

Getting Started

ServerStor

McAfee, Inc.

2710 Walsh Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 am - 5:00 pm

FAX: (408) 970-9727
BBS: (408) 988-4004

(For international contact information, see the following page.)

COPYRIGHT

Copyright © 1996 by McAfee, Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc.

TRADEMARK NOTICES

McAfee is a registered trademark of McAfee, Inc. SiteMeter, SiteExpress, ServerStor, and NetRemote are trademarks of McAfee, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to Saber Software Corporation, a wholly owned subsidiary of McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

A Reader's Comment Form is provided in the back of this publication. McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. If the form has been removed, please address your comments to: McAfee, Inc., Documentation, P.O. Box 9088, Dallas, Texas 75209.

SUPPORT

For fast and accurate help, please have the following ready when you contact McAfee:

- Program name and version number
- Type and brand of your computer, hard drive, and any peripherals
- DOS type and version
- Network name, operating system, and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem.

INTERNATIONAL CONTACT INFORMATION

McAfee Canada

178 Main Street
Unionville, Ontario
Canada L3R 2G9
Voice: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.

Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Voice: (0) 31 20 6815500
Fax: (0) 31 20 6810229

McAfee (UK) Ltd.

Hayley House, London Road
Bracknell, Berkshire
RG12 2TH United Kingdom
Voice: 44 1344 304730
Fax: 44 1344 306902

McAfee France S.A.

50 rue de Londres
75008 Paris
France
Voice: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH

Weltenburger Strasse 70
81677 Munich
Germany
Voice: 49 89 92404214
Fax: 49 89 92404211

What's in This Book?

We at McAfee Associates know you are anxious to install your software. We want you to get started as soon as possible, so we have provided this Getting Started guide to help you install the product quickly and easily. After you've completed the installation, you can use the checklists in this manual to start using the ServerStor components.

Here's what you'll find in the rest of the manual:

Chapter 2, "Product Overview"

Gives a brief description of the product features and functions. Also introduces the McAfee product line and services.

Chapter 3, "Installing ServerStor's Tape Backup Component"

Provides step-by-step procedures that you can follow as you install the tape backup component.

Chapter 4, "Installing the HSM Component"

Gives you the prerequisites for installing the software as well as the system requirements. Provides step-by-step procedures that you can follow as you install the HSM component.

Chapter 5, "Installing the High-Availability Server Component (LANtegrity)"

Gives you the system requirements for installing the software. Provides step-by-step procedures that you can follow as you install the LANtegrity component.

Chapter 6, “Getting the Basics”

Provides checklists that help you to learn use the basic functions of the three ServerStor components.

Introducing ServerStor

ServerStor includes the following software components:

Client/server tape backup solution—automates your tape backup process for Novell 3.1x and 4.x environments, including support for NetWare Directory Services (NDS).

Hierarchical Storage Management (HSM)—continually monitors available disk space on the server and offers a “secondary” data storage strategy for up to 2GB of data. It supplements, not replaces, your backup system.

High Availability Server through LANtegrity—enables a single Novell NetWare 4.1 server to provide Instant Recovery™ and data protection for a maximum of 50 users on a NetWare 3.x and 4.1 servers.

Review the following paragraphs for an introduction to each of these components.

Client/server tape backup

ServerStor for Windows is McAfee's file server backup, restoration, and data management application for the NetWare and Windows environments. ServerStor offers an easy-to-use method of backing up and recovering data for any NetWare 3.1x or 4.x server volume.

ServerStor features and functions include the following:

- A Librarian that tracks and organizes all of your media cartridges, a feature that makes it easier to locate files you need to restore. In addition, the Librarian offers a tape rotation feature which provides added data protection by allowing data to be stored on more than one tape.
- A built-in data protection strategy. ServerStor comes equipped with pre-defined backup jobs that allow you to restore your system to its condition on any given day. For example, this feature makes it easy to restore data that has been lost due to situations such as a system failure.
- An easy method of creating and scheduling backup jobs so that they can be run at the times that are most convenient for you (for example, at times other than regular working hours).

To get started using ServerStor, see [“Installing ServerStor’s Tape Backup Component” on page 11](#).

HSM component

Hierarchical Storage Management (HSM) is a data storage management system. It automates data storage on a variety of devices, including hard disks, optical jukeboxes, and tape autoloaders. This data management system automatically monitors the amount of available space on one or more servers (called managed servers), and takes action when the amount of free space falls below the specified level. Using HSM, the “out-of-disk-space” problem so common on today’s crowded networks is virtually eliminated.



A maximum of 2GB of data can be migrated to a secondary storage server.

When the amount of available disk space falls below the specified minimum, inactive data (files that have not been accessed for a certain time period) is automatically migrated to the specified, secondary storage server so that space is made available on the primary server. Likewise, files can be automatically “recalled” from migration when users request to access them. Therefore, network users’ work is not interrupted, and there are no additional tasks for you to perform.

HSM is not a backup system like the ServerStor tape backup component, and it should not be used in place of your backup system—they each serve different purposes. Unlike a backup system, HSM manages data by migration, that is, moving files from one online storage device to another. To get started using HSM, see [“Installing the HSM Component” on page 23](#).

High-availability server component

ServerStor provides the LANtegrity component—technology for instant server recovery. Using LANtegrity, you can specify that your primary, 50-user servers be automatically protected against data loss by a second server which acts as a repository for all current and historical files on the primary server. Using a default configuration, the secondary server transfers a copy of the protected server’s files within 15 minutes after users create or change a file.

When a protected server goes down for scheduled maintenance or because of a system failure, the secondary (stand in) server can provide the file and print services of the downed server within 15 seconds. Stand-in service is completely unnoticed by DOS and Windows IPX network users since they see the same server name, volume mappings, and directory structures as when the protected server is up and running. In addition, the stand-in server continues to protect the other specified servers even while standing in for a server that has gone down.

When you’re ready to bring the downed server back online, the stand-in server completely automates the process of synchronizing (updating) files between the servers. This feature ensures that all changes made by users of the stand-in service are transferred to the primary, protected server before it comes back online.

You can apply this continuous protection to all files or a subset of files on a protected server. In addition, you can place files that are not suitable for continuous protection (such as large data base files) on protection schedules (for example, once a night at 1:00 AM). Also, temporary files that do not need to be protected can be placed on a protection schedule to reduce unnecessary network overhead. To get started using LANtegrity, see [“Installing the High-Availability Server Component \(LANtegrity\)” on page 34](#).

Where to Go from Here

This Getting Started guide gives you the instructions you need to install and start using the ServerStor components. The table below shows where to go for more information.

If you want to. . .	See. . .
Learn about McAfee products and services	“McAfee at a Glance” on page 7
Install the tape backup component	“Installing ServerStor’s Tape Backup Component” on page 11,
Install the HSM component	“Installing the HSM Component” on page 23
Install the High-Availability Server component	“Installing the High-Availability Server Component (LANtegrity)” on page 34
Get the basic procedures for using the ServerStor components	“Getting the Basics” on page 48

McAfee at a Glance

McAfee's mission

McAfee's mission is to help our customers operate their computers and networks more efficiently and economically. We do this by offering a variety of tools—from our family of anti-virus products to our network management tools. Our electronic distribution system lets you evaluate our software before purchasing it, and our products are supported by an award-winning technical support staff.

McAfee is committed to developing products that are compatible with enterprise-wide network tools and industry-standard databases. Read on to discover how our products can help you work smarter.

Preview of McAfee's product line

The McAfee family of anti-virus products is a collection of workstation and server-based software packages. We provide the most comprehensive suite of network security management tools available today—not only in terms of the extensive functionality these products put at your fingertips, but also the wide range of operating systems, workstations, and network systems they support.

McAfee provides a single source for the most extensive and best integrated line of network management tools on the market. Using these tools allows you as the LAN administrator to automate tasks required to manage assets and protect the integrity of your network, both now and in the future.

