HP ProLiant ML310 Storage Server

user guide

This guide provides installation, configuration, and administration information for the HP ProLiant ML310 Storage Server with Microsoft® Windows® Storage Server 2003 R2.



Part number: AG620-96001
First edition: November 2006



Legal and notice information

© Copyright 2006 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, Windows XP, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.

Contents

About this guide . . . 11
Intended audience . . . 11
Getting help . . . 11
Related documentation . . . 11
Conventions . . . 11
Document conventions and symbols . . . 12
Text symbols . . . 12
HP technical support . . . 12
HP subscriber's choice . . . 13
HP-authorized reseller . . . 13
Other helpful web sites . . . 13
HP hardware support services . . . 13

1 Installing and configuring the server . . . 15
Setup overview . . . 15
Planning for installation . . . 15
Planning a network configuration . . . 16
Configuration checklist . . . 16
Installing the server . . . 16
Locating and writing down the serial number . . . 16
Checking kit contents . . . 17
Powering on the server . . . 17
Factory image . . . 17
Physical configuration . . . 17
Default boot sequence . . . 18
Accessing the HP Storage Server Management console . . . 18
Using the Direct attach method . . . 19
Using the Remote browser method . . . 19
Using the Remote desktop method . . . 22
Logging off and disconnecting . . . 23
Telnet Server . . . 23
Enabling Telnet Server . . . 23
Using the Integrated Lights-Out 2 method . . . 23
Configuring the server on the network . . . 25
Before you begin . . . 25
Running the Rapid Startup Wizard . . . 26
Completing system configuration . . . 26

2 Storage management overview . . . 29
Storage management elements . . . 29
Storage management example . . . 29
Physical storage elements . . . 30
Arrays . . . 31
Fault tolerance . . . 31
Online Spares . . . 32
Logical storage elements . . . 32
Logical drives (LUNs) . . . 32
Partitions . . . 33
Volumes . . . 33
File system elements . . . 34

File sharing elements . . . 34
Volume Shadow Copy Service overview . . . 34
Using storage elements . . . 34
Clustered server elements . . . 34
Network adapter teaming . . . 35

3 File server management . . . 37
New or improved file services features in Windows Storage Server 2003 R2 . . . 37
Storage Manager for SANs . . . 37
Single Instance Storage . . . 37
Search enhancements . . . 37
File Server Resource Manager . . . 37
Windows SharePoint Services . . . 38
HP Storage Server Management Console . . . 38
File services management . . . 38
Configurable and pre-configured storage . . . 38
Storage management utilities . . . 39
Array management utilities . . . 39
Array Configuration Utility . . . 40
Disk Management utility . . . 40
Guidelines for managing disks and volumes . . . 41
When managing disks and volumes: . . . 41
Scheduling defragmentation . . . 41
Disk quotas . . . 42
Adding storage . . . 42
Expanding storage . . . 43
Extending storage using Windows Storage Utilities . . . 43
Expanding storage for EVA arrays using Command View EVA . . . 44
Expanding storage using the Array Configuration Utility . . . 44
Volume shadow copies . . . 44
Shadow copy planning . . . 45
Identifying the volume . . . 45
Allocating disk space . . . 45
Identifying the storage area . . . 46
Determining creation frequency . . . 46
Shadow copies and drive defragmentation . . . 46
Mounted drives . . . 47
Managing shadow copies . . . 47
The shadow copy cache file . . . 48
Enabling and creating shadow copies . . . 49
Viewing a list of shadow copies . . . 50
Set schedules . . . 50
Viewing shadow copy properties . . . 50
Redirecting shadow copies to an alternate volume . . . 50
Disabling shadow copies . . . 51
Managing shadow copies from the storage server desktop . . . 51
Shadow Copies for Shared Folders . . . 52
SMB shadow copies . . . 52
NFS shadow copies . . . 53
Recovery of files or folders . . . 54
Recovering a deleted file or folder . . . 54
Recovering an overwritten or corrupted file . . . 55
Recovering a folder . . . 55
Backup and shadow copies . . . 55
Shadow Copy Transport . . . 56
Folder and share management . . . 56
Folder management . . . 57
Share management . . . 63
Share considerations . . . 63

Defining Access Control Lists . . . 64
Integrating local file system security into Windows domain environments . . . 64
Comparing administrative (hidden) and standard shares . . . 64
Managing shares . . . 64
File Server Resource Manager . . . 65
Quota management . . . 65
File screening management . . . 65
Storage reports . . . 65
Other Windows disk and data management tools . . . 66
Additional information and references for file services . . . 66
Backup . . . 66
HP StorageWorks Library and Tape Tools . . . 66
Antivirus . . . 66
Security . . . 66
More information . . . 66

4 Print services . . . 69
Microsoft Print Management Console . . . 69
New or improved HP print server features . . . 69
HP Web Jetadmin . . . 69
HP Install Network Printer Wizard . . . 69
HP Download Manager for Jetdirect Print Devices . . . 69
Microsoft Print Migrator Utility . . . 69
Network printer drivers . . . 69
Print services management . . . 70
Microsoft Print Management Console . . . 70
HP Web Jetadmin installation . . . 70
Web-based printer management and Internet printing . . . 70
Planning considerations for print services . . . 70
Print queue creation . . . 71
Sustaining print administration tasks . . . 71
Driver updates . . . 72
Print drivers . . . 72
User-mode vs. kernel-mode drivers . . . 72
Kernel-mode driver installation blocked by default . . . 72
HP Jetdirect firmware . . . 72
Printer server scalability and sizing . . . 72
Backup . . . 72
Best practices . . . 73
Troubleshooting . . . 73
Additional references for print services . . . 73

5 Microsoft Services for Network File System (MSNFS) . . . 75
MSNFS Features . . . 75
UNIX Identity Management . . . 75
MSNFS use scenarios . . . 76
MSNFS components . . . 76
Administering MSNFS . . . 77
Server for NFS . . . 77
User Name Mapping . . . 81
Microsoft Services for NFS troubleshooting . . . 83
Microsoft Services for NFS command-line tools . . . 83
Optimizing Server for NFS performance . . . 83
Print services for UNIX . . . 83

6 Other network file and print services . . . 85
File and Print Services for NetWare (FPNW) . . . 85
Installing Services for NetWare . . . 85

Managing File and Print Services for NetWare . . . 86
Creating and managing NetWare users . . . 87
Adding local NetWare users . . . 87
Enabling local NetWare user accounts . . . 88
Managing NCP volumes (shares) . . . 89
Creating a new NCP share . . . 89
Modifying NCP share properties . . . 90
Print Services for NetWare . . . 90
Point and Print from Novell to Windows Server 2003 . . . 90
Additional resources . . . 90
AppleTalk and file services for Macintosh . . . 91
Installing the AppleTalk protocol . . . 91
Installing File Services for Macintosh . . . 91
Completing setup of AppleTalk protocol and shares . . . 91
Print services for Macintosh . . . 92
Installing Print Services for Macintosh . . . 92
Point and Print from Macintosh to Windows Server 2003 . . . 92

7 Troubleshooting, servicing, and maintenance . . . 93
Troubleshooting the storage server . . . 93
Maintenance and service . . . 93
Maintenance and service documentation . . . 94
Maintenance updates . . . 94
System updates . . . 94
Customer self repair . . . 94
Firmware updates . . . 94
Certificate of Authenticity . . . 95

8 System installation and recovery . . . 97
The Installation and Recovery DVD . . . 97
To restore a factory image . . . 97
Systems with a DON'T ERASE partition . . . 97
Managing disks after a restoration . . . 97

A Server components . . . 99
ML310 hardware components . . . 99

B Configuring storage server for Web access (optional) . . . 103
Setting up an Internet connection . . . 103

C Regulatory compliance and safety . . . 105
Federal Communications Commission notice . . . 105
Class A equipment . . . 105
Class B equipment . . . 105
Declaration of conformity for products marked with the FCC logo, United States only . . . 105
Modifications . . . 106
Cables . . . 106
Laser compliance . . . 106
International notices and statements . . . 107
Canadian notice (Avis Canadien) . . . 107
Class A equipment . . . 107
Class B equipment . . . 107
European Union notice . . . 107
BSMI notice . . . 107
Japanese notice . . . 108
Korean notice A&B . . . 108
Class A equipment . . . 108

Class B equipment . . . 108
Safety . . . 108
Battery replacement notice . . . 108
Taiwan battery recycling notice . . . 109
Power cords . . . 109
Japanese power cord notice . . . 109
Electrostatic discharge . . . 109
Preventing electrostatic discharge . . . 109
Grounding methods . . . 109
Waste Electrical and Electronic Equipment (WEEE) directive . . . 110
Czechoslovakian notice . . . 110
Danish notice . . . 110
Dutch notice . . . 110
English notice . . . 111
Estonian notice . . . 111
Finnish notice . . . 111
French notice . . . 111
German notice . . . 112
Greek notice . . . 112
Hungarian notice . . . 112
Italian notice . . . 112
Latvian notice . . . 113
Lithuanian notice . . . 113
Polish notice . . . 113
Portuguese notice . . . 113
Slovakian notice . . . 114
Slovenian notice . . . 114
Spanish notice . . . 114
Swedish notice . . . 114

. . . 117

Figures

1 ML310 hardware RAID . . . 18
2 Internet options screen . . . 20
3 HP Storage Server Management console . . . 22
4 Storage management process example . . . 30
5 Configuring arrays from physical drives . . . 31
6 RAID 0 (data striping) (S1-S4) of data blocks (B1-B12) . . . 31
7 Two arrays (A1, A2) and five logical drives (L1 through L5) spread over five physical drives 33
8 System administrator view of Shadow Copies for Shared Folders . . . 48
9 Shadow copies stored on a source volume . . . 48
10 Shadow copies stored on a separate volume . . . 49
11 Accessing shadow copies from My Computer . . . 52
12 Client GUI . . . 53
13 Recovering a deleted file or folder . . . 55
14 Properties dialog box, Security tab . . . 58
15 Advanced Security settings dialog box, Permissions tab . . . 59
16 User or group Permission Entry dialog box . . . 60
17 Advanced Security Settings dialog box, Auditing tab . . . 61
18 Select User or Group dialog box . . . 61
19 Auditing Entry dialog box for folder name NTFS Test . . . 62
20 Advanced Security Settings dialog box, Owner tab . . . 63
21 Accessing MSNFS from HP Storage Server Management console . . . 77
22 File and Print Services for NetWare dialog box . . . 87
23 New User dialog box . . . 88
24 NetWare Services tab . . . 89
25 Front panel . . . 100
26 Rear panel . . . 101
27 Automatic configuration settings . . . 103
28 Proxy server settings . . . 103

Tables

1 Document conventions 12
2 Network access methods 15
3 Installation and Configuration checklist 16
4 Server configuration worksheet 25
5 Summary of RAID methods 32
6 Tasks and utilities needed for storage server configuration 39
7 Authentication table 78
8 MSNFS command-line administration tools 83
9 Front panel components 101
10 Rear panel components 101

About this guide

This guide provides information for setting up, configuring, and administering the HP ProLiant ML310 Storage Server.

This guide is available on the HP web site and is also provided as a PDF document on the HP ProLiant Storage Server documentation CD.

Intended audience

This book is intended for use by technical professionals who are experienced with the following:

- Microsoft® administrative procedures
- System and storage configurations

Getting help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

NOTE:

Known issues and work arounds for the storage server products and the service release are addressed in release notes. To view the latest version, visit http://www.hp.com/go/support. Select **See support and troubleshooting** information and enter a product name/number. Under self-help resources, select **manuals (guides, supplements, addendums, etc.)**.

Related documentation

In addition to this guide, refer to the following document for more information:

- *HP Integrated Lights-Out 2 User Guide*

This document is available on the Documentation CD or it can be obtained at http://www.hp.com/go/storageservers. Select your product, then click **Technical documentation** under the Support section.

For product specifications, see the HP Network Attached Storage (NAS) Web site at http://h18006.www1.hp.com/storage/nas.html.

Conventions

This document contains the following conventions and symbols:

- Document conventions
- Text symbols

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italic font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

Text symbols

⚠ **WARNING!**

Indicates that failure to follow directions could result in bodily harm or death.

△ **CAUTION:**

Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT:

Provides clarifying information or specific instructions.

NOTE:

Provides additional information.

TIP:

Provides helpful hints and shortcuts.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: http://www.hp.com/support/.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

HP subscriber's choice

HP strongly recommends that customers sign up online using the Subscriber's choice web site: http://www.hp.com/go/e-updates.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates, as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support**, and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-282-6672.
- Elsewhere, visit the HP web site: http://www.hp.com. Then, click **Contact HP** to find locations and telephone numbers.

Other helpful web sites

For other product information, see the following HP web sites:

- http://www.hp.com/go/storage
- http://www.hp.com/support/
- http://www.docs.hp.com
- http://www.microsoft.com

HP hardware support services

HP Instant Support Enterprise Edition (ISEE) provides proactive remote monitoring, diagnostics, and troubleshooting to help you enhance the availability of your servers, as well as storage and network devices. The ISEE software is located on the storage server in the `c:\hpnas\components\ISEE` folder. For more information, go to the HP web site: http://h20219.www2.hp.com/services/cache/10707-0-0-225-121.aspx.

HP Services provides service tools that notify you when a significant system event has or will occur. These tools, WEBES System Event Analyzer (SEA) and OSEM, are used both as part of the ISEE remote service offering and as standalone tools to HP service customers. They are designed to send a notification only when an event or series of events has occurred that require service action. They are not intended to be real-time system state monitors that trigger with every event. Most system components have the capability of sending hundreds of state events during normal operation. SEA and OSEM are designed to filter these component events and only notify customers and/or HP Services when action needs to be taken to resolve or prevent an outage. As designed they will not report all events. Other utilities are available to monitor real time system state. The software is located on the storage server in the `c:\hpnas\components\ISEE\OSEM` and `c:\hpnas\components\ISEE\WEBES` folders.

1 Installing and configuring the server

Setup overview

Your HP ProLiant storage server comes pre-installed with the Windows® Storage Server™ 2003 R2 operating system. Windows Storage Server 2003 R2 extends the Windows Storage Server 2003 operating system, providing a more efficient way to manage and control access to local and remote resources. In addition, Windows Storage Server 2003 R2 provides a scalable, security-enhanced Web platform for simplified branch server management, improved identity and access management, and more efficient storage management.

Planning for installation

Before you install your HP ProLiant storage server, you need to make a few up-front decisions.

Determining a network access method

Before beginning setup and startup procedures, you should decide upon an access method to connect to the storage server. The type of network access you select is determined by whether or not the network has a Dynamic Host Configuration Protocol (DHCP) server. If the network has a DHCP server, you can access the storage server through the direct attachment, remote browser, remote desktop, or iLO 2 methods. If your network does not have a DHCP server, you must access the storage server through the direct attachment method.

NOTE:

The direct attachment method requires a display, keyboard, and mouse.

Table 2 Network access methods

Access method	I.E. 5.5 or later required?	Storage server desktop accessible?	HP ProLiant Rapid Startup Wizard access	Notes
Direct attachment	No	Yes	Directly from the storage server desktop.	Requires a monitor, mouse, and keyboard.
Remote browser	Yes	No	Directly from the HP ProLiant Storage Server Management console.	Does not display the storage server desktop.
Remote desktop	No	Yes	Indirectly from the storage server desktop.	Windows remote desktop capability required on client.
HP Integrated Lights-Out 2 (iLO 2) connectivity	Yes	Yes	Indirectly from the storage server desktop.	See the *HP Integrated Lights-Out 2 User Guide* for server access instructions.

Planning a network configuration

You use the Rapid Startup Wizard to configure your storage server. This wizard is displayed automatically when you first start your system. Before you run the Rapid Startup Wizard, it is helpful to gather together the network configuration information you need, including:

- User name and administrator password (the system provides you with defaults you need to change)
- E-mail addresses to set up system alerts
- SNMP settings
- Local area network (LAN) configuration settings

To help you gather this information, see "Configuring the server on the network" on page 25.

Configuration checklist

Use the following checklist to make sure you have completed all configuration tasks for your HP ProLiant storage server. The steps for each task are explained in more detail in subsequent chapters of this guide.

