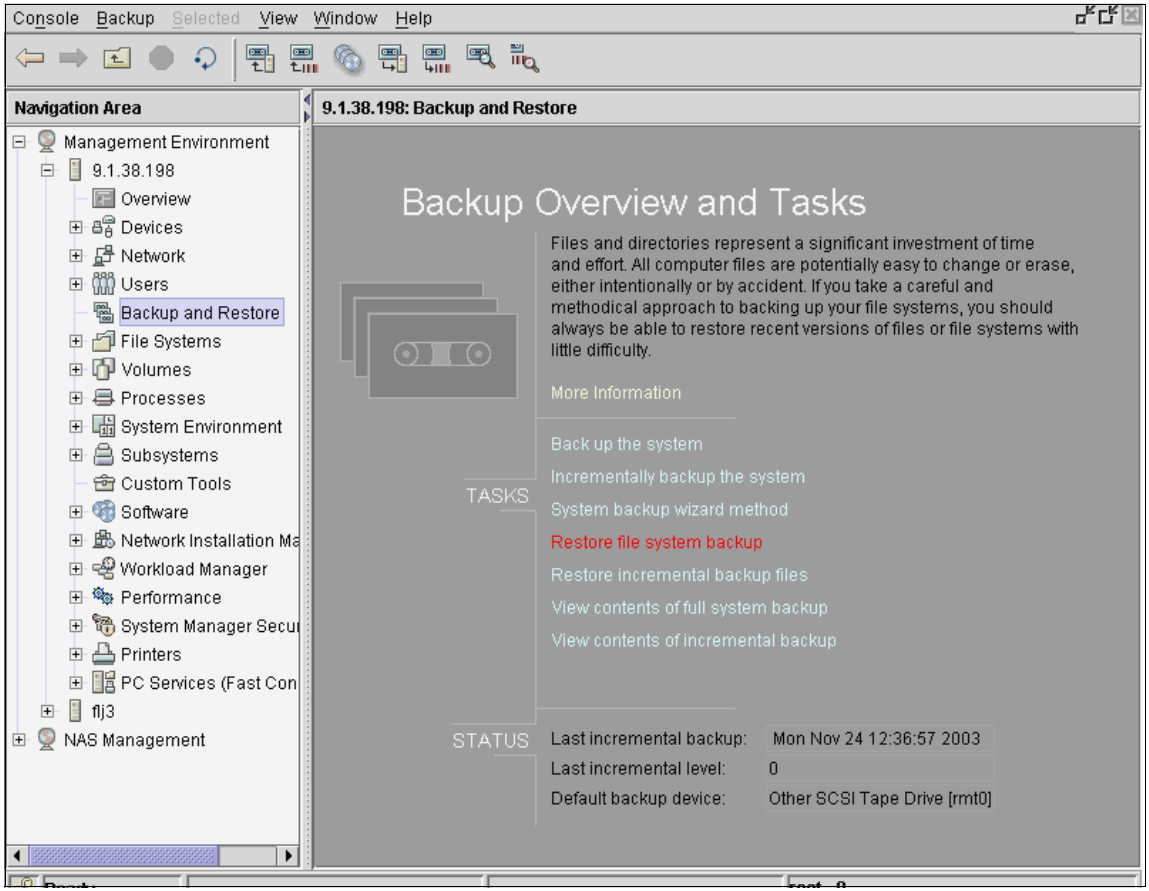


Figure 15-11 Restore full file system from system backup image

We specified the /home file system (./home) to be restored. Because we did not want to overwrite the existing data, we restored to a different location (/tmp). See Figure 15-12 and Figure 15-13.

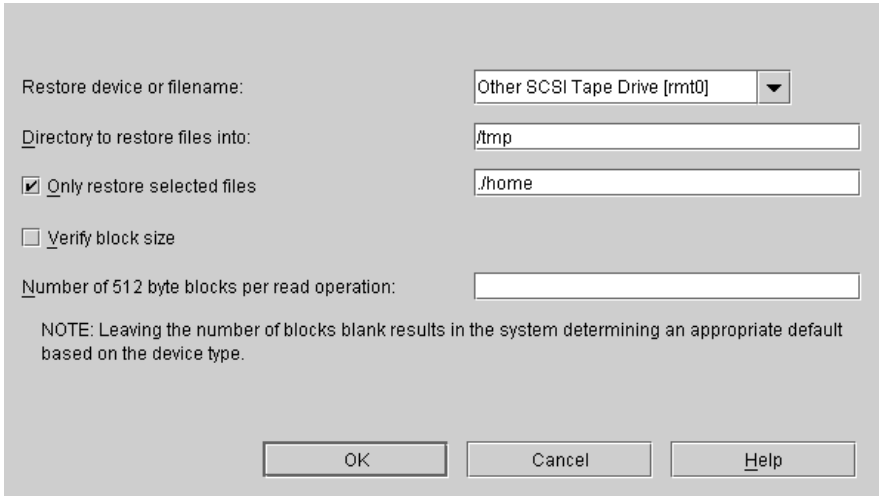


Figure 15-12 Restore file system options

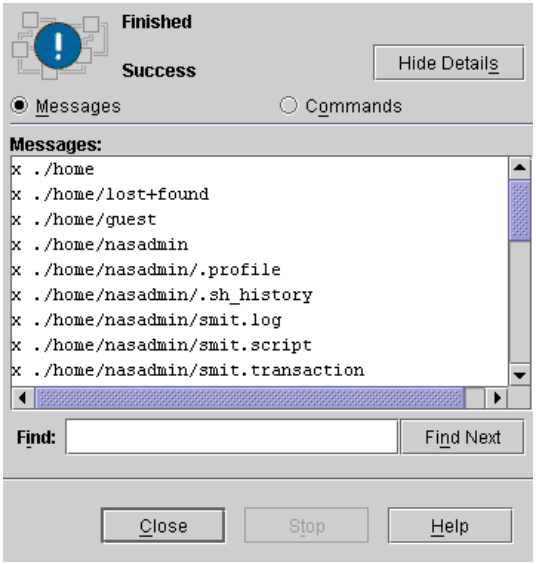


Figure 15-13 Successfully restored full file system

Example 2: Restore of single files

For this operation we chose the WebSM interface.

The **mksysb** can used to restore single files from a backup. This means, not the whole system has to be restored, just particular files can be chosen.

The following example shows the restore of a single file from the system backup. We chose WebSM to do the restore.

We backed up our system containing the file /hone/user01/userfile.txt (Figure 15-14).

```
(/home)--)ls -al user*
user01:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 14:25 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..
-rw-r--r--   1 root     system           19 Nov 17 14:25 userfile.txt

user02:
total 0
drwxr-xr-x   2 root     system          256 Nov 17 14:27 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..
(/home)--)_
```

Figure 15-14 Preparation for the backup and restore of a single file

After creation of the file, we backed up the entire system with WebSM -> **Backup and Recovery -> Back up the system**. After successfully completed, we deleted the file /home/user01/userfile.txt just for testing purposes (Figure 15-15).

```
(/home/user01)--)ls
(/home)--)ls -al user*
user01:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 14:25 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..
-rw-r--r--   1 root     system           19 Nov 17 14:25 userfile.txt

user02:
total 0
drwxr-xr-x   2 root     system          256 Nov 17 14:27 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..
(/home)--)rm /home/user01/userfile.txt
(/home)--)ls -al user*
user01:
total 0
drwxr-xr-x   2 root     system          256 Nov 17 14:39 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..

user02:
total 0
drwxr-xr-x   2 root     system          256 Nov 17 14:27 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..
(/home)--)_
```

Figure 15-15 File deleted prior to restore from system backup

In WebSM we opened the **Backup and Recovery -> Restore file system backup** panel (Figure 15-16).

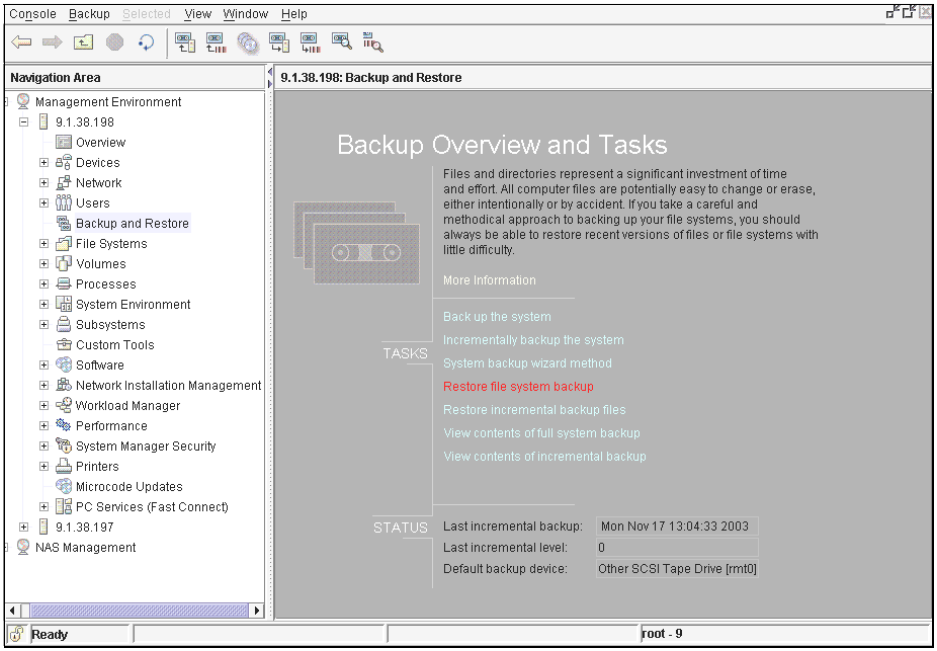


Figure 15-16 Restore file system backup

We specified the directory where the restore should be copied to (/home/user02) and the file we wish to restore (Figure 15-17).

Tip: Use the dot (.) in the path and specify the file which should be restored.

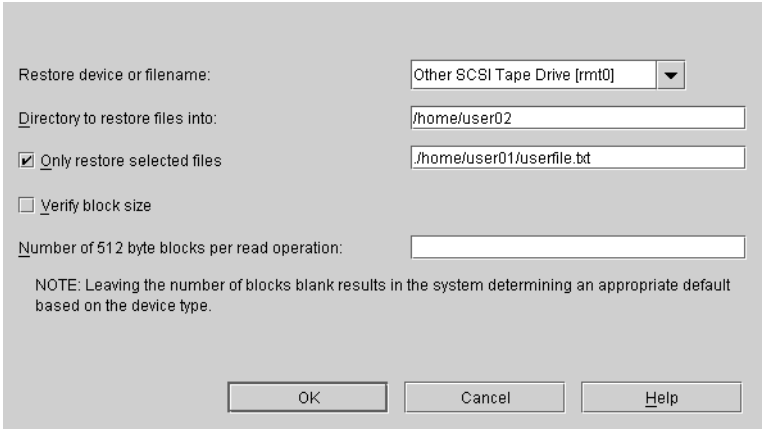


Figure 15-17 Specify copy to destination and source (object) to be restored

A successful completion message should appear (Figure 15-18).

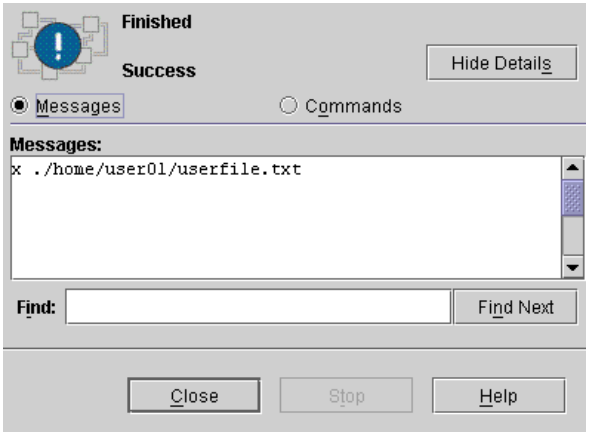


Figure 15-18 Restore of single file completed

Finally, verify that the file has been restored (Figure 15-19).

```
(/)--)ls -alR /home/user01
total 0
drwxr-xr-x   2 root     system          256 Nov 17 14:39 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..
(/)--)ls -alR /home/user02
total 0
drwxr-xr-x   3 root     system          256 Nov 17 14:42 .
drwxr-xr-x   9 bin      bin             256 Nov 17 14:27 ..
drwxr-xr-x   3 root     system          256 Nov 17 14:42 home
/home/user02/home:
total 0
drwxr-xr-x   3 root     system          256 Nov 17 14:42 .
drwxr-xr-x   3 root     system          256 Nov 17 14:42 ..
drwxr-xr-x   2 root     system          256 Nov 17 14:42 user01

/home/user02/home/user01:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 14:42 .
drwxr-xr-x   3 root     system          256 Nov 17 14:42 ..
-rw-r--r--   1 root     system           19 Nov 17 14:25 userfile.txt
(/)--)_
```

Figure 15-19 Verification of completed single file restore

View contents of a full system backup

This section shows an example of viewing the contents of a backup. The administrator can check which files reside on the backup device. The following example shows this by means of WebSM.

Choose **View contents of full system backup** in WebSM (Figure 15-20).

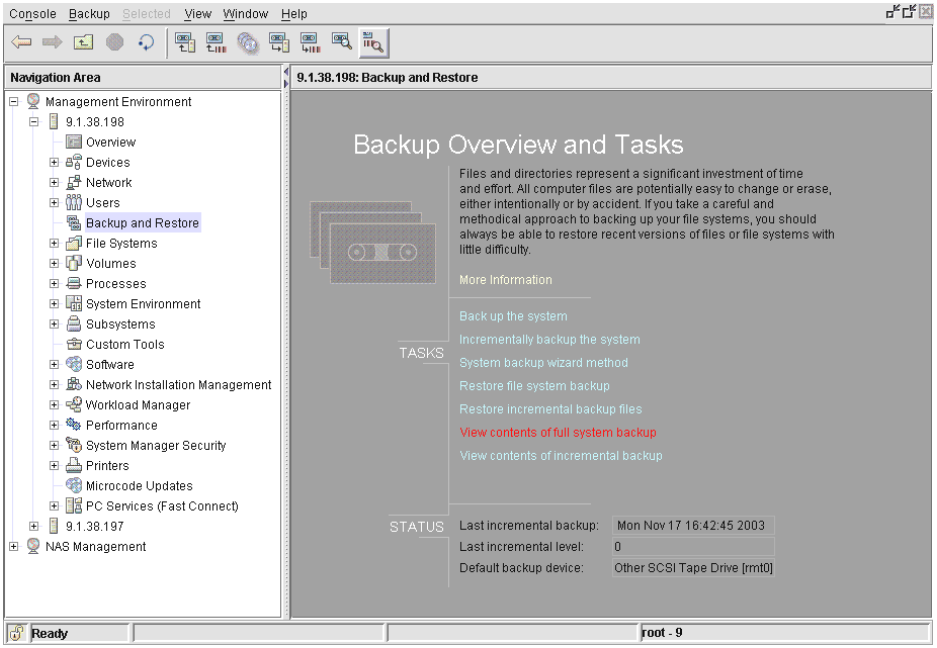


Figure 15-20 WebSM view contents of full system backup

Select the appropriate options in the screen shown in Figure 15-21.

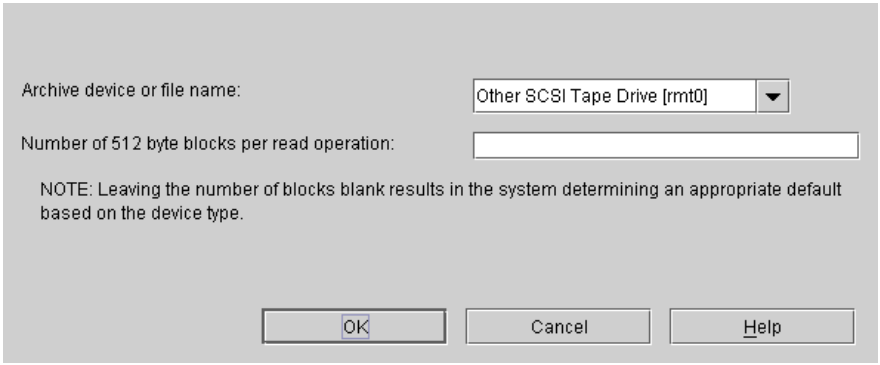


Figure 15-21 View contents of system full backup specify options

Browse the results of this task (Figure 15-22).

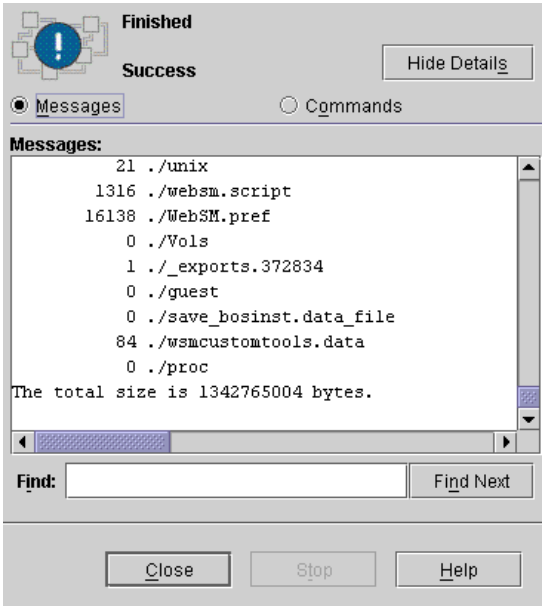


Figure 15-22 result of view contents of full system backup

15.3 Recovery using the Recovery CDs

If you find that your NAS Gateway 500 develops operating problems that cannot be repaired using the CLI or WebSM, you can restore the system to the factory default configuration. It was delivered with a set of bootable Recovery CDs. By booting the NAS Gateway 500 with those CDs, the internal disks will be completely erased and the factory preload will be put on the disk. Keep in mind that you have to reconfigure or restore from other tools or applications to get your system into the production state.

Important: After reloading the NAS Gateway 500, you have to connect to it with a browser and accept the licensing terms. If you don't do this, you will not be able to connect to the NAS Gateway 500 using any configuration tool.

To start the recovery procedure of the NAS Gateway 500, it is necessary to direct the NAS Gateway 500 to boot from the Recovery CDs.

The procedure varies depending on the powered state of the NAS Gateway 500.

15.3.1 The system is powered off

Power on the NAS Gateway 500 and insert the Recovery CD #1 into the CD-ROM device. Connect through the serial port using an ASCII terminal and observe the startup sequence of the SAN Gateway 500 (Figure 15-23).

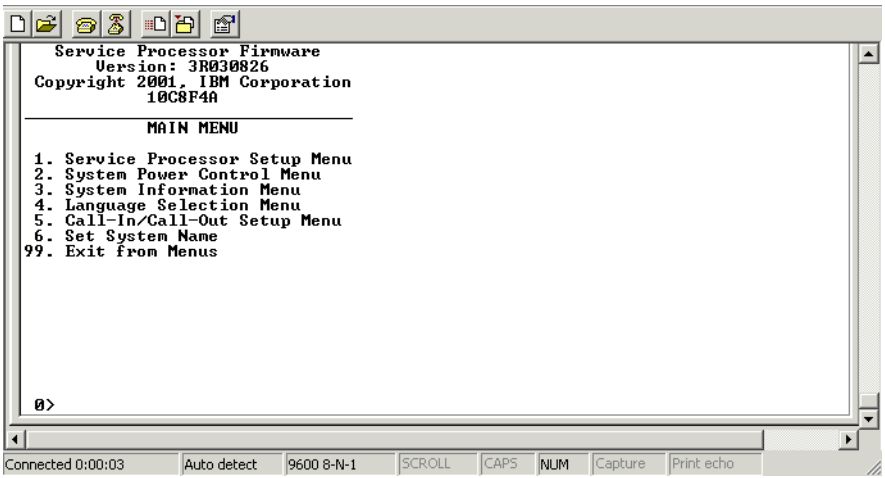


Figure 15-23 NAS Gateway 500 Startup sequence

As the system goes through the startup sequence, it shows the POST codes (Figure 15-24).

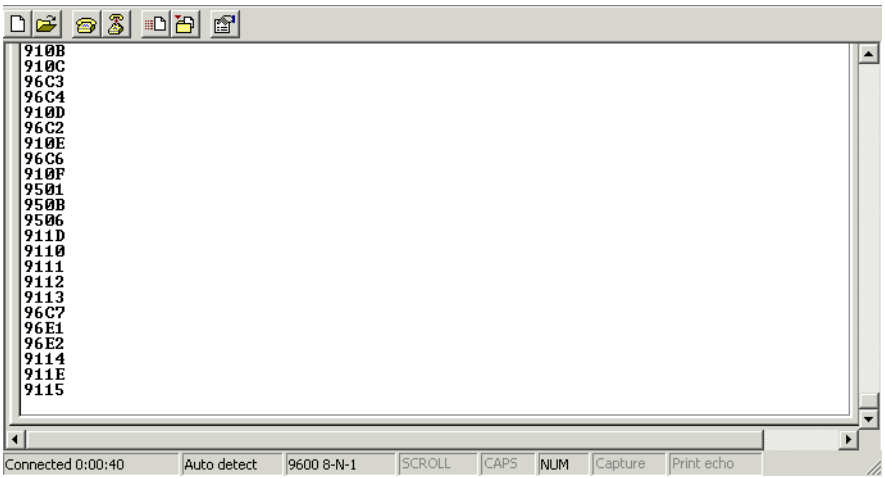


Figure 15-24 POST codes

After the POST sequence is completed, the system starts detecting hardware devices. The last devices shown before the Options list are Fibre Channel adapters, as shown in Figure 15-25.

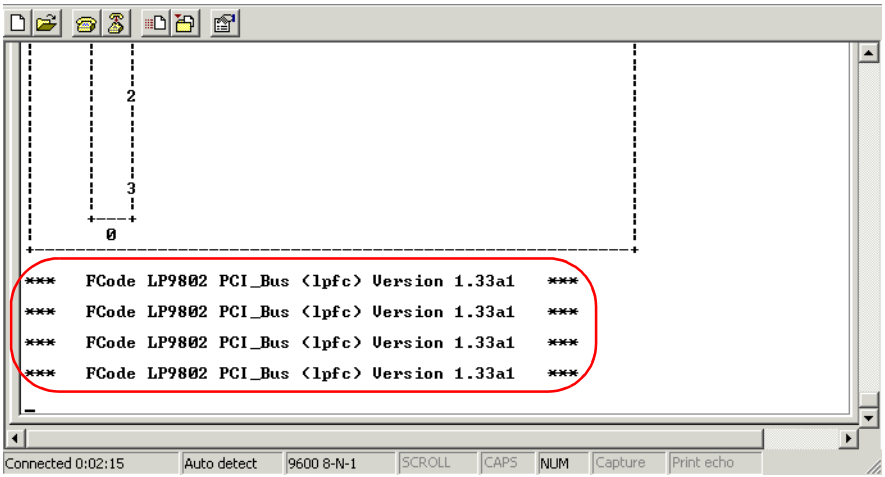


Figure 15-25 Hardware detection - Fibre Channel adapters

After the keyboard indicator is displayed on the console (you will hear the first beep) and before the last indicator (speaker) displays, press the numeric 5 key on the ASCII terminal to indicate that a default boot list should be temporarily modified (Figure 15-26).

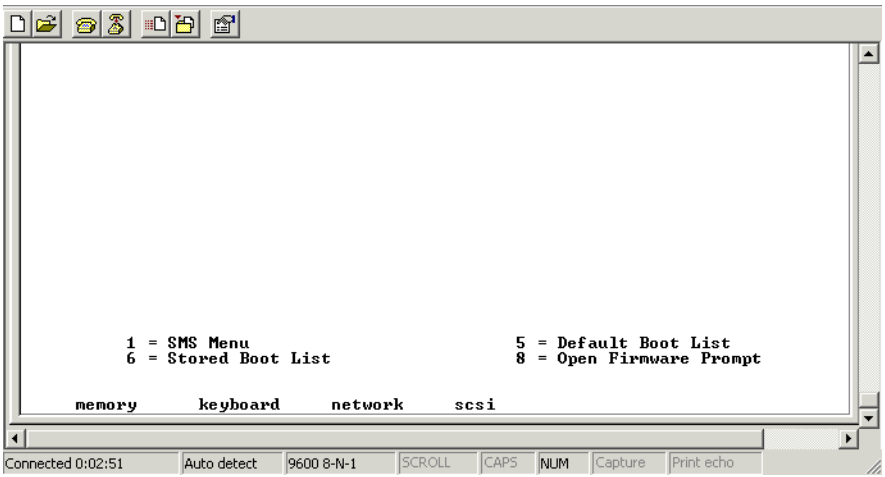


Figure 15-26 Options list

The system will start the recovery procedure (Figure 15-27).