We continually update our product line to include the tools you need to be effective in this fast-paced and changing computing environment. Our product line includes those described below. Check out the details:

To automate. . .	McAfee offers. . .
Security management	<p>VirusScan—World's #1 selling anti-virus product for PC desktops (DOS, Windows 3.1, Windows 95, Windows NT, OS/2, and Macintosh).</p> <p>NetShield—server-based anti-virus product that protects against virus infections.</p> <p>BootShield—anti-virus technology that protects against boot virus infections.</p> <p>WebScan—provides instant access to the Internet, while protecting against possible virus infections in files downloaded from the Internet.</p>
Network management	<p>Saber LAN Workstation—integrated LAN management tool that incorporates the best of McAfee's asset, desktop and configuration, support, and storage management products.</p>
Asset management	<p>BrightWorks—integrated software metering, asset management, software distribution, and help desk components.</p> <p>LAN Inventory—complete hardware and software asset management for NetWare.</p> <p>SiteMeter—best-selling software license metering product that helps companies maintain license compliance and minimize software costs.</p> <p>SiteExpress—enterprise-wide electronic software distribution product for automating the process of distributing applications and operating systems, including Windows 95.</p>
Desktop configuration management	<p>NetTools—centralized management of Windows desktops (Windows 3.1, Windows NT, Windows 95) in NetWare and Microsoft NT environments.</p>

To automate. . .	McAfee offers. . .
Support management	LAN Support Center —centralized help desk for problem tracking and resolution. NetRemote —lets LAN administrators control remote workstation processes without leaving their desks.
Storage management	ServerStor — file server backup, restoration, and data storage solution for the Novell NetWare environment. FileStor — Windows-based storage management solution for file-by-file backup and recovery. ImageStor — DOS-based disaster recovery solution for disk image backup and restoration.

How to contact us

To order or for more information about our products, we invite you to contact our Customer Service department at (408) 988-3832. Or you can contact us at the following address:

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A

McAfee's customer and technical support

McAfee is famous for its dedication to customer satisfaction. McAfee's customer support, technical support, and product development departments provide real-time technical support and problem resolutions.

Use the following information to contact McAfee Technical Support.

Phone	(408) 988-3832
FAX	(408) 970-9727
FAX-back automated response system	(408) 988-3034
Hours	6 a.m. to 5 p.m. PST Monday through Friday
McAfee BBS	(408) 988-4004 1200 bps to 28,800 bps 8 bits, no parity, 1 stop bit 24 hours, 365 days a year
CompuServe	GO MCAFEE
Internet	support@mcafee.com
America On-line	Keyword: MCAFEE
MicroSoft Network (MSN)	GO MCAFEE

To speed the process of helping you use our products, please make note of the following before you call:

- Product name and version
- Computer name and model, and the name of any additional hardware
- DOS type and version
- Network name, operating system, and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem, if applicable.

McAfee Training

For more information about scheduling onsite training for any McAfee product, call Customer Service at 800/338-8754.

3


Installing ServerStor's Tape Backup Component

Before You Begin

Before you begin the ServerStor tape backup component installation, make sure your server and workstation systems meet the requirements listed in “[System Requirements](#)” on [page 12](#). Also, you should make decisions about how you want to install ServerStor based on the following checklist:

What you should consider

- ✓ Decide where and on which server you want to install ServerStor. By default, ServerStor is installed in the directory SYS:\SYSTEMMSN. However, you can change this target directory during installation.

 If you will be backing up servers that have different versions of Novell NetWare installed (for example, 3.1x or 4.x), make sure ServerStor is installed on a server that is running the most current version of NetWare. Also, make sure the tape drive is connected to this server.
- ✓ Install the SCSI adapter and tape drive you want to use on the server with ServerStor. Be sure to load the necessary drivers (for more information, see the documentation you received with the adapter). You can specify up to five backup devices from a single adapter.
- ✓ Decide the workstation on which you want to run the Master Scheduler program. (ServerStor looks for the “Rescue” disk on the workstation that is running the Master Scheduler when setting up protection for a volume.) The default drive is A:, but you can choose another drive during installation.

System Requirements

ServerStor runs on NetWare versions 3.x and 4.x and works with any ASPI-compliant SCSI host adapter. To install and run ServerStor successfully, make sure the workstations and servers on your network meet the requirements described in this section.

Workstation configuration

The workstation you use to run ServerStor should have the configuration described in the following paragraphs. The workstation hardware configuration should be as follows:

- 386 or 486 PC.
- At least 4 MB extended memory and 640K conventional memory.
- Hard disk or access to a network volume with at least 7 MB of available disk space.
- Diskette drive with a blank, formatted floppy disk inserted (to hold your Rescue function information).

The workstation should have the following software installed:

- DOS 3.3 or higher.
- Microsoft Windows 3.1 or higher, enhanced mode only.

Server hardware configuration

The server on which you choose to install ServerStor should have the following configuration:

- A 386 or 486 PC.
- At least 8 MB (for NetWare 3.x) or 12 MB (for NetWare 4.x) extended memory and 640K conventional memory.
- A diskette drive.

Compatible backup devices

ServerStor works with the following types of backup devices:

- DAT Backup Devices
- QIC SCSI Backup Devices
- 8mm Backup Devices (Exabyte 8200 is not supported).

Compatible media cartridges

The media cartridges you use with ServerStor depend on the type of backup device you're using. For recommendations on the type of media cartridge to use, refer to the hardware manual that was shipped with your backup device.


Installation Procedures

The ServerStor installation consists of two tasks:

- Installing the program files
- Loading the NLM.

Installing the program files

Follow the procedure below to install the ServerStor program files.

Step	Action
1.	<p>Log in to the server as SUPERVISOR (NetWare 3.x) or ADMIN (NetWare 4.x) and make sure there is a logical drive letter mapped to the volume which you want to install ServerStor.</p> <p> <i>If you have multiple network servers running different versions of NetWare (for example., 3.x and 4.x), be sure to install ServerStor on a server that is running the most current version of NetWare. Also, make sure the tape drive is connected to this server.</i></p>
2.	<p>Start Windows and do one of the following:</p> <ul style="list-style-type: none">■ If you're installing from the CD or diskettes, insert the CD or the first diskette into the appropriate drive. <p>or</p> <ul style="list-style-type: none">■ If you're installing from files downloaded from the BBS, decompress the zipped files into a directory on the network or your local drive. (Refer to the README.1ST file for details about the files you downloaded.)

3. Do one of the following:

- If you're installing from the CD or diskettes, enter the following command:

x: \SERVSTOR\SETUP

where *x* is the drive that contains the CD or diskette.

- If you're installing from files you downloaded from the BBS, enter the following command:

x: \path\SETUP

where *x*: is the drive and *path* is the path to the directory where you decompressed the files.


Response: The ServerStor Setup screen is displayed and the Welcome dialog is opened.

4. Click the Continue button.

Response: The Installation Information dialog is displayed.

5. Under 'Registration Information', enter your user name and company name.

6. Under 'Installation Destination', select a network drive and enter the destination directory for installing ServerStor.

 *Check the dialog to be sure there is enough space to install ServerStor. The amount of space required to install ServerStor is shown as well as the available disk space on the selected volume.*

7. Click the Continue button to display the Confirm Setup Information dialog.

Action: If the Setup Information is correct, click the Continue button to display the Question dialog.

8. Click Yes to replace out-of-date system files, or No to leave the files as they are.

Response: ServerStor is installed to the destination directory. Then the Select Device Type dialog is displayed.

9. Select the type of SCSI tape device attached to the server.

Response: The ServerStor program group is created and the Automated Features dialog is displayed.

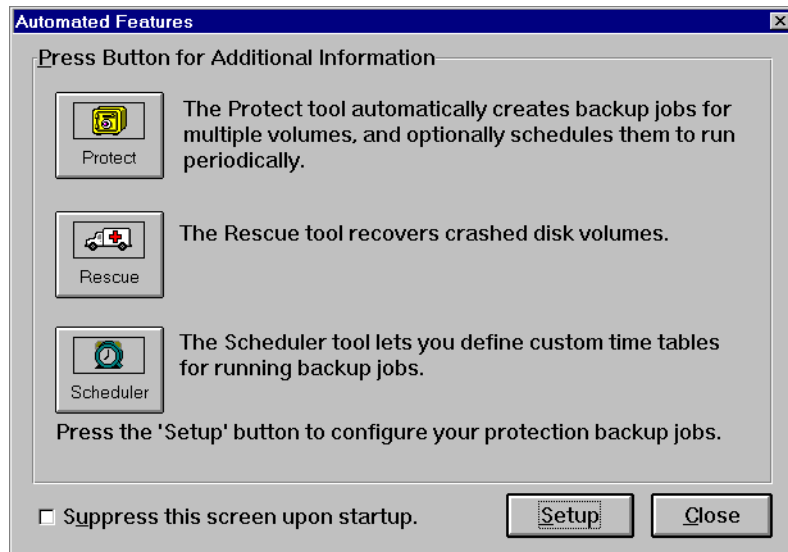


Figure 3-1. Automated Features dialog

10. Click the Close button and then exit Windows.


Action: Load the RESQMAIN NLM (see [“Loading the NLM” on page 17](#)).