Table 3 Installation and Configuration checklist

	Steps	Reference
☐	1. Unpack server, check kit contents, and become familiar with front and back panels of storage server. Locate and write down serial number of storage server.	See "Checking kit contents" on page 17.
☐	2. If you plan to rack the server, complete the rail installation instructions.	See the HP ProLiant rail installation instructions and tower-to-rack conversion instructions, if applicable.
☐	3. Connect cables; (optional) connect a keyboard, mouse, and monitor; power on server, and log in to the server.	See Powering on the server and Direct attach method.
☐	4. Access the HP Storage Server Management console.	See "Accessing the HP Storage Server Management console" on page 18.
☐	5. Complete the storage server configuration worksheet.	See "Server configuration worksheet" on page 25.
☐	6. Run Rapid Startup Wizard.	See "Rapid Startup Wizard" on page 26.
☐	7. Complete system configuration.	See "Completing system configuration" on page 26.
☐	8. Configure storage server for Web access, if necessary.	See "Configuring storage server for Web access (optional)" on page 103.

Installing the server

To install your HP ProLiant storage server, follow the instructions in the sections below:

- Locating and writing down the serial number
- Checking kit contents
- Powering on the server

Locating and writing down the serial number

Before completing the installation portion of this guide, locate and write down the storage server's serial number, which may be needed to access the HP Storage Server Management console later on during the set up process.

The HP ProLiant storage server's serial number is located in three places:

- Top of the storage server
- Back of the storage server
- Inside the storage server shipping box

Checking kit contents

Remove the contents, making sure you have all the components listed below. If components are missing, contact HP technical support.

1	HP ProLiant Storage Server (with operating system preloaded)	5	*End User License Agreement*
2	Power cord(s)	6	Certificate of Authenticity Card
3	Product Documentation and Safety and Disposal Documentation CD	7	*ProLiant Essentials Integrated Lights-Out 2 Advanced Pack*
4	*HP ProLiant Storage Server Installation and System Recovery DVD*		

Powering on the server

Power on the server after connecting the cables. For more information on your storage server model's hardware components, see "Server components" on page 99.

1. Power on server by pushing the power button. The power LED illuminates green.
2. When the server powers on, an installation progress screen is displayed. The installation process takes approximately 10 to 15 minutes to complete and the server will reboot twice. No user interaction is required.

△ **CAUTION:**

Do not interrupt the installation process; when the installation sequence is complete, the system prompt appears.

3. Go to "Accessing the HP Storage Server Management console" on page 18 to set up server access.

Factory image

HP ProLiant Storage Servers are preconfigured with default storage settings and preinstalled with the Windows Storage Server 2003 R2 operating system (OS). This section provides additional details about the preconfigured storage.

Physical configuration

The logical drives reside on all four physical disks as shown in Figure 1. The DON'T ERASE volume contains an image that is deployed onto the OS partition during system installation.

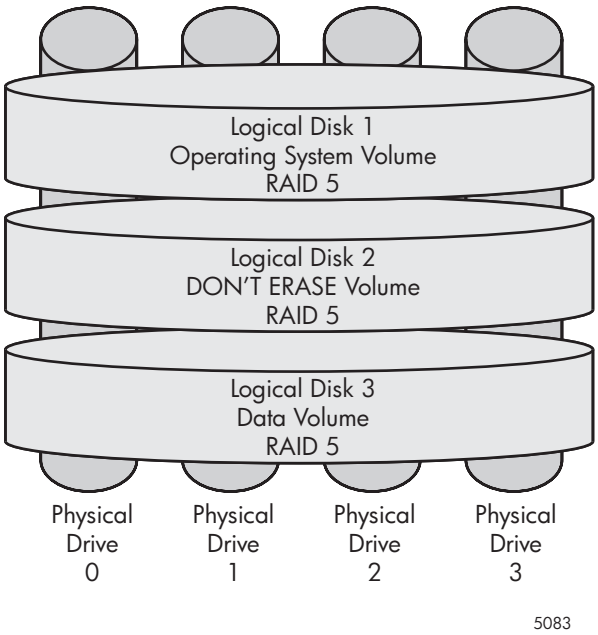


Figure 1 ML310 hardware RAID

NOTE:

In the HP Array Configuration Utility (ACU), logical drives are labeled 1 and 2. In Microsoft Disk Manager, logical drives are displayed as 0 and 1. For HP Smart Array configuration information, see http://h18004.www1.hp.com/products/servers/proliantstorage/arraycontrollers/.

The DON'T ERASE logical disk supports the recovery process only and does not host a secondary operating system. If the operating system has a failure that might result from corrupt system files, a corrupt registry, or the system hangs during boot, refer to "System installation and recovery" on page 97.

Data volumes are not carved at the factory or by the System Installation and Recovery DVD, and must be configured manually by the end user. Be sure to back up your user data, and then use the System Installation and Recovery DVD to restore the server to the factory default state as soon as conveniently possible.

Default boot sequence

The BIOS supports the following default boot sequence:

1. DVD-ROM
2. HDD
3. PXE (network boot)

Under normal circumstances, the storage servers boot up from the OS logical drive.

- If the system experiences a drive failure, the drive displays an amber disk failure LED.
- If a single drive failure occurs, it is transparent to the OS.

Accessing the HP Storage Server Management console

Before accessing the HP Storage Server Management console, verify that the storage server is completely installed in the rack, and that all cables and cords are connected.

To access the HP Storage Server Management console, you can use these access methods:

Direct attach	To connect directly to the storage server without using the network.
Remote browser	To establish a browser-based connection to the HP ProLiant Storage Server Management console from a remote client running Internet Explorer 5.5 (or later).
Remote desktop	To establish a connection from a remote client without using a browser. This method requires the client to have Windows remote desktop capability.
HP Integrated Lights-Out 2 (iLO 2)	To establish a browser-based connection from a remote client using the iLO 2 interface.

For more information, see "Planning for installation" on page 15.

IMPORTANT:

An IP address can be substituted for a storage server's serial number and hyphen when using either remote browser or remote desktop methods to access the HP Storage Server Management console. For example: 192.0.0.1 can be substituted for TWT08466-.

Using the Direct attach method

You can access the HP Storage Server Management console using a monitor, mouse, and keyboard directly attached to the storage server.

To connect the storage server to a network using the direct attach method

1. Log in to the HP ProLiant Storage Server with the default user name `administrator` and the password `hpinvent`.

   The HP ProLiant Storage Server Management console and Rapid Startup Wizard will start automatically.

   NOTE:

   You can change the administrator name and password when you configure the server using the "Rapid Startup Wizard" on page 26.

2. To complete network configuration using the Rapid Startup Wizard, see "Configuring the server on the network" on page 25.

Using the Remote browser method

The storage server ships with DHCP enabled on the network port. If the server is placed on a DHCP-enabled network and the serial number of the device is known, the server can be accessed through a client running Internet Explorer 5.5 (or later) on that network, using the TCP/IP 3202 port.

IMPORTANT:

Before you begin this procedure, ensure that you have the following:

- Windows-based PC loaded with Internet Explorer 5.5 (or later) on the same local network as the storage server
- DHCP-enabled network
- Serial number or IP address of the storage server

To connect the server to a network using the remote browser method, you must first ensure that the client is configured to download signed ActiveX controls.

To enable ActiveX controls

1. On the remote client machine, open the Internet Explorer web browser and select **Tools > Internet Options > Security**.

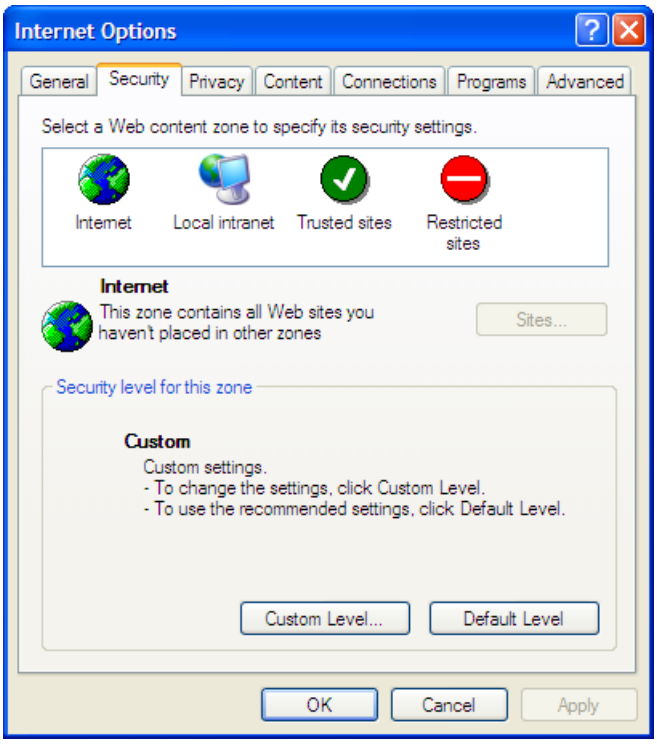
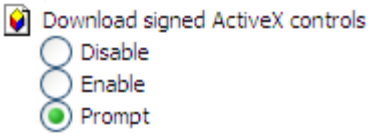


Figure 2 Internet options screen

2. On the Security screen, select **Internet** or **Local intranet** web content zone, then click **Custom Level**.
3. Scroll down to locate the **ActiveX Controls and plug-ins settings**.
4. At **Download signed ActiveX controls settings**, select **Enable** to enable ActiveX or **Prompt** to launch a notice requiring approval before ActiveX is enabled.



5. Click **OK** to close the **Security Settings** dialog box.
6. If prompted **Are you sure you want to change the security settings for this zone** click **YES**.
7. On the **Internet Options** dialog box, click **OK** to finish.

To connect the storage server to a network using the remote browser method

1. On the remote client machine open Internet Explorer and enter `https://` and the serial number of the storage server followed by a hyphen (-), and then`:3202`. For example, `https://D4059ABC3433-:3202` Press **Enter**.

NOTE:

If you are able to determine the IP address from your DHCP server, you can substitute the IP address for the serial number and hyphen (-). For example: 192.100.0.1:3202.

2. Click **OK** on the **Security Alert** prompt.
3. Log in to the HP ProLiant Storage Server Management console with the default user name `administrator` and the password `hpinvent`.

NOTE:

You can change the administrator name and password when you configure the server using the "Rapid Startup Wizard" on page 26.

4. To complete network configuration using the Rapid Startup Wizard, see "Configuring the server on the network" on page 25.

IMPORTANT:

If you are using the remote browser method to access the HP Storage Server Management console and Rapid Startup Wizard, always close the remote session before closing your Internet browser. Closing the Internet browser does not close the remote session. Failure to close your remote session impacts the limited number of remote sessions allowed on the storage server at any given time.

Connecting to the storage server permits you to access the HP Storage Server Management console (Figure 3). From the console, you can access snap-ins that allow complete server system management.

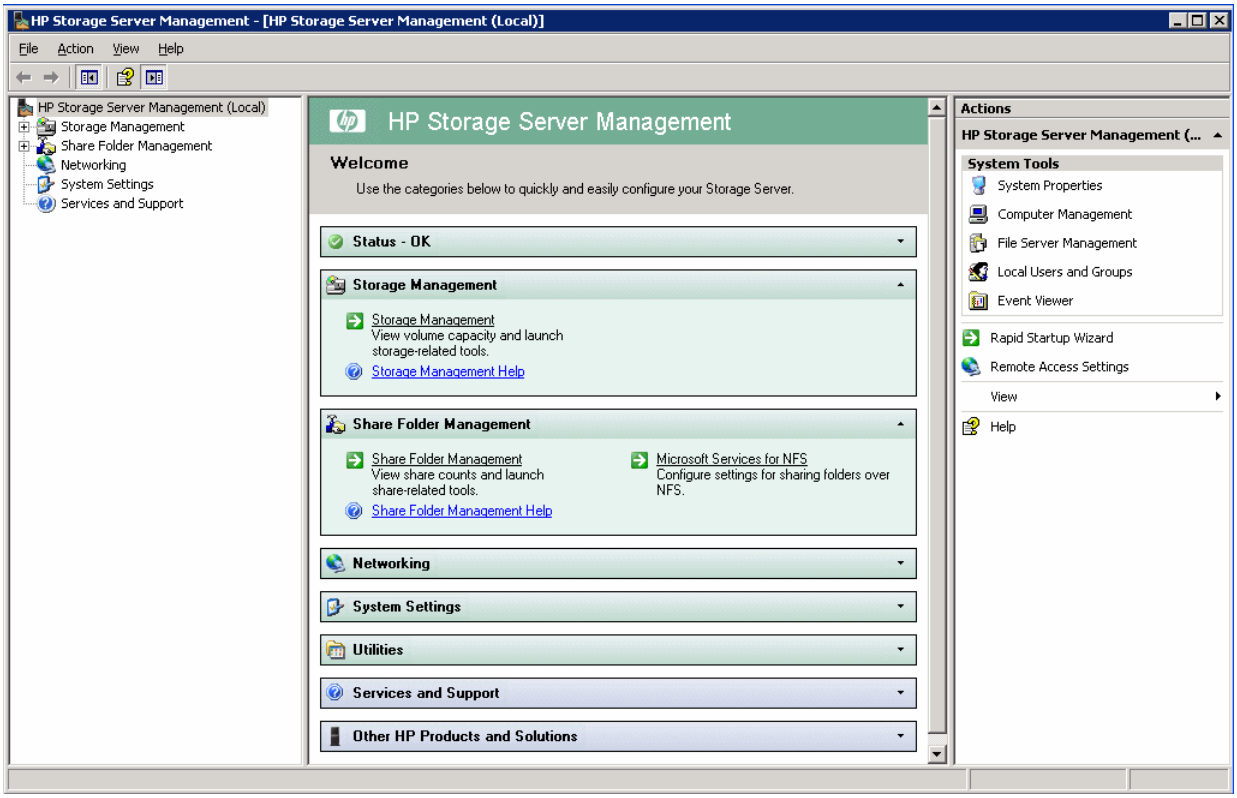


Figure 3 HP Storage Server Management console

Using the Remote desktop method

Remote Desktop provides the ability for you to log onto and remotely administer your server, giving you a method of managing it from any client. Installed for remote administration, Remote Desktop allows only two concurrent sessions. Leaving a session running takes up one license and can affect other users. If two sessions are running, additional users will be denied access.

To connect the storage server to a network using the remote desktop method

1. On the PC client, select **Start > Run**. At **Open**, type `mstsc`, then click **OK**.
2. Enter the serial number of the storage server followed by a hyphen (-) in the **Computer** box and click **Connect**. For example: D4059ABC3433-.

NOTE:

If you are able to determine the IP address from your DHCP server, you can substitute the IP address for the serial number and hyphen (-). For example: 192.100.0.1.

3. Log in to the HP ProLiant Storage Server with the default user name `administrator` and the password `hpinvent`.

   The HP ProLiant Data Protection Storage Server Management console and Rapid Startup Wizard will start automatically.

NOTE:

You can change the administrator name and password when you configure the server using the "Rapid Startup Wizard" on page 26.

4. To complete network configuration using the Rapid Startup Wizard, see "Configuring the server on the network" on page 25.

Logging off and disconnecting

Remote Desktop provides two options when closing a client: you can either disconnect or log off the system.

Disconnecting leaves the session running on the server. You can reconnect to the server and resume the session. If you are performing a task on the server, you can start the task and disconnect from the session. Later, you can log back on the server, re-enter the session, and either resume the task or check results. This is especially helpful when operating over a remote connection on a long-distance toll line.

Ending the session is known as *logging off*. Logging off ends the session running on the server. Any applications running within the session are closed, and unsaved changes made to open files will be lost. The next time you log onto the server, a new session is created.

Remote Desktop requires that all connecting users be authenticated, which is why users must log on each time they start a session.

Telnet Server

Telnet Server is a utility that lets users connect to machines, log on, and obtain a command prompt remotely. Telnet Server is preinstalled on the storage server, but must be activated before use.

△ **CAUTION:**

For security reasons, the Telnet Server is disabled by default. The service needs to be modified to enable access to the storage server with Telnet.