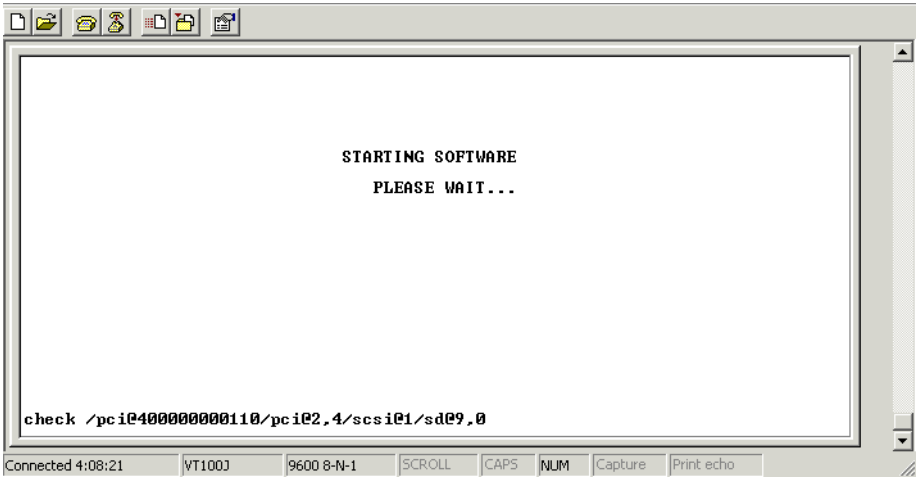


Figure 15-27 Starting software from CD

You can double-check if it is booting from the CD-ROM by looking at the line in the terminal starting with the booting device (Figure 15-28).

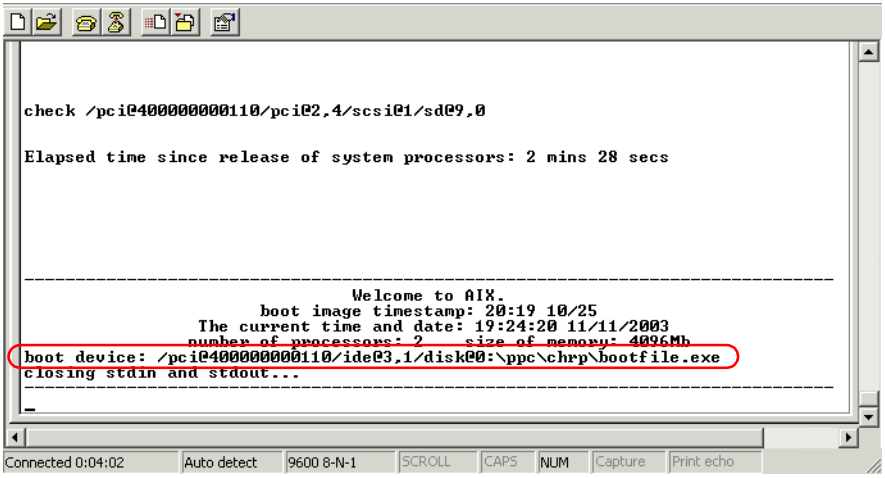


Figure 15-28 Booting from CD-ROM

Note: If the system does not boot from the CD-ROM but boots from the hard drive instead, there is a problem with the media or the CD-ROM drive. Check if the media is correctly inserted and undamaged. Reinsert the media or replace the media and start again.

Select the terminal by pressing 1 and Enter (Figure 15-29).

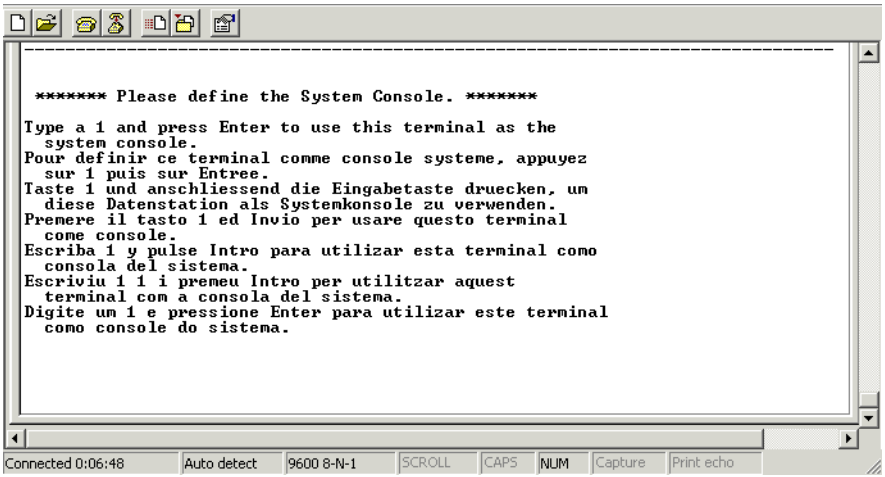


Figure 15-29 Terminal selection

The system starts to load the code from the Recovery CD (Figure 15-30).

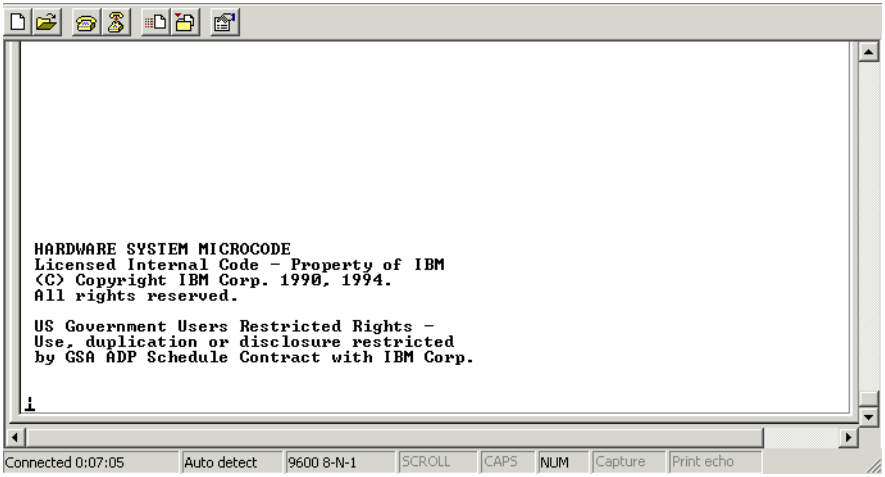


Figure 15-30 Loading installation code from the CD

The recovery procedure starts and prompts you to select the language. Press 1 and Enter to continue (Figure 15-31).

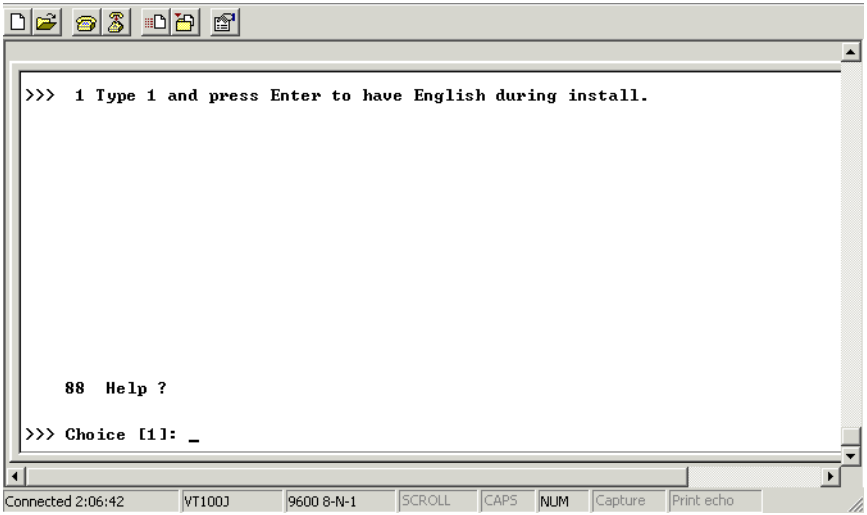


Figure 15-31 Language selection

On the Installation and Maintenance panel, press 1 to select the installation with default settings and confirm it by pressing the Enter key (Figure 15-32).

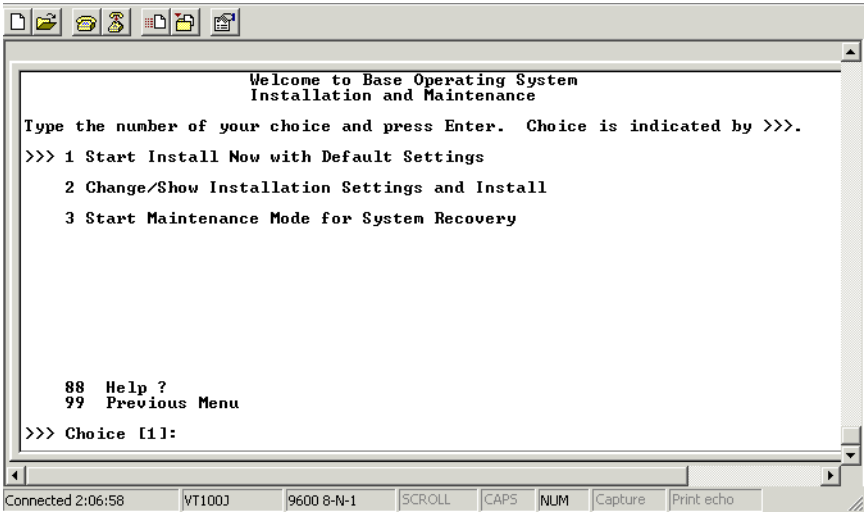


Figure 15-32 Installation and Maintenance panel

The selected option will be shown on the summary panel. To start the recovery procedure, confirm the choices by pressing 1 and Enter (Figure 15-33).

Important: Proceeding beyond this point will erase all data on the internal hard disk of the NAS Gateway 500.

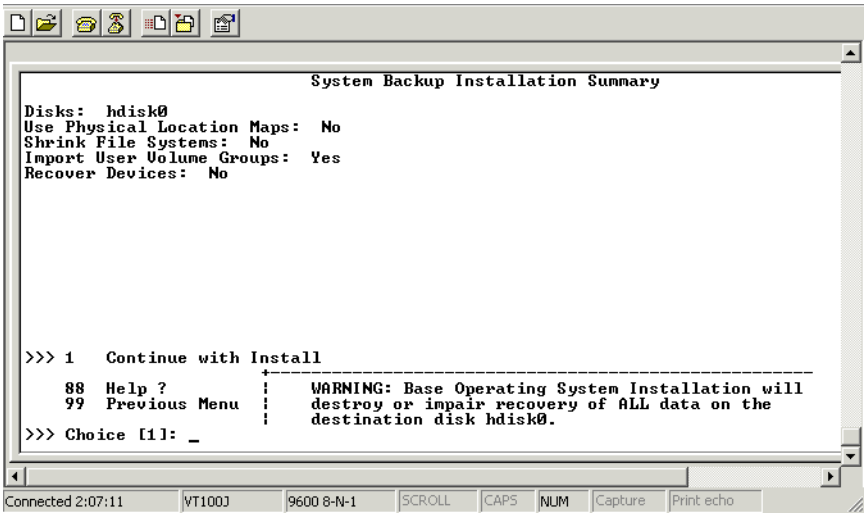


Figure 15-33 System Backup Installation Summary

The system loads the image. The progress of the recovery procedure is shown in percentage and elapsed time in minutes (Figure 15-34).

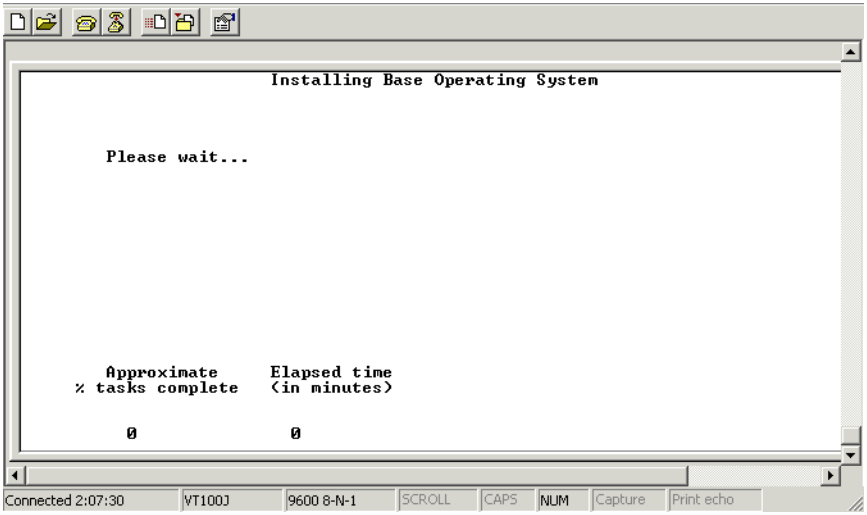


Figure 15-34 Progress indicator

When Recovery CD #1 is complete, it prompts you to insert Recovery CD #2. Continue by pressing the Enter key (Figure 15-35).

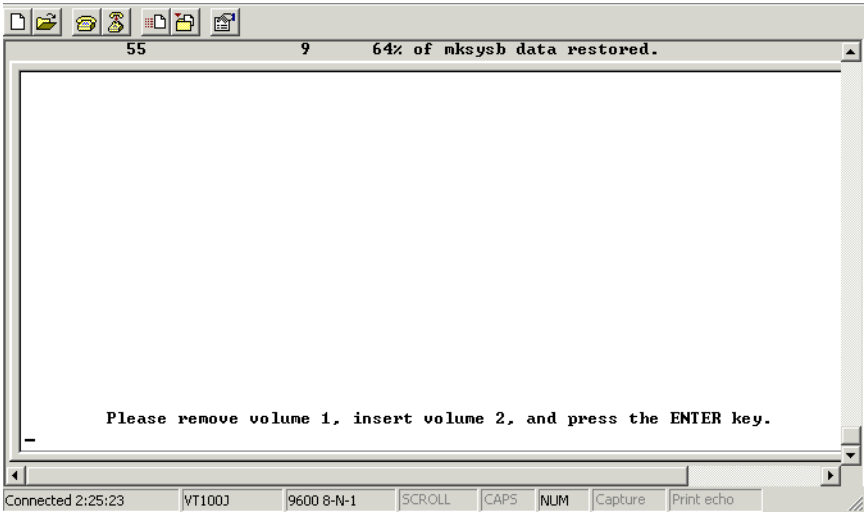


Figure 15-35 Prompt for Recovery CD #2

After the install is complete, the system reboots automatically.

15.3.2 The system is powered on

Insert the Recovery CD-ROM and run the following commands:

```
boot list -m normal cd0 hdisk0
shutdown -Fr
```

The NAS Gateway 500 shuts down and boots from the media in the CD-ROM drive (Figure 15-36).

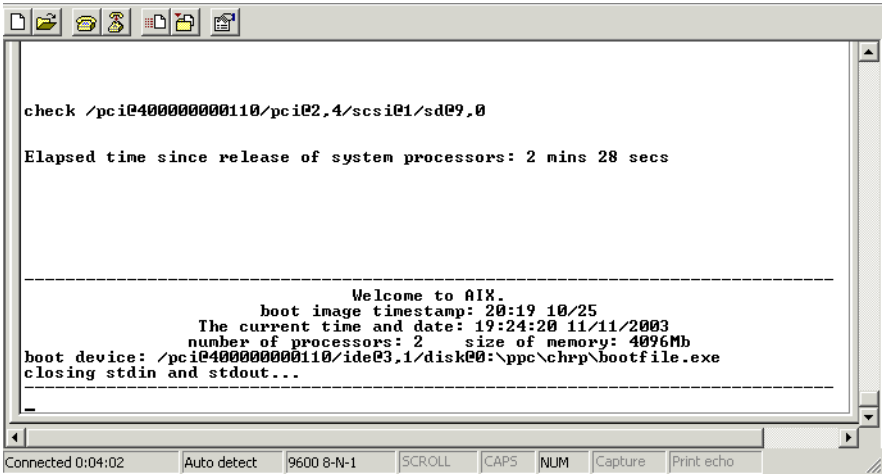


Figure 15-36 Booting from CD-ROM

The rest of the procedure is done exactly as if the machine were in the powered-off state. For detailed steps, please refer to “The system is powered off” on page 312.

15.4 Network Install Manager (NIM)

In this section we discuss the Network Install Manager features that you can use with the NAS Gateway 500.

15.4.1 NIM basics

NIM is a very flexible way to back up and restore system data and to maintain software levels. NIM permits the installation and maintenance of AIX, its basic operating system, and additional software and fixes that may be applied over a period of time over a network. As a result, NIM has eliminated the reliance on tapes and CD-ROMs for backups by exploiting a server and the network for doing backups. NIM will allow one machine to act as a master in the environment. This machine will be responsible for storing information about the clients it supports, the resources it or other servers provide to these clients, and the networks on which they operate.

As described before, using the NIM feature assumes a NIM master (server) to be installed. The NIM master server stores data, and NIM clients access this server to read or write their data. A NIM server can be primary or secondary (redundancy). NIM image data of NIM Clients can be copied to the NIM Server or shared via NFS.

The principal workflow of a NIM based backup starts with a a system backup by using **mksysb** to create the system backup image files to keep on the disk spaces. The disk space in here may be a local file system on an AIX machine, then you FTP the backup image files to the NIM server. Otherwise, you create a network file system on a NIM server, then export the NFS to another AIX machine for use as the file system to keep the system backup images. To restore the bare machine, do a network boot to the NIM server, then restore the NAS system software from the system backup images, which were kept on the hard disk of the NIM server

15.4.2 NIM installation and configuration

First do the basic setup of the NIM Server (AIX machine) including the code for the NIM master (bos.sysmgt.nim.master file set) and file sets for the client.

Configure the master and define resources (fastpath: **smitty nim_config_en**v).

To define the NAS Gateway 500 as NIM clients, you can even configure the NIM client on the master (fastpath: **smitty nim_mkmac**). Next, you install bos.sysmgt.nim.client and then run the **smitty niminit** fastpath on the NAS Gateway 500.

Install clients using the **smitty nim_bosinst** fastpath on the master machine. If the clients are not running, set Initiate reboot and installation now? to NO and press Enter. Then, go to the clients and boot into a firmware menu. If the client is running, set Initiate reboot and installation now? to YES and press Enter. It will be rebooted; the install menus will be shown, and you can then proceed with the install.

More information can be obtained from the *Network Installation Management Guide and Reference*.

15.5 SysBack for Bare Machine Recovery

This section offers a brief introduction into the IBM Tivoli Storage Manager for System Backup and Recovery, also known as SysBack. For more in-depth coverage, please refer to the following sources: *IBM Tivoli Storage Manager: Bare Machine Recovery for AIX with SYSBACK*, REDP-3705, and to Chapter 20 “Bare Machine Recovery” from the *IBM Tivoli Storage Manager Implementation Guide,* SG24-5416.

15.5.1 SysBack introduction

IBM Tivoli Storage Manager for System Backup and Recovery will be referred to as *SysBack* within this book.

SysBack provides facilities to perform Bare Machine Recovery from tape. The purpose of this part is to show how SysBack may help to protect systems integrated with IBM Tivoli Storage Manager to protect from catastrophic server failures

IBM Tivoli Storage Manager for System Backup and Recovery provides system administrators and other system users with a simple, efficient way to back up and recover data from a command line or a SMIT menu-driven interface. SysBack lets you recover all or part of the system. SysBack is also flexible; you can install one system installation image to another system with either identical or different hardware configurations called “cloning”.

IBM Tivoli Storage Manager for System Backup and Recovery (SysBack) is an optional tool which can be used to back up the system. The tool can be utilized via SMIT or command line and allows you to back up various levels:

- Full backup (installable system image)
- Volume groups
- Logical volumes
- File systems
- Directory / file level

Furthermore, the tool is able to integrate into IBM Tivoli Storage Manager or NIM Resource Network Boot.

The IBM Tivoli Storage Manager for System Backup and Recovery (SysBack) version 5.6 and later allows for the storage of backup objects into an IBM Tivoli Storage Manager server. Backups to a IBM Tivoli Storage Manager Server may be manipulated like any other SysBack backup. They may be listed, verified, restored, and used for system reinstallation.

Combining the SysBack backup, restore, and network boot and install functions with a IBM Tivoli Storage Manager Server provides Bare Machine Recovery (BMR) capability for IBM Tivoli Storage Manager configurations. SysBack will back up and recover a system’s volume group, logical volume, and file system information. Optionally, SysBack will back up any non-rootvg data specified. Clients may use SysBack simply to recover the rootvg volume group, and then use IBM Tivoli Storage Manager to restore and manage other user data.

The backup images of root volume group (rootvg) from any AIX machine by using SysBack are stored on the IBM Tivoli Storage Manager Server. You can query the backup images by using the **smitty sysback** command. You can query the content inside each backup image from Sysback on the client side.

SysBack provides several methods to do Bare Machine Recovery. SysBack may utilize the Tivoli Storage Manager API unlike NIM.

If SysBack will be integrated with Tivoli Storage Manager Server, you need to install 32-bit IBM Tivoli Storage Manager API along with SysBack software on the AIX client, and on the AIX network boot server. The 32-bit IBM Tivoli Storage Manager API will generate virtual devices for SysBack to use as devices to send backup images to IBM Tivoli Storage Manager Server. These backup images will be sent to the storage pool of the IBM Tivoli Storage Manager Server. The SysBack software provides a variety of backup/restore methods.

SysBack, integrating with IBM Tivoli Storage Manager Server, provides a good consolidated backup/restore methodology especially when you have already used the IBM Tivoli Storage Manager Server to do our application data backups in this environment. In this case, the IBM Tivoli Storage Manager Server will manage the version control and Storage Pool of backup images. The benefit of the integrated SysBack solution is, the NAS Administrator does not have to manage the tapes, where the backups had been taken.

15.5.2 Backup with SysBack

The following diagram (Figure 15-37) shows a sample configuration where the Network Boot Server and the IBM Tivoli Storage Manager Server resides on the same machine. They may reside on different systems.

Boot Images are sent from the client (for example, NAS Gateway 500) to the Network Boot Server. System images are send to the IBM Tivoli Storage Manager Server where the reside on a IBM Tivoli Storage Manager Storage Pool (for example, tape or disk). The IBM Tivoli Storage Manager Server keeps track of the objects (images) in its database (IBM Tivoli Storage Manager Database). The Bare Machine Backup (BMR) process from a single server (IBM Tivoli Storage Manager Server and network boot server on one system) is explained SysBack in the next Image (see Figure 15-37).

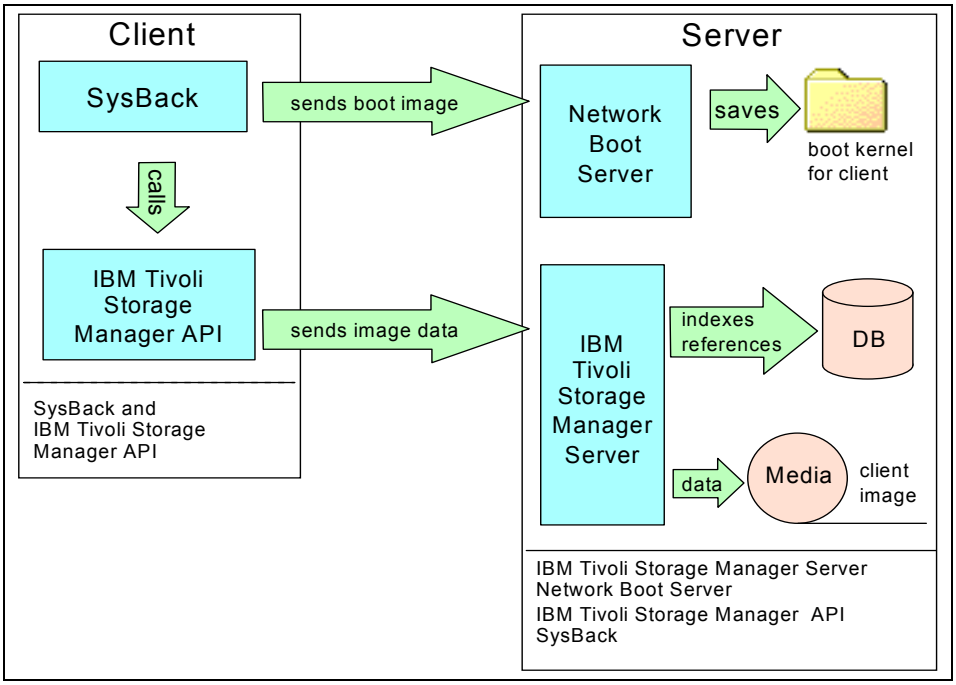


Figure 15-37 BMR backup to a single Server

15.5.3 Restore with SysBack

For a complete restore of the system (Bare Machine Recovery), including boot information, the client system does a **bootp** request to the network boot server. The Network boot server responds and sends the AIX boot kernel, the sysback program and a IBM Tivoli Storage Manager API package. These programs are kept in the memory of the client system.

After the system administrator completes the setup and configures the parameters on the SysBack menu (with network boot) we start the installation process. SysBack sends a request to the virtual device (32-bit IBM Tivoli Storage Manager API) and a request for restoration to the IBM Tivoli Storage Manager Server. The IBM Tivoli Storage Manager Server responds to the request from the SysBack client and then sends the restore image to be installed on the bare machine until successful. SysBack will then reboot the machine automatically twice.