Loading the NLM

After you have installed the ServerStor program files, you need to activate ServerStor by loading the RESQMAIN NLM. This NLM checks the NetWare operating system to determine whether the server has a tape drive and then activates ServerStor.


Enter the following command at the server console to load the NLM:

LOAD RESQMAIN



 *If the tape drive is detected, ServerStor is loaded immediately. However, if NetWare doesn't recognize the tape drive then ServerStor does not load. For troubleshooting tips, see our Fax-back document #STO-0007. You can find the McAfee phone numbers under "How to contact us" on page 9.*

Setting Up the Rescue Function

ServerStor's Rescue function allows you to restore data lost in a system crash. You can specify the volumes that you want to be protected by the Rescue function and create a Rescue Disk for each volume. Backup jobs are automatically created to back up these volumes, and the Rescue Disk is updated during each backup. Then, if data is lost on one of these volumes, you can use the Rescue Disk to restore the data.

 *Be sure you have supervisory rights (for NetWare 3.x) or administrator rights (for NetWare 4.x) to every volume you want to protect with the Rescue function. You will be asked to enter the Supervisor or Admin password for each server to be protected using the Rescue function.*

Log into and map a drive to each of the servers you want to protect and then follow the procedure below to setup the Rescue function.

- | Step | Action |
|------|--|
| 1. | <p>Click the Setup button on the Automated Features dialog (Figure 3-1).</p> <p>Response: The Rescue Setup dialog is displayed. Listed are all the server volumes to which you have access. These are the volumes you can protect with the Rescue function. By default, all available volumes are highlighted.</p> |
| 2. | <p>If necessary, deselect volumes until only the ones you intend to protect with the Rescue function are highlighted. Then click the Add button to display the volumes in the 'Protected' list.</p> |
| 3. | <p>Enter the drive and path to the Rescue disk (the default is A:).</p> <p> <i>Be sure there's an empty, formatted, high-density diskette labeled "Rescue Disk" in the drive you select.</i></p> |
| 4. | <p>Select the 'Enable Auto Updating' checkbox to automatically update the Rescue disk each time you perform a rescue backup.</p> <p> <i>If this option is not activated, the necessary information is not copied to the rescue disk automatically, and you may not be able to restore your data in the event of a system crash.</i></p> |

5. Activate the 'Use Default Protection Schedule' option if you want the system to automatically load the Scheduler at ServerStor startup.
6. Click OK.

Response: A message is displayed that prompts you to enter the network password for each server specified in Step 2 above.

7. Enter the password for each server and then click OK.

Response: The ServerStor files are copied to the Rescue disk. Then, the Automated Features dialog is displayed again.

Action: Do one of the following:


- If you plan to back up data on multiple servers, continue with the procedure under ["Setting Up Additional Servers" on page 20](#).

or

- If you want to get more information about these features, click the Protect, Rescue, or Scheduler buttons.

or

- Click Close to continue working in ServerStor.

 *If you don't want to see this dialog each time you run ServerStor, just activate the option not to display this dialog again.*

Setting Up Additional Servers


If you plan to back up data on multiple servers, you need to setup each server to work with ServerStor. You don't need to perform this procedure for the server on which you originally installed ServerStor since this server was automatically set up during installation.

Perform the procedure below to set up multiple servers for ServerStor backup.

Step

Action

1. Log into each server as SUPERVISOR (NetWare 3.x) or ADMIN (NetWare 4.x).
2. Make a backup copy of the current TSA and SMDR files located on each server. Then copy the TSA and SMDR files from the ServerStor directory to SYS:\SYSTEM on each server.

 *The names of the files you need to copy vary, depending on the version of NetWare you are running. Refer to the list below for the ServerStor-related file names.*

NetWare Version	Files to Copy
3.11	TSA311.NLM SMDR.NLM
3.12	TSA312.NLM SMDR.NLM
4.01/4.02	TSA400.NL SMDR.NLM TSANDS.NLM
4.10	TSA410.NLM SMDR.NLM TSANDS.NLM

Action: Make a note of these file names. You will need them for the next step.

3. Insert a LOAD command for each of these files into the AUTOEXEC.NCF file for each server to be protected. (Refer to your NetWare documentation for instructions on how to insert a LOAD command.)
4. Down the servers and bring them up again so the LOAD commands are executed.
5. Specify these servers as protected servers. To do so, perform the procedure under ["Setting Up the Rescue Function" on page 18](#).

Now That You've Installed

Now that you have successfully installed and setup ServerStor, you are ready to explore the features available for protecting server data. The table below shows where you can find the instructions for the task you want to perform.

If you want to. . .	See. . .
Start ServerStor	"Starting ServerStor" on page 49
Create a custom backup job	"Creating a custom backup job" on page 49
Schedule backup jobs	"Using the Job Scheduler" on page 51
Restore data	"Restoring files" on page 52

4

Installing the HSM Component

Before You Begin

ServerStor's Hierarchical Storage Management (HSM) is a storage management system which requires both software and hardware to operate. You'll want to review the checklist below as well as the system requirements in this section before you install the product. (For an overview of the HSM features and functions, see ["HSM component" on page 4.](#))

What you must consider

For a minimum implementation, HSM uses a set of NLMs running on a Novell NetWare server in a SCSI environment, a dedicated backup device, and an administrator interface running on a client workstation. If you do some planning before you start, the HSM installation process can be very short and very easy.

In preparation for installing and setting up HSM, you'll need to have the answers to the following questions:

- ✓ For which servers do you want to monitor the available disk space levels in preparation for migration to secondary storage? These servers are called the managed servers.
- ✓ Which server do you want to be the storage server? This is the server to which data is migrated when the managed servers reach the maximum specified disk usage threshold.
- ✓ What is the appropriate maximum usage threshold for each managed server?

- ✓ Which will be the domain server for maintaining a “mirror image” of the storage server databases? We recommended that you use a disk other than the storage server disk as the domain server. By using separate disks for storage and database mirroring, one set of databases is always available to network users; thereby providing the best data protection.
- ✓ Which workstation do you want to use to run the Administrator Interface application for configuring volume management?


System Requirements

To use the HSM component successfully, be sure your system meets the following configuration.

Storage server configuration

We recommend that the storage server be dedicated to HSM functions. The storage server should have the following configuration:

- IBM-compatible 486 system running at 60 MHz or higher
- 8MB of RAM, plus the memory that Novell specifies as required for running NetWare, and the memory you'll need for running other NLMs
- 100MB of disk space (the minimum requirements is 50MB)
- NetWare version 3.1x or 4.1
- HSM-supported NLM revision levels.

 *You can download a list of the supported NLM revision levels from Avail's BBS at 303/546-4239. The modem transfer rate is 8,N,1.*


- At least one ASPI compliant, HSM-supported SCSI controller card
- Dedicated tape backup device for disaster recovery
- Access to a CD ROM for installation
- A separate physical drive (domain server) from the installation volume for storing and maintaining copies of the HSM databases and other system files.

Domain server configuration

During installation, you will need to identify a server on the network as the domain server, and to allocate space on this server for the domain volume. Because it will be used to mirror the HSM databases and other system files, the domain server and volume must have continuous communication with the HSM storage server. (If you wish, you can also specify the domain server as a managed server.)

The domain server should have the following configuration:


- 1MB of RAM over the NetWare requirement
- Minimum of 10MB of free disk space
- NetWare version 3.1x or 4.x
- HSM-supported NLM revision levels.

 You can download a list of the supported NLM revision levels from Avail's BBS at 303/546-4239. The modem transfer rate is 8,N,1.

Managed server configuration

Any Novell NetWare server with a volume configured for management by HSM can be a managed server (a server for which disk space usage is monitored). The managed servers should have the following configuration:

- 1MB of RAM plus what's required for running NetWare
- NetWare version 3.1x or 4.1
- HSM-supported NLM revision levels.