Enabling Telnet Server

The Telnet Server service needs to be enabled prior to its access. The service can be enabled by opening the services MMC:

1. Select **Start > Run**, and then enter **services.msc**.
2. Locate and right-click the Telnet service and then select **Properties**.
3. Choose one of the following:
   - For the Telnet service to start up automatically on every reboot, in the Startup Type drop-down box, click **Automatic**, and then click **OK**.
   - For the Telnet service to be started manually on every reboot, in the Startup Type drop-down box, click **Manual**, and then click **OK**.

On the storage server, access the command line interface, either by Remote Desktop or a direct connection, and then enter the following command:

net start tlntsvr

Sessions information

The sessions screen provides the ability to view or terminate active sessions.

Using the Integrated Lights-Out 2 method

Integrated Lights-Out 2 (iLO 2) is HP's fourth generation of Lights-Out management technology that allows you to perform virtually any system administrator or maintenance task remotely as if you were using its keyboard, mouse and monitor, power button and floppy, CD or USB key, whether or not the server is operating. It is available in two forms, iLO 2 Standard and iLO 2 Advanced. iLO 2 Standard provides basic system board management functions, diagnostics and essential Lights-Out functionality on supported ProLiant servers. iLO 2 Advanced provides advanced remote administration functionality as a licensed option, which is included with the ProLiant Storage Server.

The Integrated Lights-Out port on the storage server can be configured through the Rapid Startup Wizard or through the iLO 2 ROM-Based Setup Utility (RBSU). SNMP is enabled and the Insight Management Agents are preinstalled.

The HP iLO 2 management processor provides multiple ways to configure, update, operate, and manage servers remotely. The HP ProLiant Storage Server comes preconfigured with iLO 2 default factory settings, including a default user account and password. These settings can be found on the iLO 2 Default Network Settings tag found on the front of the server. If iLO 2 is connected to a network running DNS and DHCP, you can use it immediately without changing any settings.

For more information on using HP iLO 2, see the *HP Integrated Lights-Out 2 User Guide*.

To quickly set up iLO 2 using the default settings for iLO 2 Standard and iLO 2 Advanced features, follow the steps below

1. Ensure that a network cable is connected to the iLO 2 port located on the back of the storage server.

NOTE:

This connection method is easiest when the connection is to a DHCP and DNS supported network.

2. If not using dynamic DHCP (IP addressing), you will need to input a static IP address by using the direct attach method and the iLO 2 RBSU.
3. Using the methods described in the *HP Integrated Lights–Out 2 User Guide*, connect to the iLO 2 port.

NOTE:

To find the default iLO 2 log in settings, see the iLO 2 Default Network Settings card attached to your server. The default DNS, administrator name, and password needed to log in will be on this card.

4. If desired, you can change the default user name and password on the administrator account to your predefined selections.
5. Set up your user accounts, if using the local accounts feature.
6. Activate iLO 2 advanced features by entering a license key from the included *ProLiant Essentials Integrated Lights-Out 2 Advanced Pack*.
7. Access the HP ProLiant Storage Server using the iLO 2 Remote Console functionality. Log in to the HP ProLiant Storage Server with the default user name `administrator` and the password `hpinvent`. The HP ProLiant Storage Server Management console starts automatically.

NOTE:

When the Remote Console feature is enabled, you can get access to the storage server's login screen.

The Integrated Lights-Out 2 port comes with factory default settings, which the administrator can change. Administrators may want to add users, change SNMP trap destinations, or change networking settings. Refer to the *HP Integrated Lights-Out 2 User Guide* for information about changing these settings. To obtain this guide, go to http://www.hp.com/support/manuals, navigate to the servers section, and select **Server management**. In the ProLiant Essentials Software section, select **HP Integrated Lights-Out 2 (iLO 2) Standard Firmware**.

Configuring the server on the network

Before you begin

When first powering on the storage server you need to have some configuration data readily available to complete the Rapid Startup Wizard. Complete the Server configuration worksheet and use the data collected to initialize the storage server.

NOTE:

Ensure you are logged into the HP ProLiant Storage Server as a local or domain administrator.

Table 4 Server configuration worksheet

Configuration Worksheet	
Administrative Identity	
User name	Change system administrator's user name, which is set by default to `administrator`.
User password	Change system administrator's password, which is set by default to `hpinvent`.
Alert E-mail Notification	
E-mail address alert sent to	E-mail address for critical, warning, or informational messages about server status.
E-mail address alert sent from	Must be a valid, well-formed e-mail address that will appear as the sender of server status e-mail alerts.
SMTP server name or IP address	Must be an e-mail server on your network that supports the Simple Mail Transfer Protocol (SMTP).
SNMP Settings (to be completed only if needed)	
Contact person	System administrator for the storage server. The contact and location will be provided to any SNMP management computer that requests them.
System location	Any text string, such as a location or phone number. For example, `Floor #3, Financial Services Bldg`.
Community name No. 1	The community name is used for network authentication when sending outgoing SNMP messages.
Trap destination No. 1	The IP address of a management computer that will receive SNMP messages from the storage server using the above community name.
Community name No. 2	Same as above.
Trap destination No. 2	Same as above.
Network Interfaces (to be completed for non-DHCP configurations)	
Local area connection 1	A local area connection is automatically created for each network adapter that is detected.
IP address	An Internet Protocol (IP) address is assigned to the server. If it is not automatically assigned, enter the IP address that you want to assign to this server.
Subnet mask	A mask is used to determine what subnet an IP address belongs to.
Default gateway	The gateway in a network that the network adapter will use to access all other networks.

Configuration Worksheet	
Local area connection 2	Any additional local area connections can be renamed to prevent confusion.
IP address	Same as above.
Subnet mask	Same as above.
Default gateway	Same as above.
iLO 2 settings	Change the host name, IP settings, and administrator settings.
DNS server	A Domain Name System (DNS) server name is required to provide for domain name to IP address resolution.
WINS server	A Windows Internet Naming Service (WINS) server name is required to determine the IP address associated with a particular network computer.
Server Name	
Server name	Assign a unique name to the storage server. This name identifies the storage server on the network.

Running the Rapid Startup Wizard

The Rapid Startup Wizard is only displayed during the initial setup process. This wizard guides you through the configuration process.

The Rapid Startup Wizard guides you through configuring the following system settings:

- Date, time, and time zone
- Administrator Identity (user name and password)
- Alert e-mail notification
- Integrated Lights-Out 2 (iLO 2) settings
- Simple Network Management Protocol (SNMP) Settings
- Network Interfaces
- Server Name

For more information about the configuration settings available in the Rapid Startup Wizard, click **Help** to see the corresponding Rapid Startup Wizard online help topic.

Completing system configuration

After the storage server is physically set up and the basic configuration is established, additional setup tasks must be completed. Depending on the deployment scenario of the storage server, these steps can vary. These additional steps can include:

- Running Microsoft Windows Update—HP highly recommends that you run Microsoft Windows updates to identify, review, and install the latest, applicable, critical security updates on the storage server. For recommendations, instructions, and documentation to help manage the software update, hotfix, and security patches process on the storage server, see *Microsoft Software Updates on HP ProLiant Storage Servers* at http://h18006.www1.hp.com/storage/storageservers.html.
- Creating and managing users and groups—User and group information and permissions determine whether a user can access files. If the storage server is deployed into a workgroup environment, this user and group information is stored locally on the device. By contrast, if the storage server is deployed into a domain environment, user and group information is stored on the domain.
- Joining workgroup and domains—These are the two system environments for users and groups. Because users and groups in a domain environment are managed through standard Windows or Active Directory domain administration methods, this document discusses only local users and

groups, which are stored and managed on the storage server. For information on managing users and groups on a domain, refer to the domain documentation available on the Microsoft web site.

- Using Ethernet NIC teaming (optional) — Select models are equipped with an HP or Broadcom NIC Teaming utility. The utility allows administrators to configure and monitor Ethernet network interface controller (NIC) teams in a Windows-based operating system. These teams provide options for increasing fault tolerance and throughput.
- Activating iLO 2 Advanced features using a license key— The Remote Console feature of iLO 2 requires a license key. The key is included with the storage server inside the Country Kit. Refer to the iLO 2 Advanced License Pack for activation instructions.
- Adjust logging for system, application and security events.
- Installing third-party software applications—For example, these might include an antivirus application that you install.

2 Storage management overview

This chapter provides an overview of some of the components that make up the storage structure of the HP ProLiant Storage Server.

Storage management elements

Storage is divided into four major divisions:

- Physical storage elements
- Logical storage elements
- File system elements
- File sharing elements

Each of these elements is composed of the previous level's elements.

Storage management example

Figure 4 depicts many of the storage elements that one would find on a storage device. The following sections provide an overview of the storage elements.

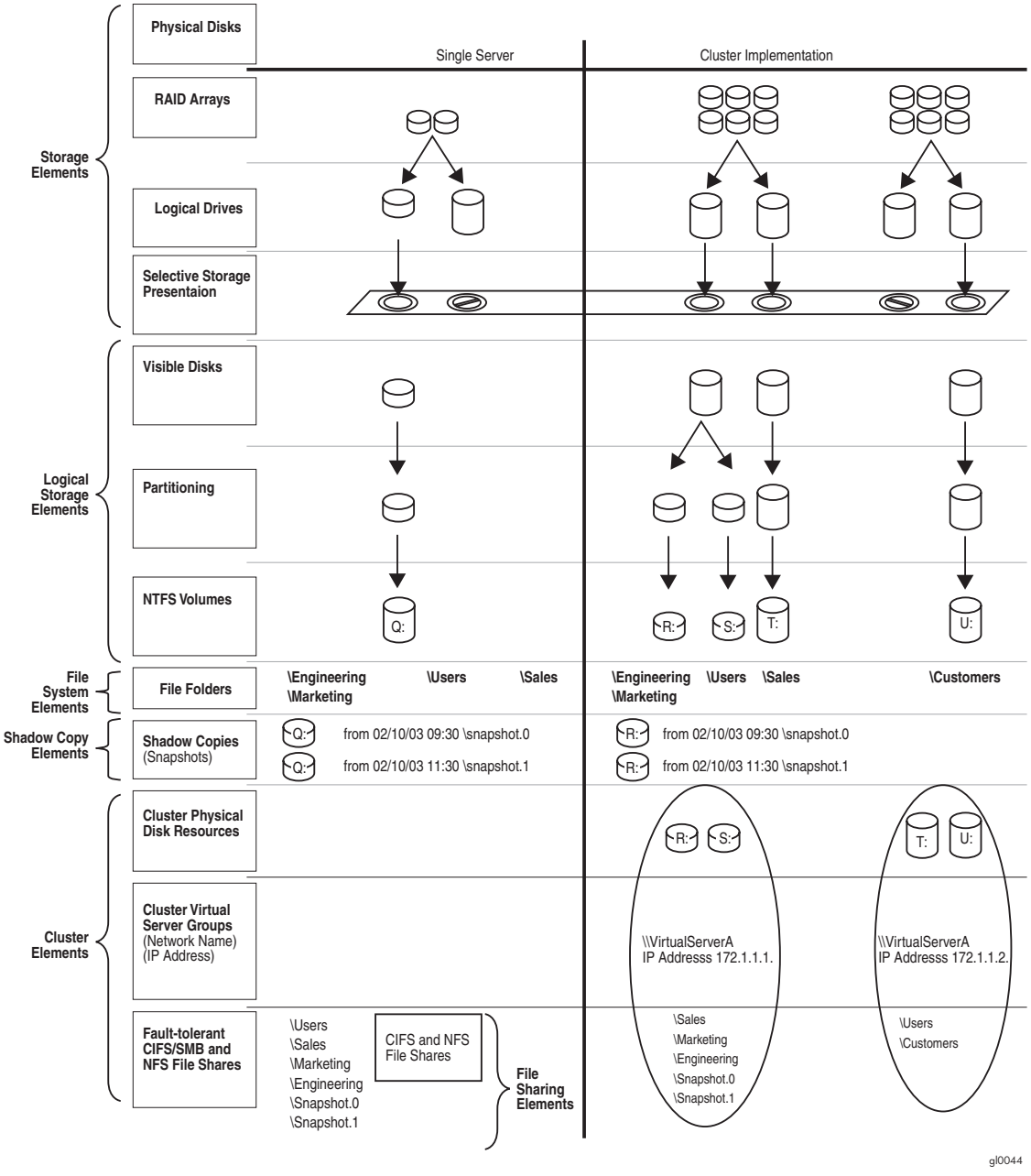


Figure 4 Storage management process example

Physical storage elements

The lowest level of storage management occurs at the physical drive level. Minimally, choosing the best disk carving strategy includes the following policies:

- Analyze current corporate and departmental structure.
- Analyze the current file server structure and environment.
- Plan properly to ensure the best configuration and use of storage.
  - Determine the desired priority of fault tolerance, performance, and storage capacity.
  - Use the determined priority of system characteristics to determine the optimal striping policy and RAID level.
- Include the appropriate number of physical drives in the arrays to create logical storage elements of desired sizes.

Arrays

See Figure 5. With an array controller installed in the system, the capacity of several physical drives (P1–P3) can be logically combined into one or more logical units (L1) called arrays. When this is done, the read/write heads of all the constituent physical drives are active simultaneously, dramatically reducing the overall time required for data transfer.

NOTE:

Depending on the storage server model, array configuration may not be possible or necessary.

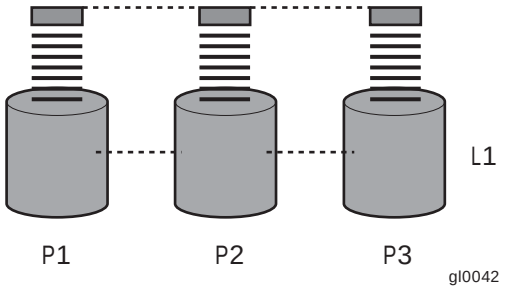


Figure 5 Configuring arrays from physical drives

Because the read/write heads are simultaneously active, the same amount of data is written to each drive during any given time interval. Each unit of data is termed a block. The blocks form a set of data stripes over all the hard drives in an array, as shown in Figure 6.

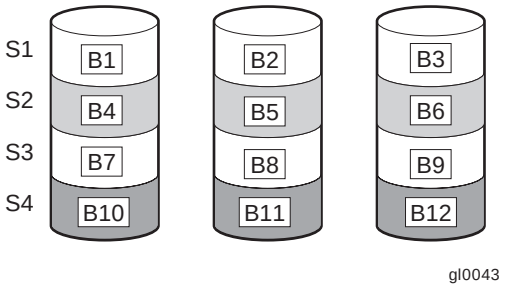


Figure 6 RAID 0 (data striping) (S1-S4) of data blocks (B1-B12)

For data in the array to be readable, the data block sequence within each stripe must be the same. This sequencing process is performed by the array controller, which sends the data blocks to the drive write heads in the correct order.

A natural consequence of the striping process is that each hard drive in a given array contains the same number of data blocks.

NOTE:

If one hard drive has a larger capacity than other hard drives in the same array, the extra capacity is wasted because it cannot be used by the array.

Fault tolerance

Drive failure, although rare, is potentially catastrophic. For example, using simple striping as shown in Figure 6, failure of any hard drive leads to failure of all logical drives in the same array, and hence to data loss.

To protect against data loss from hard drive failure, storage servers should be configured with fault tolerance. HP recommends adhering to RAID 5 configurations.

The table below summarizes the important features of the different kinds of RAID supported by the Smart Array controllers. The decision chart in the following table can help determine which option is best for different situations.

Table 5 Summary of RAID methods

	RAID 0 Striping (no fault tolerance)	RAID 1+0 Mirroring	RAID 5 Distributed Data Guarding	RAID ADG
Maximum number of hard drives	N/A	N/A	14	Storage system dependent
Tolerant of single hard drive failure?	No	Yes	Yes	Yes
Tolerant of multiple simultaneous hard drive failures?	No	If the failed drives are not mirrored to each other	No	Yes (two drives can fail)

Online Spares

Further protection against data loss can be achieved by assigning an online spare (or hot spare) to any configuration except RAID 0. This hard drive contains no data and is contained within the same storage subsystem as the other drives in the array. When a hard drive in the array fails, the controller can then automatically rebuild information that was originally on the failed drive onto the online spare. This quickly restores the system to full RAID level fault tolerance protection. However, unless RAID Advanced Data Guarding (ADG) is being used, which can support two drive failures in an array, in the unlikely event that a third drive in the array should fail while data is being rewritten to the spare, the logical drive still fails.