The process of a Bare Machine Recovery with SysBack to a single server (IBM Tivoli Storage Manager Server and network boot server on one system) is described in Figure 15-38.

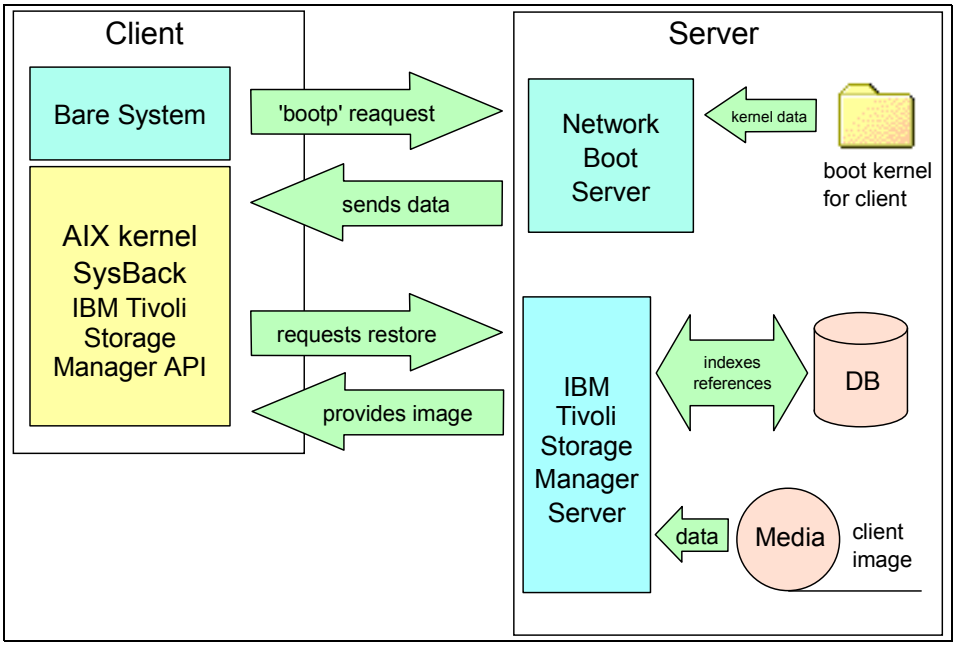


Figure 15-38 Restoring a bare system with SysBack

For more information about the product, please take a look at:

http://www-3.ibm.com/software/tivoli/products/storage-mgr-sysback/

16

File, file system, and volume group backup and restore

This chapter provides details on how to handle backup and restore tasks for files, file systems, and volumes on the NAS Gateway 500.

16.1 Basics for file and file system backup

Unlike bootable backups, this section describes techniques to back up and restore data on file, file system and volume base. The main focus of backing up and restoring this data is the data and file structure itself. An AIX user space consists usually of logical volumes, file systems, directories, and files.

What to restore depends on what data should be restored from a backup due to being missing, corrupted, or for duplication reasons. This can be caused by a corrupted file system, lost volumes, or simply deleted files.

Before restoring single files and directory structures, the administrator should check if the logical volumes (including volume groups) and file systems exist and are OK. If the volume group structure or file system structure is missing or corrupted, the administrator first has to rebuild the structure (volume groups / logical volumes / file systems).

Most backup tools and applications are not aware of the underlying volume structure, but commands like **savevg** and **restvg** will help to get back on track.

Numerous possibilities exist to back up and restore data by files. In this section of the redbook we show just a few of them.

File, file system, and volume group backup:

- Operating system based backup tools and commands
  - **mknasb** / **restnasb** (files)
  - **backup** / **restore** commands (full and incremental)
  - **backsnap** (snapshot + backup)
  - **restvg**/**savevg** (volume groups)
  - **dd**, **cpio**, **tar** (files / objects)
- Backup applications (for example, IBM Tivoli Storage Manager Client backup and restore):
  - LAN based
  - LAN free

The next section provides information about some operating system based backup commands and tools.

16.1.1 The mknasb and restnasb commands

The NAS Gateway 500 provides two new commands to back up and restore data of the Systems. Thiese two commands cover a defined set of files (configuration files) which are being backed up or restored.

The basic application area of **mknasb** and **restnasb** is to back up operating system user, operating system group, security, mapped user and groups, and file system configuration.

Note: For CIFS mapping, remember that Win and UNIX users have to be mapped, if you use the NAS Gateway 500 in a mixed environment.

mknasb and restnasb basics

Command syntax of **mknasb** and **restnasb**:

```
mknasb -d device
restnasb -d device
```

The default device is tape drive /dev/rmt0.

The **mknasb** command backs up several configuration settings contained in the following files, as shown in Example 16-1.

Example 16-1 The mknasb configuration files backup list

```
/.rhosts
/etc/.nas
/etc/cifs/cifsConfig
/etc/cifs/cifsPasswd
/etc/dhcpcd.ini
/etc/exports
/etc/filesystems
/etc/ftpaccess.ctl
/etc/ftpusers
/etc/group
/etc/hosts
/etc/hosts.equiv
/etc/inetd.conf
/etc/inittab
/etc/netsvc.conf
/etc/ntp.conf
/etc/passwd
/etc/rc.net
/etc/rc.tcpip
/etc/resolv.conf
/etc/security/acl
/etc/security/audit
/etc/security/environ
/etc/security/group
/etc/security/limits
/etc/security/login.cfg
/etc/security/passwd
/etc/security/priv
```

```
/etc/security/roles
/etc/security/user
/etc/security/user.roles
/etc/sendmail.cf
/etc/services
/etc/snmpd.boots
/etc/snmpd.conf
/etc/snmpd.peers
/etc/snmpdv3.conf
/etc/snmpmibd.conf
/etc/syslog.conf
/opt/nas/lib/data
/usr/HTTPServer/conf/admin.conf
/usr/HTTPServer/conf/httpd.conf
/usr/Tivoli/TSRM/log/localhost/agent_*.log
/usr/es/sbin/cluster/etc/exports
/usr/tivoli/itsanm/agent/log
/usr/tivoli/tsm/StorageAgent/bin/dsmsta.err
/usr/tivoli/tsm/client/ba/bin/dsmerror.log
```

Actually, the **mknasb** command stores the files (utilizing the **pax** command) to the device specified, or uses the default value /dev/rmt0.

Attention: The **mknasb** and **restnasb** commands do not cover all configuration settings. Some configurations and settings are not saved with the two commands; for example, the cluster configuration, ODM and IP settings, etc.

Backup with mknasb

This section shows how to use the **mknasb** command with WebSM and SMIT.

WebSM interface

The **mknasb** command can be executed via WebSM. Start the WebSM application, proceed to **NAS Management**, choose the system the **mknasb** command should be executed from (in our example, the IP address). Then click **System Environment** -> **Backup and Restore** -> **Backup Configuration Files** (Figure 16-1).

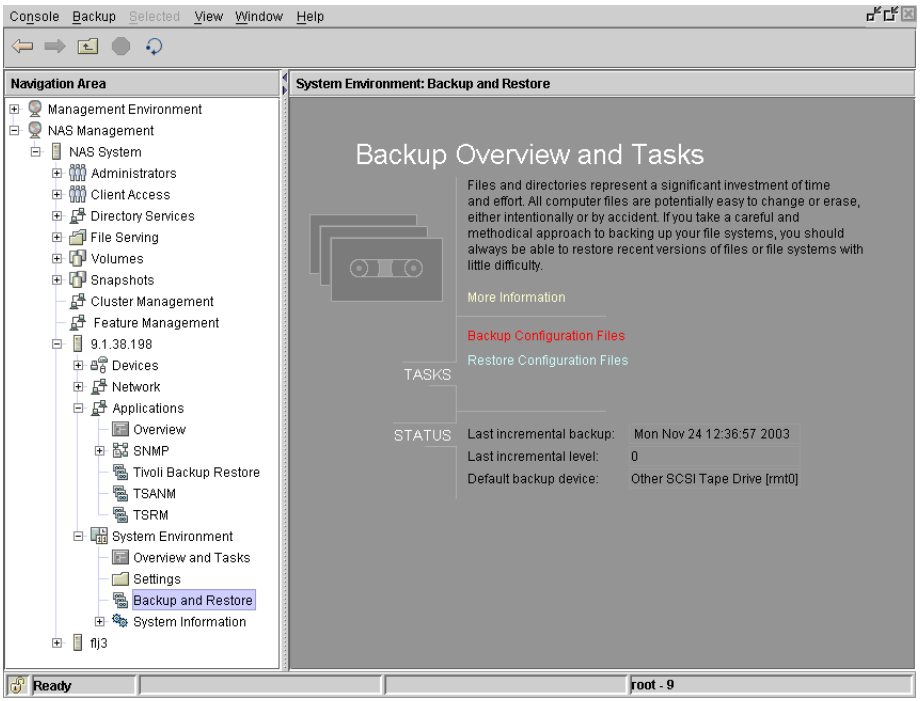


Figure 16-1 WebSM entry for backup of configuration files

Choose a device (for example, /dev/fd0 or /dev/rmt0) at which the files should be stored (Figure 16-2).

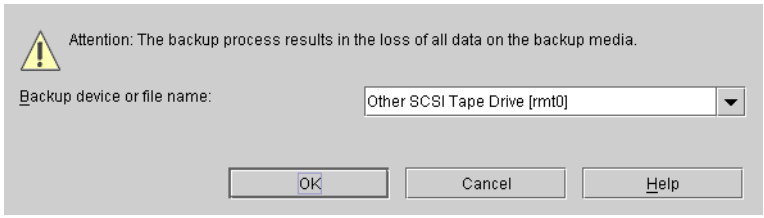


Figure 16-2 WebSM mknasb option screen

An operational message appears (Figure 16-3).

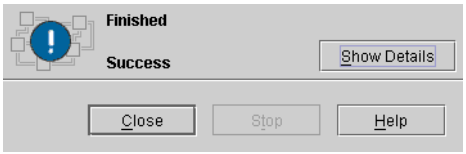


Figure 16-3 Mknasb successfully finished

SMIT interface

To utilize **mknasb** via the SMIT interface, proceed as follows with the NAS Administrator user (we used nasadmin). You can use the SMIT fastpath **smit backup**. Select **Backup Configuration Files** and specify the device or file where to back up (see Figure 16-4 and Figure 16-5).

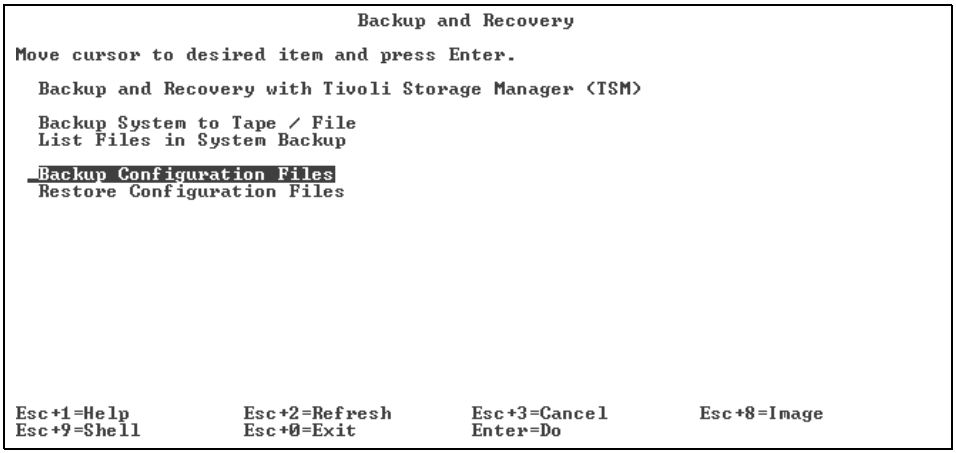


Figure 16-4 Mknasb entry in SMIT menu

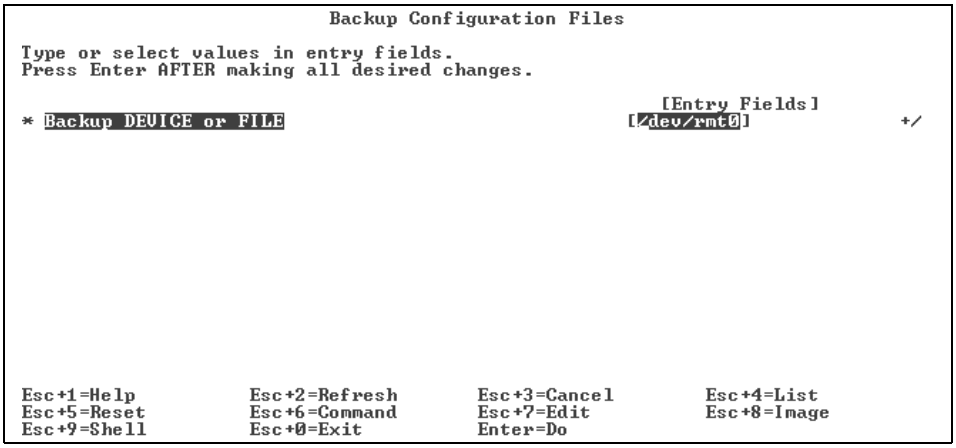


Figure 16-5 Select an appropriate device

Verification of a mknasb backup

If you want to verify the correctness of mknasb logon as root to the NAS, and execute on command line (Figure 16-6), use this command:

```
pax -f /dev/rmt0
```

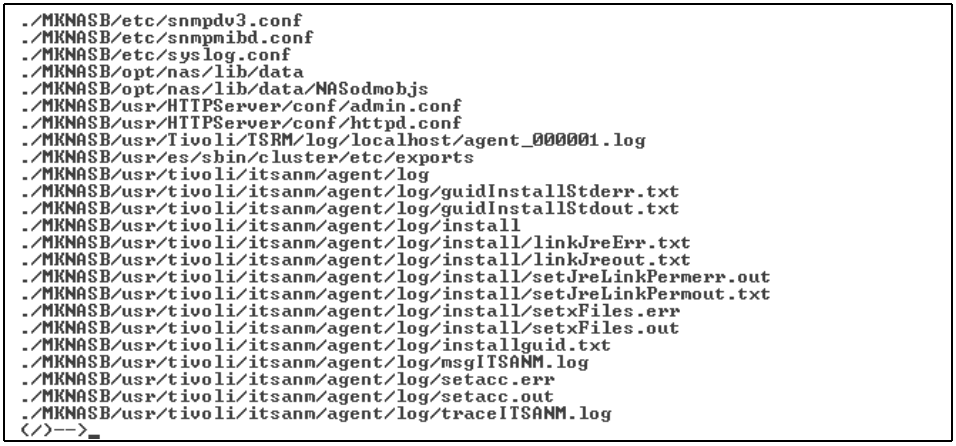


Figure 16-6 Verify the backup

Restore with restnasb

This section shows how to use the **restnasb** command with WebSM and SMIT.

Restore of configuration files with the WebSM interface

Figure 16-7 shows how we restored files with the WebSM interface.

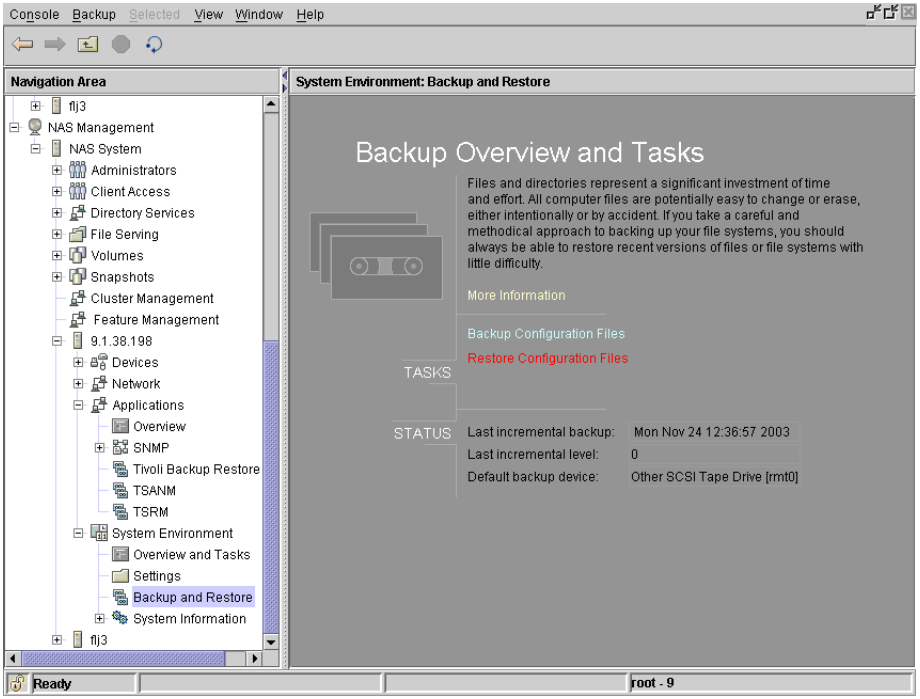


Figure 16-7 WebSM panel for Restore configuration

Insert the device where the files reside and proceed (Figure 16-8).

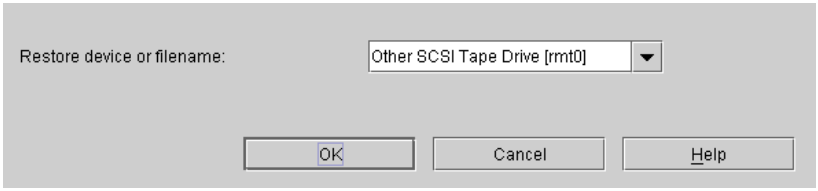


Figure 16-8 Option of the restore configuration operation

Finally, a successful completion message should appear (Figure 16-9).

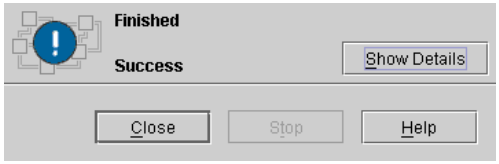


Figure 16-9 Result screen of restoring configuration files

Restore of configuration files with the SMIT interface

To utilize **restnasb** via the SMIT interface, proceed as follows with the NAS administrator user (nasadmin). You can use the SMIT fastpath **smit backup**, then choose Restore Configuration Files (see Figure 16-10 and Figure 16-11).

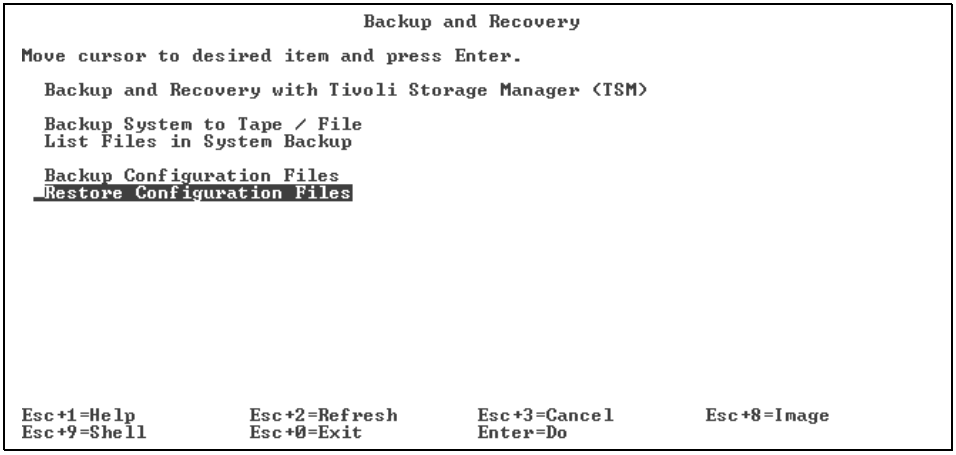


Figure 16-10 Restore with restnasb

Figure 16-11 shows how to choose the device to which you would like to restore the data.

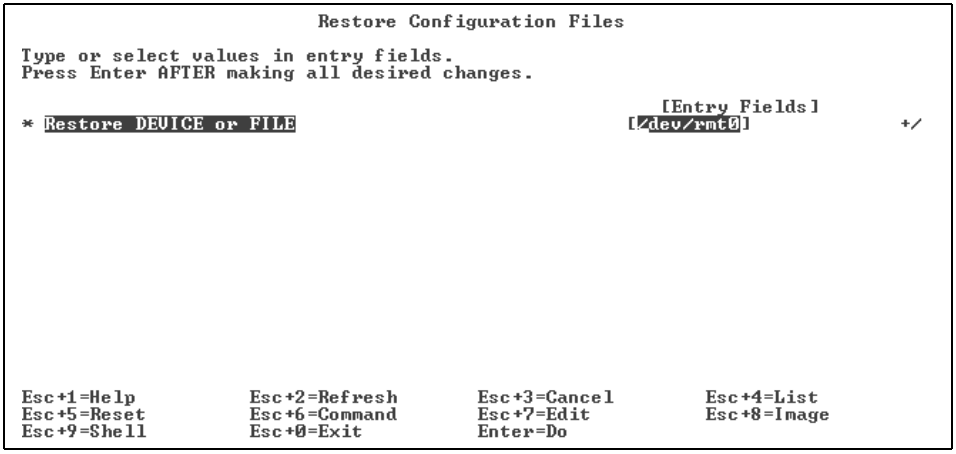


Figure 16-11 Choose device

16.1.2 The backup and restore commands (full and incremental)

Another backup and restore practice is provided by the **backup** and **restore** commands. These commands can be executed via command line, SMIT interface, or the WebSM, and enables the NAS administrator to back up and restore files and directories, including subdirectories. The functionality does not cover the underlying structure like volume groups and logical volumes. Use the commands to restore to an existing structure or use **restvg** to restore the structure if needed.

Remember: You can restore si331ngle files from a **mksysb** backup as well.

Basics of the file system backup and restore

The **backup** command allows you to back up files and directories on your NAS Gateway 500. No boot image will be created, because this function is intended to create backups on a file based archive.

Actually, the **backup** commands work on a leveled base and you are able to specify level 0 to 9. Level 0 means full backup, and levels 1 to 9 are incremental backups (9 is default). Each level (x) depends on its upper level (x-1). Backing up with level n will save all data changed, since the most recent backup n-1 (or lower).

Suppose backup level 3 has been done. After that you are doing level 4 backup. During this backup, all files changed since the last level 3 backup will be saved.

The command can be executed with WebSM, **smitty**, or a regular command line interface.

File system backups

Command Syntax:

backup [[-Level] [-b Number] [-c] [-f Device] [-L Length] [-u]] [FileSystem]

-Level — Specifies the level of backup (default is -9)
-b — Number of 512 blocks
-c — For cartridge instead of a nine track
-f — Device specifies the output device (for example, /dev/rmt0)
-L — Length in bytes of the tape (Overwrites -c and -d)
-u — Updates /etc/dumpdates (information about the backup)
FileSystem — Specifies the file system that should be backed up

See the manual pages for more detail on the **backup** command. Go to a NAS Gateway 500 command line and type: man backup.

The following example describes a file system backup (/) done with the WebSM (see Figure 16-12).

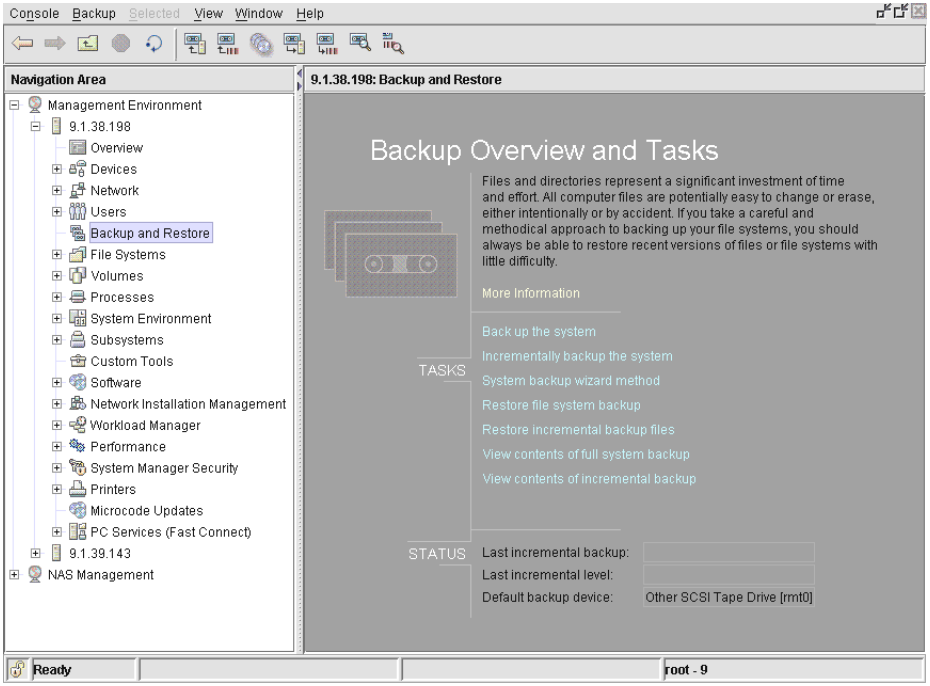


Figure 16-12 Starting the WebSM for file backups restore incremental

Figure 16-13 shows the settings for a backup to tape (/dev/rmt0) with level 9.