 You can download a list of the supported NLM revision levels from Avail's BBS at 303/546-4239. The modem transfer setting is 8,N,1.

Client administration workstation

For configuring volume management through the Administrator Interface application, you need at least one workstation with Windows installed. This workstation should have the following configuration:

- 8MB of RAM
- Windows version 3.1x, Windows 95, or Windows NT
- Access to the storage server.

Preparing the hardware

Before you begin the HSM installation, you should have a Novell NetWare server set up with the required components and configuration (see [“What you must consider” on page 23](#) and [“System Requirements” on page 24](#)). Here is a list of the hardware you'll need to implement ServerStor's HSM system:

- HSM storage server
- Domain server
- Managed servers
- SCSI adapter
- HSM backup device
- Tape drive
- CD ROM drive
- Client workstation.


Follow the steps below to prepare the hardware for HSM installation and configuration. You may have already completed some of these steps; however, review the procedure to be sure your hardware has been setup appropriately.


Step

Action

1. Install a SCSI adapter card.
2. Make sure that there are only two terminations on the SCSI bus and that the terminations are located at each end of the bus.

3. Connect the tape drive to the storage server's SCSI bus.
4. Set a unique SCSI address for each device to prevent access conflicts during HSM operations. (The primary SCSI adapter card usually uses address 7.)

 *For instructions on how to change SCSI address settings, see the manual that you received with each device.*
5. Install DOS version 5.0, 6.0, or 6.2 on the HSM storage server, according to Novell NetWare recommendations.
6. Install NetWare version 3.1x or 4.1 on the HSM storage server. During the "Volume Options" section of the Novell NetWare install, create an HSM volume with sufficient space for running the necessary executable files and storing the databases (at least 50MB of free space, but 100 MB is recommended) and assign it a descriptive name.

 *The name that you give this storage server during NetWare installation is the name you'll use to identify this server in the HSM system. This name will appear at the top of the Administrator Interface (see "[HSM Checklist](#)" on [page 53](#) for instructions on using the HSM Administrator Interface application).*
7. Create migration volumes. Create at least three migration volumes—each one should be the same size. Recommended names for the migration volumes are: MIGRATE1, MIGRATE2, and MIGRATE3. The size of the migration volumes must be at least the size of the largest file that will be migrated.
8. Create an HSM user name. Since this account must have supervisory equivalence (plus be in the same level of the structure as the volume objects for NetWare 4.x), we recommend that you also assign a password. Then use the NetWare utility to create a user account on the HSM storage, domain, and managed servers. Assign the same exact user name and password on all three servers.

Installation Procedures

This section provides procedures for installing the HSM storage server software and the Administrator Interface application. Read the following prerequisites before installing the server software.

Prerequisites

Before you start the installation process for the storage server, be sure your system meets the requirements listed under “[System Requirements](#)” on [page 24](#). Specifically, you’ll need a minimum of 50MB of disk space (100MB recommended) to complete this installation procedure.

If the server does *not* have sufficient disk space to complete the installation, you need to create an installation diskette. To do so, insert a formatted diskette and then run the batch file DISK1.BAT (this file is found under \NETSPACE). Then follow the installation procedure below.


Server installation procedure

Follow the procedure below to install HSM on the storage server.


Step	Action
1.	Do one of the following: <ul style="list-style-type: none">■ If you’re installing from the CD, mount the CD as a volume and insert the CD. or <ul style="list-style-type: none">■ If you’re installing from files downloaded from the BBS, locate the drive and directory where the files are stored. (See the README.1ST file for details about the files you downloaded.)

2. Enter the following command at the console prompt:

```
LOAD volumename\NETSPACE\SERVER\AVINST
```

 *If the server does not have sufficient disk space (50MB minimum) for the installation, insert the installation diskette you created (see “Prerequisites” on page 28). Then enter the command A:\AVINST.*


3. When you're prompted for the location of the rest of the install files, select the 'Server Volume' option and then select the volume on which the program files reside.
4. Enter the information on the installation screens as it is requested.

 *When you run the installation program, all volumes on the local server are checked for ServerStor HSM installations. If none are found, the installation process is performed as usual. If an existing installation is identified but the installation is not complete, you can complete the installation on the volume. If a complete installation is found, the program automatically performs an update.*

What happens during server installation

The following paragraphs explain what happens at the server during the HSM installation process:

- ✓ A welcome screen is displayed.
- ✓ After you enter your user name and password a list of servers is displayed so that you can select the domain server. Then the NetWare user name and password are verified on the server you selected. If they are not valid, an error message is displayed, and you must add the user name and password before you can continue. Or you can select another server as the domain server.

 *The domain server volume should not be the same as the installation volume.*


- ✓ After you identify the domain volume and the installation path, you identify the migrate volumes using one of these two options:
 - Express—automatically looks for MIGRATE1, MIGRATE2, and MIGRATE3 volumes and configures them.
 - Custom—allows you to select from a list of all volumes on the HSM storage server.

Then your volume selections are checked to ensure that they have not already been identified for use by this HSM system.

- ✓ After you select the backup rotation scheme, a confirmation screen is displayed. All of the settings you've selected are shown, and you can make changes, if you wish.
- ✓ When you've confirmed the installation settings, the data is saved in a file so that it can be used again if you stop the installation process before it is complete. Also, all of the necessary directories are created on the storage and domain servers. And all executable files, drivers, and system files are copied to appropriate locations.
- ✓ After the installation settings are saved and files are copied, the proposed changes to the AUTOEXEC.NCF and STARTUP.NCF files are displayed and you can choose to modify these files or create an example file for each.

If you choose to modify the files, you're asked to verify your choice to make changes to these files. Otherwise, example files are created and stored in the same location as the original files.

- ✓ Then the HSM databases are created and a final status message is displayed. It shows the installation status and errors, if any.

 *Some installation settings can be changed using the AVSETUP utility. See the online help for further instructions on how to use AVSETUP.*

Administrator Interface client installation

Follow the procedure below to install the Administrator Interface client application for configuring volume management.

Step	Action
1.	<p>Run the NetSpace SETUP.EXE program (by default, this program is located under \NETSPACE\CLIENT or in the directory specified during installation).</p> <p>Response: The Welcome screen is displayed. All installation options are selected.</p>
2.	<p>If you wish, deselect the options you don't want to install. Otherwise, proceed to the next step.</p>
3.	<p>Enter the destination for the NetSpace application files or accept the default (C:\NETSPACE).</p> <p>Response: The program files are copied to the destination directory. The file PROTOCOL.INI is modified if an adequate number of connections are not specified (a backup of the file is created, PROTOCOL.001).</p>
4.	<p>Choose from these options for completing the installation process:</p> <ul style="list-style-type: none">■ View ReadMe File■ Start NetSpace■ Exit to Windows. <p>Response:</p> <ul style="list-style-type: none">■ If you chose to view the ReadMe file, the release notes information is displayed. <p>or</p>

- If you chose to start NetSpace, a message is displayed that prompts you to enter the NetSpace login.

Action: Enter the server user name and password and then click OK. To identify the HSM servers, click Yes and then continue with the next step.

5. When the Preference dialog is displayed, click the Add HSM Server button on the HSM Working Set page. Then enter the HSM server name and password—this is the same name that was specified when the HSM server software was installed (see Step 8 on [page 27](#)).

Response: The name of the server is displayed in the list.

6. Click OK to close the dialog and display the NetSpace main window.

Action: See “[HSM Checklist](#)” on [page 53](#) to configure volume management.

Now That You've Installed

Congratulations! Now that you have successfully installed ServerStor's HSM component, you are ready to explore the features available for managing data storage. To learn how to configure HSM volume management, see the section ["HSM Checklist" on page 53.](#)

5

Installing the High-Availability Server Component (LANtegrity)

Before You Begin

Before you begin the installation of the ServerStor LANtegrity component, make sure your server and workstation systems meet the requirements listed in “[System Requirements](#)” on page 36. In addition, you’ll need to make decisions about how you want to implement the high-availability server based on the following checklist:

- ✓ Decide which servers you want to protect against system failure by using a stand-in server. Each server is called a protected server.
- ✓ Decide which server you’ll use as the stand-in server (LANtegrity server). This server needs to be running NetWare 4.x and have about twice the amount of disk space available as the protected server.
- ✓ Choose the workstation on which you want to install the interactive “client” application for controlling LANtegrity operations.