Logical storage elements

Logical storage elements consist of those components that translate the physical storage elements to file system elements. The storage server uses the Window Disk Management utility to manage the various types of disks presented to the file system. There are two types of LUN presentation: basic disk and dynamic disk. Each of these types of disk has special features that enable different types of management.

Logical drives (LUNs)

While an array is a physical grouping of hard drives, a logical drive consists of components that translate physical storage elements into file system elements.

It is important to note that a LUN may extend over (span) all physical drives within a storage controller subsystem, but cannot span multiple storage controller subsystems.

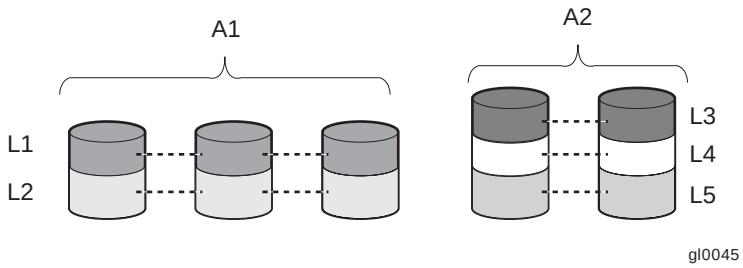


Figure 7 Two arrays (A1, A2) and five logical drives (L1 through L5) spread over five physical drives

NOTE:

This type of configuration may not apply to all storage servers and serves only as an example.

Through the use of basic disks, primary partitions or extended partitions can be created. Partitions can only encompass one LUN. Through the use of dynamic disks, volumes can be created that span multiple LUNs. The Windows Disk Management utility can be used to convert disks to dynamic and back to basic, and manage the volumes residing on dynamic disks. Other options include the ability to delete, extend, mirror, and repair these elements.

Partitions

Partitions exist as either primary partitions or extended partitions and can be composed of only one basic disk no larger than 2 TB. Basic disks can also only contain up to four primary partitions, or three primary partitions and one extended partition. In addition, the partitions on them cannot be extended beyond the limits of a single LUN. Extended partitions allow the user to create multiple logical drives. These partitions or logical disks can be assigned drive letters or be used as mount points on existing disks. If mount points are used, it should be noted that Services for UNIX (SFU) does not support mount points at this time. The use of mount points in conjunction with NFS shares is not supported.

Volumes

When planning dynamic disks and volumes, there is a limit to the amount of growth a single volume can undergo. Volumes are limited in size and can have no more than 32 separate LUNs, with each LUN not exceeding 2 terabytes (TB), and volumes totaling no more than 64 TB of disk space.

The RAID level of the LUNs included in a volume must be considered. All of the units that make up a volume should have the same high-availability characteristics. In other words, the units should all be of the same RAID level. For example, it would not be a good practice to include both a RAID 1+0 and a RAID 5 array in the same volume set. By keeping all the units the same, the entire volume retains the same performance and high-availability characteristics, making managing and maintaining the volume much easier. If a dynamic disk goes offline, the entire volume dependent on the one or more dynamic disks is unavailable. There could be a potential for data loss depending on the nature of the failed LUN.

Volumes are created out of the dynamic disks, and can be expanded on the fly to extend over multiple dynamic disks if they are spanned volumes. However, after a type of volume is selected, it cannot be altered. For example, a spanning volume cannot be altered to a mirrored volume without deleting and recreating the volume, unless it is a simple volume. Simple volumes can be mirrored or converted to spanned volumes. Fault-tolerant disks cannot be extended either. Therefore, selection of the volume type is important. The same performance characteristics on numbers of reads and writes apply when using fault-tolerant configurations, as is the case with controller-based RAID. These volumes can also be assigned drive letters or be mounted as mount points off existing drive letters.

The administrator should carefully consider how the volumes will be carved up and what groups or applications will be using them. For example, putting several storage-intensive applications or groups into the same dynamic disk set would not be efficient. These applications or groups would be better served by being divided up into separate dynamic disks, which could then grow as their space requirements increased, within the allowable growth limits.

NOTE:

Dynamic disks cannot be used for clustering configurations because Microsoft Cluster only supports basic disks.

File system elements

File system elements are composed of the folders and subfolders that are created under each logical storage element (partitions, logical disks, and volumes). Folders are used to further subdivide the available file system, providing another level of granularity for management of the information space. Each of these folders can contain separate permissions and share names that can be used for network access. Folders can be created for individual users, groups, projects, and so on.

File sharing elements

The storage server supports several file sharing protocols, including Distributed File System (DFS), Network File System (NFS), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Microsoft Server Message Block (SMB). On each folder or logical storage element, different file sharing protocols can be enabled using specific network names for access across a network to a variety of clients. Permissions can then be granted to those shares based on users or groups of users in each of the file sharing protocols.

Volume Shadow Copy Service overview

The Volume Shadow Copy Service (VSS) provides an infrastructure for creating point-in-time snapshots (shadow copies) of volumes. VSS supports 64 shadow copies per volume.

Shadow Copies of Shared Folders resides within this infrastructure, and helps alleviate data loss by creating shadow copies of files or folders that are stored on network file shares at pre-determined time intervals. In essence, a shadow copy is a previous version of the file or folder at a specific point in time.

By using shadow copies, a storage server can maintain a set of previous versions of all files on the selected volumes. End users access the file or folder by using a separate client add-on program, which enables them to view the file in Windows Explorer.

Shadow copies should not replace the current backup, archive, or business recovery system, but they can help to simplify restore procedures. For example, shadow copies cannot protect against data loss due to media failures; however, recovering data from shadow copies can reduce the number of times needed to restore data from tape.

Using storage elements

The last step in creating the element is determining its drive letter or mount point and formatting the element. Each element created can exist as a drive letter, assuming one is available and/or as mount points off of an existing folder or drive letter. Either method is supported. However, mount points can not be used for shares that will be shared using Microsoft Services for Unix. They can be set up with both but the use of the mount point in conjunction with NFS shares causes instability with the NFS shares.

Formats consist of NTFS, FAT32, and FAT. All three types can be used on the storage server. However, VSS can only use volumes that are NTFS formatted. Also, quota management is possible only on NTFS.

Clustered server elements

Select storage servers support clustering. The HP ProLiant storage server supports several file sharing protocols, including DFS, NFS, FTP, HTTP, and Microsoft SMB. Only NFS, FTP, and Microsoft SMB are cluster-aware protocols. HTTP can be installed on each node but the protocols cannot be set up through cluster administrator, and they will not fail over during a node failure.

△ CAUTION:

AppleTalk shares should not be created on clustered resources as this is not supported by Microsoft Clustering, and data loss may occur.

Network names and IP address resources for the clustered file share resource can also be established for access across a network to a variety of clients. Permissions can then be granted to those shares based on users or groups of users in each of the file sharing protocols.

Network adapter teaming

Network adapter teaming is software-based technology used to increase a server's network availability and performance. Teaming enables the logical grouping of physical adapters in the same server (regardless of whether they are embedded devices or Peripheral Component Interconnect (PCI) adapters) into a virtual adapter. This virtual adapter is seen by the network and server-resident network-aware applications as a single network connection.

3 File server management

This chapter begins by identifying new or improved file services in Windows Storage Server 2003 R2. The remainder of the chapter describes the many tasks and utilities that play a role in file server management.

New or improved file services features in Windows Storage Server 2003 R2

Storage Manager for SANs

The Storage Manager for SANs (also called Simple SAN) snap-in enables you to create and manage the LUNs that are used to allocate space on storage arrays. Storage Manager for SANs can be used on SANs that support Virtual Disk Server (VDS). It can be used in both Fibre Channel and iSCSI environments.

For more information on Storage Manager for SANs, refer to the online help. A Microsoft document titled *Storage Management in Windows Storage Server 2003 R2: File Server Resource Manager and Storage Manager for Storage Area Networks* is available at http://download.microsoft.com/download/7/4/7/7472bf9b-3023-48b7-87be-d2cedc38f15a/WS03R2_Storage_Management.doc.

NOTE:

Storage Manager for SANs is only available on Standard and Enterprise editions of Windows Storage Server 2003 R2.

Single Instance Storage

Single Instance Storage (SIS) provides a copy-on-write link between multiple files. Disk space is recovered by reducing the amount of redundant data stored on a server. If a user has two files sharing disk storage by using SIS, and someone modifies one of the files, users of the other files do not see the changes. The underlying shared disk storage that backs SIS links is maintained by the system and is only deleted if all the SIS links pointing to it are deleted. SIS automatically determines that two or more files have the same content and links them together.

NOTE:

Single Instance Storage is only available on Standard and Enterprise editions of Windows Storage Server 2003 R2.

Search enhancements

The Indexing service is tuned for additional indexing and query performance. Prior to the R2 release, if the Indexing service on a Windows Storage Server was not entirely up-to-date, the client-side search engine needed to "walk through" all the files within the scope of the search on the server. With the performance tuning in R2, the Indexing service no longer needs to be entirely up-to-date.

File Server Resource Manager

File Server Resource Manager is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. By using Storage Resource

Manager, administrators can place quotas on volumes, actively screen files and folders, and generate comprehensive storage reports.

By using Storage Resource Manager, you can perform the following tasks:

- Create quotas to limit the space allowed for a volume or folder and to generate notifications when the quota limits are approached and exceeded.
- Create file screens to screen the files that users can save on volumes and in folders and to send notifications when users attempt to save blocked files.
- Schedule periodic storage reports that allow users to identify trends in disk usage and to monitor attempts to save unauthorized files, or generate the reports on demand.

Windows SharePoint Services

Windows SharePoint Services is an integrated set of collaboration and communication services designed to connect people, information, processes, and systems, both within and beyond the organization firewall.

NOTE:

Windows SharePoint Services is only available on Standard and Enterprise editions of Windows Storage Server 2003 R2.

HP Storage Server Management Console

The HP Storage Server Management Console (Figure 3) is a new user interface in Windows Storage Server 2003 R2 that provides one place to manage files or print serving components. The console is accessible using Remote Desktop or a web browser.

The Storage Management page provides a portal to:

- File Server Resource Manager
- DFS Management
- Disk and Volume Management
- Indexing Service
- MSNFS (under Share folder)
- Cluster Management (under "Utilities")

The Share Folder Management page provides a portal to Shared Folders, consisting of:

- Shares
- Sessions
- Open Files

File services management

Information about the storage server in a SAN environment is provided in the *HP ProLiant Storage Server SAN Connection and Management* document located on the storage server documentation CD, or the latest update is available from the HP web site at http://www.hp.com/support/manuals. Under the storage section, click **NAS** and then select your product.

Configurable and pre-configured storage

Certain storage servers ship with storage configured only for the operating system. The administrator must configure data storage for the storage server. Other storage servers ship with pre-configured storage for data. Depending on the type of storage server purchased, additional storage configuration is required.

Configuring additional storage involves creating arrays, logical disks, and volumes. Table 6 shows the general task areas to be performed as well as the utilities needed to configure storage for an HP Smart Array-based storage server.

Table 6 Tasks and utilities needed for storage server configuration

Task	Storage management utility
Create disk arrays	HP Array Configuration Utility or Storage Manager
Create logical disks from the array space	HP Array Configuration Utility or Storage Manager
Verify newly created logical disks	Windows Disk Management
Create a volume on the new logical disk	Windows Disk Management

NOTE:

The type of configuration may not apply to all supported storage components and serves only as an example providing basic guidance.

- Create disk arrays—On storage servers with configurable storage, physical disks can be arranged as RAID arrays for fault tolerance and enhanced performance, and then segmented into logical disks of appropriate sizes for particular storage needs. These logical disks then become the volumes that appear as drives on the storage server.

CAUTION:

The first two logical drives are configured for the storage server operating system and should not be altered in any manner.

The fault tolerance level depends on the amount of disks selected when the array was created. A minimum of two disks is required for RAID 0+1 configuration, three disks for a RAID 5 configuration, and four disks for a RAID 6 (ADG) configuration.

- Create logical disks from the array space—Select the desired fault tolerance, stripe size, and size of the logical disk.
- Verify newly created logical disks—Verify that disks matching the newly created sizes are displayed.
- Create a volume on the new logical disk—Select a drive letter and enter a volume label, volume size, allocation unit size, and mount point (if desired).

NOTE:

Do not tamper with the "DON'T ERASE" or local C: volume. These are reserved volumes and must be maintained as they exist.

Storage management utilities

The storage management utilities pre-installed on the storage server include the HP Array Configuration Utility (ACU).

Array management utilities

Storage devices for RAID arrays and LUNs are created and managed using the array management utilities mentioned previously. For HP Smart Arrays use the ACU.

NOTE:

The ACU is used to configure and manage array-based storage. Software RAID-based storage servers use Microsoft Disk Manager to manage storage. You need administrator or root privileges to run the ACU.

Array Configuration Utility

The HP ACU supports the Smart Array controllers and SCSI hard drives installed on the storage server.

To open the ACU from the storage server desktop:

NOTE:

If this is the first time that the ACU is being run, you will be prompted to select the Execution Mode for ACU. Selecting Local Application Mode allows you to run the ACU from a Remote Desktop, Remote Console, or storage server web access modes. Remote Service Mode allows you to access the ACU from a remote browser.

1. Select **Start > Programs > HP Management Tools > Array Configuration Utility**.
2. If the Execution Mode for ACU is set to Remote Mode, log in to the HP System Management Homepage. The default user name is **administrator** and the default password is **hpinvent**.

To open the ACU in browser mode:

NOTE:

Confirm that the ACU Extension Mode is set to remote service.

1. Open a browser and enter the server name or IP address of the destination server. For example, http://servername:2301 or http://192.0.0.1:2301.
2. Log in to the HP System Management Homepage. The default user name is **administrator** and the default password is **hpinvent**.
3. Click **Array Configuration Utility** on the left side of the window. The ACU opens and identifies the controllers that are connected to the system.

Some ACU guidelines to consider:

- Do not modify the first two logical drives of the storage server; they are configured for the storage server operating system.
- Spanning more than 14 disks with a RAID 5 volume is not recommended.
- Designate spares for RAID sets to provide greater protection against failures.
- RAID sets cannot span controllers.
- A single array can contain multiple logical drives of varying RAID settings.
- Extending and expanding arrays and logical drives is supported.

The *HP Array Configuration Utility User Guide* is available for download at http://www.hp.com/support/manuals.

Disk Management utility

The Disk Management tool is a system utility for managing hard disks and the volumes, or partitions, that they contain. Disk Management is used to initialize disks, create volumes, format volumes with the FAT, FAT32, or NTFS file systems, and create fault-tolerant disk systems. Most disk-related tasks can be performed in Disk Management without restarting the system or interrupting users. Most configuration

changes take effect immediately. A complete online help facility is provided with the Disk Management utility for assistance in using the product.

NOTE:

- When the Disk Management utility is accessed through a Remote Desktop connection this connection can only be used to manage disks and volumes on the server. Using the Remote Desktop connection for other operations during an open session closes the session.
- When closing Disk Management through a Remote Desktop connection, it may take a few moments for the remote session to log off.

Guidelines for managing disks and volumes

When managing disks and volumes:

- Do not alter the operating system disk labeled Local Disk C: or Primary OS C:.
- Do not alter the disk labeled "DON'T ERASE."
- HP does not recommend spanning array controllers with dynamic volumes. The use of software RAID-based dynamic volumes is not recommended. Use the array controller instead; it is more efficient.
- Use meaningful volume labels with the intended drive letter embedded in the volume label, if possible. (For example, volume e: might be named "Disk E:.") Volume labels often serve as the only means of identification.
- Record all volume labels and drive letters in case the system needs to be restored.
- When managing basic disks, only the last partition on the disk can be extended unless the disk is changed to dynamic.
- Basic disks can be converted to dynamic, but cannot be converted back to basic without deleting all data on the disk.
- Basic disks can contain up to four primary partitions (or three primary partitions and one extended partition).
- Format drives with a 16 K allocation size for best support of shadow copies, performance, and defragmentation.
- NTFS formatted drives are recommended, because they provide the greatest level of support for shadow copies, encryption, and compression.
- Only basic disks can be formatted as FAT or FAT32.
- Read the online Disk Management help found in the utility.