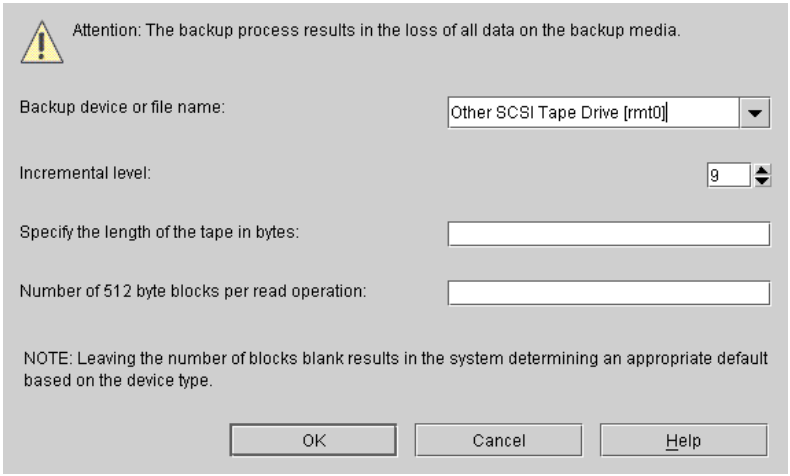


Figure 16-13 Specify backup options

If the process went successfully, you will get output like the one in Figure 16-14.

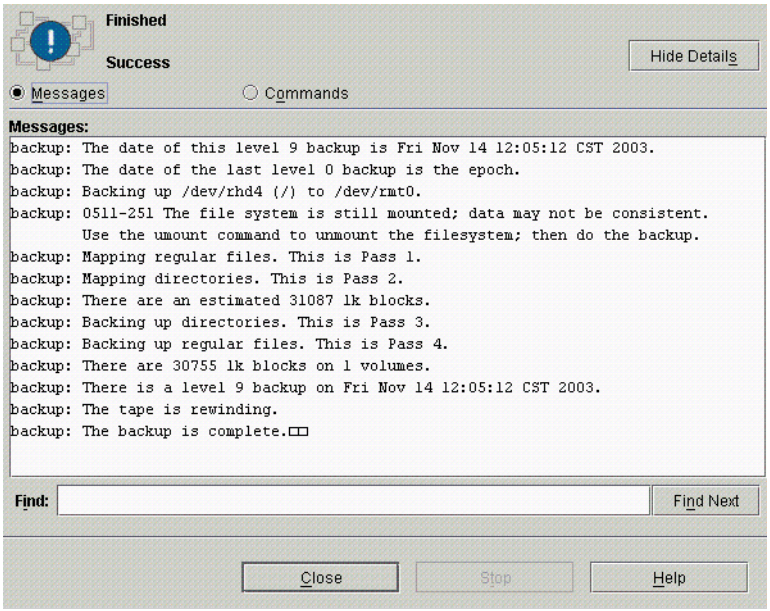


Figure 16-14 Successfully backed up files

Attention: Keep in mind that the WebSM only backs up the root (/) file system with the incremental backup system option. (In the version we used during the redbook tests, we used the command line and SMIT interface to back up other file systems.)

File system restore with the restore command

The **restore** command is used to copy data by file system from the backup archive back to the system. The **restore** command can be used to restore all data or parts of the data (like files or directories) from the backup.

Command syntax:

restore -r [B q v y] [-b Number] [-f Device]

-r — Restores file by archive (complete Level 0 restore or restore incremental after Level 0 restore)
B — Archive should be read from standard input
q — No prompt to mount volume
v — Verbose shows additional information
y — Continue after tape errors
-b — Number of 512 byte blocks (if left blank, system will determine)
-f Device — Specifies the restore Device (for example, /dev/rmt0)
For example: **restore -rvqf /dev/rmt0**

Restores whole file system from backup, will not prompt for a tape mount (expects a mounted tape), backup device is /dev/rmt0 and shows additional information during the restore.

restore -x [d M v q e] [-b Number] [-f Device] [-X VolumeNumber] [File ...]

-x — Specifies files restored by name (single files)
-d — If file parameter is a directory, all files in that directory will be restored
-M — Sets access and modification time of restored files to the current restoration time
-v — Verbose shows additional information
-q — No prompt to mount volume
-e — restore non sparse files
-b — Number of 512 byte blocks (if left blank, system will determine
-f — Device specifies the restore device (for example, /dev/rmt0)
-X VolumeNumber — Specifies the volume
File — Specifies the file name to be restored

See the manual pages for more details on the **restore** command. Go to a NAS Gateway 500 command line and type: **man restore**.

This functionality can be accessed through the WebSM interface, SMIT interface, or command line interface.

File system restore using WebSM

In WebSM, choose **Backup and Restore -> Restore incremental backup files** (Figure 16-15).

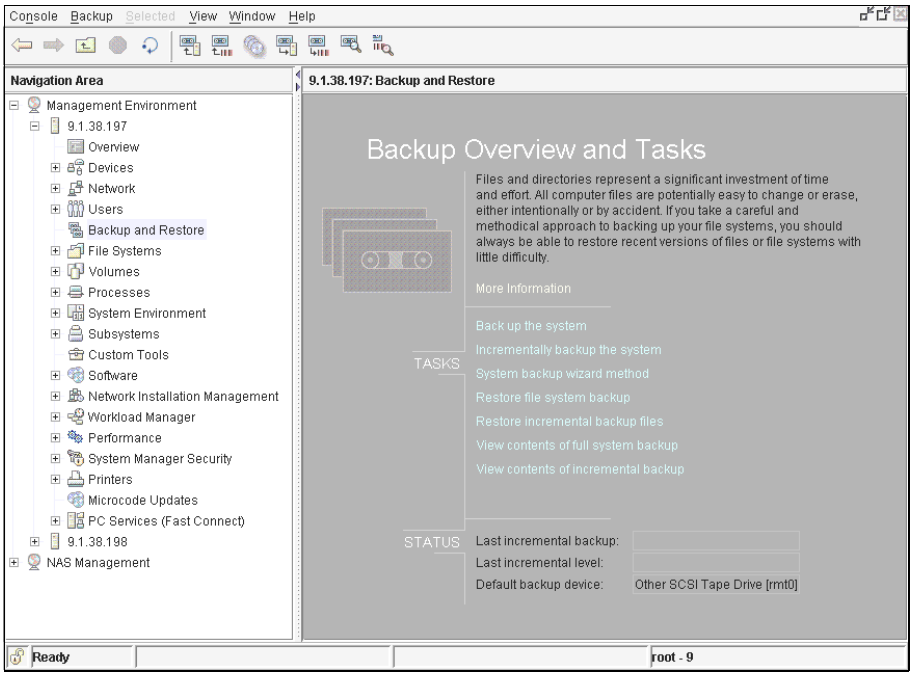


Figure 16-15 Restoring a complete file system with WebSM

The next panel shows that we chose the root (/) file system to be restored (Figure 16-16).

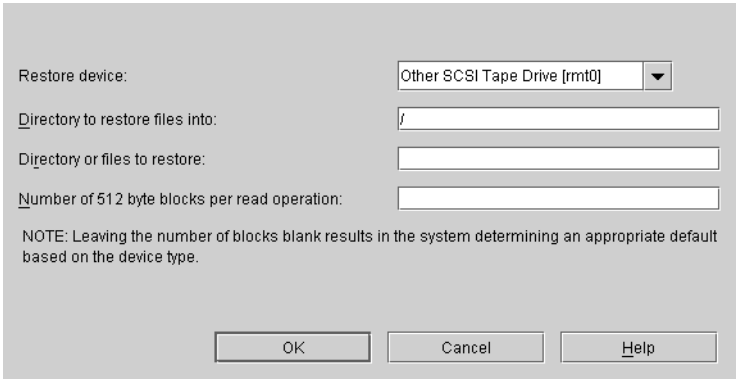


Figure 16-16 Restoring the root file system with WebSM

The operation finished successfully (Figure 16-17).

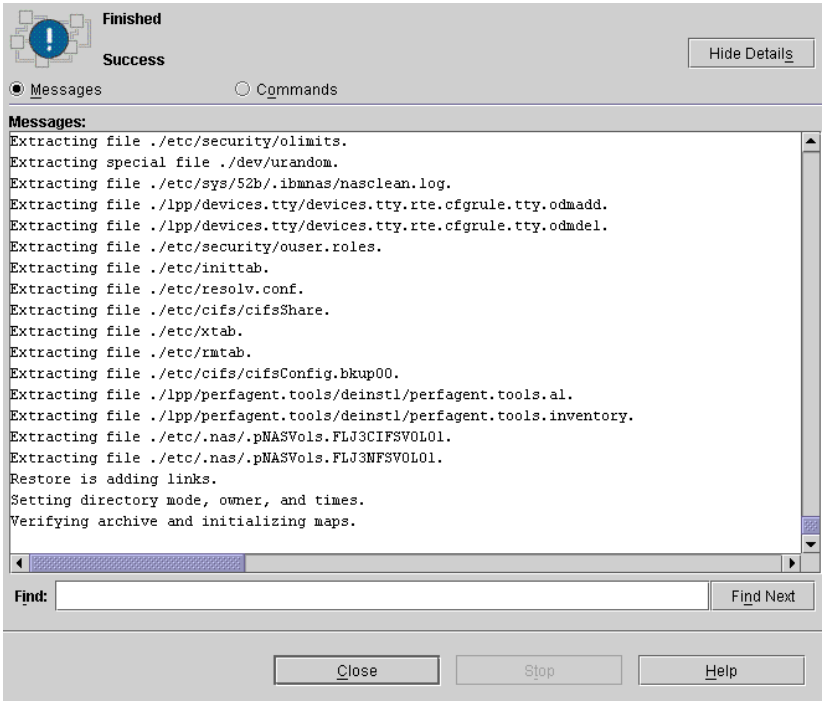


Figure 16-17 WebSM restore of file system completed

File system restore using the SMIT interface

Use the following path to access the restore functionality in SMIT:

smit -> **System Storage Management** -> **File Systems** -> **Restore a File System**

Specify the options and execute the command with **Enter** (Figure 16-18).

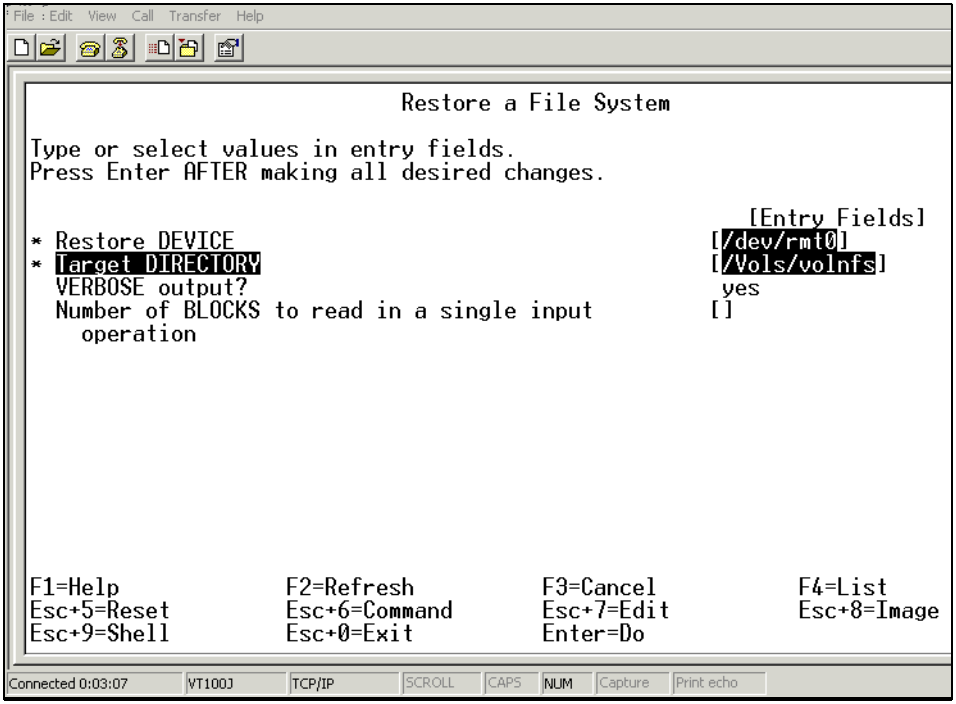


Figure 16-18 Restore a filesystem with SMIT

File system restore using the command line

The next example shows backup and restore done with the command line interface of the complete file system /home (Figure 16-19).

```
(/)-->backup -f /dev/rmt0 -0 /home
backup: The date of this level 0 backup is Mon Nov 17 17:59:13 CST 2003.
backup: The date of the last level 0 backup is the epoch.
backup: Backing up /dev/rhd1 (/home) to /dev/rmt0.
backup: 0511-251 The file system is still mounted; data may not be consistent.
        Use the umount command to unmount the filesystem; then do the backup.
backup: Mapping regular files. This is Pass 1.
backup: Mapping directories. This is Pass 2.
backup: There are an estimated 208 1k blocks.
backup: Backing up directories. This is Pass 3.
backup: Backing up regular files. This is Pass 4.
backup: There are 350 1k blocks on 1 volumes.
backup: The tape is rewinding.
backup: The backup is complete.
(/)-->
```

Figure 16-19 Backup file system /home via command line

The content to the created backup can be verified with the -T option of the **restore** command (used just to see that the right files are on the backup) — see Figure 16-20 and Figure 16-21.

```
(/)-->restore -Tqf /dev/rmt0
The dump date is Mon Nov 17 17:59:13 CST 2003.
Dumped from: Wed Dec 31 18:00:00 CST 1969.
         2       .
        32       ./guest
         3       ./lost+found
        64       ./nasadmin
        65       ./nasadmin/.profile
        66       ./nasadmin/.sh_history
        71       ./nasadmin/WebSM.pref
        67       ./nasadmin/smit.log
        68       ./nasadmin/smit.script
        69       ./nasadmin/smit.transaction
        70       ./nasadmin/websm.script
         4       ./nasuser
         5       ./nasuser/.profile
         9       ./restoresymtable
         8       ./user01
        12       ./user01/back.out
        13       ./user01/test.txt
        10       ./user02
        11       ./user03
         6       ./w2kadmin
         7       ./w2kadmin/.profile
(/)-->
```

Figure 16-20 Verify content of backup

```
(/home)-->ls -al user0*
user01:
total 216
drwxr-xr-x   2 root     system          256 Nov 17 16:51 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..
-rw-r--r--   1 root     system       102086 Nov 17 16:40 back.out
-rw-r--r--   1 root     system           24 Nov 17 16:51 test.txt

user02:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 14:54 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..

user03:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 17:37 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..
(/home)-->
```

Figure 16-21 List content of file system on disk (should be on the backup)

The following screen shows the removal of some files in the filesystem, which will be restored. This was done just for testing reasons to see that the restore will work (Figure 16-22).

```
(/home)-->rm -R user01/*
(/home)-->ls -al user0*
user01:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 18:04 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..

user02:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 14:54 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..

user03:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 17:37 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..
(/home)-->_
```

Figure 16-22 Remove files for a test for our test

Now the **restore** command can be run (Figure 16-23).

```
Warning: ./nasadmin: Do not specify an existing file.
Warning: ./nasuser: Do not specify an existing file.
Warning: ./user01: Do not specify an existing file.
Warning: ./user02: Do not specify an existing file.
Warning: ./user03: Do not specify an existing file.
Warning: ./w2kadmin: Do not specify an existing file.
Extracting new leaves.
Checkpointing the restore.
Extracting file ./nasuser/.profile.
Extracting file ./w2kadmin/.profile.
Extracting file ./restoresymtable.
Extracting file ./user01/back.out.
Extracting file ./user01/test.txt.
Extracting file ./nasadmin/.profile.
Extracting file ./nasadmin/.sh_history.
Extracting file ./nasadmin/smit.log.
Extracting file ./nasadmin/smit.script.
Extracting file ./nasadmin/smit.transaction.
Extracting file ./nasadmin/websm.script.
Extracting file ./nasadmin/WebSM.pref.
Restore is adding links.
Setting directory mode, owner, and times.
Checking the symbol table.
Checkpointing the restore.
(/home)-->_
```

Figure 16-23 restore completed successfully

Verify if the data had been restored to the file system structure (Figure 16-24).

```
(/home)-->ls -al user*
user01:
total 216
drwxr-xr-x   2 root     system          256 Nov 17 16:51 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..
-rw-r--r--   1 root     system       102086 Nov 17 16:40 back.out
-rw-r--r--   1 root     system           24 Nov 17 16:51 test.txt

user02:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 14:54 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..

user03:
total 8
drwxr-xr-x   2 root     system          256 Nov 17 17:37 .
drwxr-xr-x  10 bin      bin            4096 Nov 17 14:27 ..
(/home)-->_
```

Figure 16-24 Verify the restoration of the files on the file system

Verification of the file system backup

The Administrator can verify which files had been backed up with the WebSM, SMIT and command line interface.

Usage of the WebSM to see what has been backed up is shown in Figure 16-25, Figure 16-26, and Figure 16-27.

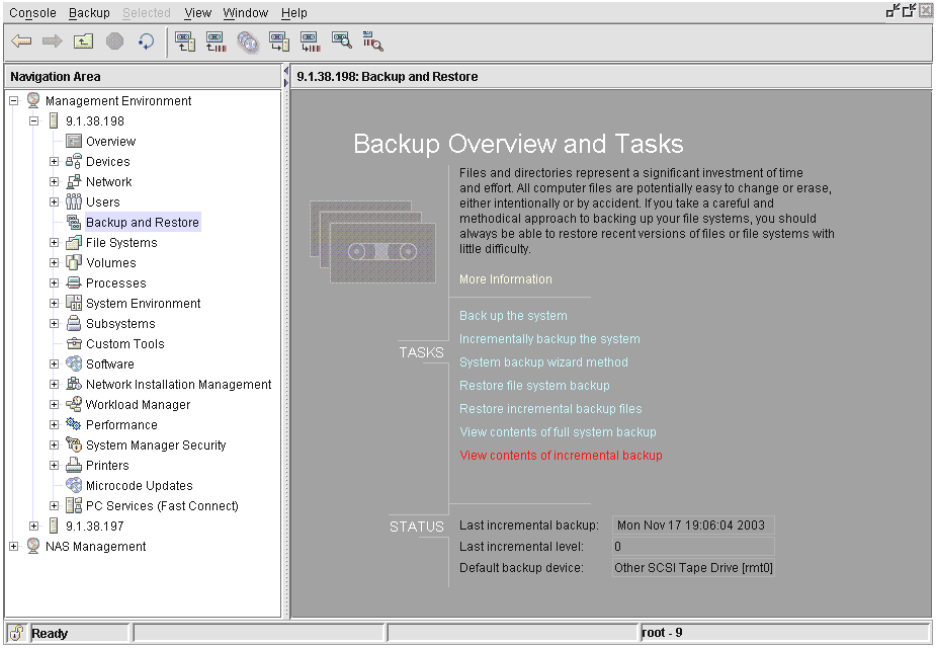


Figure 16-25 Verify file system backup with WebSM

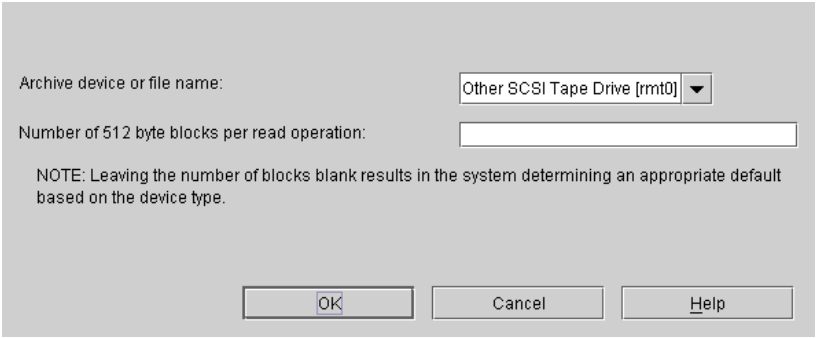


Figure 16-26 Specify the tape drive

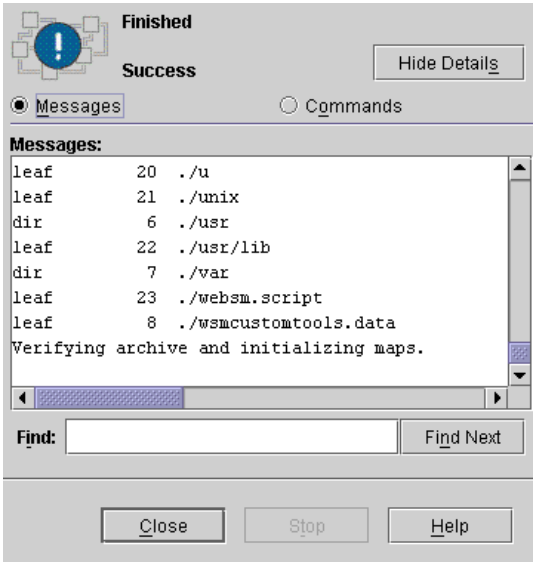


Figure 16-27 Success - list all objects

The underlaying command (restore) uses the -T option to list what has been backed up. The option -T will not restore files, it is used just for displaying the content of the backup. Try this to see if all file systems you want to back up are backed up.

You can use the command line to execute the command:

```
restore -Tq -f /dev/rmt0
```

The **restore** command reads from device /dev/rmt0 and displays all filenames and directories contained on the tape media. The -q option allows you to proceed without mounting the first volume. The backup may span various tape medias.

Another way is to use the SMIT interface:

smitty -> **System Storage Management** -> **File Systems** -> **List Contents of a backup**

16.1.3 The restvg and savevg commands

This section describes backup and restores with **savevg**, **restvg**, and the associated **mkvgdata** command.

As discussed before, you cannot use **mksysb** to back up other volume groups than the rootvg, and other **backup** and **restore** commands/tools may not offer a way to back up and restore the LVM (Logical Volume Manager) structure of the AIX file system (such as volume groups, logical volumes, etc.).

The two commands **savevg** and **restvg** will help us to save data in a very similar way as the **mksysb** does. The **savevg** command backs up data belonging to a specific volume group, and the **restvg** command restores data belonging to a specific volume. Both commands are very helpful, because most backup tools and commands are only capable of doing backups and restores on a file/directory base and do not backup and restore volume group, logical volume or file system data.

Tip: It may be a good idea to combine **savevg** and **restvg** and **mksysb** with other backup tools like IBM Tivoli Storage Manager backups.

Attention: If you are running a multipathing environment (Subsystem Device Driver) with volume groups using vpath devices, consider using **savevg4vp** to back up and **restvg4vp** to restore these volume groups.

mkvgdata command

The **mkvgdata** command creates information about a specific volume group and its logical volumes, file systems, etc. and is used in conjunction with savevg and restvg.

Since the **mksysb** command is only used for the rootvg, a user may use **savevg** and **restvg** in order to back up and restore other data volume groups.

Example:

```
mkvgdata -X -m datavg
```

The **mkvgdata** command, if used in conjunction with a data volume group (not the rootvg), creates a directory in /tmp/vgdata.

The name of the directory is the same as the volume group name which has been used. This directory contains several files with information about this volume group like logical volumes, filesystems, etc.

The -X option expands the /tmp filesystem if needed, option -m is used to store mapping information (logical to physical) partitions for each logical volume in the specify volume group.

savevg command

Saving a volume group with the **savevg** command.

The **savevg** command backs up a volume group and associated files with this Volume group. The **savevg** command uses the data file created by the **mkvgdata** command.

savevg [-b Blocks] [-e] [-f Device] [-i | -m] [-p] [-v] [-V] [-X] VGName

-b Blocks — Number of 512-byte blocks
-f Device — Specifies the device file where the backup resides.
-e — Excludes files
-i — Creates data file (mkvgdata command)
-m — Created map files (mkvgdata command)
-p — Disables software packing
-v — Verbose mode
-V — Verifies file header on tape
-X — Expands /tmp if needed
VGName — Name of the volume group

Example:

```
savevg -if /dev/rmt0 -V datavg
```

This command saves datavg on /dev/rmt0, creates a new data file, and verifies the readability of file headers.

restvg command

Restoring a volume group can be done with the **restvg** command. The command **restvg** is used to restore a volume group which has previously been backed up with the **savevg** command.

All data specified in /tmp/vgdata/vgname/vgname.data will be rebuild (vgname is the name of your volume group).