Have the following information handy as you install, set up, and configure LANtegrity. If you are running NetWare Directory Services (NDS), you can choose to specify the user name and password shown in the table below for accessing the server. For Bindery Emulation, you can enter the information for your current configuration.

You will be asked to supply...	Do this...
User name and password for authenticating the LANtegrity Server. This is the distinguished name of the administrator you specified when you installed NetWare on your LANtegrity Server.	Enter the name and password Admin.INTEGRITY/admin . Or enter the values you choose.

You will be asked to supply...	Do this...
Port address of the host adapter for the autoloader on the LANtegrity Server if one is installed.	Make a note of the address here: _____
User name and password for authenticating each protected server. For NetWare 4 servers, this is the name and password you entered above. For NetWare 3 servers this is the name and password of a supervisor equivalent.	Make a note of the authenticating passwords here: _____ _____ _____
For each protected server, specify a unique, alternate IPX address. The protected server uses the alternate IPX address when it is rebooted while the LANtegrity server is standing in.	Make a note of the IPX addresses you'll use here: _____ _____
The distinguished name of the NDS container used to hold the Lantegrity server object.	Make a note of the name here: _____
Other applications running on the protected servers that set and clear the archive.	Note whether these types applications exist on the server: _____
A Server Bindery Context, if you're protecting a NetWare 4 server that supports Bindery logins.	Make a note of the Binder context here: _____
The time needed to reboot each protected server.	Specify the appropriate value for the server. _____


System Requirements

To install and use the ServerStor LANtegrity component successfully, make sure the workstation and servers you'll use within this data protection system meet the requirements described in this section.

Secondary server (LANtegrity server)

The LANtegrity server must be running NetWare 4.1 and should have the following minimum configuration:

- Memory—48MB.
- Disk space—minimum requirement is 250 MB, or twice the amount of disk space as the protected server.
- Tape autoloader—a highly recommended configuration since many key LANtegrity features are not available without it.
- SCSI Host Adapter—if possible, use DMA 5, IRQ 11, and port address 330, since these are the default parameters. Also, set the BIOS OFF. We recommend that you dedicate this adapter to the tape autoloader, if it is installed.

 *To prevent problems during installation, make sure that the settings on the Host Adapter do not conflict with other boards in the server.*

Protected server

You can use an existing NetWare server running NetWare 3.1x or 4.1 as the protected server. It should have the following minimum configuration:

- 2GB or less of disk capacity.
- Minimal SYS volume size to reduce the amount of time required to reboot the system during stand-in.

Workstation for the administrator application

For the LANtegrity Administrator application, you should use a workstation running Windows version 3.x in 386 enhanced mode.

Installation Procedures

Once you've made sure that your system meets the requirements described under [“System Requirements” on page 36](#), you can install and set up LANtegrity. When your systems are configured correctly, installing and setting up LANtegrity is a simple process.

LANtegrity consists of three software components:

- The LANtegrity Server NLM, LSSERVER.NLM, for a dedicated NetWare 4 server, called the LANtegrity Server.
- The LANtegrity agent NLMs, LSAGENT.NLM and LSSTART.NLM, for each of the NetWare 3 and NetWare 4 servers you want to protect.
- The LANtegrity Administrator application, for one or more Windows workstations. You can use this application to monitor and control LANtegrity operations.

Your main steps

Your main steps for installation and setup are described below.

1. Load the LANtegrity INSTALL NLM to copy the software to the LANtegrity server. (See [“Installing the LANtegrity software to the server” on page 38](#).)
2. Install the LANtegrity software on the protected servers. (See [“Installing the protected server software” on page 39](#).)
3. Run the setup program to configure the LANtegrity server. (See [“Setting up a LANtegrity server” on page 41](#).)
4. Run the setup program to configure the protected servers. (See [“Setting up a protected server” on page 43](#).)
5. Set up the LANtegrity administrator application. (See [“Installing the LANtegrity administrator application” on page 45](#).)

Installing the LANtegrity software to the server

Follow the procedure below to install the software on the LANtegrity server:

Step

Action

1. Do one of the following:
 - If you're installing from the CD, insert the CD into the appropriate drive.

or


 - If you're installing from files downloaded from the BBS, locate the drive where the files are stored. (See the README.1ST file for details about the files you downloaded.)
2. Load the LANtegrity INSTALL NLM.

Example: With the CD ROM mounted as a volume, enter the following command:

LOAD NICD:INSTALL

Response: The main menu is displayed.
3. Choose **Install LANtegrity Server** from the menu.

Response: A list the available servers is displayed.
4. Select the NetWare 4.1 server that you'll use as the LANtegrity Server.
5. Log in to the LANtegrity server as ADMIN.


 *You must be able to write to the destination path (below) and to create and modify files in directories such as SYS:SYSTEM and SYS.*

6. Specify the destination for the LANtegrity server software. (We recommend that you accept the default SYS:\LANTEG; however, you can enter a different destination path.)

Response: If the installation program needs to update (overwrite) system files, the Select Handling of Overwrites menu is displayed.

Action: Select the option that best describes how you want the file updates to be handled.

7. Press ENTER to accept the updates.

 *Although you can choose not to accept the update, we recommend that you do to ensure consistent LANtegrity operation. Make a note of the files that were updated so that you can restore the original system files should you want to remove LANtegrity from the server.*

Response: A message is displayed that indicates that the installation process is complete.

8. Press the ENTER key to return to the main menu.

Action: Continue with the following procedure.

Installing the protected server software

Follow the procedure below to install the necessary software on the protected server.

Step

Action

1. If the LANtegrity INSTALL NLM is not currently loaded, load it to display the main menu.

Example:


LOAD NICD:INSTALL

2. Choose **Install Protected Server** from the menu.

Response: A list the available servers is displayed.

3. Select the server that you want to protect.

4. Enter the user name (for example, SUPERVISOR for NetWare 3.x).


 *You must be able to write to the destination path (indicated below) as well as to create and modify files in directories such as SYS:SYSTEM and SYS.*

5. Specify the destination for the protected server software. (We recommend that you accept the default SYS:\LANTEG.)

Response: If the installation program needs to update (overwrite) system files, the Select Handling of Overwrites menu is displayed.

Action: Select the option that best describes how you want the file updates to be handled.

6. Press ENTER to accept the updates.

 *Although you can choose not to accept the update, we recommend that you do to ensure consistent operation. Make a note of the files that were updated so that you can restore the original system files should you want to remove LANtegrity from the server.*

Response: A message is displayed that indicates the installation is complete.

7. Press the ENTER key to return to the main menu.

8. Do one of the following:

- If you want to install the protected server software on another server, repeat Steps 2 through 7.

or

- To set up the LANtegrity server, choose **Exit** from the menu and then continue to the next procedure.

Setting up a LANtegrity server

After you install the software on the LANtegrity server (see “[Installing the LANtegrity software to the server](#)” on page 38), follow the procedure below to configure the LANtegrity server.

Step

Action

1. At the LANtegrity server’s system console, load the SETUP program from the LANtegrity installation directory (the default is SYS:\LANTEG).


Example: If you copied the software files to the default directory, enter the following command:

```
LOAD SYS:LANTEG\SETUP
```

Response: The following message is displayed:

```
Choose the volume for the data storage
```

2. Enter the name of the volume that you want to set up for data storage (for example, CACHE).

 *To ensure that there’s enough disk space to handle the LANtegrity data storage requirements, we recommend that you do not use the SYS volume for data storage.*

Response: The following message is displayed:

```
Where is the local SERVER.EXE program loaded from?
```

3. If necessary, specify the correct path to the file.

Response: The Host Adapter menu is displayed. A list of host adapter configurations is shown.

4. Choose the host adapter configuration that matches the autoloader on the LANtegrity server. (If the Host adapter for your autoloader is not listed, choose the option 'No predefined host adapter.')

Response: A comment line is added to the AUTOEXEC.NCF that indicates where you have to add information about the autoloader.

Action: Enter the port address for the autoloader if the message that prompts you to do so is displayed.

Response: The Tape Device menu is displayed. A list of types of tape devices is shown.