Scheduling defragmentation

Defragmentation is the process of analyzing local volumes and consolidating fragmented files and folders so that each occupies a single, contiguous space on the volume. This improves file system performance. Because defragmentation consolidates files and folders, it also consolidates the free space on a volume. This reduces the likelihood that new files will be fragmented.

Defragmentation for a volume can be scheduled to occur automatically at convenient times. Defragmentation can also be done once, or on a recurring basis.

NOTE:

Scheduling defragmentation to run no later than a specific time prevents the defragmentation process from running later than that time. If the defragmentation process is running when the time is reached, the process is stopped. This setting is useful to ensure that the defragmentation process ends before the demand for server access is likely to increase.

If defragmenting volumes on which shadow copies are enabled, use a cluster (or allocation unit) size of 16 KB or larger during the format. Otherwise defragmentation registers as a change by the Shadow Copy process. This increase in the number of changes forces Shadow Copy to delete snapshots as the limit for the cache file is reached.

CAUTION:

Allocation unit size cannot be altered without reformatting the drive. Data on a reformatted drive cannot be recovered.

For more information about disk defragmentation, read the online help.

Disk quotas

Disk quotas track and control disk space use in volumes.

NOTE:

To limit the size of a folder or share, see "Directory quotas" on page 65 .

Configure the volumes on the server to perform the following tasks:

- Prevent further disk space use and log an event when a user exceeds a specified disk space limit.
- Log an event when a user exceeds a specified disk space warning level.

When enabling disk quotas, it is possible to set both the disk quota limit and the disk quota warning level. The disk quota limit specifies the amount of disk space a user is allowed to use. The warning level specifies the point at which a user is nearing his or her quota limit. For example, a user's disk quota limit can be set to 50 megabytes (MB), and the disk quota warning level to 45 MB. In this case, the user can store no more than 50 MB on the volume. If the user stores more than 45 MB on the volume, the disk quota system logs a system event.

In addition, it is possible to specify that users can exceed their quota limit. Enabling quotas and not limiting disk space use is useful to still allow users access to a volume, but track disk space use on a per-user basis. It is also possible to specify whether or not to log an event when users exceed either their quota warning level or their quota limit.

When enabling disk quotas for a volume, volume usage is automatically tracked from that point forward, but existing volume users have no disk quotas applied to them. Apply disk quotas to existing volume users by adding new quota entries on the Quota Entries page.

NOTE:

When enabling disk quotas on a volume, any users with write access to the volume who have not exceeded their quota limit can store data on the volume. The first time a user writes data to a quota-enabled volume, default values for disk space limit and warning level are automatically assigned by the quota system.

For more information about disk quotas, read the online help.

Adding storage

Expansion is the process of adding physical disks to an array that has already been configured. Extension is the process of adding new storage space to an existing logical drive on the same array, usually after the array has been expanded.

Storage growth may occur in three forms:

- Extend unallocated space from the original logical disks or LUNs.
- Alter LUNs to contain additional storage.

- Add new LUNs to the system.

The additional space is then extended through a variety of means, depending on which type of disk structure is in use.

NOTE:

This section addresses only single storage server node configurations. If your server has Windows Storage Server 2003 R2 Enterprise Edition, see the Cluster Administration chapter for expanding and extending storage in a cluster environment.

Expanding storage

Expansion is the process of adding physical disks to an array that has already been configured. The logical drives (or volumes) that exist in the array before the expansion takes place are unchanged, because only the amount of free space in the array changes. The expansion process is entirely independent of the operating system.

NOTE:

See your storage array hardware user documentation for further details about expanding storage on the array.

Extending storage using Windows Storage Utilities

Volume extension grows the storage space of a logical drive. During this process, the administrator adds new storage space to an existing logical drive on the same array, usually after the array has been expanded. An administrator may have gained this new storage space by either expansion or by deleting another logical drive on the same array. Unlike drive expansion, the operating system must be aware of changes to the logical drive size.

You extend a volume to:

- Increase raw data storage
- Improve performance by increasing the number of spindles in a logical drive volume
- Change fault-tolerance (RAID) configurations

For more information about RAID levels, refer to the *Smart Array Controller User Guide*, or the document titled *Assessing RAID ADG vs. RAID 5 vs. RAID 1+0*. Both are available at the Smart Array controller web page or at http://h18000.www1.hp.com/products/servers/proliantstorage/arraycontrollers/documentation.html.

Extend volumes using Disk Management

The Disk Management snap-in provides management of hard disks, volumes or partitions. It can be used to extend a dynamic volume only.

NOTE:

Disk Management cannot be used to extend basic disk partitions.

Guidelines for extending a dynamic volume:

- Use the Disk Management utility.
- You can extend a volume only if it does not have a file system or if it is formatted NTFS.
- You cannot extend volumes formatted using FAT or FAT32.
- You cannot extend striped volumes, mirrored volumes, or RAID 5 volumes.

For more information, see the Disk Management online help.

Expanding storage for EVA arrays using Command View EVA

Presenting a virtual disk offers its storage to a host. To make a virtual disk available to a host, you must present it. You can present a virtual disk to a host during or after virtual disk creation. The virtual disk must be completely created before the host presentation can occur. If you choose host presentation during virtual disk creation, the management agent cannot complete any other task until that virtual disk is created and presented. Therefore, HP recommends that you wait until a virtual disk is created before presenting it to a host.

For more information, see the *HP StorageWorks Command View EVA User Guide*.

Expanding storage using the Array Configuration Utility

The Array Configuration Utility enables online capacity expansion of the array and logical drive for specific MSA storage arrays, such as the MSA1000 and MSA1500. For more information, use the ACU online help, or the procedures to "Expand Array" in the *Array Configuration Utility User Guide*

Expand logical drive

This option in the ACU increases the storage capacity of a logical drive by adding unused space on an array to the logical drive on the same array. The unused space is obtained either by expanding an array or by deleting another logical drive on the same array. For more information, use the ACU online help, or the "Extend logical drive" procedure in the *Array Configuration Utility User Guide*

Volume shadow copies

NOTE:

Select storage servers can be deployed in a clustered as well as a non-clustered configuration. This chapter discusses using shadow copies in a non-clustered environment.

The Volume Shadow Copy Service provides an infrastructure for creating point-in-time snapshots (shadow copies) of volumes. Shadow Copy supports 64 shadow copies per volume.

A shadow copy contains previous versions of the files or folders contained on a volume at a specific point in time. While the shadow copy mechanism is managed at the server, previous versions of files and folders are only available over the network from clients, and are seen on a per folder or file level, and not as an entire volume.

The shadow copy feature uses data blocks. As changes are made to the file system, the Shadow Copy Service copies the original blocks to a special cache file, to maintain a consistent view of the file at a particular point in time. Because the snapshot only contains a subset of the original blocks, the cache file is typically smaller than the original volume. In the snapshot's original form, it takes up no space because blocks are not moved until an update to the disk occurs.

By using shadow copies, a storage server can maintain a set of previous versions of all files on the selected volumes. End users access the file or folder by using a separate client add-on program, which enables them to view the file in Windows Explorer. Accessing previous versions of files, or shadow copies, enables users to:

- Recover files that were accidentally deleted. Previous versions can be opened and copied to a safe location.
- Recover from accidentally overwriting a file. A previous version of that file can be accessed.
- Compare several versions of a file while working. Use previous versions to compare changes between two versions of a file.

Shadow copies cannot replace the current backup, archive, or business recovery system, but they can help to simplify restore procedures. Because a snapshot only contains a portion of the original data blocks, shadow copies can not protect against data loss due to media failures. However, the strength

of snapshots is the ability to instantly recover data from shadow copies, reducing the number of times needed to restore data from tape.

Shadow copy planning

Before setup is initiated on the server and the client interface is made available to end users, consider the following:

- From what volume will shadow copies be taken?
- How much disk space should be allocated for shadow copies?
- Will separate disks be used to store shadow copies?
- How frequently will shadow copies be made?

Identifying the volume

Shadow copies are taken for a complete volume, but not for a specific directory. Shadow copies work best when the server stores user files, such as documents, spreadsheets, presentations, graphics, or database files.

NOTE:

Shadow copies should not be used to provide access to previous versions of application or e-mail databases.

Shadow copies are designed for volumes that store user data such as home directories and My Documents folders that are redirected by using Group Policy or other shared folders in which users store data.

Shadow copies work with compressed or encrypted files and retain whatever permissions were set on the files when the shadow copies were taken. For example, if a user is denied permission to read a file, that user would not be able to restore a previous version of the file, or be able to read the file after it has been restored.

Although shadow copies are taken for an entire volume, users must use shared folders to access shadow copies. Administrators on the local server must also specify the `\\servername\sharename` path to access shadow copies. If administrators or end users want to access a previous version of a file that does not reside in a shared folder, the administrator must first share the folder.

NOTE:

Shadow copies are available only on NTFS, not FAT or FAT32 volumes.

Files or folders that are recorded by using Shadow Copy appear static, even though the original data is changing.

Allocating disk space

When determining the amount of space to allocate for storing shadow copies, consider both the number and size of files that are being copied, as well as the frequency of changes between copies. For example, 100 files that only change monthly require less storage space than 10 files that change daily. If the frequency of changes to each file is greater than the amount of space allocated to storing shadow copies, no shadow copy is created.

Administrators should also consider user expectations of how many versions they will want to have available. End users might expect only a single shadow copy to be available, or they might expect three days or three weeks worth of shadow copies. The more shadow copies users expect, the more storage space administrators must allocate for storing them.

Setting the limit too low also affects backup programs that use shadow copy technology because these programs are also limited to using the amount of disk space specified by administrators.

NOTE:

Regardless of the volume space that is allocated for shadow copies, there is a maximum of 64 shadow copies for any volume. When the 65th shadow copy is taken, the oldest shadow copy is purged.

The minimum amount of storage space that can be specified is 350 megabytes (MB). The default storage size is 10 percent of the source volume (the volume being copied). If the shadow copies are stored on a separate volume, change the default to reflect the space available on the *storage* volume instead of the *source* volume. Remember that when the storage limit is reached, older versions of the shadow copies are deleted and cannot be restored.

△ **CAUTION:**

To change the storage volume, shadow copies must be deleted. The existing file change history that is kept on the original storage volume is lost. To avoid this problem, verify that the storage volume that is initially selected is large enough.

Identifying the storage area

To store the shadow copies of another volume on the same file server, a volume can be dedicated on separate disks. For example, if user files are stored on *H:*, another volume such as *S:* can be used to store the shadow copies. Using a separate volume on separate disks provides better performance and is recommended for heavily used storage servers.

If a separate volume will be used for the storage area (where shadow copies are stored), the maximum size should be changed to **No Limit** to reflect the space available on the storage area volume instead of the source volume (where the user files are stored).

Disk space for shadow copies can be allocated on either the same volume as the source files or a different volume. There is a trade-off between ease of use and maintenance versus performance and reliability that the system administrator must consider.

By keeping the shadow copy on the same volume, there is a potential gain in ease of setup and maintenance; however, there may be a reduction in performance and reliability.

△ **CAUTION:**

If shadow copies are stored on the same volume as the user files, note that a burst of disk input/output (I/O) can cause all shadow copies to be deleted. If the sudden deletion of shadow copies is unacceptable to administrators or end users, it is best to use a separate volume on separate disks to store shadow copies.

Determining creation frequency

The more frequently shadow copies are created, the more likely that end users will get the version that they want. However, with a maximum of 64 shadow copies per volume, there is a trade-off between the frequency of making shadow copies and the amount of time that the earlier files will be available.

By default, the storage server creates shadow copies at 0700 and 1200, Monday through Friday. However, these settings are easily modified by the administrator so that the shadow copy schedule can better accommodate end user needs.

Shadow copies and drive defragmentation

When running Disk Defragmenter on a volume with shadow copies activated, all or some of the shadow copies may be lost, starting with the oldest shadow copies.

If defragmenting volumes on which shadow copies are enabled, use a cluster (or allocation unit) size of 16 KB or larger. Using this allocation unit size reduces the number of copy outs occurring on the

snapshot. Otherwise, the number of changes caused by the defragmentation process can cause shadow copies to be deleted faster than expected. Note, however, that NTFS compression is supported only if the cluster size is 4 KB or smaller.

NOTE:

To check the cluster size of a volume, use the `fsutil fsinfo ntfsinfo` command. To change the cluster size on a volume that contains data, back up the data on the volume, reformat it using the new cluster size, and then restore the data.

Mounted drives

A mounted drive is a local volume attached to an empty folder (called a mount point) on an NTFS volume. When enabling shadow copies on a volume that contains mounted drives, the mounted drives are not included when shadow copies are taken. In addition, if a mounted drive is shared and shadow copies are enabled on it, users cannot access the shadow copies if they traverse from the host volume (where the mount point is stored) to the mounted drive.

For example, assume there is a folder *F:\data\users*, and the *Users* folder is a mount point for *G:*. If shadow copies are enabled on both *F:* and *G:*, *F:\data* is shared as *\\server1\data*, and *G:\data\users* is shared as *\\server1\users*. In this example, users can access previous versions of *\\server1\data* and *\\server1\users* but not *\\server1\data\users*.

Managing shadow copies

The vssadmin tool provides a command line capability to create, list, resize, and delete volume shadow copies.

The system administrator can make shadow copies available to end users through a feature called "Shadow Copies for Shared Folders." The administrator uses the Properties menu (see Figure 8) to turn on the Shadow Copies feature, select the volumes to be copied, and determine the frequency with which shadow copies are made.

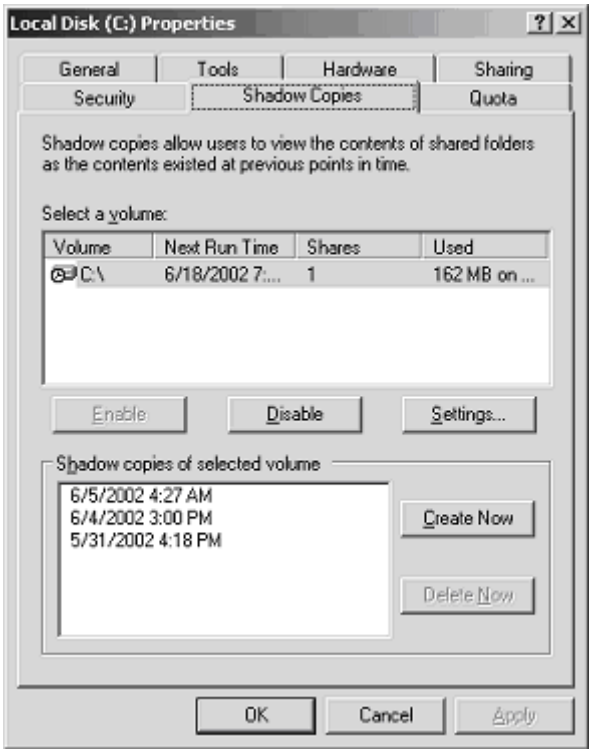


Figure 8 System administrator view of Shadow Copies for Shared Folders

The shadow copy cache file

The default shadow copy settings allocate 10 percent of the source volume being copied (with a minimum of 350 MB), and store the shadow copies on the same volume as the original volume. (See Figure 9). The cache file is located in a hidden protected directory titled "System Volume Information" off of the root of each volume for which shadow copy is enabled.

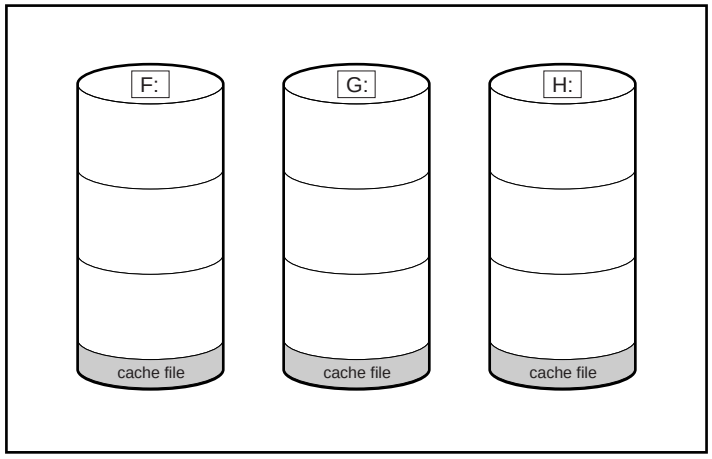


Figure 9 Shadow copies stored on a source volume

The cache file location can be altered to reside on a dedicated volume separate from the volumes containing files shares. (See Figure 10).