The **restvg** command restores the user volume group and all its containers and files, as specified in the /tmp/vgdata/vgname/vgname.data file (where vgname is the name of the volume group) contained within the backup image created by the savevg command.

```
restvg [ -b Blocks ] [ -d FileName ][ -f Device ] [ -l ] [ -q ] [ -r ] [
-s ] [-n ] [ -P PPsize ] [ DiskName ... ]
```

-b Blocks — Number of 512-byte blocks
DiskName — Name of the physical disk (for example, hdiskx)
-d FileName — Filename used as vgname.data
-f Device — Specifies the device file where the backup resides.
-l — Display information about the backup
-n — Ignore existing map file
-P PPsize — in megabytes
-q — No prompt before restoring volume group
-r — Only structure of VG is created, no files or data are restored
This option can be used if you want to use Tivoli Storage Manager backup and restore.
- s — VG is created with minimum size (vgname.data input for specific file system information needed)

The first example shows how to restore a volume group from device /dev/rmt0 to hdisk3:

```
restvg -f/dev/rmt0 hdisk3
```

The second example shows how to restore the structure of a volume group prior to a restore of files with IBM Tivoli Storage Manager Client. The volume group information is taken from the image on the tape media in /dev/rmt0:

```
restvg -r -f /dev/rmt0
```

16.1.4 Split mirror backup

The NAS Gateway 500 provides snapshot support for a mirrored volume group. A mirrored copy of a fully mirrored volume group can be split into a snapshot volume group. This feature is a function which comes with AIX 5.2.

In order to split a volume group, all logical volumes in that volume group must have a mirror copy. The disk(s) where the mirror resides must only contain data from this specific set of mirrors.

The disk(s) will be part of the new snapshot volume group and the original volume group will discontinue using the disk(s). The new snapshot volume group will contain new logical volumes and mount points.

Since the mirror may be rejoined to the original volume group and consistent data is required, both volume groups have to keep track of the changes in physical partitions (PPs).

splitvg command

Some restrictions appear with the **splitvg** command. See the manual pages of the **splitvg** command for more details (**man splitvg**)

Attention: **splitvg** is not supported for the rootvg.

splitvg [-y SnapVGname] [-c Copy] [-f] [-i] VGname

-y — SnapVGname Specifies the name of the snapshot volume group to use instead of a system-generated name.

-c — Copy Specifies which mirror to split. Valid values are 1, 2, or 3. The default is the second copy.

-f — Will force the split even if the mirror copy specified to create

-i — Will split the mirror copy of a volume group into a independent volume group that cannot be rejoined into the original.

VGname specifies the volume group.

joinvg command

To rejoin the snapshot volume group with the original volume group use the **joinvg** command.

The rejoin command syntax is as follows:

joinvg [-f] VGname

-f — Force to join when disks in the snapshot volume group are not active. The mirror copy on the inactive disks will be removed from the original volume group.

VGname — Specifies the volume group.

split mirror backup procedure

In the following example, the file system /cifsfs is a file system in the volume group datavg mirrored from hdisk2 to hdisk3. To split the mirror in the snapshot volume group, run the **snapvg** command and take an online backup of the data, then run the following command sequence:

1. **splitvg -y snapvg datavg**

   The VG datavg is split and the VG snapvg is created. Furthermore, the mount point /fs/cifsfs is created.

2. **backup -f /dev/rmt0 /fs/cifsfs**

   An inode based backup of the unmounted file system /fs/cifsfs /fs/data is created on tape (rmt0). Instead of using the **backup** command, you can run a IBM Tivoli Storage Manager backup as well.

3. **joinvg datavg**

   The snapshot VG snapvg is rejoined with the original VG datavg and synchronized in the background.

16.1.5 The backsnap (JFS2 command)

The **backsnap** command can be used to create a snapshot (JFS2 file systems) and will backup the snapshot. The command combines both functions in one step.

Syntax:

```
backsnap [ -R ] -m MountPoint -s size=Size [ BackupOptions ] FileSystem
```

The following example shows the creation of a snapshot followed by a backup:

```
backsnap -m /tmp/snapshot/nasuser_fs -s size=16M -i -f/dev/rmt0
/home/nasuser/fs
```

Filesystem to snap: /home/nasuser/fs

New mountpoint: /tmp/snapshot/nasuser_fs

Due to this command, a logical volume is created (size 16 megabytes), a snapshot of the file system

/home/nasuser/fs in been created on the new logical volume. After that the snapshot will be mounted to /tmp/snapshot/nasuser_fs and all files and directories will be backed up to /dev/rmt0.

The previously created backup can be restored via the **restore** command.

16.1.6 The dd, cpio, tar, pax and other commands

AIX offers several commands to back up files to local attached devices or file systems. We decided to skip most of them and to describe the most important ones. Nevertheless, some of them are listed here; basic operating system commands such as:

- **tar** (for tape archives)
- **cpio** (copies files into and out of archive storage and directories)
- **dd** (reads from standard in and converts and copies to standard out)
- **pax** (extracts, writes, and lists members of archive files)

For more detailed information on commands and options, please refer to the command reference, manual pages (AIX man command), AIX documentation, or AIX related redbooks. You can use the following link to find AIX related redbooks:

http://publib-b.boulder.ibm.com/cgi-bin/searchsite.cgi?query=aix

Or, you can browse the IBM Redbook Web site:

http://www.redbooks.ibm.com/

17

IBM Tivoli Storage Manager integration

This chapter describes the use of IBM Tivoli Storage Manager with the NAS Gateway 500. The software is pre-loaded and non-configured. We will explain in the next chapter how to set up IBM Tivoli Storage Manager in a LAN-based and LAN-free environment. If you would like learn more details about IBM Tivoli Storage Manager, please refer to the IBM Redbooks, *IBM Tivoli Storage Management Concepts*, SG24-4877, and *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416.

17.1 Introduction to IBM Tivoli Storage Manager

The IBM Tivoli Storage Manager product set is an enterprise-wide solution integrating automated network backup, archive and restore, storage management, and disaster recovery. The IBM Tivoli Storage Manager product set is ideal for heterogeneous, data-intensive environments, supporting a huge range of platforms and over 250 storage devices across LANs, WANs, and SANs, plus providing protection for leading databases and e-mail applications.

IBM Tivoli Storage Manager supports backup via LAN (LAN based backup) as well over a SAN (LAN-free backup). LAN-free backup is giving multiple servers the ability to share an automated library in a high-performance Storage Area Network (SAN) configuration. The LAN-free client data transfer feature reduces network traffic and improves bandwidth by backing up and restoring data directly to and from SAN-attached disk or tape storage.

Figure 17-1 shows how the data is transported by LAN based and LAN-free backups.

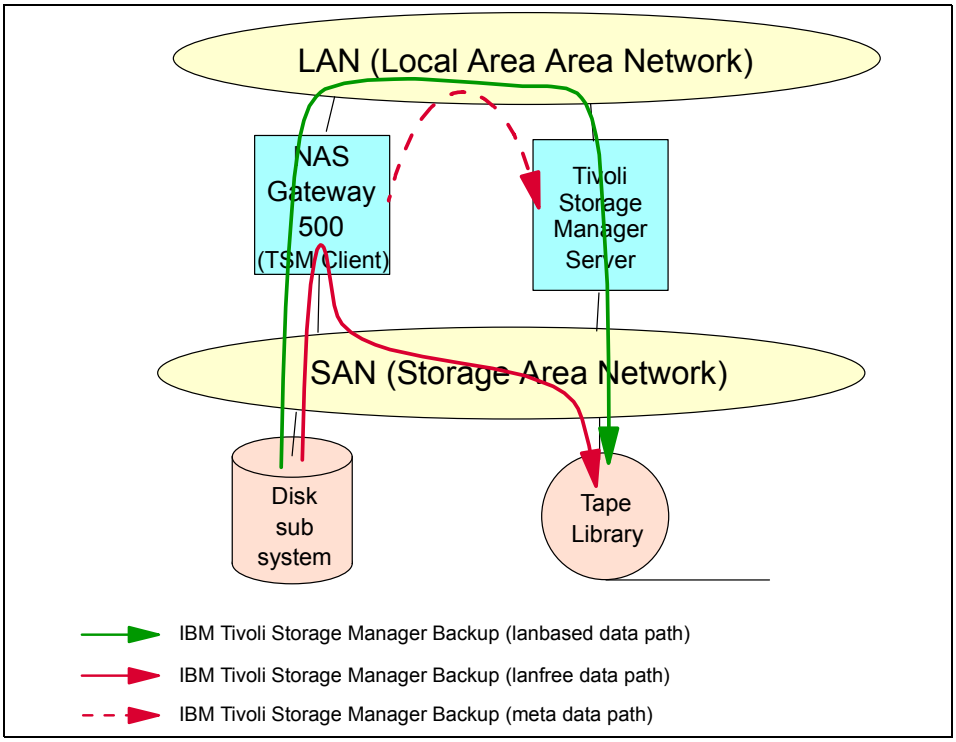


Figure 17-1 LAN-free and LAN based backups

Utilizing IBM Tivoli Data Protection products, IBM Tivoli Storage Manager supports most enterprise management, database, and groupware applications.

17.1.1 NAS Gateway 500 and IBM Tivoli Storage Manager

The Tivoli Storage Manager Server should have been properly set up. If existing IBM Tivoli Storage Manager policy and storage settings won't be used, remember to configure Storage Pools, Policy Domains and Policy Sets, etc.

IBM Tivoli Storage Manager Client software is pre-loaded, non-configured on the NAS Gateway 500. The following versions were supplied at the time this redbook was written.

- IBM Tivoli Storage Manager Client Version 5.2
- IBM Tivoli Storage Manager for AIX: StorageAgent Version 5.2 AIX
- IBM Tivoli Storage Manager AIX Client API Version 5.2

We will show in the following section how we configured the IBM Tivoli Storage Manager Server and Client.

17.1.2 IBM Tivoli Storage Manager Server configuration

IBM Tivoli Storage Manager runs in a client / server environment. Prior to using the IBM Tivoli Storage Manager Client, you have to configure a IBM Tivoli Storage Manager Server. Please refer to the IBM Tivoli Storage Manager Server documentation for more details on how to set up and configure a IBM Tivoli Storage Manager Server.

We give a short overview of our IBM Tivoli Storage Manager Server configuration used for the redbook. Usually your policies and definitions would be different. You can use previously defined policies and configurations from your IBM Tivoli Storage Manager environment or define new settings for the NAS Gateway 500.

We created these settings:

- Device Class: FILEDEV1 (file device class)
  (keep in mind: mount limit, max capacity)
- Storage Pool: FILEPOOL1
  Points to the previously configured file device class
  (keep in mind: max scratch allowed parameter)
- Policy Domain: NAS500_DOM
- Policy Set: NAS500_POLSET
- Management Class: NAS500_CLASS
- Backup Copy Group: standard (points to FILEPOOL1)
- Archive Copy Group: standard (points to FILEPOOL1)

Do not forget to assign a default management class. After successfully validating the policy set, the policy set can be activated. Register the clients in case of closed registration in you IBM Tivoli Storage Manager environment

17.1.3 IBM Tivoli Storage Manager Client configuration

Before starting IBM Tivoli Storage Manager backups the client nodes must be configured.

Make sure that the basic TCP/IP configuration on your NAS Gateway 500 is correct and client nodes are registered if your IBM Tivoli Storage Manager Server runs with closed configuration (registration: closed).

The IBM Tivoli Storage Manager Client configuration on the NAS Nodes can be setup via WebSM, using SMIT interface or editing the IBM Tivoli Storage Manager configuration files directly.

Configure using WebSM (preferred way)

You can easily configure your IBM Tivoli Storage Manager Client with the WebSM interface. Open the WebSM, select **NAS Management**, your system (for example, IP Address), **Applications**, **Tivoli Backup Restore**, **Configure TSM Client** (Figure 17-2).

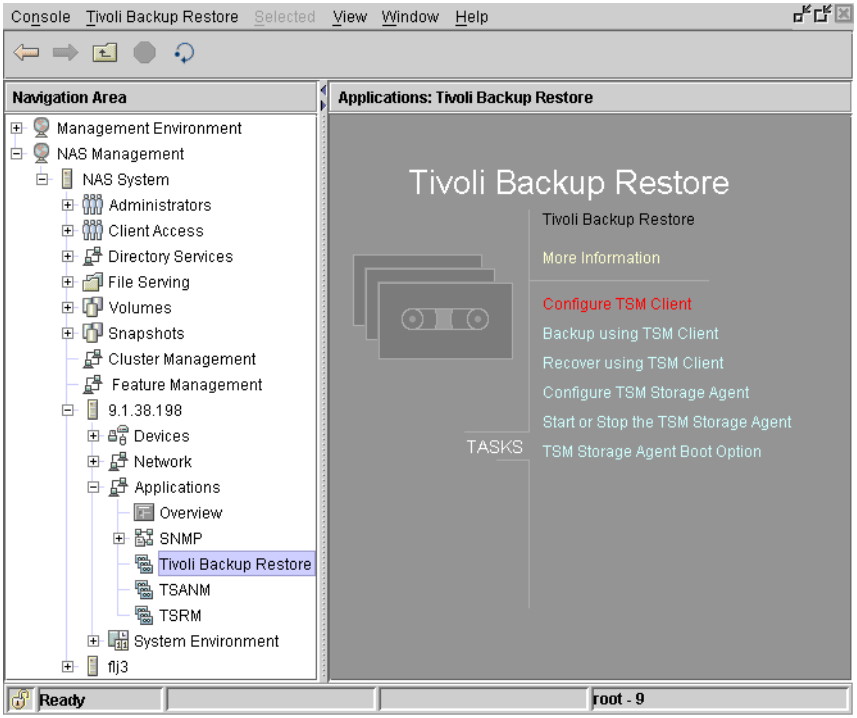


Figure 17-2 WebSM interface for the IBM Tivoli Storage Manager Client

Choose the right settings for IBM Tivoli Storage Manager server name, port number, IBM Tivoli Storage Manager Server address, IBM Tivoli Storage Manager Client nodename, IBM Tivoli Storage Manager Client password. Then proceed with **OK**.

Configuration using SMIT

The IBM Tivoli Storage Manager SMIT menu for the IBM Tivoli Storage Manager Client configuration will only appear if you are logged on as the NAS Administrator user created at the initial setup. Run **`smit`** on a command line and choose **Manage Applications** in the SMIT menu (Figure 17-3).

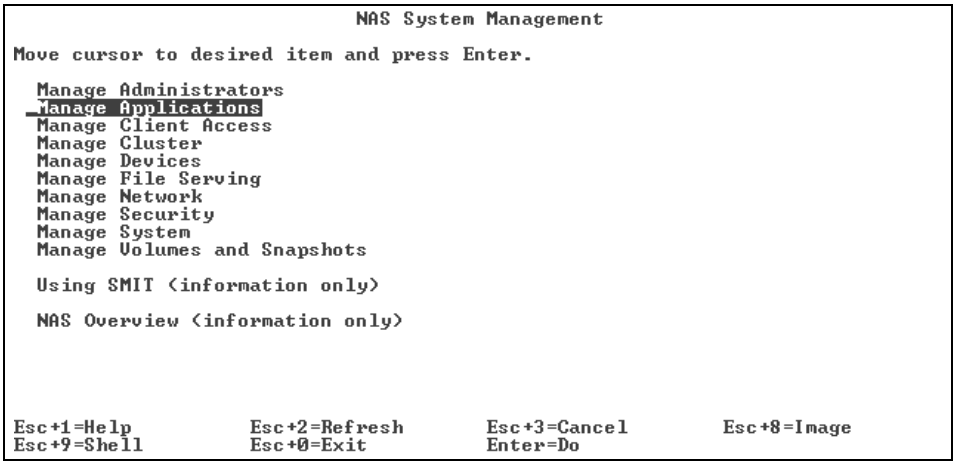


Figure 17-3 SMIT menu entry

In the next panel, highlight **Backup and Recovery with Tivoli Storage Manager (TSM)** and press Enter (Figure 17-4).

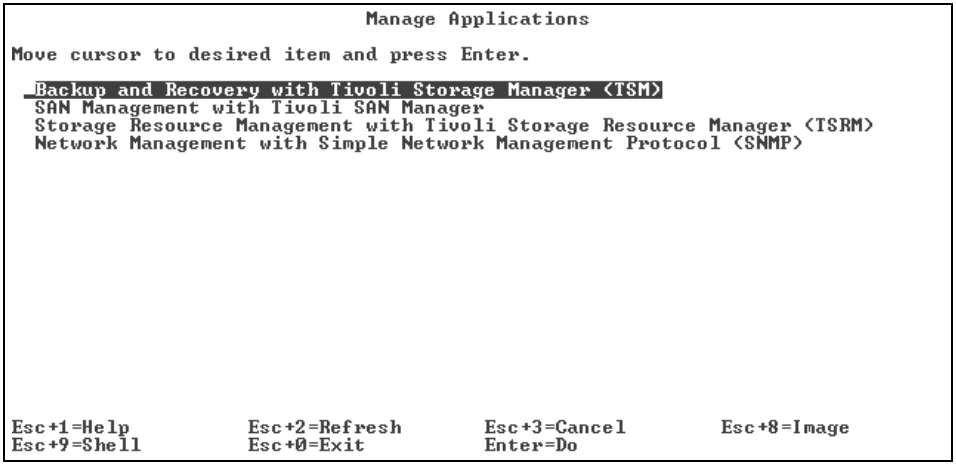


Figure 17-4 Tivoli Storage Manager menu in the SMIT

Choose **Configure TSM Client** in the next panel.

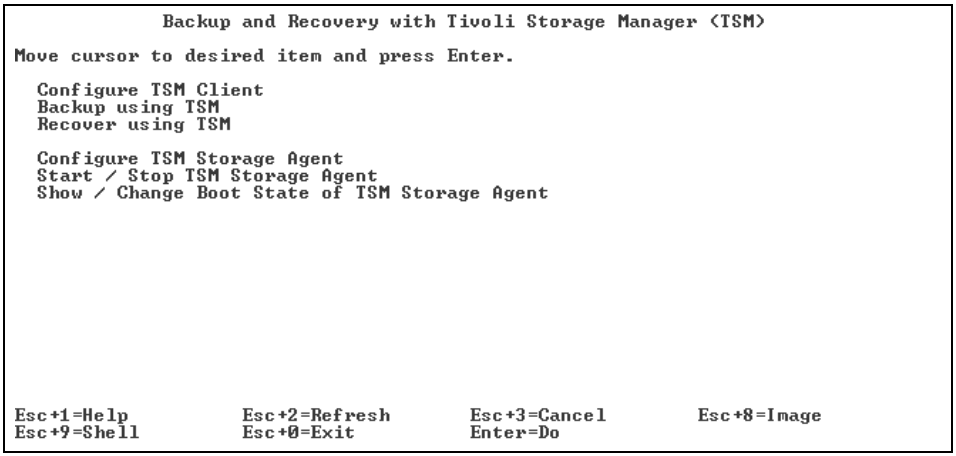


Figure 17-5 Configure IBM Tivoli Storage Manager Client

Now you can enter the right settings for the Tivoli Storage Manager environment. Specify the **TSM Server NAME**, **TSM Server ADDRESS**, the correct **TSM Server Port**, **NODEname** and **PASSWORD** (Your Tivoli Storage Manager Administrator will probably provide you the necessary information) (Figure 17-6).

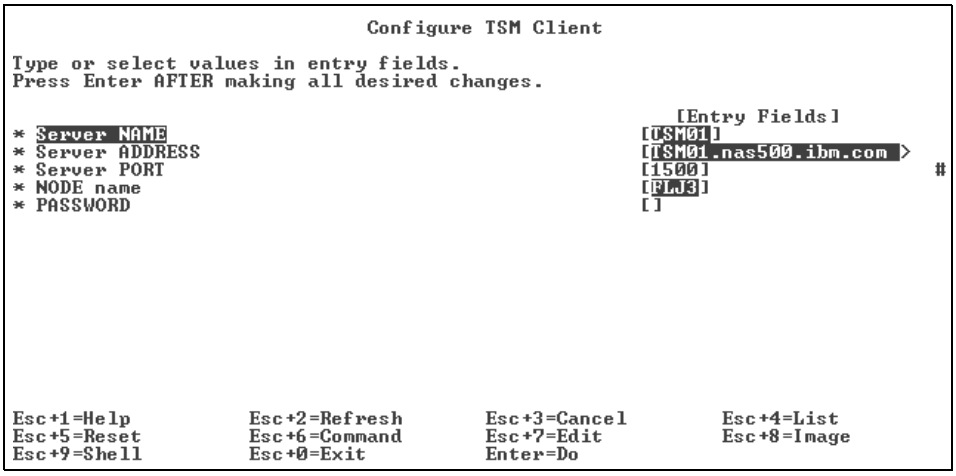


Figure 17-6 IBM Tivoli Storage Manager Client settings

This will update the Tivoli Storage Manager configuration files. An underlying automatism enables you to simplify the configuration if the cluster works properly. This means that some settings are passed to the other clustered node (Figure 17-7).

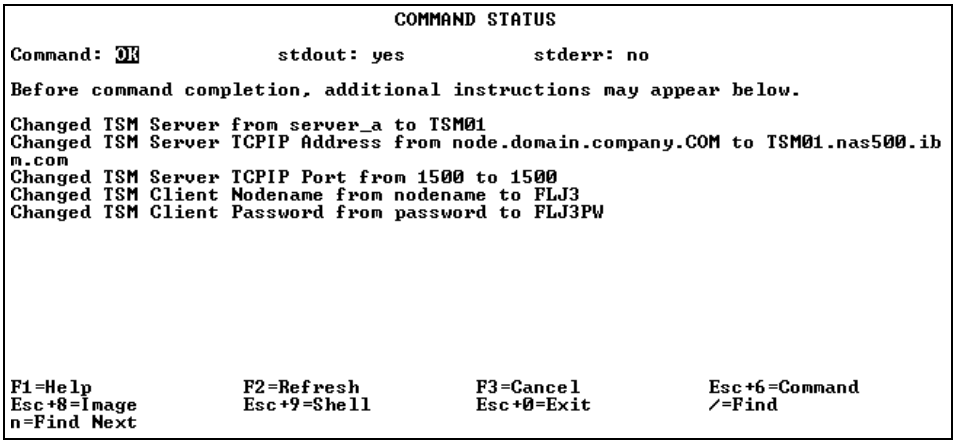


Figure 17-7 Tivoli Storage Manager Client update

Configure Tivoli Storage Manager Client via editing the IBM Tivoli Storage Manager configuration files. Compared to the WebSM and SMIT configuration, all settings have to be done on both cluster nodes (applies for clustered environments).

Remember that UNIX Clients use dsm.opt and dsm.sys files. In your environment the files should be located in /usr/tivoli/tsm/client/ba/bin.

IBM Tivoli Storage Manager Client configuration via editing configuration files:

Here are only the initial configuration settings described. Other specific settings are required to optimize the environment.

Configure dsm.sys file:

SErvername — TSM01
COMMethod — TCPip
TCPPort — 1500
TCPServeraddress — 192.168.244.11 * User your IBM Tivoli Storage Manager Server address instead of this placeholder address
NODEname — FLJ3 * We used FLJ3
Passwordaccess — Generate

Configure dsm.opt file:

SErvername — TSM01 * reference to the dsm.sys

LAN based backup and restore

This section describes IBM Tivoli Storage Manager and LAN based backups. If a LAN based backup job is started, the IBM Tivoli Storage Manager Client tries to connect to the IBM Tivoli Storage Manager Server to authenticate this session. If the server and client are correctly set up, the session will be established. Then the IBM Tivoli Storage Manager Client sends its data via TCP/IP to the IBM Tivoli Storage Manager Server. The IBM Tivoli Storage Manager Server stores references and version information in its database; however, the data will be stored in storage pools.

The next example shows how to back up data via the WebSM interface.

Open WebSM, select **NAS Management**, your system (for example, IP Address), **Applications**, **Tivoli Backup Restore**, **Backup using TSM Client** (Figure 17-8).

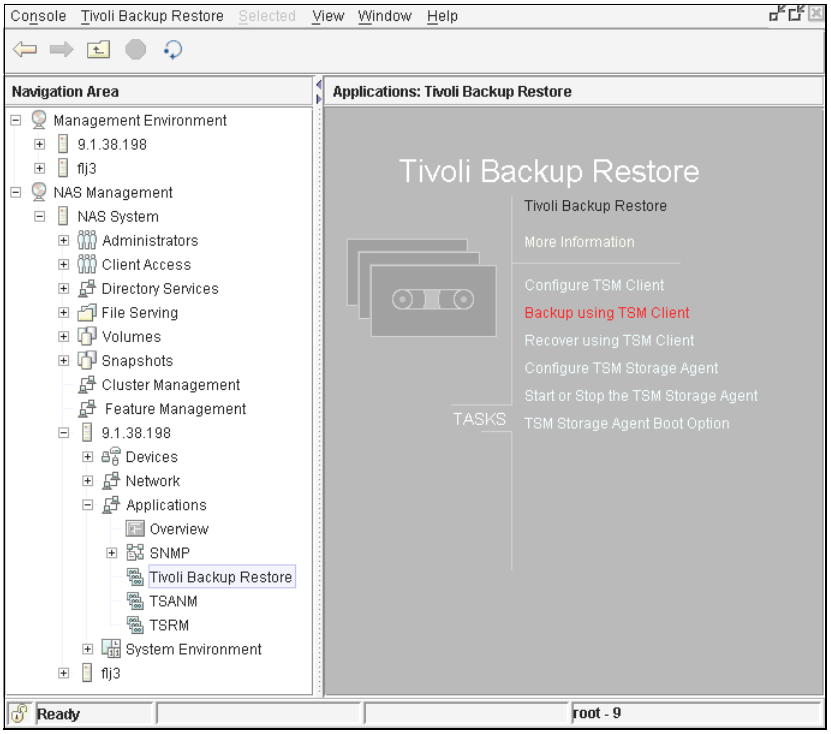


Figure 17-8 IBM Tivoli Storage Manager Client backup WebSM start screen

We specified the file system /Vols/FJL3VOL01 and the Incremental backup method (Figure 17-9).