5. Select the type of tape device that is installed on the LANtegrity Server. (If your tape device is not listed, choose the option 'No predefined tape device.')

Response: The following message is displayed:

```
[PATH] AUTOEXEC.NCF requires modifications
```

6. Choose to save the changes or choose to view the changes and then save them.

Response: The following message is displayed:

```
[PATH] STARTUP.NCF requires modifications
```

7. Choose to save the changes or choose to view the changes and then save them.

Response: A status message is displayed that indicates that the setup process is complete.

8. Press Enter to return to the main menu and then choose **Exit**.

Response: A message is displayed that tells you to cold boot the server

Action: Press the ENTER key to return to the console prompt.

9. To cold boot the server, enter the Down command and then enter Exit. At the DOS prompt, press Reset.

Response: The following LANtegrity status message is displayed

LANtegrity Server operating

Action: In preparation for data storage, add blank tapes to the autoloader. If your autoloader requires a cleaning tape, insert a new one into the last slot. Then follow the procedure below to set up the protected server.

Setting up a protected server

After you install the protected server software (see “[Installing the protected server software](#)” on page 39), follow the procedure below to configure the protected server.

Step

Action

1. At the protected server’s system console, enter the following command:

LOAD SYS:LANTEG\SETUP

Response: A list of all the servers available to the protected server is displayed.

2. Select the LANtegrity Server that will protect this server.

Response: The following message is displayed:


Where is the local SERVER.EXE program loaded from?

3. If necessary, specify the correct path to the file.

Response: Information about the original and alternate IPX addresses is displayed followed by this message:

Enter alternate internal IPX address

4. Enter the unique, alternate IPX address for the protected server.

 *The protected server uses the alternate IPX address when it is rebooted while the LANtegrity server is standing in. The alternate names are stored in AUTOEXEC.NCF.*

Response: The following message is displayed:

```
[PATH] AUTOEXEC.NCF requires modifications
```

5. Choose to save the changes or choose to view the changes and then save them.

Response: The following message is displayed:


```
[PATH] STARTUP.NCF requires modifications
```

6. Choose to save the changes or choose to view the changes and then save them.

Response: The following message is displayed:

```
[PATH] AUTOEXEC.BAT requires modifications
```

7. Choose to save the changes or choose to view the changes and then save them.

 *Use this file to automate the reboot process—doing so ensures that the server is not brought up under its normal name while the LANtegrity server is standing in. If you choose to boot the server without using this batch file, enter this command: LSSTART—do not enter the normal SERVER command.*

Response: The batch file LSSTART.BAT is automatically created and stored in the same location you specified for SERVER.EXE in Step 2 on [page 43](#)). Then a message is displayed that indicates that the installation process is complete.

8. Press the ENTER key to return to the main menu and then choose **Exit**.

Response: A message is displayed that tells you to cold boot the server.

Action: Press the ENTER key to return to the console prompt.

9. To cold boot the server, enter the Down command and then enter Exit. At the DOS prompt, press the Reset button.

Response: The following LANtegrity status message is displayed:

LANtegrity agent connected and operating

Action: Run the batch file LSSTART.BAT (found in the same location you specified for SERVER.EXE in Step 2 on [page 43](#)) to bring the server back up. Then follow the procedure below to set up the administrator program.

Installing the LANtegrity administrator application

You use the administrator application to control LANtegrity operations. Be sure the workstation on which you plan to run the program meets the requirements specified under [“Workstation for the administrator application” on page 36](#).

Follow the procedure below to install the administrator application.

- | Step | Action |
|------|--|
| 1. | Start Windows and connect to the LANtegrity Server. |
| 2. | Map a drive to the LANtegrity product directory, SYS:\LANTEG (or the directory you specified during installation). |
| 3. | Enter the following command in the Windows Run box:

x:SETUP.EXE


where, x is the drive mapped to the LANtegrity product directory. |

Response: The LANtegrity Administrator Setup dialog is displayed.

4. Enter the location of the LANtegrity administrator source files. Or, if you have not moved the SETUP.EXE file, accept the default path. Then click Continue.

Response: A destination dialog appears.

5. Specify the destination on the workstation to install the software. (The default is C:\LANTEG.)
6. Follow the instructions on the screen to create the Program Manager Group and complete the installation.

 *When the message is displayed that prompts you to enter the license number, use the number specified in the McAfee License section of LSADMIN.INI. This file is located under C:\LANTEG.*

Now That You've Installed

Congratulations! Now that you have successfully installed and setup Server-Stor's high availability server components, you are ready to explore the features available for protecting your data. See the section "[LANtegrity Checklist](#)" on [page 55](#) for instructions on controlling LANtegrity operations through the administrator application.

This chapter helps you learn to use the ServerStor components by walking you through the most common tasks you'll perform with the product. The checklists in this chapter give you an idea of what you can accomplish with ServerStor, as well as gives you step-by-step instructions for completing each task.

ServerStor Checklist

Use the steps below to become familiar with ServerStor's tape backup and restoration features and functions.

Your Main Steps:

1. Starting ServerStor
2. Creating a custom backup job
3. Using the Job Scheduler
4. Restoring files

1. Starting ServerStor

- A. Double-click the ServerStor icon in the ServerStor program group.

Response: The main ServerStor window is displayed.

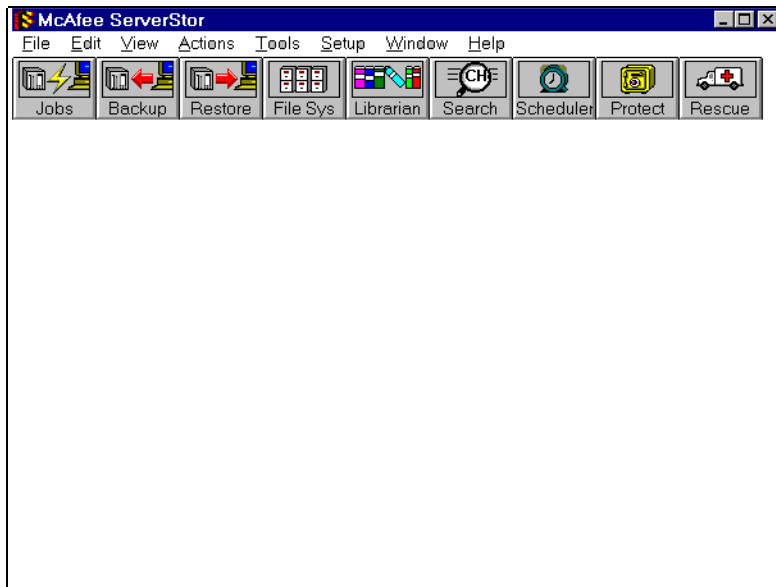


Figure 6-1. ServerStor main window

- B. From here, you can click a toolbar icon or select a menu command to perform a function.

2. Creating a custom backup job


You can create custom backup jobs to back up specific directories and files. These custom jobs can be run immediately or scheduled to run on a certain day of the week at a certain time (overnight, for example). You assign each backup job you create to a category (job group). ServerStor includes pre-defined job groups, which we will use in this exercise.

Info-map

For a detailed description of job groups, please refer to Chapter 3, "The Librarian and File System," in the manual *Using ServerStor*.

A. Create the backup job.

- Click the Backup button on the toolbar.
- Select the volume to back up.
- Click the Select Files button and then “tag” (mark for backup) the desired files. Double-click the volume, directory, or file name:

 *If you want to select a particular group of files, click once on the volume and directory name to expand the list. Select the files and then double-click on the last file in the list to tag the group of files for backup.*

- Click the Done button to accept the file selections and return to the Backup dialog.

- Verify the job group for this backup job in ‘Target Media To’. If this information is not correct, click Target to select the correct job group. For this exercise, select the ‘Free Pool’ job group. This job group serves as a catch-all pool of media cartridges that you, rather than ServerStor, manage. These media cartridges can be overwritten at any time.

Info-map

For more information about media cartridge management, see Chapter 3, “The Librarian and File System,” in the manual *Using ServerStor*.

- Click Options to display the Backup Options dialog. Make sure the ‘Update Library’ option is selected if you want to record this backup in the Librarian database.
- Click ‘Append’ to append the backup data to the end of the tape or ‘Overwrite’ to replace the contents of the tape with the data from this backup.