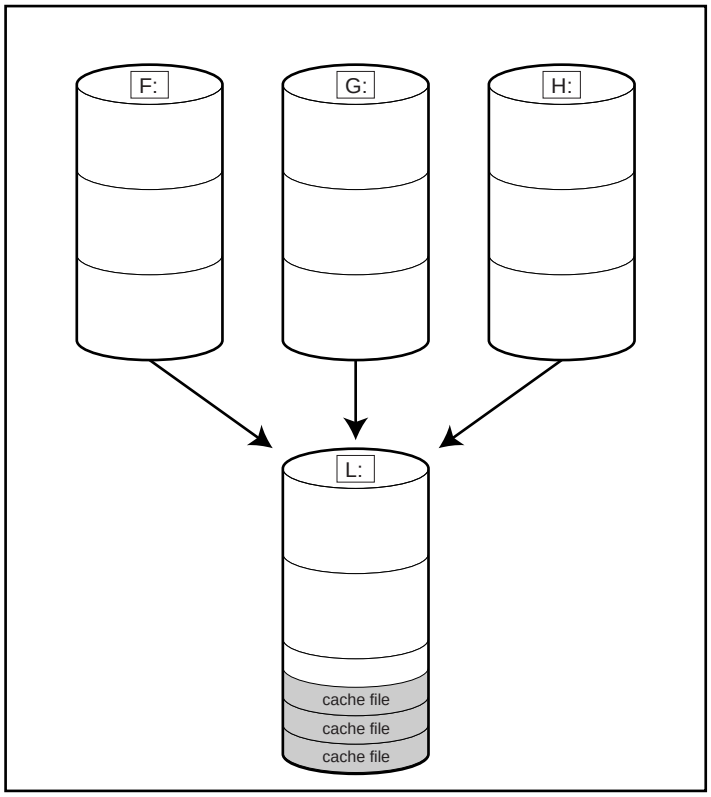


Figure 10 Shadow copies stored on a separate volume

The main advantage to storing shadow copies on a separate volume is ease of management and performance. Shadow copies on a source volume must be continually monitored and can consume space designated for file sharing. Setting the limit too high takes up valuable storage space. Setting the limit too low can cause shadow copies to be purged too soon, or not created at all. By storing shadow copies on a separate volume space, limits can generally be set higher, or set to No Limit. See the online help for instructions on altering the cache file location.

△ CAUTION:

If the data on the separate volume L: is lost, the shadow copies cannot be recovered.

Enabling and creating shadow copies

Enabling shadow copies on a volume automatically results in several actions:

- Creates a shadow copy of the selected volume.
- Sets the maximum storage space for the shadow copies.
- Schedules shadow copies to be made at 7 a.m. and 12 noon on weekdays.

NOTE:

Creating a shadow copy only makes one copy of the volume; it does not create a schedule.

NOTE:

After the first shadow copy is created, it cannot be relocated. Relocate the cache file by altering the cache file location under Properties prior to enabling shadow copy. See "Viewing shadow copy properties" on page 50.

Viewing a list of shadow copies

To view a list of shadow copies on a volume:

1. Access Disk Management.
2. Select the volume or logical drive, then right-click on it.
3. Select **Properties**.
4. Select **Shadow Copies** tab.

All shadow copies are listed, sorted by the date and time they were created.

NOTE:

It is also possible to create new shadow copies or delete shadow copies from this page.

Set schedules

Shadow copy schedules control how frequently shadow copies of a volume are made. There are a number of factors that can help determine the most effective shadow copy schedule for an organization. These include the work habits and locations of the users. For example, if users do not all live in the same time zone, or they work on different schedules, it is possible to adjust the daily shadow copy schedule to allow for these differences.

Do not schedule shadow copies more frequently than once per hour.

NOTE:

When deleting a shadow copy schedule, that action has no effect on existing shadow copies.

Viewing shadow copy properties

The Shadow Copy Properties page lists the number of copies, the date and time the most recent shadow copy was made, and the maximum size setting.

NOTE:

For volumes where shadow copies do not exist currently, it is possible to change the location of the cache file. Managing the cache files on a separate disk is recommended.

CAUTION:

Use caution when reducing the size limit for all shadow copies. When the size is set to less than the total size currently used for all shadow copies, enough shadow copies are deleted to reduce the total size to the new limit. A shadow copy cannot be recovered after it has been deleted.

Redirecting shadow copies to an alternate volume

IMPORTANT:

Shadow copies must be initially disabled on the volume before redirecting to an alternate volume. If shadow copies are enabled and you disable them, a message appears informing you that all existing shadow copies on the volume will be permanently deleted.

To redirect shadow copies to an alternate volume:

1. Access Disk Management.
2. Select the volume or logical drive, then right-click on it.
3. Select **Properties**.
4. Select the **Shadow Copies** tab.
5. Select the volume that you want to redirect shadow copies from and ensure that shadow copies are disabled on that volume; if enabled, click **Disable**.
6. Click **Settings**.
7. In the **Located on this volume** field, select an available alternate volume from the list.

NOTE:

To change the default shadow copy schedule settings, click **Schedule**.

8. Click **OK**.
9. On the **Shadow Copies** tab, ensure that the volume is selected, and then click **Enable**.

Shadow copies are now scheduled to be made on the alternate volume.

Disabling shadow copies

When shadow copies are disabled on a volume, all existing shadow copies on the volume are deleted as well as the schedule for making new shadow copies.

CAUTION:

When the Shadow Copies Service is disabled, all shadow copies on the selected volumes are deleted. Once deleted, shadow copies cannot be restored.

Managing shadow copies from the storage server desktop

The storage server desktop can be accessed by using Remote Desktop to manage shadow copies.

To access shadow copies from the storage server desktop:

1. Access the storage server desktop from the primary navigation bar by selecting **Maintenance > Remote Desktop**.
2. Click **My Computer**.
3. Right-click the volume name, and select **Properties**.
4. Click the **Shadow Copies** tab. See Figure 11.

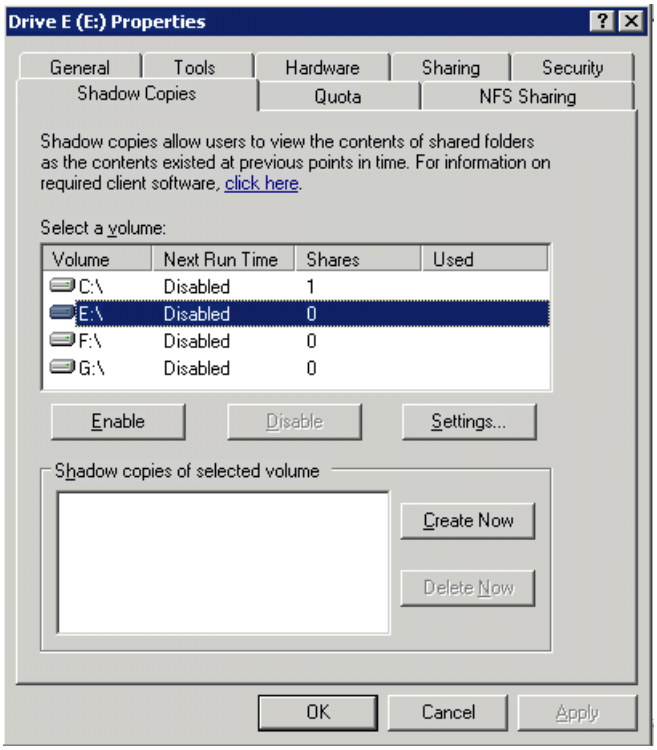


Figure 11 Accessing shadow copies from My Computer

Shadow Copies for Shared Folders

Shadow copies are accessed over the network by supported clients and protocols. There are two sets of supported protocols, SMB and NFS. All other protocols are not supported; this would include HTTP, FTP, AppleTalk, and NetWare Shares. For SMB support, a client-side application denoted as Shadow Copies for Shared Folders is required. The client-side application is currently only available for Windows XP and Windows 2000 SP3+.

No additional software is required to enable UNIX users to independently retrieve previous versions of files stored on NFS shares.

NOTE:

Shadow Copies for Shared Folders supports retrieval only of shadow copies of network shares. It does not support retrieval of shadow copies of local folders.

NOTE:

Shadow Copies for Shared Folders clients are not available for HTTP, FTP, AppleTalk, or NetWare shares. Consequently, users of these protocols cannot use Shadow Copies for Shared Folders to independently retrieve previous versions of their files. However, administrators can take advantage of Shadow Copies for Shared Folders to restore files for these users.

SMB shadow copies

Windows users can independently access previous versions of files stored on SMB shares by using the Shadow Copies for Shared Folders client. After the Shadow Copies for Shared Folders client is installed on the user's computer, the user can access shadow copies for a share by right-clicking on the share to open its Properties window, clicking the **Previous Versions** tab, and then selecting the desired shadow copy. Users can view, copy, and restore all available shadow copies.

Shadow Copies for Shared Folders preserves the permissions set in the access control list (ACL) of the original folders and files. Consequently, users can only access shadow copies for shares to which they have access. In other words, if a user does not have access to a share, he also does not have access to the share's shadow copies.

The Shadow Copies for Shared Folders client pack installs a **Previous Versions** tab in the **Properties** window of files and folders on network shares.

Users access shadow copies with Windows Explorer by selecting **View**, **Copy**, or **Restore** from the **Previous Versions** tab. (See Figure 12). Both individual files and folders can be restored.

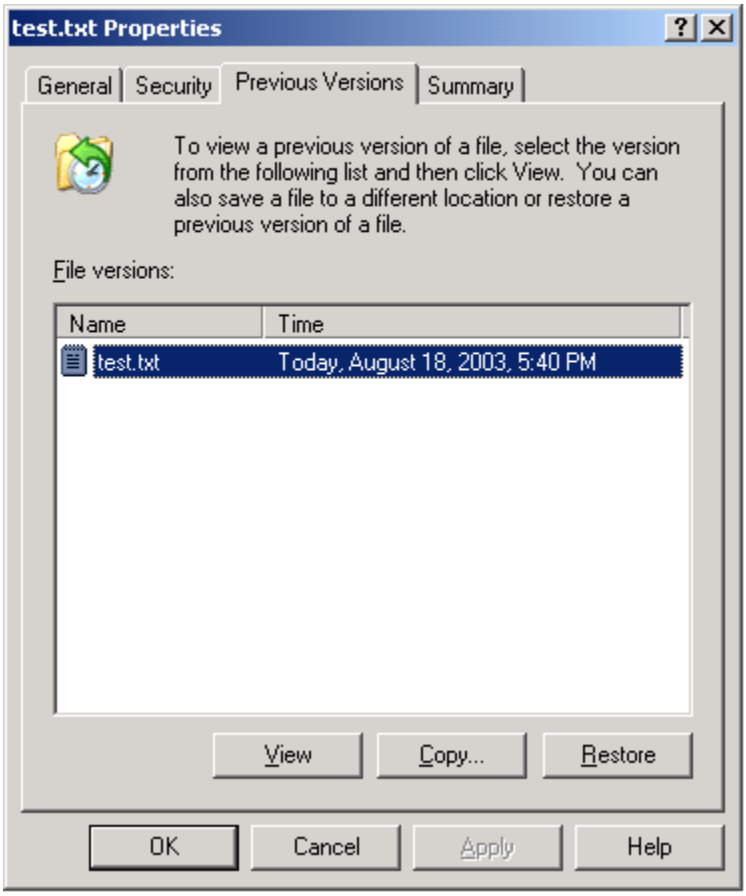


Figure 12 Client GUI

When users view a network folder hosted on the storage server for which shadow copies are enabled, old versions (prior to the snapshot) of a file or directory are available. Viewing the properties of the file or folder presents users with the folder or file history—a list of read-only, point-in-time copies of the file or folder contents that users can then open and explore like any other file or folder. Users can view files in the folder history, copy files from the folder history, and so on.

NFS shadow copies

UNIX users can independently access previous versions of files stored on NFS shares via the NFS client; no additional software is required. Server for NFS exposes each of a share's available shadow copies as a pseudo-subdirectory of the share. Each of these pseudo-subdirectories is displayed in exactly the same way as a regular subdirectory is displayed.

The name of each pseudo-subdirectory reflects the creation time of the shadow copy, using the format .@GMT-YYYY.MM.DD-HH:MM:SS. To prevent common tools from needlessly enumerating the pseudo-subdirectories, the name of each pseudo-subdirectory begins with the dot character, thus rendering it hidden.

The following example shows an NFS share named “NFSShare” with three shadow copies, taken on April 27, 28, and 29 of 2003 at 4 a.m.

NFSShare

.@GMT-2003.04.27-04:00:00

.@GMT-2003.04.28-04:00:00

.@GMT-2003.04.29-04:00:00

Access to NFS shadow copy pseudo-subdirectories is governed by normal access-control mechanisms using the permissions stored in the file system. Users can access only those shadow copies to which they have read access at the time the shadow copy is taken. To prevent users from modifying shadow copies, all pseudo-subdirectories are marked read-only, regardless of the user's ownership or access rights, or the permissions set on the original files.

Server for NFS periodically polls the system for the arrival or removal of shadow copies and updates the root directory view accordingly. Clients then capture the updated view the next time they issue a directory read on the root of the share.

Recovery of files or folders

There are three common situations that may require recovery of files or folders:

- Accidental file deletion, the most common situation
- Accidental file replacement, which may occur if a user selects Save instead of Save As
- File corruption

It is possible to recover from all of these scenarios by accessing shadow copies. There are separate steps for accessing a file compared to accessing a folder.

Recovering a deleted file or folder

To recover a deleted file or folder within a folder:

1. Access to the folder where the deleted file was stored.
2. Position the cursor over a blank space in the folder. If the cursor hovers over a file, that file is selected.
3. Right-click, select **Properties** from the bottom of the menu, and then click the **Previous Versions** tab.
4. Select the version of the folder that contains the file before it was deleted, and then click **View**.
5. View the folder and select the file or folder to recover. The view may be navigated multiple folders deep.
6. Click **Restore** to restore the file or folder to its original location. Click **Copy...** to allow the placement of the file or folder to a new location.

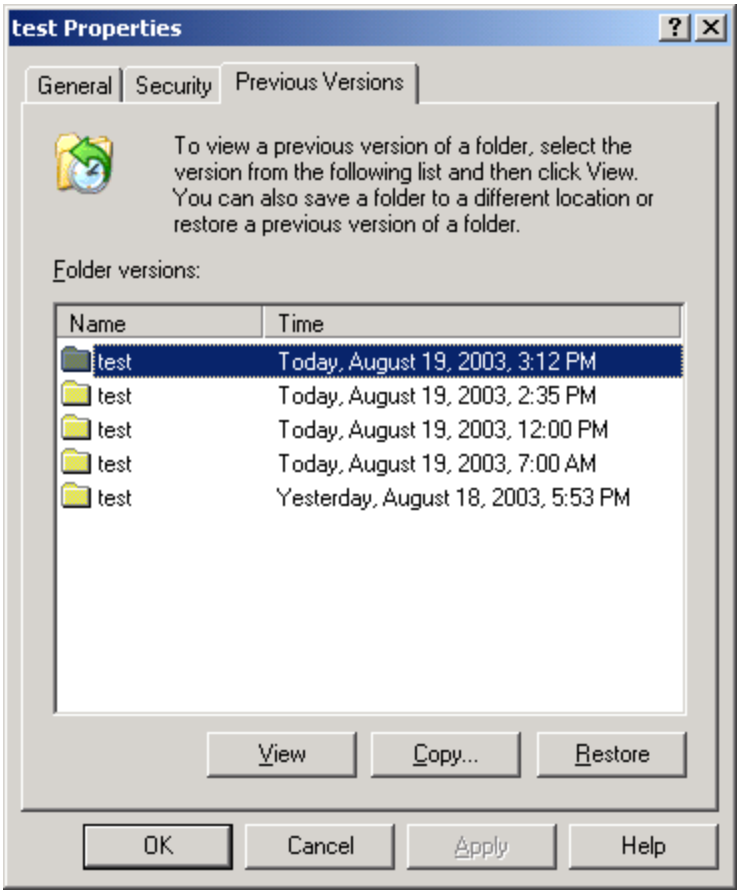


Figure 13 Recovering a deleted file or folder

Recovering an overwritten or corrupted file

Recovering an overwritten or corrupted file is easier than recovering a deleted file because the file itself can be right-clicked instead of the folder. To recover an overwritten or corrupted file:

1. Right-click the overwritten or corrupted file, and then click **Properties**.
2. Click **Previous Versions**.
3. To view the old version, click **View**. To copy the old version to another location, click **Copy...** to replace the current version with the older version, click **Restore**.