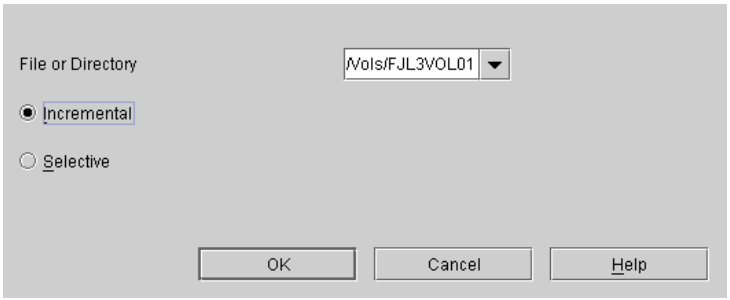


Figure 17-9 IBM Tivoli Storage Manager Client backup options

Tip: If you use Selective to back up a file system (for example, /home or /Vols/volcifs) you may use a trailing slash (for example /home/ or /Vols/volcifs/).

Note: The results of backing up with WebSM selective an object with the * wildcard differs from the original command, such as, if the asterisk is used at the end of the expression. (for example, command **`dsmc selective /home/*`** WebSM **Selective File or Directory /home/***)

Note: Verify if subdirectories are backed up or should be backed up. WebSM selective backup does not use the IBM Tivoli Storage Manager Client -subdir option.

The result will be displayed on the screen shown in Figure 17-10.

.

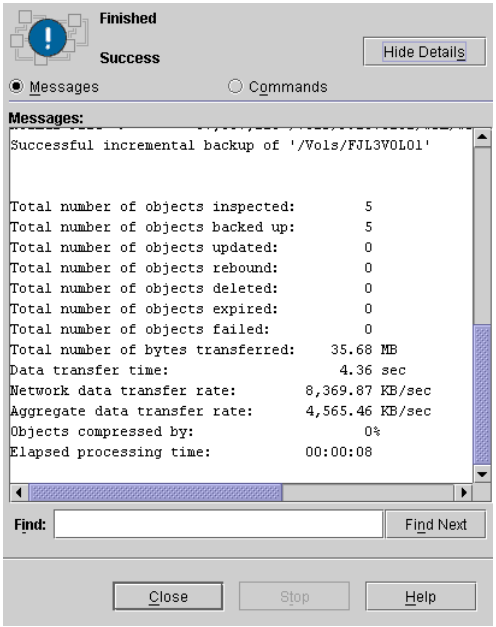


Figure 17-10 Backup successfully completed

Tip: The WebSM IBM Tivoli Storage Manager backup always uses the standard IBM Tivoli Storage Manager configuration settings in /usr/tivoli/tsm/client/ba/bin/dsm.sys and the standard path to the IBM Tivoli Storage Manager executables in /usr/tivoli/tsm/client/ba/bin.

Performing a restore with IBM Tivoli Storage Manager:

Restore of a single file. We used the WebSM to restore the file /Vols/FJL3VOL01/work/zyx. The filesystem /Vols/FJL3VOL01 was previously backed up. To restore a file open the WebSM, select **NAS Management**, your system (for example, IP Address), **Applications**, **Tivoli Backup Restore**, **Recover using TSM Client** (Figure 17-11).

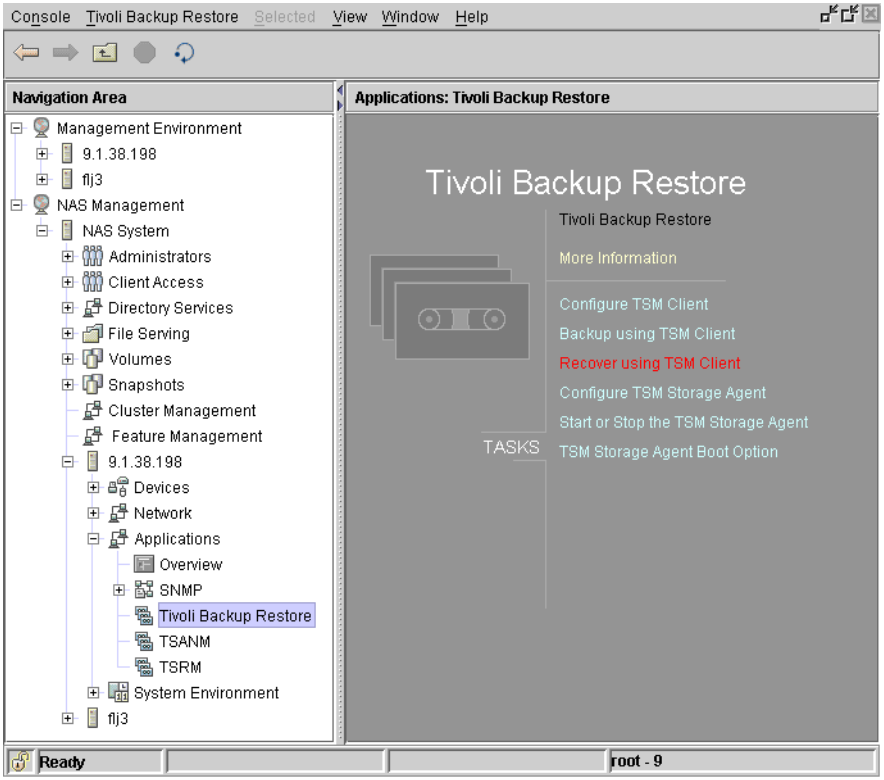


Figure 17-11 WebSM entry to restore a single file

We deleted file xyz on command line, to be sure the restore was OK. Our file system was /Vols/FJL3VOL01(Figure 17-12).

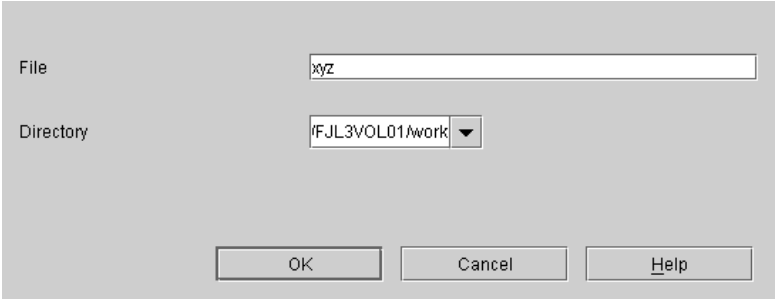


Figure 17-12 WebSM restore options

The result will be displayed on the screen shown in Figure 17-13.

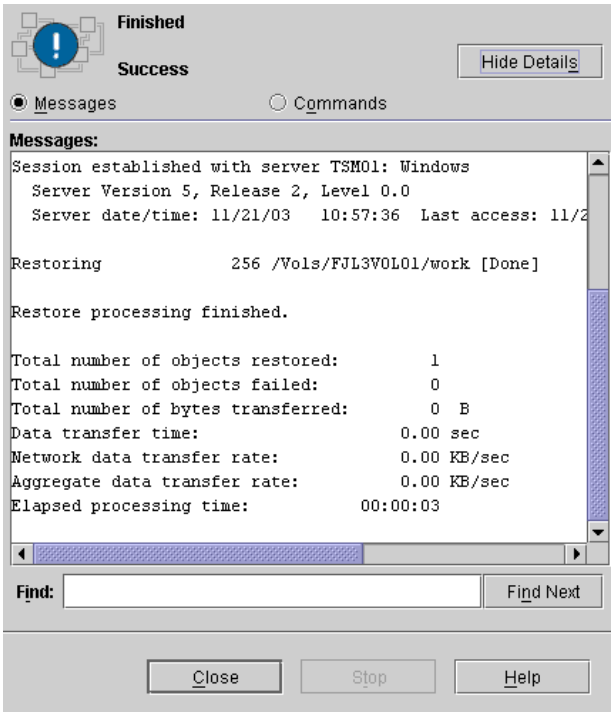


Figure 17-13 Successfully restored file

Instead of using the WebSM, you can also use the SMIT interface to restore file, directories, etc. The following example shows a restore of a single file as NAS Administrator (we used nasadmin). To start, use **`smit backup`** (Figure 17-14).

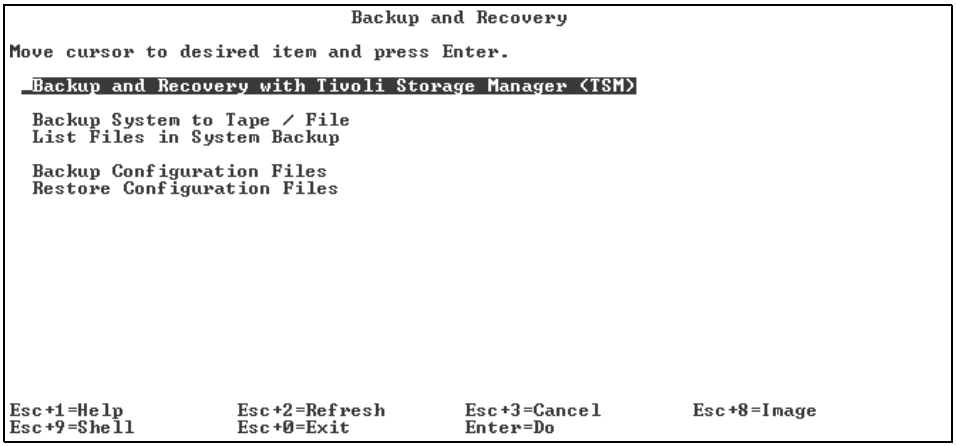


Figure 17-14 Single file restore using SMIT part1

Select **Recover using TSM** (Figure 17-15).

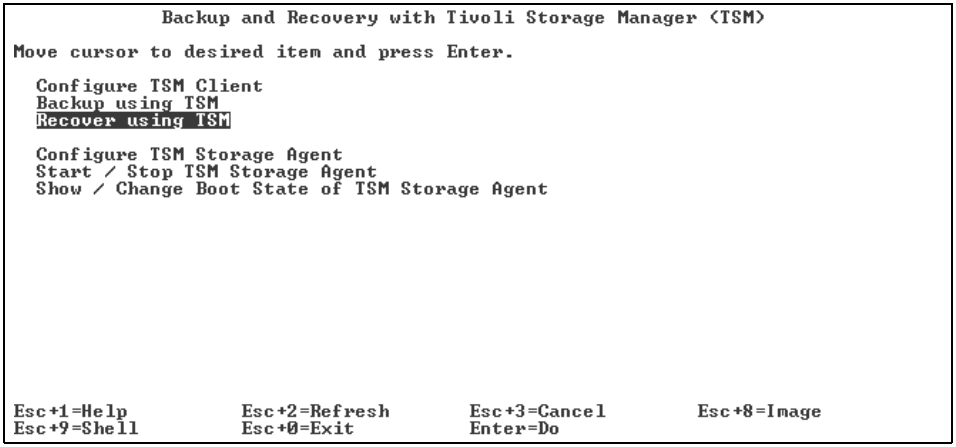


Figure 17-15 Single file restore using SMIT part2

Select **TSM Restore file(s)** (Figure 17-16).

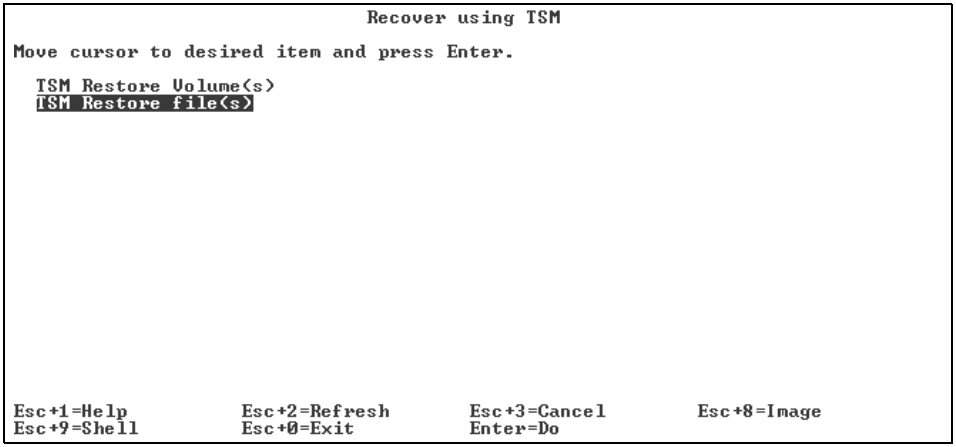


Figure 17-16 Select restore function

Then specify the file which has to be restored. In our example, this is again file xyz (Figure 17-17).

```
                                TSM Restore file(s)

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                          [Entry Fields]
* File(s) to restore                                    <ls/FJL3VOL01/work/xyz]



Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel        Esc+4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 17-17 Specify the file(s) to be restored

The restore process should end successfully (Figure 17-18).

```
                                COMMAND STATUS

Command: OK             stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...14]
ANS1114I Waiting for mount of offline media.
Restoring              11 /Vols/FJL3VOL01/work/xyz [Done]

Restore processing finished.

Total number of objects restored:         1
Total number of objects failed:           0
Total number of bytes transferred:       43  B
Data transfer time:                    0.00 sec
Network data transfer rate:        2,624.51 KB/sec
Aggregate data transfer rate:          0.01 KB/sec
Elapsed processing time:           00:00:03

[BOTTOM]

Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel        Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

Figure 17-18 Restore results

LAN-free backup and restore

Principally, the output of a LAN-free or LAN based backup should look very similar, because you use the same tools (GUI, command line). Just the manner of how the data is transferred differs; but this is transparent to the user.

We give a short overview of how to back up with IBM Tivoli Storage Manager in LAN free mode. Detailed information can be found in IBM Tivoli Storage Manager documentation or IBM Redbooks.

Note: You should look for the requirements regarding software, driver versions and which devices are supported before you start with the configuration.

First prepare your IBM Tivoli Storage Manager Server.

Note: IBM Tivoli Storage Manager Server to Server Communication should be set up previously.

Tell the IBM Tivoli Storage Manager Server about the new StorageAgent (NAS Gateway 500):

```
define server flj3_ag serverpassword=xxxx hladdress=9.1.38.198
lladdress=1500 validateprotocol=all
```

Then prepare the IBM Tivoli Storage Manager Server for the LAN-free tasks:

- Update or create policy (for your clients which will backup LAN-free)
- Register node (all new LAN-free clients)
- Define library (used for IBM Tivoli Storage Manager Server and IBM Tivoli Storage Manager Storage Agents)
- Define path to library
- Define drives
- Define path to drives
- Define device class,
- Define storage pool
- Verification of LAN and SAN

Configure the IBM Tivoli Storage Manager Storage Agent on the NAS Node (WebSM or smit / command line)

We used root and command line:

```
/usr/tivoli/tsm/StorageAgent/bin/dsmsta SETSTORAGESERVER
MYName=FLJ3_AG MYPassword=xxxxx MYHLAddress=9.1.38.198
SERVERName=TSM01 SERVERPAssword=yyyyy HLAddress=9.1.38.199
LLAddress=1500
```

The output should look similar to Figure 17-19:

```
(/usr/tivoli/tsm/StorageAgent/bin)--> /usr/tivoli/tsm/StorageAgent/bin/dsmsta)
ANR7800I DSMSERV generated at 09:57:11 on Jun 13 2003.

Tivoli Storage Manager for AIX-RS/6000
Version 5, Release 2, Level 0.0

Licensed Materials - Property of IBM

(C) Copyright IBM Corporation 1999,2003. All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corporation.

ANR0900I Processing options file dsmsta.opt.
ANR7811I Direct I/O will be used for all eligible disk files.
ANR1432I Updating device configuration information to defined files.
ANR1433I Device configuration information successfully written to devconfig.
ANR2119I The SERVERNAME option has been changed in the options file.
ANR0467I The SETSTORAGESERVER command completed successfully.(/usr/tivoli/tsm/St
orageAgent/bin)-->
```

Figure 17-19 Configuration output

The file dsmsta.opt (/usr/tivoli/tsm/StorageAgent/bin) should have at least a SERVERENAME and DEVCONFIg entry. For example:

```
DEVCONFIg devconfig
```

The DEVCONFIg entry names the file which keeps information regarding the StorageAgent configuration. In our case the file name is devconfig. Figure 17-20 shows our configuration.

```
SET STANAME FLJ3_AG
SET STAPASSWORD 254875763jfcgh3
SET STAHLADDRESS 192.168.38.198
DEFINE SERVER TSM01 HLADDRESS=192.168.38.199 LLADDRESS=1500 SERVERPA=12532hfdhgj
hdj
~
~
```

Figure 17-20 Sample IBM Tivoli Storage Manager Storage Agent configuration file

The IBM Tivoli Storage Manager Client configuration must be updated. The following entries are necessary to enable LAN free data transfer:

```
enablelanfree yes
LANFREEC TCPIP
LANFREETCPPORT 1500
```

Note: Do not forget to set the IBM Tivoli Storage Manager environment variables on the client node.

17.1.4 Automation of backups

Automating IBM Tivoli Storage Manager backups can be done in several ways. The Administrator can use tools from the operating system or functions offered by IBM Tivoli Storage Manager. The backup task can be triggered, for example, by an AIX **cron** job, the **at** command, or an IBM Tivoli Storage Manager Client schedule. The **cron** job allows you to run a job at the specified time and date. The **crontab** file can be updated via the **crontab** command. See the manual pages for detailed information regarding the **crontab** and the **at** command.

The IBM Tivoli Storage Manager Scheduler is a function provided by the IBM Tivoli Storage Manager Client. It allows you to poll or query the IBM Tivoli Storage Manager Server for scheduled tasks (backup, restore, and many more). Before the scheduler is started, the IBM Tivoli Storage Manager Server administrator has to define scheduled tasks on the IBM Tivoli Storage Manager Server.

The IBM Tivoli Storage Manager Scheduler is basically started by the **dsmc schedule** command. This command runs the scheduler until the user who executed the command logs off, closes the window, or ends the process.

On an AIX powered system, you should provide more information (for example, do not terminate the scheduler if the user who started the command logs off, closes the window, etc.)

For example, on your IBM Tivoli Storage Manager Client, you can start the scheduler in the background and keep it running even after a logoff:

```
nohup dsmc schedule 2>/dev/null &
```

Tip: You can specify the **passwordaccess generate** option in your IBM Tivoli Storage Manager Client configuration file (dsm.sys) if you do not want to specify the client password in the **dsmc schedule** command. If you use the default setting, you can provide the password with the **dsmc** command.

Instead of sending the output to /dev/null, you can send the standard error output to for example, nohup.out.

Root User: To start the client scheduler automatically, ensure that the passwordaccess option is set to generate in your client system options file (dsm.sys), then follow the procedure below for your operating system:

Add the following entry to the /etc/inittab file:

```
tsm::once:/usr/bin/dsmc sched >/dev/null 2>&1 #TSM scheduler
```

Note: You *must* include the redirection to /dev/null in the command here. The respawn option in the inittab allows you to restart the process if it terminates.

17.1.5 Clustering considerations

If you work with cluster protected resources, your configuration will be different tor a regular IBM Tivoli Storage Manager Client configuration. In a clustered environment you usually partition your data in two sections: the node related (bound to a specific hardware) and the resource group related data (virtual data).

The node related data, for example, is the data in the rootvg. Every cluster node has its own operating system and settings. This configuration is bound to the one node.

The resource group related data is the user data which can theoretically reside on either node A or node B of the cluster. Therefore we call this data virtual data, because the user accesses the data in a virtual manner by a dedicated IP address and network name.

Since the purpose of HACMP is to take over / fail over resources to other nodes, the IBM Tivoli Storage Manager configuration and the backup automatism should be passed to the other node as well. This enables you to back up or restore data independent of which node the resource is using.

This means that you probably use multiple IBM Tivoli Storage Manager Client configurations for each resource and the both nodes. The node related IBM Tivoli Storage Manager backup related configuration could reside in the standard IBM Tivoli Storage Manager directory (/usr/tivoli/tsm/client/ba/bin). Resource group related data should reside on the shared disk (volume group which is part of the HACMP managed resource). So only the node who owns the data at this time is able to read the information and to avoid to have different configurations on both machines. If each node could store its own configuration file for the HACMP managed resource, both files have to be updated if the configuration of this particular IBM Tivoli Storage Manager Client configuration changes.

Choose “virtual” names for the resources, maybe with a hint as to whom the resource “belongs” normally.

If you want to integrate automated IBM Tivoli Storage Manager scheduling tasks in a HACMP clustered environment, remember to generate start and stop scripts. They will start the IBM Tivoli Storage Manager Scheduler on a node after the resource group gets online on a node and stops the IBM Tivoli Storage Manager Scheduler on a node if the resource groups takes / fails over to another node.

The SMIT path for adding a start / stop script in SMIT is:

smit hacmp -> Extended Configuration -> Extended Resource configuration -> HACMP Extended Resources Configuration -> Configure HACMP Application Servers -> Add an Application Server

Do not forget to provide the correct IBM Tivoli Storage Manager environment variables (DSM_DIR, DSM_CONFIG, etc) in your start and stop scripts, assuming not to use the standard IBM Tivoli Storage Manager configuration which should be used for the node related data.

The start script should contain at least the IBM Tivoli Storage Manager environment variables and the start of **dsmc schedule** with **nohup**.

In the stop script, the IBM Tivoli Storage Manager Scheduler should be stopped. This can be done by killing the process by the belonging process ID. The process ID can be tracked during the start of the process (for example, save to a file in order to read the process ID and pass to a section of the stop script which kills the IBM Tivoli Storage Manager Scheduler).

In a clustered environment, the IBM Tivoli Storage Manager Scheduler entry should be removed from the /etc/inittab. The control should be done by the HACMP cluster.

Part 5

Appendixes

In this part of the book, we provide the following supplementary information:

- Appendix A, “Error log information” on page 373
- Appendix B, “Windows networking basic definitions” on page 381
- Appendix C, “NFS networking basic definitions” on page 389
- Appendix D, “Additional material” on page 393

A

Error log information

The following topics are included in this appendix:

- A general discussion about the error logging subsystem
- An explanation of how to read error logs

Overview

The error-logging process begins when an operating system module detects an error. The error-detecting segment of code then sends error information to either the **errsave** and **errlast** kernel services or the **errlog** application subroutine where the information is, in turn, written to the /dev/error special file. This process then adds a timestamp to the collected data. The **errdemon** daemon constantly checks the /dev/error file for new entries, and when new data is written, the daemon conducts a series of operations.

Before an entry is written to the error log, the **errdemon** daemon compares the label sent by the kernel or application code to the contents of the *error record template repository*. If the label matches an item in the repository, the daemon collects additional data from other parts of the system.

The system administrator can look at the error log to determine what caused a failure, or to periodically check the health of the system when it is running.

Clearing the error log

Clearing of the error log implies deleting old or unnecessary entries from the error log. Clearing is normally done as part of the daily **cron** command execution. To check it, type:

```
# crontab -l | grep errclear
0 11 * * * /usr/bin/errclear -d S,O 30
0 12 * * * /usr/bin/errclear -d H 90
```

If it is not done automatically, you should probably clean the error log regularly.

To delete all the entries from the error log, use the following command:

```
# errclear 0
```

To selectively remove entries from the error log, for example, to delete all software error entries, use the following command:

```
# errclear -d S 0
```

To selectively remove entries from the error log, for example, to delete all hardware error entries, use the following command:

```
# errclear -d H 0
```

Alternatively, use the **smitty errclear** command.

Reading error logs in detail

You can generate an error report from data collected in the error log. There are two main ways to view the error log:

- The easiest way to read the error log entries is with the **smitty errpt** command. Output from this command is shown in Figure A-1.