Info-map

For more information about the Librarian database, see Chapter 3, “The Librarian and File System,” in the manual *Using ServerStor*.

- To save the job definition, click the Save Job button and enter a name for the job. For this example, enter “MYJOB” as the name of the job. Then, click OK.

- B. Click the Backup button to immediately run the job. (Since this job was saved in the previous step, you can also run it at a later time by clicking the Jobs button on the toolbar.)

3. Using the Job Scheduler

You can schedule backup jobs to run at specified times on specified days with the Job Scheduler. To schedule a backup job:

Info-map

For complete information on using the Job Scheduler, please refer to Chapter 8, “Job Scheduler,” in the manual *Using ServerStor*.

- A. Select **Setup/Activate Schedule** from the menu bar. Then click the Scheduler button on the toolbar.
- B. Select “MYJOB” (the job created in Step 2 from the ‘Job file’ drop-down list).
- C. Click the Clock button to display the When dialog.
- D. Select the ‘Time’ and ‘Date’ options as appropriate and click OK.
- E. In the ‘Message’ group, select the visual and audible signals that tell you a job is about to start, as follows:
 - Select one of the available ‘Types’ of Messages below:
 - **Confirm.** Delays the start of a job until you confirm or cancel it.
 - **Countdown.** Delays the start of a job for a specified amount of time in case you want to cancel. When the time runs out, the backup job begins.
 - **Invisible.** Turns off the Message box. The job will run, but there will be no visual prompt.
 - **Text.** Enter the text you want to appear in the Message box when a job is about to begin.
 - **Beep.** When an “X” appears, the audible signal for a backup job is activated. Select the type of signal you want from the drop-down list. Click the Musical Note button if you want to test the beep.

- F. Click Add to add the backup job to the 'Events' list and then click OK.

Response: The backup job runs based on your selections.

4. Restoring files

- A. Use the Search function to find the files to be restored.

- Click the Search button on the toolbar.
- Enter the 'Search for' criteria. You can specify the full file name or use DOS wild card characters.
- Under 'From Volume', select the volume to search or select 'All volumes.'
- Select 'Search All Subdirectories' to search all subdirectories on the volume.
- Click Search.

Response: The system searches for and displays a list of files that match the criteria you specified.

- B. Select a file name from the list and then click View.

Response: The location of the file in the media cartridge library is displayed.

- C. Click on the Versions button and then tag the files you want to restore (see Step 2B [page 49](#) for more on tagging files).

- D. Click the Restore button.

- E. Verify the Source and Target for the restore operation. (If you need to make changes, click Source or Target.)

- F. Click the Restore button to start the process.

- G. When the message is displayed to do so, load the appropriate media cartridge and then click OK.

Response: The selected files are restored on the server.

Info-map

For more information on the Search function, see Chapter 3, "The Librarian and File System," in the manual *Using ServerStor*.

HSM Checklist

Use the following checklist to get the basics for configuring HSM volume management. These procedures are written with the assumption that you have already specified your HSM servers (see “[Administrator Interface client installation](#)” on page 31 for instructions).

Your Main Steps:

1. Start the HSM administrator application.
2. Double-click on the storage server you want to administer.
3. Identify the managed servers.
4. Identify the managed volumes.
5. Backup the managed servers.

1. Start the HSM administrator application.

- A. Double-click the NetSpace icon in the program group.

Response: The HSM Storage Manager main window is displayed.

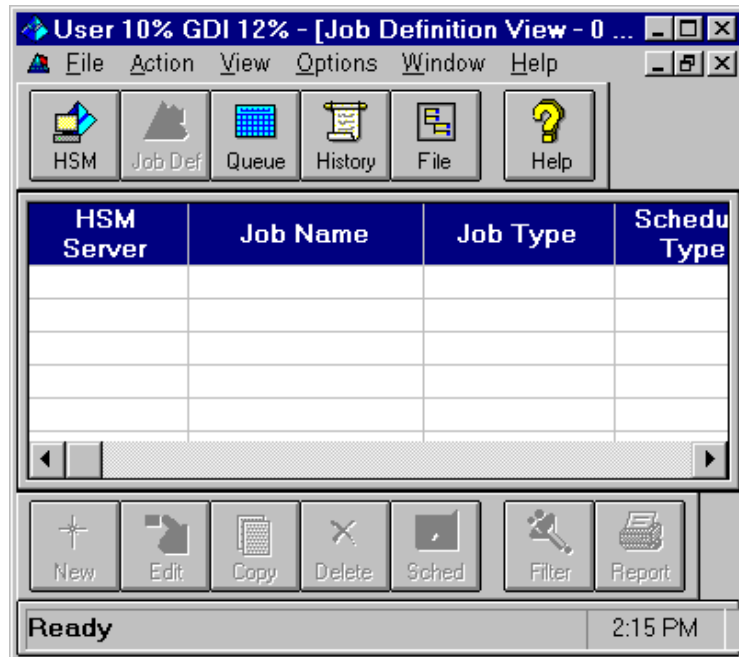


Figure 6-2. HSM Storage Manager main window


- B. Select **View/HSM** from the menu bar.

2. Double-click on the storage server you want to administer.

3. Identify the managed servers.

- A. On the HSM Server dialog, select the Servers tab.
- B. Drag and drop the desired server names from the 'Available Servers' list to the 'Managed Servers' list.

Action: Repeat this step to identify more managed servers.

 *Be sure you've loaded the AVRECALL NLM on each managed server so that files can automatically be recalled from migration when users request access to them.*

4. Identify the managed volumes.

- A. On the HSM server dialog, select the Volumes tab.
- B. Drag and drop the desired volumes from the 'Available Volumes list to the 'Managed Volumes' list.

Action: Repeat this step to identify more managed servers.

5. Backup the managed servers.

Before data can be migrated when a protected server's usage reaches the specified threshold, you must backup the server data. Once the server has been backed up, data migration takes place automatically. See "[ServerStor Checklist](#)" on [page 48](#) for instructions on backing up the server.

LANtegrity Checklist

Use the following checklist to get the basics for controlling LANtegrity operations through the Storage Manager administrator application.

Your Main Steps:


1. Log into the LANtegrity server.
2. Specify the LANtegrity server settings.
3. Configure each protected server

1. Log into the LANtegrity server.

- A. Double-click the LANtegrity icon in the program group.

Response: The Login to LANtegrity dialog is displayed.

- B. In the list box, select the LANtegrity server you want to log into.
- C. Enter the user name and password for the server.

 *To log in as the administrator for the first time, use the administrator name you specified when you installed NetWare on the LANtegrity Server. (See “[Server installation procedure](#)” on page 28.)*

- D. Click the Login button.

Response:

- If the LANtegrity server settings have not been established, a message is displayed that tells you that these settings must be specified. This message is only displayed if the server settings have not been saved.

Action: Click OK and then go to the next step.

or


- The Configure LANtegrity Server dialog is displayed. This is the screen where you enter information about the LANtegrity server.

Action: Go to the next step.

2. Specify the LANtegrity server settings.

A. Enter the following information on the Configure LANtegrity Server dialog:


- User name in the 'Distinguished Name' field. This setting is used to access NDS data, the LANtegrity server's file system, and protect files while they are stored on the stand-in server.

 *The user name should be the distinguished name of the administrator you specified when you installed NetWare on your LANtegrity server (see ["Preparing the hardware" on page 26](#)).*

- Password for the user name in the 'Password' field.
- NDS container in which to store protected NetWare 3 Bindery objects. Using this information, two organization units (OU) are automatically created for each NetWare 3x protected server in the NDS container. They are called LANtegrity Bindery A and LANtegrity Bindery B. Then the NetWare 3 Bindery objects are converted to NetWare 4 NDS objects. The files that contain Bindery information are protected on tape.
- Click on 'Use' to select the Archive Bit method.

By default, LANtegrity uses a file's archive bit to detect if the file has been modified on a protected server and, if so, to copy it to the LANtegrity Server. LANtegrity clears the attribute of each file that it copies. If your protected servers load other NLMs that set or clear the archive bit, you will need to indicate to the LANtegrity server that it should ignore the archive bit and instead use an alternate method of detecting change.

- B.** Click Close to save your changes.

 *You can accept the default values until you have had a chance to evaluate them.*

Info-map

For more information on these options, please refer to the online *Administrator's Guide*.