Recovering a folder

To recover a folder:

1. Position the cursor so that it is over a blank space in the folder to be recovered. If the cursor hovers over a file, that file is selected.
2. Right-click, select **Properties** from the bottom of the menu, and then click the **Previous Versions** tab.
3. Click either **Copy...** or **Restore**.

   Clicking **Restore** enables the user to recover everything in that folder as well as all subfolders. Clicking **Restore** does not delete any files.

Backup and shadow copies

Shadow copies are only available on the network via the client application, and only at a file or folder level as opposed to the entire volume. Hence, the standard backup associated with a volume backup

will not work to back up the previous versions of the file system. To answer this particular issue, shadow copies are available for back up in two situations. If the backup software in question supports the use of shadow copies and can communicate with underlying block device, it is supported, and the previous version of the file system will be listed in the backup application as a complete file system snapshot. If the built-in backup application NTbackup is used, the backup software forces a snapshot, and then uses the snapshot as the means for back up. The user is unaware of this activity and it is not self-evident although it does address the issue of open files.

Shadow Copy Transport

Shadow Copy Transport provides the ability to transport data on a Storage Area Network (SAN). With a storage array and a VSS-aware hardware provider, it is possible to create a shadow copy on one server and import it on another server. This process, essentially "virtual" transport, is accomplished in a matter of minutes, regardless of the size of the data.

NOTE:

Shadow copy transport is supported only on Windows Server 2003 Enterprise Edition, Windows Storage Server 2003 Enterprise Edition, and Windows Server 2003 Datacenter Edition. It is an advanced solution that works only if it has a hardware provider on the storage array.

A shadow copy transport can be used for a number of purposes, including:

- Tape backups

  An alternative to traditional backup to tape processes is transport of shadow copies from the production server onto a backup server, where they can then be backed up to tape. Like the other two alternatives, this option removes backup traffic from the production server. While some backup applications might be designed with the hardware provider software that enables transport, others are not. The administrator should determine whether or not this functionality is included in the backup application.

- Data mining

  The data in use by a particular production server is often useful to different groups or departments within an organization. Rather than add additional traffic to the production server, a shadow copy of the data can be made available through transport to another server. The shadow copy can then be processed for different purposes, without any performance impact on the original server.

The transport process is accomplished through a series of DISKRAID command steps:

1. Create a shadow copy of the source data on the source server (read-only).
2. Mask off (hide) the shadow copy from the source server.
3. Unmask the shadow copy to a target server.
4. Optionally, clear the read-only flags on the shadow copy.

The data is now ready to use.

Folder and share management

The HP ProLiant Storage Server supports several file-sharing protocols, including DFS, NFS, FTP, HTTP, and Microsoft SMB. This section discusses overview information as well as procedures for the setup and management of the file shares for the supported protocols. Security at the file level and at the share level is also discussed.

NOTE:

Detailed information on setting up and managing NFS and NCP shares is discussed in Microsoft Services for Network File System (MSNFS).

NOTE:

Select servers can be deployed in a clustered or non-clustered configuration. This section discusses share setup for a non-clustered deployment.

Folder management

Volumes and folders on any system are used to organize data. Regardless of system size, systematic structuring and naming conventions of volumes and folders eases the administrative burden. Moving from volumes to folders to shares increases the level of granularity of the types of data stored in the unit and the level of security access allowed.

Folders can be managed using the HP Storage Server Management Console. Tasks include:

- Accessing a specific volume or folder
- Creating a new folder
- Deleting a folder
- Modifying folder properties
- Creating a new share for a volume or folder
- Managing shares for a volume or folder

Managing file-level permissions

Security at the file level is managed using Windows Explorer.

File level security includes settings for permissions, ownership, and auditing for individual files.

To enter file permissions:

1. Using Windows Explorer, access the folder or file that needs to be changed, and then right-click the folder.
2. Click **Properties**, and then click the **Security** tab.

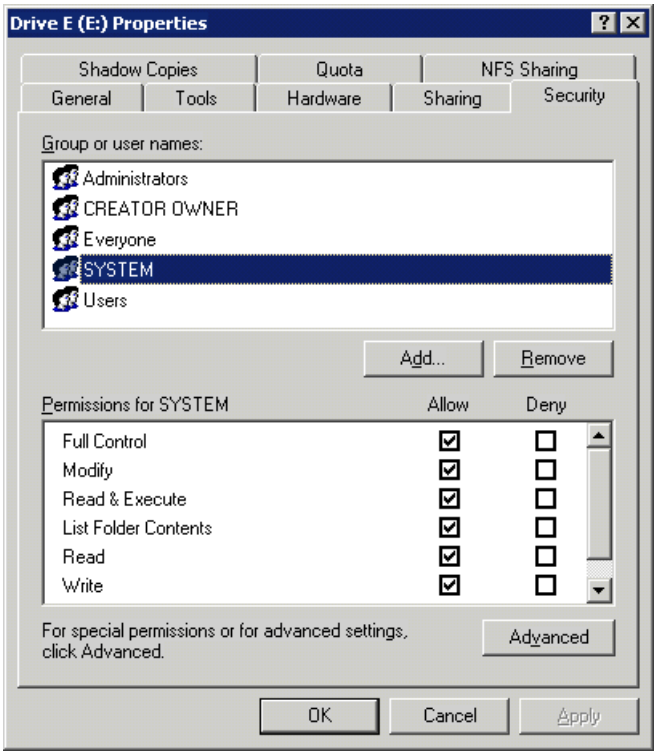


Figure 14 Properties dialog box, Security tab

Several options are available on the **Security** tab:

- To add users and groups to the permissions list, click **Add**. Follow the dialog box instructions.
- To remove users and groups from the permissions list, highlight the desired user or group, and then click **Remove**.
- The center section of the **Security** tab lists permission levels. When new users or groups are added to the permissions list, select the appropriate boxes to configure the common file-access levels.

3. To modify ownership of files, or to modify individual file access level permissions, click **Advanced**.

   Figure 15 illustrates the properties available on the **Advanced Security Settings** dialog box.

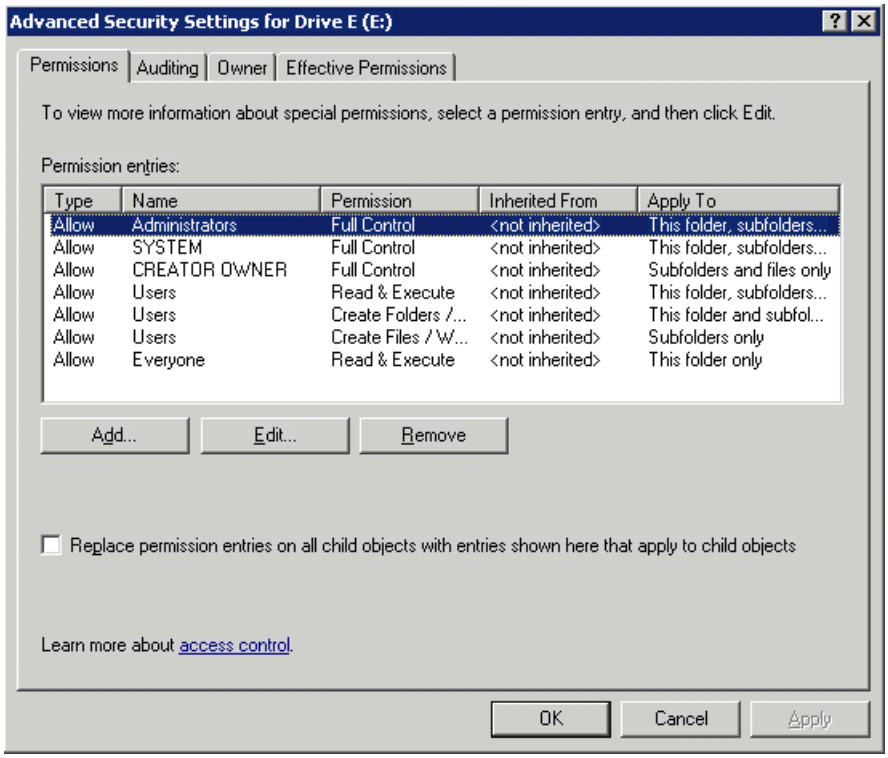


Figure 15 Advanced Security settings dialog box, Permissions tab

Other functionality available in the **Advanced Security Settings** dialog box is illustrated in Figure 15 and includes:

- Add a new user or group—Click **Add**, and then follow the dialog box instructions.
- Remove a user or group— Click **Remove**.
- Replace permission entries on all child objects with entries shown here that apply to child objects—This allows all child folders and files to inherit the current folder permissions by default.
- Modify specific permissions assigned to a particular user or group—Select the desired user or group, and then click **Edit**.

4. Enable or disable permissions by selecting the **Allow** box to enable permission or the **Deny** box to disable permission. If neither box is selected, permission is automatically disabled. Figure 16 illustrates the **Edit** screen and some of the permissions.

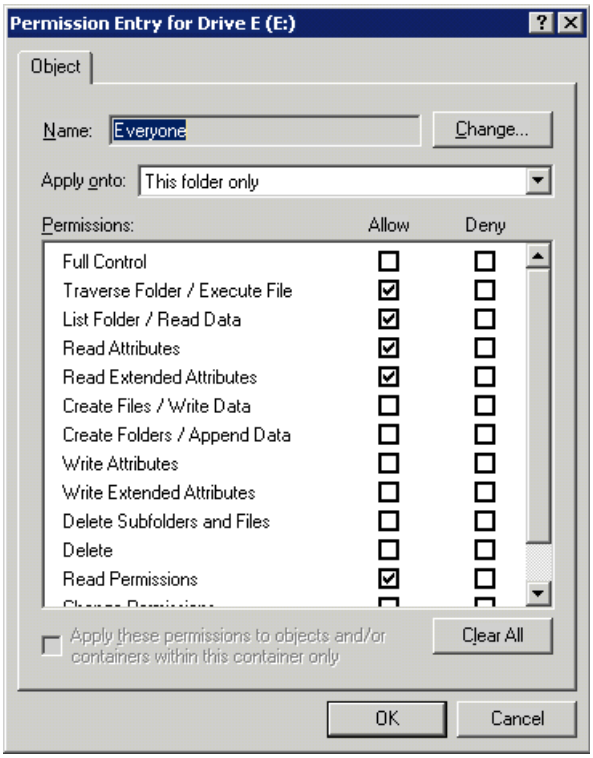


Figure 16 User or group Permission Entry dialog box

Another area of the **Advanced Security Settings** is the **Auditing** tab. Auditing allows you to set rules for the auditing of access, or attempted access, to files or folders. Users or groups can be added, deleted, viewed, or modified through the **Advanced Security Settings Auditing** tab.

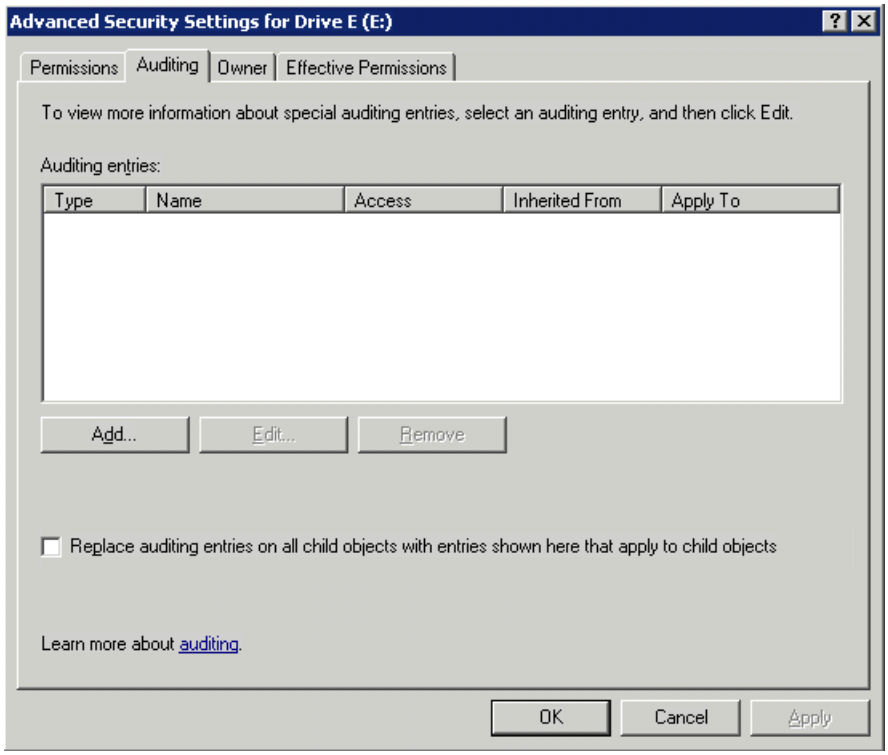


Figure 17 Advanced Security Settings dialog box, Auditing tab

5. Click **Add** to display the Select User or Group dialog box.

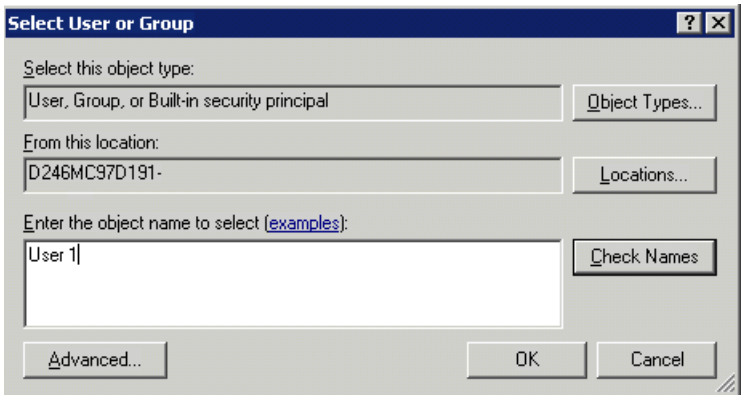


Figure 18 Select User or Group dialog box

NOTE:

Click Advanced to search for users or groups.

6. Select the user or group.
7. Click **OK**.

   The **Auditing Entry** dialog box is displayed.