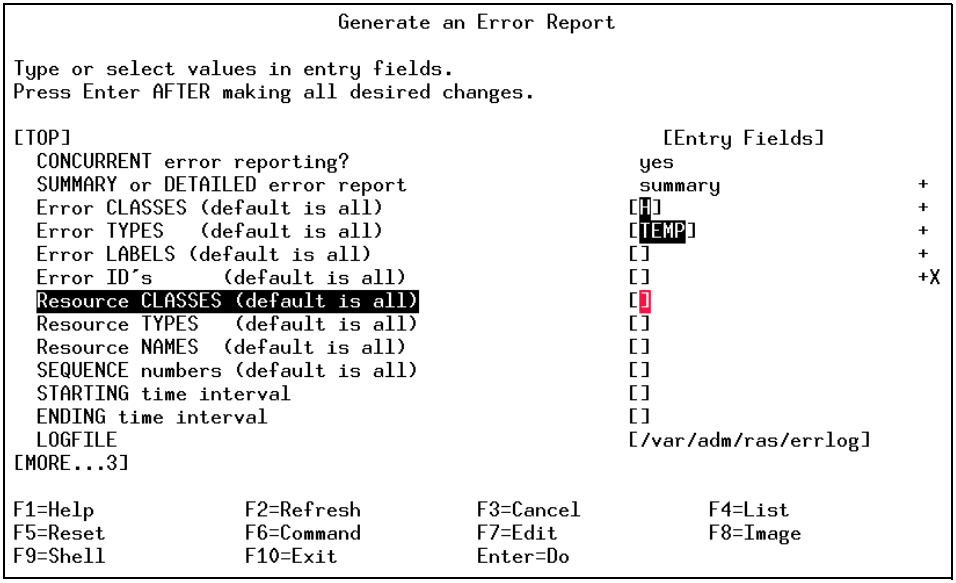


Figure A-1 smitty errpt output

- The second way to display error log entries is with the **errpt** command. It allows flags for selecting errors that match specific criteria. By using the default condition, you can display error log entries in the reverse order they occurred and were recorded.

The errpt command output

By using the -c flag, you can display errors as they occur. The default summary report contains one line of data for each error:

```
# errpt | pg
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
2BFA76F6   0627172400 T S SYSPROC        SYSTEM SHUTDOWN BY USER
9DBCFDEE   0627172700 T O errdemon       ERROR LOGGING TURNED ON
192AC071   0627172300 T O errdemon       ERROR LOGGING TURNED OFF
1581762B   0627132600 T H cd0            DISK OPERATION ERROR
1581762B   0627132000 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
E18E984F   0627100000 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0627095400 P S SRC            SOFTWARE PROGRAM ERROR
```

The fields used in this report are discussed in the following sections.

Identifier

Numerical identifier for the event.

Timestamp

Time when the error occurs in format mmddhhmmyy. The timestamp 0627172400 indicates that the error occur June 27th at 17:24 (5:24 p.m.) year 00 (year 2000).

Type

Severity of the error that has occurred. There are six possible values:

PEND The loss of availability of a device or component is imminent.

PERF The performance of the device or component has degraded to below an acceptable level.

PERM A condition has occurred that could not be recovered from. Error types with this value are usually the most severe errors and are more likely to mean that you have a defective hardware device or software module. Error types other than PERM usually do not indicate a defect, but they are recorded so that they can be analyzed by the diagnostics programs.

TEMP A condition occurred that was recovered from after a number of unsuccessful attempts.

UNKN It is not possible to determine the severity of the error.

INFO The error log entry is informational and was not the result of an error.

Class

General source of the error. The possible error classes are:

H Hardware. When you receive a hardware error, refer to your system operator guide for information about performing diagnostics on the problem device or other piece of equipment.

S Software.

O Informational messages.

U Undetermined (for example, network).

Resource name

For software errors, this is the name of a software component or an executable program. For hardware errors, this is the name of a device or system component. It is used to determine the appropriate diagnostic modules that are to be used to analyze the error.

Description

A brief summary of the error.

Formatted output from errpt command

The following list provides a series of format options for the **errpt** command.

- To list all hardware errors, enter:

```
# errpt -d H
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
1581762B   0627132600 T H cd0            DISK OPERATION ERROR
1581762B   0627132000 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
5BF9FD4D   0615173700 T H tok0           PROBLEM RESOLVED
2A9F5252   0615161700 P H tok0           WIRE FAULT
2A9F5252   0615161600 P H tok0           WIRE FAULT
2A9F5252   0615161600 P H tok0           WIRE FAULT
5BF9FD4D   0615155900 T H tok0           PROBLEM RESOLVED
2A9F5252   0615151400 P H tok0           WIRE FAULT
2A9F5252   0615151300 P H tok0           WIRE FAULT
2A9F5252   0615151300 P H tok0           WIRE FAULT
2A9F5252   0615151300 P H tok0           WIRE FAULT
```

- To get a detailed report of all software errors, enter:

```
# errpt -a -d S | pg
---------------------------------------------------------------------------
LABEL:          REBOOT_ID
IDENTIFIER:     2BFA76F6

Date/Time:       Tue Jun 27 17:24:55
Sequence Number: 33
Machine Id:      006151424C00
Node Id:         server4
Class:           S
Type:            TEMP
Resource Name:   SYSPROC

Description
SYSTEM SHUTDOWN BY USER

Probable Causes
SYSTEM SHUTDOWN

Detail Data
USER ID
           0
0=SOFT IPL 1=HALT 2=TIME REBOOT
           0
TIME TO REBOOT (FOR TIMED REBOOT ONLY)
           0
---------------------------------------------------------------------------
...
```

- To display a report of all errors logged for the error identifier E18E984F, enter:

```
# errpt -j E18E984F
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
E18E984F   0627100000 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0627095400 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0627093000 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0626182100 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0626181400 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0626130400 P S SRC            SOFTWARE PROGRAM ERROR
```

- To display a report of all errors that occur after June 26, 2000 at 18:14 (time), enter:

```
# errpt -s 0626181400
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
2BFA76F6   0627172400 T S SYSPROC        SYSTEM SHUTDOWN BY USER
9DBCFDEE   0627172700 T O errdemon       ERROR LOGGING TURNED ON
192AC071   0627172300 T O errdemon       ERROR LOGGING TURNED OFF
```

```
1581762B   0627132600 T H cd0            DISK OPERATION ERROR
1581762B   0627132000 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
E18E984F   0627100000 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0627095400 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0627093000 P S SRC            SOFTWARE PROGRAM ERROR
2BFA76F6   0627092700 T S SYSPROC        SYSTEM SHUTDOWN BY USER
9DBCFDEE   0627092900 T O errdemon       ERROR LOGGING TURNED ON
192AC071   0627092500 T O errdemon       ERROR LOGGING TURNED OFF
369D049B   0626183400 I O SYSPFS         UNABLE TO ALLOCATE SPACE IN FILE
SYSTEM
E18E984F   0626182100 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0626181400 P S SRC            SOFTWARE PROGRAM ERROR
```

- To obtain all the errors with resource name cd0 from the error log, enter:

```
# errpt -N cd0
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
1581762B   0627132600 T H cd0            DISK OPERATION ERROR
1581762B   0627132000 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
1581762B   0627131900 T H cd0            DISK OPERATION ERROR
```

- The -c flag formats and displays each of the error entries concurrently, that is, at the time they are logged. The existing entries in the log file are displayed in the order in which they were logged. An example below:

```
# errpt -c
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
9DBCFDEE   0823160702 T O errdemon       ERROR LOGGING TURNED ON
2BFA76F6   0823160002 T S SYSPROC        SYSTEM SHUTDOWN BY USER
FFE305EE   0823160702 P H tok0           WIRE FAULT
75CE5DC5   0823160702 I H tok0           ADAPTER ERROR
E18E984F   0823160802 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0823160802 P S SRC            SOFTWARE PROGRAM ERROR
E18E984F   0823160802 P S SRC            SOFTWARE PROGRAM ERROR
FFE305EE   0823160802 P H tok0           WIRE FAULT
```

The errpt command

The **errpt** command generates an error report from entries in an error log. The command has the following syntax:

```
errpt [ -a ] [ -c ] [ -d ErrorClassList ] [ -e EndDate ] [ -j ErrorID ]
[ -s StartDate ] [ -N ResourceNameList ] [ -S ResourceClassList ]
[ -T ErrorTypeList ]
```

The commonly used flags are listed in Table A-1.

Table A-1 Commonly used flags of the errpt command

Flag	Description
-a	Displays information about errors in the error log file in detailed format.
-c	Formats and displays each of the error entries concurrently, that is, at the time they are logged. The existing entries in the log file are displayed in the order in which they were logged.
-d *ErrorClassList*	Limits the error report to certain types of error records specified by the valid ErrorClassList variables: H (hardware), S (software), 0 (errlogger command messages), and U (undetermined).
-e *EndDate*	Specifies all records posted prior to and including the EndDate variable.
-j *ErrorID*	Includes only the error-log entries specified by the ErrorID (error identifier) variable.
-s *StartDate*	Specifies all records posted on and after the StartDate variable.
-N *ResourceNameList*	Generates a report of resource names specified by the ResourceNameList variable. The ResourceNameList variable is a list of names of resources that have detected errors.
-S *ResourceClassList*	Generates a report of resource classes specified by the ResourceClassList variable.
-T *ErrorTypeList*	Limits the error report to error types specified by the valid ErrorTypeList variables: INFO, PEND, PERF, PERM, TEMP, and UNKN.

B

Windows networking basic definitions

This appendix explains some common Windows networking terms.

B-node (Broadcast node)

This is a type of NetBIOS end node that supports the NetBIOS service and contains applications. B-nodes communicate using a mix of UDP datagrams and TCP connections. B-nodes can freely interoperate with one another within a broadcast area; typically a single LAN segment. Other standard end nodes are point-to-point nodes (P-nodes) and mixed-mode nodes (M-nodes).

Browsing

This refers to viewing the resources available on a network. The browse list on a Windows network is the list of other hosts and domains available on a network. Windows maintains the browse list to present other hosts offering network services through a point-and-click user interface rather than asking users to remember the names of remote hosts and services. Windows clients use the browse list to construct the view of the network shown in the Network Neighborhood (renamed My Network Places in Windows 2000) and Windows Explorer. The browse list is also accessible from the command line using the NET VIEW command.

Windows for Workgroups and Windows NT domains maintain the browse list on a computer called the Master Browser. Whenever a computer offers a network service for the first time, it broadcasts a server announcement packet. The Master Browser receives this packet and adds the computer's name to its browse list. In response, the Master Browser transmits a list of backup browsers to the new computer.

Each domain or workgroup contains at least one backup browser. A copy of the browse list is maintained on the backup browser to eliminate the need to rebuild the browse list if the Master Browser goes down. For more information about NT domains and network browsing, see the related Microsoft technet site on the World Wide Web.

CIFS

CIFS stands for Common Internet File System protocol. CIFS provides an open cross-platform mechanism for client systems to request file services from server systems over a network. It is based on the SMB protocol widely used by PCs and workstations running a wide variety of operating systems.

NetBIOS

The Network Basic Input/Output System (NetBIOS) is a vendor-independent network interface originally designed for IBM PC computer systems running PC-DOS or MS-DOS. NetBIOS is a software interface, not an actual networking protocol. It specifies the services that should be available without putting any restrictions on the protocol used to implement those services.

No officially defined NetBIOS standard exists. The original version, as described by IBM in 1984 in the IBM PC Network Technical Reference Manual, and is treated as the standard. Since its introduction, the following versions of NetBIOS have emerged, each using its own transport protocol: NetBEUI, NetBIOS over IPX, and NetBIOS over TCP/IP.

The CIFS server in the NAS Gateway 500 uses NetBIOS over TCP/IP.

NetBIOS interface to Application Programs

On PCs, NetBIOS includes both a set of services and an exact program interface to those services. The following types of NetBIOS services exist:

Name Service

NetBIOS resources are referenced by name. Lower-level addresses are not available to NetBIOS applications. An application representing a resource registers one or more names that it wants to use.

The name space is flat and not hierarchically organized. It uses 15 alphanumeric characters, plus a 16th •subcode• byte. Names cannot start with an asterisk (*).

Registration implies bidding for use of a name. The bid may be for exclusive (unique) or shared (group) ownership. Each application contends with other applications in real time. No two applications on the NetBIOS network can use the same unique name until the originating application requests that its name be deleted or the host is powered off or reset.

Name Service provides the Add Name, Add Group Name, and Delete Name primitive operations.

Session Service

A session is a full-duplex, sequenced, and reliable message exchange conducted between a pair of NetBIOS applications. Data is organized into messages.

Multiple sessions can exist between any two applications. Both applications participating in the session have access to the name of the remote application. No specification is given for resolving session requests to a group name into a data connection. A service is provided for the detection of a session failure by an application.

The Session Service provides the Call, Listen, Hang Up, Send, Receive, and Session Status primitive operations.

Datagram Service

The Datagram Service is an unreliable, nonsequenced, and connectionless communication between two NetBIOS applications. It is analogous to UDP service under TCP/IP.

Datagrams are sent under cover of a name properly registered to the sender. Datagrams can be sent to a specific name or be explicitly broadcast.

Datagrams sent to an exclusive name are received, if at all, by the holder of that name. Datagrams sent to a group name are multicast to all holders of that name. The sending application cannot distinguish between group and unique names and thus must act as if all nonbroadcast datagrams are multicast.

As with the Session Service, the receiver of the datagram is provided with the sending and receiving names.

The Datagram Service provides the Send Datagram, Send Broadcast Datagram, Receive Datagram, and Receive Broadcast Datagram primitive operations.

NetBIOS Name Resolution

This means mapping a NetBIOS name to its corresponding IP address. The techniques commonly used for name resolution are the Windows Internet Name Service (WINS), the LMHOSTS file, and the domain name system (DNS).The other techniques are defined as follows:

WINS/NBNS

When a new service is made available on the network, such as when a Windows machine boots or when CIFS is started, the service must be registered with a WINS server before it can be available to clients located on other subnets. The WINS server records the name of the host, the NT domain the host is part of, and the IP address of the host. Whenever a machine attempts to resolve a host name, it first checks with the WINS server. If the host is not registered there, it attempts to find the host using a broadcast. If the host is still not found, the system returns the message A computer or sharename could not be found. CIFS registers itself with any WINS server.

WINS also includes a method for replicating its database of host names with other WINS servers to create a backup WINS server that can host queries if the primary WINS server is unavailable. It also allows large networks that are encumbered by slow links to distribute WINS servers closer to clients and provide faster name resolution. (WINS is a proprietary Microsoft protocol.)

The CIFS file server can be configured to act as an NBNS (NetBIOS Name Service) server, providing most WINS functionality. CIFS can also be configured to act as a WINS proxy to other WINS or NBNS servers.

LMHOSTS file

The LMHOSTS (LAN Manager hosts) file is analogous to the UNIX /etc/hosts file. The LMHOSTS file allows specific NetBIOS server names to be mapped to IP addresses. It also provides a syntax for defining the domain in which a NetBIOS server resides, as well as loading an LMHOSTS file from a shared directory on a server.

Broadcast

NetBIOS names may be resolved using broadcast on the local subnet. It is analogous to address resolution protocol (ARP) in TCP/IP. The requesting machine broadcasts a NetBIOS Name Query. If the requested host receives the broadcast, it replies with its IP address. Because broadcasts are not forwarded, only hosts on local subnets may be resolved in this manner.

NetBIOS over TCP/IP

NetBIOS over TCP/IP was first proposed in Request for Comments (RFCs) 1001 and 1002. These RFCs describe an implementation of NetBIOS using Transmission Control Protocol (TCP) for connection-oriented session services and User Datagram Protocol (UDP) for datagram services.

This design has some significant advantages over NetBEUI and NetBIOS over IPX, as follows:

- NetBIOS uses the existing TCP/IP protocols, so it can be routed across the global Internet and any other wide area networks.
- Software implementing the NetBIOS interface can be built using existing TCP/IP implementation without requiring any new network drivers.Because most operating systems already support TCP/IP, most are capable of supporting NetBIOS with minimal additional effort.

NetBIOS scope

This is the population of computers across which a registered NetBIOS name is known. NetBIOS broadcast and multicast datagram operations must reach the entire extent of the NetBIOS scope.

The net command

The **net** command and its subcommands can be used to configure and administer the CIFS server from the command line. Alternatively, the Web-based System Manager and SMIT offer menu-driven interfaces for the same tasks.

Passthrough authentication

This is a mechanism employed by the CIFS server to validate user credentials with a domain controller and, if validated, to grant the user access to a resource on the CIFS server.

Server Message Block (SMB)

The Server Message Block protocol used to run on NetBIOS to implement Windows file sharing and print services. With this protocol, clients exchange messages (called server message blocks) with a server to access resources on that server. Every SMB message has a common format, consisting of a fixed-sized header followed by a variable-sized parameter and data component.

SMB messages are of the following types:

- Session control messages start, authenticate, and terminate sessions.
- File messages control file access.
- Message commands allow an application to send or receive messages to or from another host.

When an SMB client negotiates a connection with an SMB server, the two parties determine a common protocol to use for communication. This capability allows protocol extensions but can make SMB quite complex.

Shares

These are resources exported to the network by the CIFS server. CIFS supports file shares.

Workgroups

A workgroup is a logical collection of workstations and servers that do not belong to a domain. In a workgroup, each computer stores its own copy of user-account and group-account information. Therefore, in workgroups, users can only log directly in to machines on which they have accounts. Workgroup members are able to view and use resources on other systems. To do this, resources are shared in the workgroup, and network users are validated by the machine owning the resource.

C

NFS networking basic definitions

NFS is an acronym for Network File System, a product developed by Sun Microsystems. This is a distributed file system implementation providing remote, transparent access to files and directories. NAS Gateway 500 supports the latest NFS protocol update, NFS Version 3. NAS Gateway 500 also provides an NFS Version 2 client and server and is therefore providing backward compatibility with existing install bases of NFS clients and servers. Negotiation will occur to check what is the highest version of NFS supported by both involved systems.

NFS operates on a client/server basis. An NFS server has files on a local disk, which are accessed through NFS on a client machine. To handle this operation, NFS consists of:

- Networking protocols
- Client and server daemon

Protocols

The NFS specific protocols are Remote Procedure Call protocol (RPC) and eXternal Data Representation (XDR) protocol.

UDP or TCP

As all traffic on the Internet is more or less defined by the use of IP at the network layer, so is NFS. On the next layer, the Transport Layer, the choice of UDP or TCP is optional on NAS Gateway 500.

RPC

RPC is a library of procedures. The procedures allow one process (the client process) to direct another process (the server process) to execute procedure calls as though the client process had executed the calls in its own address space. Because the client and the server are two separate processes, they are not required to be on the same physical system, although they can. The RPC call used is based on the file system action taken by the user. For example, when issuing an `ls -la` command on an NFS mounted directory, the long listing will be done through a RPC named NFSPROC3_FSINFO, which will initiate the long listing on the server, which in turn will send the output from the command through RPC back to the client. To the user, this transaction is totally transparent.

XDR

Because the server and client processes can reside on two different physical systems, which may have completely different architectures, RPC must address the possibility that the two systems may not represent data in the same manner. Therefore, RPC uses data types defined by the eXternal Data Representation (XDR) protocol.

XDR is the specification for a standard representation of various data types. By using a standard data type representation, data can be interpreted correctly, even if the source of the data is a machine with a completely different architecture. XDR is used when the vnode points out that the file or directory accessed is not a local file or directory, but resides on a remote system. A conversion of data into XDR format is needed before sending the data. Conversely, when it receives data, it converts the data from XDR format into its own specific data type representation.

Daemons

Depending on the task, some of the NFS-related daemons are started on a system. Servers need the following daemons in an active state:

- **portmap**
- **nfsd**
- **rpc.mountd**

The client only needs the following daemons to be able to mount a remote directory:

- **portmap**
- **biod**

The portmap daemon

The **portmap** daemon converts RPC program numbers into Internet port numbers. When an RPC server starts up, it registers with the **portmap** daemon. The server tells the daemon which port number it is listening to and which RPC program numbers it serves. By this process, the **portmap** daemon knows the location of every registered port used by RPC servers on the host, and which programs are available on each of these ports. When mounting, the mount request starts with an RPC call named GETPORT that calls the **portmap** which, in turn, will inform the client of the port number that the called RPC server listens to. After this, the port number is used as reference for further communication. This is why the NFS daemons need to be registered with the **portmap** daemon.

A client consults the **portmap** daemon only once for each program the client tries to call. The **portmap** daemon tells the client which port to send the call to. The client stores this information for future reference. Since standard RPC servers are normally started by the **inetd** daemon, the **portmap** daemon must be started before the **inetd** daemon is invoked.

Note: If the **portmap** daemon is stopped or comes to an abnormal end, all RPC servers on the host must be restarted.

The rpc.mountd daemon

The **rpc.mountd** daemon handles the actual mount service needed when a client sends a mount request with an RPC procedure named MOUNTPROC3_MNT to the server. In addition, the **mountd** daemon provides a list of currently mounted file systems and the clients on which they are mounted.

The nfsd daemon

The **nfsd** daemon runs on a server and handles client requests for file system operations. Each daemon handles one request at a time. This means that on the server side, the receipt of any one NFS protocol request from a client requires the dedicated attention of an **nfsd** daemon until that request is satisfied, and the results of the request processing are sent back to the client. The **nfsd** daemons are the active agents providing NFS services.

The NFS daemons are inactive if there is no NFS requests to handle. When the NFS server receives RPC calls on the **nfsd**'s receive socket, **nfsd**'s are awakened to pick the packet of the socket and invoke the requested operations.

The biod daemon

The block I/O daemon (**biod**) runs on all NFS client systems. When a user on a client wants to read or write to a file on a server, the **biod** daemon sends this request to the server. For each read or write request, one biod is requested. The **biod** daemon is activated during system startup and runs continuously. The number of biods are limited on a per-mount-point basis.

D

Additional material

This redbook refers to additional material that can be downloaded from the Internet as described below.

Locating the Web material

The Web material associated with this redbook is available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser to:

ftp://www.redbooks.ibm.com/redbooks/SG247081

Alternatively, you can go to the IBM Redbooks Web site at:

ibm.com/redbooks

Select the **Additional materials** and open the directory that corresponds with the redbook form number, SG247081.

Using the Web material

The additional Web material that accompanies this redbook includes the following files:

File name	*Description*
batch.zip	This file contains the batch files for Windows that we discussed in this book.
corrections.zip	If it exists, this file can contain corrections, updates, and additions for the book.

Other files might be added to provide current coverage of the NAS Gateway 500.

How to use the Web material

Create a subdirectory (folder) on your workstation, and unzip the contents of the Web material zip file into this folder.