3. Configure each protected server

To support communications between the LANtegrity Server and its protected servers, you authenticate the protected servers by supplying the user name and password. You must perform this procedure once for each protected server.


To authenticate a Protected Server and enable protection:

- A.** Select **Tools/General Configuration** from the menu bar.





Response: The General Configuration dialog is displayed.

- B.** Select 'Protected Servers' from the icon list.

Response: The Configure Protected Servers dialog is displayed. It shows a list of the NetWare file servers that have been setup as protected servers.

 *You will not see the protected server in the list unless it is connected to the LANtegrity Server, and shows the status 'LANtegrity server operating.'*

You can identify the protection status of the listed servers by the type of icon shown next to the server name. The types are icons that may be displayed are described below:

This icon...	Means the server...
	is online and fully protected.
	has been authenticated and protection is enabled but not verified; therefore, the server is not ready for stand-in service.
	has the Agent loaded but not authenticated; therefore, the server is not ready for stand-in service.
	has the LANtegrity agent loaded, but the server has not been authenticated; therefore, the server is not ready for stand-in service.


- C.** Select the protected server you want to authenticate and click the Authenticate button.

Response: The LANtegrity Administrator window is displayed.


- D.** Do one of the following:
- For a NetWare 3 server, enter the name of a supervisor-equivalent.
 - For a NetWare 4 server, enter the distinguished name of the administrator that was specified when NetWare was installed on the LANtegrity server (see [“Preparing the hardware” on page 26](#)).

- E. Enter the appropriate password.
- F. Click OK to register the user name and password with the LANtegrity server and return to the Configure Protected Servers dialog.
- G. Click 'Enable Protection' to start protecting the selected server.


Response: The icon that represents the server shows a red X until an initial verify job completes successfully.

 *Until the initial verify job for the protected server completes successfully, the LANtegrity Server cannot stand-in for this server. By default, a verify job runs nightly at 7PM.*

- H. For a NetWare 3.x server, you must enter an Alternate NDS Bindery Context to enable protection of the server's Bindery. Enter the distinguished name of the NDS container that holds the LANtegrity Server object.
- I. For a NetWare 4.x server, enter a Server Bindery Context to enable Bindery logins to this protected server while the LANtegrity server is standing in. Enter the first distinguished name that appears in a SET BINDERY CONTEXT command on the protected server.
- J. Review the value for the 'Reboot timeout' setting and increase it, if necessary. The reboot timeout is the amount of time that the LANtegrity server waits after synchronization for the selected protected server to reboot before it returns to a stand-in operation.

 *The amount of time must be about twice the time it usually takes to reboot the selected server; otherwise the LANtegrity server will not be able to exit stand-in reliably.*

- K. Click OK to save the settings.

 *You can review Chapter 2, "Protecting Server Data," in the LANtegrity Administrator's Guide to understand the protection options and to decide if you need to customize LANtegrity for your environment.*

A

Additional servers
setting up20

Administrator Inter-
face client applica-
tion

installation
procedure31

Appending
to tape the backup
data50

Automated fea-
tures dialog
*illus.*16

B

Backup
creating a custom
backup job49
creating job for
ServerStor50
scheduling jobs51
the managed servers
for HSM use54

Backup Devices
compatible13

Backup rotation
setting in HSM
installation30

C

Cartridges
compatible13

CD ROM drive
preparing for HSM
installation26

Checklist
for LANtegrity55
HSM53

Client workstation
preparing for HSM
installation26

Command
to install HSM29
to load the LANtegrity
INSTALL NLM38

Compatible
backup devices
ServerStor13

Components
of LANtegrity37

Configuring
protected servers for
LANtegrity57

D

Destination
for LANtegrity server
software, specifying39

Domain server
HSM requirements25
preparing for HSM
installation26

F

Files
restoring52
restoring from
backup52
selecting for
ServerStor50
SMDR ~ to copy20
tagging for backup or
restore50
TSA ~ to copy20

H

HSM
Checklist53
command to install29
domain server
configuration25
managed server
configuration25
server installation28
storage server
configuration24

HSM administrator
application
starting53

HSM backup
device
preparing for HSM
installation26

HSM storage
server
preparing for HSM
installation26

I

Icons
displayed for LANteg-
rity protected status58

Identifying
managed servers for
HSM54
managed volumes for
HSM54

Install
LANtegrity37

Installation
of ServerStor14

Installing
administrator interface
client application31
LANtegrity software to
the server38
protected server soft-
ware for LANtegrity39
ServerStor11-21, 23-
32, 34-46

J

Job Scheduler
using51

Jobs
backup49
scheduling51
setting a job start
message51

L

LANtegrity
checklist55
components37
installing37
installing software to
server38
logging in to server55
providing port
address35

LANtegrity admin-
istrator application
setting up45

LANtegrity
INSTALL NLM
loading38, 39

LANtegrity installa-
tion
entering user name
and password for LAN-
tegrity server34
information required34
IPX address for pro-
tected servers35
Other applications that
affect archive35
User name and pass-
word for protected
server35

LANtegrity server
providing user name
and password34
setting up41

LANtegrity server
settings
specifying56

Library
updating for
ServerStor50

LOAD RESQMAIN
command to load
NLM17

Loading
LANtegrity INSTALL
NLM38, 39
the LANtegrity
INSTALL NLM38
the NLM for
ServerStor17

M

Managed server
HSM requirements25

Managed servers
preparing for HSM
installation26

McAfee
contact information9
overview7
product line7
support9
training10

Media cartridge
to use with
ServerStor13

Microsoft Windows
supported versions12

Migration volumes
creating for HSM
installation27
recommended names
for HSM ~27

Modifying
 PROTOCOL.INI[31](#)

N

NLM
 command to load LAN-
 integrity INSTALL ~[38](#)

O

Overwriting
 backup tapes[50](#)

P

Port address
 providing for
 LANtegrity[35](#)

Preparing
 to install HSM[23](#)

Protected server
 setting up for
 LANtegrity[43](#)

 system requirements
 to install LANtegrity[36](#)

Protected server
 software
 installing for
 LANtegrity[39](#)

Protected servers
 configuring for
 LANtegrity[57](#)

Protected status
 icons representing[58](#)

PROTOCOL.INI
 modifying during
 installation[31](#)

R

Rescue Disk
 updating[18](#)

Rescue drive
 assigning[11](#)

Rescue function
 for ServerStor[18](#)

Restoring
 files using
 ServerStor[52](#)

S

Saving
 job definition[50](#)

SCSI adapter
 preparing for HSM
 installation[26](#)

Search
 using[52](#)

Secondary server
 system requirements
 to install LANtegrity[36](#)

Selecting
 cues to indicate a
 backup job is
 starting[51](#)

 files for ServerStor[50](#)

Server
 hardware configura-
 tion for ServerStor[12](#)

Server installation
 for HSM[28](#)

 process[29](#)

Server settings
 specifying for LANteg-
 rity use[56](#)

ServerStor
 before beginning[11](#)
 compatible backup
 devices[13](#)
 deciding where to
 install[11](#)
 features, overview[22](#)
 installation[14](#)
 installing[11-21, 34-46](#)
 installing HSM[23-32](#)
 loading NLM[17](#)
 media cartridge to
 use[13](#)
 rescue function[18](#)
 server hardware[12](#)
 system
 requirements[12](#)
 using with Novell[11](#)
 workstation
 configuration[12](#)

ServerStor LAN-
 integrity
 preparing to install[34](#)

ServerStor main
 window
 illus.[49](#)

Setting Up
 rescue function for
 ServerStor[18](#)

Setting up
 additional servers for
 ServerStor[20](#)
 LANtegrity administra-
 tor application[45](#)
 LANtegrity server[41](#)
 protected server[43](#)

setting up HSM
 preparation[23](#)

SMDR
 files to copy[20](#)

Specifying

destination for LANtivity server software39

Starting

HSM administrator application53

Storage server

identifying for HSM54

installation requirements for HSM24

System failure

protecting servers from34

System Requirements

defined12-13, 24-26, 36

ServerStor12

W

Workstation configuration

to run ServerStor12

T

Tagging files

for backup or restore50

Tape

appending to50

overwriting50

Tape drive

preparing for HSM installation26

Tape Drives

compatible13

TSA

files to copy20

U

Updating

Library50