Abbreviations and acronyms

ABI	Application Binary Interface
ACE	Access Control Entries
ACL	Access Control List
AD	Microsoft Active Directory
ADSM	ADSTAR Distributed Storage Manager
AFS®	Andrew File System
AIX	Advanced Interactive eXecutive
ANSI	American National Standards Institute
APA	All Points Addressable
API	Application Programming Interface
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking
ARC	Advanced RISC Computer
ARPA	Advanced Research Projects Agency
ASCII	American National Standard Code for Information Interchange
ATE	Asynchronous Terminal Emulation
ATM	Asynchronous Transfer Mode
AVI	Audio Video Interleaved
BDC	Backup Domain Controller
BIND	Berkeley Internet Name Domain
BNU	Basic Network Utilities
BOS	Base Operating System
BRI	Basic Rate Interface
BSD	Berkeley Software Distribution
BSOD	Blue Screen of Death
BUMP	Bring-Up Microprocessor
CA	Certification Authorities
CAL	Client Access License
C-SPOC	Cluster single point of control
CDE	Common Desktop Environment
CDMF	Commercial Data Masking Facility
CDS	Cell Directory Service
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication
CIDR	Classless InterDomain Routing
CIFS	Common Internet File System
CMA	Concert Multi-threaded Architecture
CO	Central Office
CPI-C	Common Programming Interface for Communications

CPU Central Processing Unit

CSNW Client Service for NetWare

CSR Client/server Runtime

DAC Discretionary Access Controls

DARPA Defense Advanced Research Projects Agency

DASD Direct Access Storage Device

DBM Database Management

DCE Distributed Computing Environment

DCOM Distributed Component Object Model

DDE Dynamic Data Exchange

DDNS Dynamic Domain Name System

DEN Directory Enabled Network

DES Data Encryption Standard

DFS Distributed File System

DHCP Dynamic Host Configuration Protocol

DLC Data Link Control

DLL Dynamic Load Library

DS Differentiated Service

DSA Directory Service Agent

DSE Directory Specific Entry

DNS Domain Name System

DTS Distributed Time Service

EFS Encrypting File Systems

EGID Effective Group Identifier

EISA Extended Industry Standard Architecture

EMS Event Management Services

EPROM Erasable Programmable Read-Only Memory

ERD Emergency Repair Disk

ERP Enterprise Resources Planning

ERRM Event Response Resource Manager

ESCON Enterprise System Connection

ESP Encapsulating Security Payload

ESS Enterprise Storage Server

EUID Effective User Identifier

FAT File Allocation Table

FC Fibre Channel

FDDI Fiber Distributed Data Interface

FDPR Feedback Directed Program Restructure

FEC Fast EtherChannel technology

FIFO First In/First Out

FIRST Forum of Incident Response and Security

FQDN Fully Qualified Domain Name

FSF File Storage Facility

FTP File Transfer Protocol

FtDisk Fault-Tolerant Disk

GC Global Catalog

GDA Global Directory Agent

GDI Graphical Device Interface

GDS Global Directory Service

GID Group Identifier

GL	Graphics Library
GSNW	Gateway Service for NetWare
GUI	Graphical User Interface
HA	High Availability
HACMP	High Availability Cluster Multiprocessing
HAL	Hardware Abstraction Layer
HBA	Host Bus Adapter
HCL	Hardware Compatibility List
HSM	Hierarchical Storage Management
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines Corporation
ICCM	Inter-Client Conventions Manual
IDE	Integrated Drive Electronics
IDL	Interface Definition Language
IDS	Intelligent Disk Subsystem
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IIS	Internet Information Server
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
I/O	Input/Output
IP	Internet Protocol
IPC	Interprocess Communication
IPL	Initial Program Load
IPsec	Internet Protocol Security
IPX	Internetwork Packet eXchange
ISA	Industry Standard Architecture
iSCSI	SCSI over IP
ISDN	Integrated Services Digital Network
ISNO	Interface-specific Network Options
ISO	International Standards Organization
ISS	Interactive Session Support
ISV	Independent Software Vendor
ITSEC	Initial Technology Security Evaluation
ITSO	International Technical Support Organization
ITU	International Telecommunications Union
IXC	Inter Exchange Carrier
JBOD	Just a Bunch of Disks
JFS	Journaled File System
JIT	Just-In-Time
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCN	Logical Cluster Number
LDAP	Lightweight Directory Access Protocol

LFS Log File Service (Windows NT)

LFS Logical File System **(**AIX)

LFT Low Function Terminal

JNDI Java Naming and Directory Interface

LOS Layered Operating System

LP Logical Partition

LPC Local Procedure Call

LPD Line Printer Daemon

LPP Licensed Program Product

LRU Least Recently Used

LSA Local Security Authority

LTG Local Transfer Group

LUID Login User Identifier

LUN Logical Unit Number

LVCB Logical Volume Control Block

LVDD Logical Volume Device Driver

LVM Logical Volume Manager

MBR Master Boot Record

MDC Meta Data Controller

MFT Master File Table

MIPS Million Instructions Per Second

MMC Microsoft Management Console

MOCL Managed Object Class Library

MPTN Multi-protocol Transport Network

MS-DOS Microsoft Disk Operating System

MSCS Microsoft Cluster Server

MSS Maximum Segment Size

MSS Modular Storage Server

MWC Mirror Write Consistency

NAS Network Attached Storage

NBC Network Buffer Cache

NBF NetBEUI Frame

NBPI Number of Bytes per I-node

NCP NetWare Core Protocol

NCS Network Computing System

NCSC National Computer Security Center

NDIS Network Device Interface Specification

NDMP Network Data Management Protocol

NDS NetWare Directory Service

NETID Network Identifier

NFS Network File System

NIM Network Installation Management

NIS Network Information System

NIST National Institute of Standards and Technology

NLS National Language Support

NNS Novell Network Services

NSAPI Netscape Commerce Server's Application

NTFS NT File System

NTLDR NT Loader

NTLM NT LAN Manager

NTP	Network Time Protocol
NTVDM	NT Virtual DOS Machine
NVRAM	Non-Volatile Random Access Memory
NetBEUI	NetBIOS Extended User Interface
NetDDE	Network Dynamic Data Exchange
OCS	On-Chip Sequencer
ODBC	Open Database Connectivity
ODM	Object Data Manager
OLTP	OnLine Transaction Processing
OMG	Object Management Group
ONC	Open Network Computing
OS	Operating System
OSF	Open Software Foundation
OU	Organizational Unit
PAL®	Platform Abstract Layer
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PBX	Private Branch Exchange
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDC	Primary Domain Controller
PDF	Portable Document Format
PDT	Performance Diagnostic Tool
PEX	PHIGS Extension to X
PFS	Physical File System
PHB	Per Hop Behavior
PHIGS	Programmer's Hierarchical Interactive Graphics System
PID	Process Identification Number
PIN	Personal Identification Number
PMTU	Path Maximum Transfer Unit
POP	Post Office Protocol
POSIX	Portable Operating System Interface for Computer Environment
POST	Power-On Self Test
PP	Physical Partition
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PReP	PowerPC® Reference Platform
PSM	Persistent Storage Manager
PSN	Program Sector Number
PSSP	Parallel System Support Program
PV	Physical Volume
PVID	Physical Volume Identifier
QoS	Quality of Service
RACF®	Resource Access Control Facility
RAID	Redundant Array of Independent Disks

RAS Remote Access Service

RDBMS Relational Database Management System

RFC Request for Comments

RGID Real Group Identifier

RISC Reduced Instruction Set Computer

RMC Resource Monitoring and Control

RMSS Reduced-Memory System Simulator

ROLTP Relative OnLine Transaction Processing

ROS Read-Only Storage

RPC Remote Procedure Call

RRIP Rock Ridge Internet Protocol

RSCT Reliable Scalable Cluster Technology

RSM Removable Storage Management

RSVP Resource Reservation Protocol

SACK Selective Acknowledgments

SAK Secure Attention Key

SAM Security Account Manager

SAN Storage Area Network

SASL Simple Authentication and Security Layer

SCSI Small Computer System Interface

SDK Software Developer's Kit

SFG Shared Folders Gateway

SFU Services for UNIX

SID Security Identifier

SLIP Serial Line Internet Protocol

SMB Server Message Block

SMIT System Management Interface Tool

SMP Symmetric Multiprocessor

SMS Systems Management Server

SNA Systems Network Architecture

SNAPI SNA Interactive Transaction Program

SNMP Simple Network Management Protocol

SP System Parallel

SPX Sequenced Packet eXchange

SQL Structured Query Language

SRM Security Reference Monitor

SSA Serial Storage Architecture

SSL Secure Sockets Layer

SUSP System Use Sharing Protocol

SVC Serviceability

TAPI Telephone Application Program Interface

TCB Trusted Computing Base

TCP/IP Transmission Control Protocol/Internet Protocol

TCSEC Trusted Computer System Evaluation Criteria

TDI Transport Data Interface

TDP Tivoli Data Protection

TLS	Transport Layer Security
TOS	Type of Service
TSM	IBM Tivoli Storage Manager
TTL	Time to Live
UCS	Universal Code Set
UDB	Universal Database
UDF	Universal Disk Format
UDP	User Datagram Protocol
UFS	UNIX File System
UID	User Identifier
UMS	Ultimedia Services
UNC	Universal Naming Convention
UPS	Uninterruptable Power Supply
URL	Universal Resource Locator
USB	Universal Serial Bus
UTC	Universal Time Coordinated
UUCP	UNIX to UNIX Communication Protocol
UUID	Universally Unique Identifier
VAX	Virtual Address eXtension
VCN	Virtual Cluster Name
VFS	Virtual File System
VG	Volume Group
VGDA	Volume Group Descriptor Area
VGSA	Volume Group Status Area
VGID	Volume Group Identifier
VIPA	Virtual IP Address
VMM	Virtual Memory Manager
VP	Virtual Processor
VPD	Vital Product Data
VPN	Virtual Private Network
VRMF	Version, Release, Modification, Fix
VSM	Virtual System Management
W3C	World Wide Web Consortium
WAN	Wide Area Network
WFW	Windows for Workgroups
WINS	Windows Internet Name Service
WLM	Workload Manager
WWN	World Wide Name
WWW	World Wide Web
WYSIWYG	What You See Is What You Get
WinMSD	Windows Microsoft Diagnostics
XCMF	X/Open Common Management Framework
XDM	X Display Manager
XDMCP	X Display Manager Control Protocol
XDR	eXternal Data Representation
XNS	XEROX Network Systems
XPG4	X/Open Portability Guide

Glossary

A

Agent A software entity that runs on endpoints and provides management capability for other hardware or software. An example is an SNMP agent. An agent has the ability to spawn other processes.

AL See arbitrated loop.

Allocated storage The space that is allocated to volumes, but not assigned.

Allocation The entire process of obtaining a volume and unit of external storage, and setting aside space on that storage for a data set.

Arbitrated loop A Fibre Channel interconnection technology that allows up to 126 participating node ports and one participating fabric port to communicate. See also Fibre Channel Arbitrated Loop and loop topology.

Array An arrangement of related disk drive modules that have been assigned to a group.

B

Bandwidth A measure of the data transfer rate of a transmission channel.

Bridge Facilitates communication with LANs, SANs, and networks with dissimilar protocols.

C

Client A function that requests services from a server, and makes them available to the user. A term used in an environment to identify a machine that uses the resources of the network.

Client authentication The verification of a client in secure communications where the identity of a server or browser (client) with whom you wish to communicate is discovered. A sender's authenticity is demonstrated by the digital certificate issued to the sender.

Client-server relationship Any process that provides resources to other processes on a network is a server. Any process that employs these resources is a client. A machine can run client and server processes at the same time.

Console A user interface to a server.

D

DATABASE 2 (DB2) A relational database management system. DB2 Universal Database is the relational database management system that is Web-enabled with Java support.

Device driver A program that enables a computer to communicate with a specific device, for example, a disk drive.

Disk group A set of disk drives that have been configured into one or more logical unit numbers. This term is used with RAID devices.

E

Enterprise network A geographically dispersed network under the backing of one organization.

Enterprise Storage Server Provides an intelligent disk storage subsystem for systems across the enterprise.

Event In the Tivoli environment, any significant change in the state of a system resource, network resource, or network application. An event can be generated for a problem, for the resolution of a problem, or for the successful completion of a task. Examples of events are: the normal starting and s ping of a process, the abnormal termination of a process, and the malfunctioning of a server.

F

Fabric The Fibre Channel employs a fabric to connect devices. A fabric can be as simple as a single cable connecting two devices. The term is often used to describe a more complex network utilizing hubs, switches, and gateways.

FC See Fibre Channel.

FCS See Fibre Channel standard.

Fiber optic The medium and the technology associated with the transmission of information along a glass or plastic wire or fiber.

Fibre Channel A technology for transmitting data between computer devices at a data rate of up to 1 Gb. It is especially suited for connecting computer servers to shared storage devices and for interconnecting storage controllers and drives.

Fibre Channel Arbitrated Loop A reference to the FC-AL standard, a shared gigabit media for up to 127 nodes, one of which can be attached to a switch fabric. See also arbitrated loop and loop topology. Refer to American National Standards Institute (ANSI) X3T11/93-275.

Fibre Channel standard An ANSI standard for a computer peripheral interface. The I/O interface defines a protocol for communication over a serial interface that configures attached units to a communication fabric. Refer to ANSI X3.230-199x.

File system An individual file system on a host. This is the smallest unit that can monitor and extend. Policy values defined at this level override those that might be defined at higher levels.

G

Gateway In the SAN environment, a gateway connects two or more different remote SANs with each other. A gateway can also be a server on which a gateway component runs.

H

Hardware zoning Hardware zoning is based on physical ports. The members of a zone are physical ports on the fabric switch. It can be implemented in the following configurations: one to one, one to many, and many to many.

HBA See host bus adapter.

Host Any system that has at least one internet address associated with it. A host with multiple network interfaces can have multiple internet addresses associated with it. This is also referred to as a server.

Host bus adapter (HBA) A Fibre Channel HBA connection that allows a workstation to attach to the SAN network.

Hub A Fibre Channel device that connects up to 126 nodes into a logical loop. All connected nodes share the bandwidth of this one logical loop. Hubs automatically recognize an active node and insert the node into the loop. A node that fails or is powered off is automatically removed from the loop.

IP Internet protocol.

J

Java A programming language that enables application developers to create object-oriented programs that are very secure, portable across different machine and operating system platforms, and dynamic enough to allow expandability.

Java runtime environment (JRE) The underlying, invisible system on your computer that runs applets the browser passes to it.

Java Virtual Machine (JVM) The execution environment within which Java programs run. The Java virtual machine is described by the Java Machine Specification which is published by Sun Microsystems. Because the Tivoli Kernel Services is based on Java, nearly all ORB and component functions execute in a Java virtual machine.

JBOD Just a Bunch Of Disks.

JRE See Java runtime environment.

JVM See Java Virtual Machine.

L

Logical unit number (LUN) The LUNs are provided by the storage devices attached to the SAN. This number provides you with a volume identifier that is unique among all storage servers. The LUN is synonymous with a physical disk drive or a SCSI device. For disk subsystems such as the IBM Enterprise Storage Server, a LUN is a logical disk drive. This is a unit of storage on the SAN which is available for assignment or unassignment to a host server.

Loop topology In a loop topology, the available bandwidth is shared with all the nodes connected to the loop. If a node fails or is not powered on, the loop is out of operation. This can be corrected using a hub. A hub opens the loop when a new node is connected and closes it when a node disconnects. See also Fibre Channel Arbitrated Loop and arbitrated loop.

LUN See logical unit number.

LUN assignment criteria The combination of a set of LUN types, a minimum size, and a maximum size used for selecting a LUN for automatic assignment.

LUN masking This allows or blocks access to the storage devices on the SAN. Intelligent disk subsystems like the IBM Enterprise Storage Server provide this kind of masking.

M

Managed object A managed resource.

Managed resource A physical element to be managed.

Management Information Base (MIB) A logical database residing in the managed system which defines a set of MIB objects. A MIB is considered a logical database because actual data is not stored in it, but rather provides a view of the data that can be accessed on a managed system.

MIB See Management Information Base.

MIB object A MIB object is a unit of managed information that specifically describes an aspect of a system. Examples are CPU utilization, software name, hardware type, and so on. A collection of related MIB objects is defined as a MIB.

N

Network topology A physical arrangement of nodes and interconnecting communications links in networks based on application requirements and geographical distribution of users.

N_Port node port A Fibre Channel-defined hardware entity at the end of a link which provides the mechanisms necessary to transport information units to or from another node.

NL_Port node loop port A node port that supports arbitrated loop devices.

O

Open system A system whose characteristics comply with standards made available throughout the industry, and therefore can be connected to other systems that comply with the same standards.

P

Point-to-point topology It consists of a single connection between two nodes. All the bandwidth is dedicated for these two nodes.

Port An end point for communication between applications, generally referring to a logical connection. A port provides queues for sending and receiving data. Each port has a port number for identification. When the port number is combined with an Internet address, it is called a socket address.

Port zoning In Fibre Channel environments, port zoning is the grouping together of multiple ports to form a virtual private storage network. Ports that are members of a group or zone can communicate with each other but are isolated from ports in other zones. See also LUN masking and subsystem masking.

Protocol The set of rules governing the operation of functional units of a communication system if communication is to take place. Protocols can determine low-level details of machine-to-machine interfaces, such as the order in which bits from a byte are sent. They can also determine high-level exchanges between application programs, such as file transfer.

R

RAID Redundant array of inexpensive or independent disks. A method of configuring multiple disk drives in a storage subsystem for high availability and high performance.

S

SAN See storage area network.

SAN agent A software program that communicates with the manager and controls the subagents. This component is largely platform independent. See also subagent.

SCSI Small Computer System Interface. An ANSI standard for a logical interface to computer peripherals and for a computer peripheral interface. The interface utilizes a SCSI logical protocol over an I/O interface that configures attached targets and initiators in a multi-drop bus topology.

Server A program running on a mainframe, workstation, or file server that provides shared services. This is also referred to as a host.

Shared storage Storage within a storage facility that is configured such that multiple homogeneous or divergent hosts can concurrently access the storage. The storage has a uniform appearance to all hosts. The host programs that access the storage must have a common model for the information on a storage device. You need to design the programs to handle the effects of concurrent access.

Simple Network Management Protocol (SNMP) A protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

SNMP See Simple Network Management Protocol.

SNMP agent An implementation of a network management application which is resident on a managed system. Each node that is to be monitored or managed by an SNMP manager in a TCP/IP network, must have an SNMP agent resident. The agent receives requests to either retrieve or modify management information by referencing MIB objects. MIB objects are referenced by the agent whenever a valid request from an SNMP manager is received.

SNMP manager A managing system that executes a managing application or suite of applications. These applications depend on MIB objects for information that resides on the managed system.

SNMP trap A message that is originated by an agent application to alert a managing application of the occurrence of an event.

Software zoning Is implemented within the Simple Name Server (SNS) running inside the fabric switch. When using software zoning, the members of the zone can be defined with: node WWN, port WWN, or physical port number. Usually the zoning software also allows you to create symbolic names for the zone members and for the zones themselves.

SQL Structured Query Language.

Storage administrator A person in the data processing center who is responsible for defining, implementing, and maintaining storage management policies.

Storage area network (SAN) A managed, high-speed network that enables any-to-any interconnection of heterogeneous servers and storage systems.

Subagent A software component of SAN products which provides the actual remote query and control function, such as gathering host information and communicating with other components. This component is platform dependent. See also SAN agent.

Subsystem masking The support provided by intelligent disk storage subsystems like the Enterprise Storage Server. See also LUN masking and port zoning.

Switch A component with multiple entry and exit points or ports that provide dynamic connection between any two of these points.

Switch topology A switch allows multiple concurrent connections between nodes. There can be two types of switches, circuit switches and frame switches. Circuit switches establish a dedicated connection between two nodes. Frame switches route frames between nodes and establish the connection only when needed. A switch can handle all protocols.

T

TCP See Transmission Control Protocol.

TCP/IP Transmission Control Protocol/Internet Protocol.

Topology An interconnection scheme that allows multiple Fibre Channel ports to communicate. For example, point-to-point, arbitrated loop, and switched fabric are all Fibre Channel topologies.

Transmission Control Protocol (TCP) A reliable, full duplex, connection-oriented, end-to-end transport protocol running on of IP.

W

WAN Wide Area Network.

Z

Zoning In Fibre Channel environments, zoning allows for finer segmentation of the switched fabric. Zoning can be used to instigate a barrier between different environments. Ports that are members of a zone can communicate with each other but are isolated from ports in other zones. Zoning can be implemented in two ways: hardware zoning and software zoning.

Other glossaries:

For more information on IBM terminology, see the IBM Storage Glossary of Terms at:

http://www.storage.ibm.com/glossary.htm

For more information on Tivoli terminology, see the Tivoli Glossary at:

http://publib.boulder.ibm.com/tividd/glossary/termsmst04.htm

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 412.

- *Implementing the IBM TotalStorage NAS 300G, High Speed Cross Platform Storage and Tivoli SANergy!*, SG24-6278
- *IBM TotalStorage NAS 100 Integration Guide*, SG24-6913
- *IBM TotalStorage NAS Backup and Recovery Solutions*, SG24-6831-00
- *Managing IBM TotalStorage NAS with IBM Director*, SG24-6830-00
- *IP Storage Networking: NAS and iSCSI Solutions*, SG24-6240
- *Implementing IBM Director Management Solutions*, SG24-6188.
- *A Practical Guide to Tivoli SANergy*, SG24-6146
- *Tivoli SANergy Administrator’s Guide*, GC26-7389
- *Tivoli Storage Management Concepts*, SG24-4877
- *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416
- *Using Tivoli Storage Manager in a SAN Environment*, SG24-6132
- *IBM Tivoli Storage Manager: Bare Machine Recovery for AIX with SYSBACK*, REDP-3705
- *Red Hat Linux Integration Guide for IBM eServer xSeries and Netfinity*, SG24-5853
- *AIX 5L and Windows 2000: Side by Side*, SG24-4784
- *Configuring Highly Available Clusters Using HACMP 4.5*, SG24-6845
- *AIX 5L Performance Tools Handbook,* SG24-6039
- *pSeries 615 Models 6C3 and 6E3 Technical Overview and Introduction,* REPD-0160
- *IBM TotalStorage: FAStT Best Practices Guide,* REDP-3690
- *IBM TotalStorage FAStT700 and Copy Services,* SG24-6808

- *IBM TotalStorage Enterprise Storage Server Implementing ESS Copy Services in Open Environments,* SG24-5757.
- *IBM TotalStorage Enterprise Storage Server: Implementing the ESS in Your Environment,* SG24-5420
- *ESS Solutions for Open Systems Storage: Compaq Alpha Server, HP and SUN*, SG24-6119
- *IBM TotalStorage, Introducing the SAN Volume Controller and SAN Integration Server*, SG24-6423
- *IBM TotalStorage SAN Volume Controller and SAN File System integration*, SG24-6097

Other resources

These publications are also relevant as further information sources:

- Larry Peterson and Bruce Davie, *Computer Networks - A Systems Approach*, Morgan Kaufmann Publishers, 1996, ISBN 1558603689
- A. S. Tanenbaum, *Computer Networks*, Prentice Hall, 1996, ISBN 0133499456
- M. Schwartz, *Telecommunication Networks: Protocols, Modeling and Analysis*, Addison-Wesley, 1986, ISBN 020116423X
- Richard Petersen and Ibrahim Haddad, *Red Hat Linux X: The Complete Reference DVD Edition*, McGraw-Hill Osborne Media, 2003, ISBN 0072230754
- Matt Welsh, Mathias Kalle Dalheimer, and Lar Kaufman, *Running Linux (4th Edition)*, O'Reilly, 2002, ISBN 0596002726
- Scott M. Ballew, *Managing IP Networks with CISCO Routers*, O'Reilly, 1997, ISBN 1565923200
- Ellen Siever, et al., *Linux in a Nutshell (3rd Edition)*, O'Reilly, 2000, ISBN 0596000251
- Andreas Siegert, *The AIX Survival Guide*, Addison-Wesley, 1996, ISBN 0201593882
- Jay Ts, Robert Eckstein, David Collier-Brown,*Using Samba (2nd Edition)*, O'Reilly, 2003, ISBN 0596002564
- John H. Terpstra and Jelmer R. Vernooij, *The Official Samba-3 HOWTO and Reference Guide,* Prentice Hall, 2003, ISBN 0131453556
- Paul Albitz and Cricket Liu, *DNS and BIND (4th Edition)*, O'Reilly, 2001, ISBN 0596001584

- William Boswell, *Inside Windows 2000 Server*, New Riders, 1999, ISBN 1562059297
- Gary L. Olsen and Ty Loren Carlson, *Windows 2000 Active Directory Design and Deployment*, New Riders, 2000, ISBN1578702429

Referenced Web sites

These Web sites are also relevant as further information sources:

- IBM TotalStorage
  http://www.storage.ibm.com/index.htm
- IBM NAS
  http://www.storage.ibm.com/snetwork/nas/index.html
- IBM TotalStorage NAS Gateway 500
  http://www.storage.ibm.com/snetwork/nas/500/index.html
- IBM NAS reference information
  http://www.storage.ibm.com/snetwork/nas/library.html
- Microsoft Technical Library
  http://www.microsoft.com/windows2000/techinfo/default.asp
- Microsoft Services for UNIX
  http://www.microsoft.com/windows/sfu/default.asp
- Tivoli
  http://www.tivoli.com/
- Tivoli Software Support
  http://www-306.ibm.com/software/sysmgmt/products/support/
- Storage Networking Industry Association
  http://www.snia.org/
- Linux Documentation
  http://www.linuxdoc.org/
- Linux Kernel Resource
  http://www.kernel.org/
- Red Hat Linux
  http://www.redhat.com/
- SUSE Linux
  http://www.suse.com/index_us.html

How to get IBM Redbooks

Search for additional IBM Redbooks or Redpieces, view, download, or order hardcopy from the Redbooks Web site:

ibm.com/redbooks

Also download additional materials (code samples or diskette/CD-ROM images) from this IBM Redbooks site.

Redpieces are IBM Redbooks in progress; not all Redpieces become IBM Redbooks, and sometimes just a few chapters will be published this way. The intent is to get the information out more quickly than the formal publishing process allows.

IBM Redbooks collections

IBM Redbooks are also available on CD-ROMs. Click the CD-ROMs button on the IBM Redbooks Web site for information about all the CD-ROMs offered, as well as updates and formats.

Index

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

X

Z

The IBM TotalStorage NAS Gateway 500 Integration Guide

(1.0” spine)
0.875”<->1.498”
460 <-> 788 pages

The IBM TotalStorage NAS Gateway 500 Integration Guide

Share data seamlessly between UNIX and Windows environments

Get the best of both NAS and SAN using the hands-on guide

Understand all aspects of NAS technology

This IBM Redbook describes how to install and configure the very latest IBM storage solution and concept, the IBM TotalStorage Network Attached Storage (NAS) Gateway 500, in heterogeneous environments.

The IBM TotalStorage NAS Gateway 500 series is an innovative Network Attached Storage device that connects clients and servers on an IP network to Fibre Channel storage, efficiently bridging the gap between LAN storage needs and SAN storage capacities. The IBM TotalStorage NAS Gateway 500 is a storage solution for UNIX/AIX/Linux, Apple, and Microsoft Windows environments. In this book, we show how to integrate the IBM TotalStorage NAS Gateway 500 and explain how it can benefit your company's business needs.

This book is an easy-to-follow guide which describes the market segment that the IBM TotalStorage NAS Gateway 500 is aimed at, and explains NAS installation, ease-of-use, remote management, expansion capabilities, high availability (clustering), and backup and recovery techniques. It also explains cross platform storage concepts and methodologies for common data sharing for UNIX/AIX/Linux, Apple, and Microsoft Windows environments.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7081-00 ISBN 0728498386