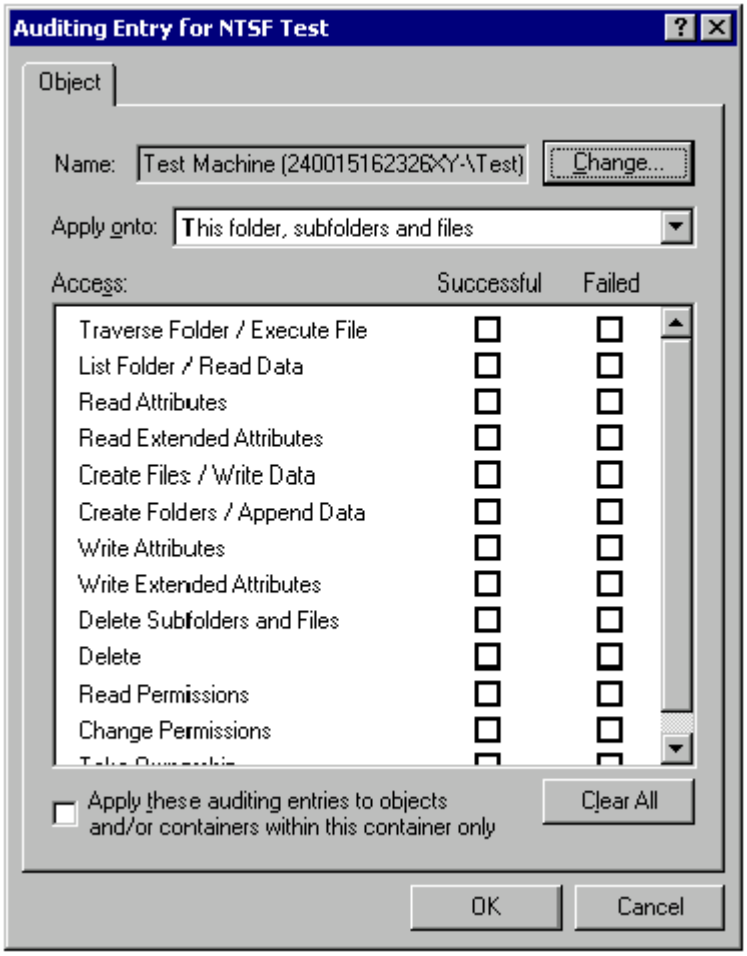


Figure 19 Auditing Entry dialog box for folder name NTFS Test

8. Select the desired **Successful** and **Failed** audits for the user or group.
9. Click **OK**.

NOTE:

Auditing must be enabled to configure this information. Use the local Computer Policy Editor to configure the audit policy on the storage server.

The **Owner** tab allows taking ownership of files. Typically, administrators use this area to take ownership of files when the file ACL is incomplete or corrupt. By taking ownership, you gain access to the files, and then manually apply the appropriate security configurations.

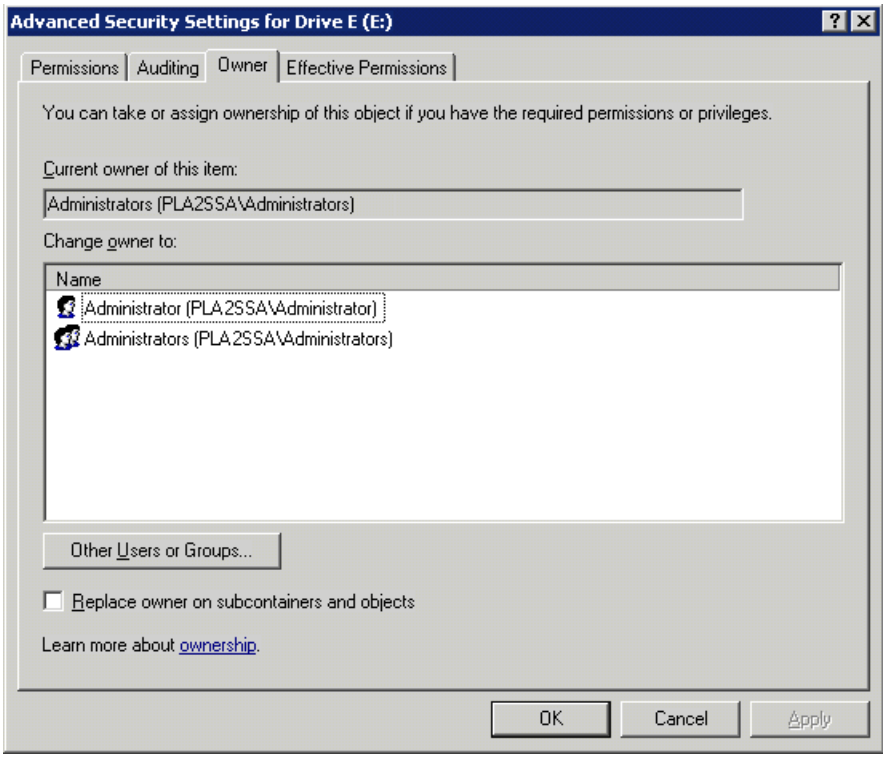


Figure 20 Advanced Security Settings dialog box, Owner tab

The current owner of the file or folder is listed at the top of the screen. To take ownership:

1. Click the appropriate user or group in the **Change owner to** list.
2. If it is also necessary to take ownership of subfolders and files, enable the **Replace owner on subcontainers and objects** box.
3. Click **OK**.

Share management

There are several ways to set up and manage shares. Methods include using Windows Explorer, a command line interface, or the HP Storage Server Management Console.

NOTE:

Select servers can be deployed in a clustered as well as a non-clustered configuration. This chapter discusses share setup for a non-clustered deployment.

As previously mentioned, the file-sharing security model of the storage server is based on the NTFS file-level security model. Share security seamlessly integrates with file security. In addition to discussing share management, this section discusses share security.

Share considerations

Planning the content, size, and distribution of shares on the storage server can improve performance, manageability, and ease of use.

The content of shares should be carefully chosen to avoid two common pitfalls: either having too many shares of a very specific nature, or of having very few shares of a generic nature. For example, shares for general use are easier to set up in the beginning, but can cause problems later. Frequently, a better approach is to create separate shares with a specific purpose or group of users in mind. However,

creating too many shares also has its drawbacks. For example, if it is sufficient to create a single share for user home directories, create a “homes” share rather than creating separate shares for each user.

By keeping the number of shares and other resources low, the performance of the storage server is optimized. For example, instead of sharing out each individual user's home directory as its own share, share out the top-level directory and let the users map personal drives to their own subdirectory.

Defining Access Control Lists

The Access Control List (ACL) contains the information that dictates which users and groups have access to a share, as well as the type of access that is permitted. Each share on an NTFS file system has one ACL with multiple associated user permissions. For example, an ACL can define that User1 has read and write access to a share, User2 has read only access, and User3 has no access to the share. The ACL also includes group access information that applies to every user in a configured group. ACLs are also referred to as permissions.

Integrating local file system security into Windows domain environments

ACLs include properties specific to users and groups from a particular workgroup server or domain environment. In a multidomain environment, user and group permissions from several domains can apply to files stored on the same device. Users and groups local to the storage server can be given access permissions to shares managed by the device. The domain name of the storage server supplies the context in which the user or group is understood. Permission configuration depends on the network and domain infrastructure where the server resides.

File-sharing protocols (except NFS) supply a user and group context for all connections over the network. (NFS supplies a machine-based context.) When new files are created by those users or machines, the appropriate ACLs are applied.

Configuration tools provide the ability to share permissions out to clients. These shared permissions are propagated into a file system ACL, and when new files are created over the network, the user creating the file becomes the file owner. In cases where a specific subdirectory of a share has different permissions from the share itself, the NTFS permissions on the subdirectory apply instead. This method results in a hierarchical security model where the network protocol permissions and the file permissions work together to provide appropriate security for shares on the device.

NOTE:

Share permissions and file-level permissions are implemented separately. It is possible for files on a file system to have different permissions from those applied to a share. When this situation occurs, the file-level permissions override the share permissions.

Comparing administrative (hidden) and standard shares

CIFS supports both administrative shares and standard shares.

- Administrative shares are shares with a last character of $. Administrative shares are not included in the list of shares when a client browses for available shares on a CIFS server.
- Standard shares are shares that do not end in a $ character. Standard shares are listed whenever a CIFS client browses for available shares on a CIFS server.

The storage server supports both administrative and standard CIFS shares. To create an administrative share, end the share name with the $ character when setting up the share. Do not type a $ character at the end of the share name when creating a standard share.

Managing shares

Shares can be managed using the HP Storage Server Management Console. Tasks include:

- Creating a new share
- Deleting a share

- Modifying share properties
- Publishing in DFS

NOTE:

These functions can operate in a cluster on select servers, but should only be used for non-cluster-aware shares. Use Cluster Administrator to manage shares for a cluster. The page will display cluster share resources.

CAUTION:

Before deleting a share, warn all users to exit that share and confirm that no one is using that share.

File Server Resource Manager

File Server Resource Manager (FSRM) is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. Some of the tasks you can perform are:

- Quota management
- File screening management
- Storage reports

The HP Storage Server Management Console provides access to FSRM tasks.

For procedures and methods beyond what are described below, refer to the online help. In addition, see a Microsoft File Server Resource Manager white paper available at http://download.microsoft.com/download/7/4/7/7472bf9b-3023-48b7-87be-d2cedc38f15a/WS03R2_Storage_Management.doc .

Quota management

On the Quota Management node of the File Server Resource Manager snap-in, you can perform the following tasks:

- Create quotas to limit the space allowed for a volume or folder and generate notifications when the quota limits are approached or exceeded.
- Generate auto quotas that apply to all existing folders in a volume or folder, as well as to any new subfolders created in the future.
- Define quota templates that can be easily applied to new volumes or folders and that can be used across an organization.

File screening management

On the File Screening Management node of the File Server Resource Manager snap-in, you can perform the following tasks:

- Create file screens to control the types of files that users can save and to send notifications when users attempt to save blocked files.
- Define file screening templates that can be easily applied to new volumes or folders and that can be used across an organization.
- Create file screening exceptions that extend the flexibility of the file screening rules.

Storage reports

On the Storage Reports node of the File Server Resource Manager snap-in, you can perform the following tasks:

- Schedule periodic storage reports that allow you to identify trends in disk usage.

- Monitor attempts to save unauthorized files for all users or a selected group of users.
- Generate storage reports instantly.

Other Windows disk and data management tools

When you install certain tools, such as Windows Support Tools or Windows Resource Kit Tools, information about these tools might appear in Help and Support Center. To see the tools that are available to you, look in the Help and Support Center under **Support Tasks**, click **Tools**, and then click **Tools by Category**.

NOTE:

The Windows Support Tools and Windows Resource Kit Tools, including documentation for these tools, are available in English only. If you install them on a non-English language operating system or on an operating system with a Multilingual User Interface Pack (MUI), you see English content mixed with non-English content in Help and Support Center. To see the tools that are available to you, click **Start**, click **Help and Support Center**, and then, under **Support Tasks**, click **Tools**.

Additional information and references for file services

Backup

HP recommends that you back up the print server configuration whenever a new printer is added to the network and the print server configuration is modified. For details on implementing the backup solution, refer to the Medium Business Guide for Backup and Recovery. The guide can be viewed or downloaded from Microsoft at http://www.microsoft.com/technet/itsolutions/smbiz/mits/br/mit_br.mspx.

HP StorageWorks Library and Tape Tools

HP StorageWorks Library and Tape Tools (L&TT) provides functionality for firmware downloads, verification of device operation, maintenance procedures, failure analysis, corrective service actions, and some utility functions. It also provides seamless integration with HP hardware support by generating and e-mailing support tickets that deliver a snapshot of the storage system.

For more information, and to download the utility, refer to the StorageWorks L&TT website at http://h18006.www1.hp.com/products/storageworks/ltt.

Antivirus

The server should be secured by installing the appropriate antivirus software. For details on implementing antivirus, refer to the Medium Business Guide for Antivirus. The guide can be viewed or downloaded from Microsoft at http://www.microsoft.com/technet/itsolutions/smbiz/mits/av/mit_av.mspx.

Security

For guidance on hardening file servers, see the Microsoft Windows Server 2003 Security Guide. The guide can be viewed or downloaded at http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx.

More information

The following web sites provide detailed information for using print services with Windows Server 2003, which also applies to Windows Storage Server 2003.

- Microsoft Storage

  http://www.microsoft.com/windowsserversystem/storage/default.mspx

- Microsoft Windows Storage Server 2003
  http://www.microsoft.com/windowsserversystem/wss2003/default.mspx
- Performance Tuning Guidelines for Windows Server 2003
  http://www.microsoft.com/windowsserver2003/evaluation/performance/tuning.mspx
- Windows SharePoint Services
  http://www.microsoft.com/windowsserver2003/technologies/sharepoint/default.mspx

4 Print services

Microsoft Print Management Console

Print Management in the Microsoft Windows Server 2003 R2 operating system is a Microsoft Management Console (MMC) snap-on that system administrators can use to perform common print management tasks in a large enterprise. It provides a single interface that administrators can use to perform printer and print server management tasks efficiently with detailed control. You can use Print Management from any computer running Windows Server 2003 R2, and you can manage all network printers on print servers running Windows 2000 Server, Windows Server 2003, or Windows Server 2003 R2.

New or improved HP print server features

HP Web Jetadmin

Integrating the HP Web Jetadmin (WJA) print management application to the HP Storage Server or File Print Appliance Management Console is new. WJA is a web-based tool for remotely installing, configuring, and managing a wide variety of HP and non-HP network peripherals using only a web browser. It supports a modular design, whereby plug-ins can be installed to provide additional device, language, and application functionality. WJA is not pre-installed on the storage server, but can be installed (see "Web Jetadmin installation" on page 70)

HP Install Network Printer Wizard

The inclusion of the HP Install Network Printer Wizard (INPW) utility on the factory image is new. INPW simplifies the process of installing network printers, including configuration settings on the print server. INPW identifies HP Jetdirect network print devices and allows the user to select the printer to install on the print server.

HP Download Manager for Jetdirect Print Devices

The inclusion of the HP Download Manager (DLM) for Jetdirect Printer Devices on the factory image is new. DLM is used to upgrade HP Jetdirect print server firmware on HP network printers. The utility obtains the latest firmware catalog from either from the Internet or from a computer with the download firmware images already in place. The DLM discovers all or user-selected Jetdirect devices and upgrades those based on the firmware catalog.

Microsoft Print Migrator Utility

The inclusion of the Microsoft Print Migrator utility on the factory image is new. The utility provides complete printer configuration backup of the print server to a user-specified CAB file. Print Migrator supports migration of print configuration data between different versions of Windows, and supports conversion of line printer remote (LPR) ports to the Standard TCP/IP Port Monitor on Windows 2000, Windows XP, and Windows Server 2003.

Network printer drivers

Updated print drivers for HP network printers are preinstalled on the storage server. If a Service Release DVD has been run on the server, there are updated HP network print drivers in the `C:\hpnas\PRINTERS` folder.

Print services management

Print services information to plan, set up, manage, administer, and troubleshoot print servers and print devices are available online using the Help and Support Center feature. To access the Help and Support Center, select **Start > Help and Support**, then **Printers and Faxes** under Help Contents.

Microsoft Print Management Console

The Print Management Console (PMC) can be started from the HP Storage Server Management Console, or the PMC snap-in can be added to the Microsoft Management Console.

HP recommends that you use the *Microsoft Print Management Step-by-Step Guide* on the Documentation CD for print concepts, use of the PMC, and management of network printers. The guide can also be downloaded from http://www.microsoft.com/printserver.

When running the PMC on a server that has Windows Firewall enabled, no printers will be displayed in the printers folder of the PMC. In order for printers to be displayed, you need to open the file and print sharing ports (TCP 139 and 445, and UDP 137 and 138). If this does not fix the problem, or if these ports are already open, you may need to turn off the Windows Firewall to display printers.

To open the file and print sharing ports:

1. Click **Start**, point to Control Panel, and click **Windows Firewall**.
2. On the Exceptions tab, ensure that the File and Printer Sharing check box is selected and click **OK**.

To turn off Windows Firewall:

1. Click **Start**, point to Control Panel, and click **Windows Firewall**.
2. Select **Off** (not recommended) and click **OK**.

HP Web Jetadmin installation

HP Web Jetadmin is used to manage a fleet of HP and non-HP network printers and other peripherals using a web browser. Although not preinstalled, the Web Jetadmin software is located in the `C:\hpnas\Components\WebJetadmin` folder, and can be installed by running the `WJA.exe` setup program. Follow the installation wizard and supply a password for the local "Admin" username account and a system name.

For more information about Web Jetadmin and Web Jetadmin plug-ins, go to http://www.hp.com/go/webjetadmin. For an article on optimizing performance, go to http://h10010.www1.hp.com/wwpc/pscmisc/vac/us/product_pdfs/weboptim.pdf.

Web-based printer management and Internet printing

Internet printing is enabled by default on the print server and File Print Appliance. Internet printing consists of two main components:

- Web-based printer management with the ability to administer, connect to, and view printers through a web browser.
- Internet printing enabling users to connect to a printer using the printer's URL.

A Microsoft white paper discussing the uses of both components can be obtained at http://www.microsoft.com/windowsserver2003/techinfo/overview/internetprint.mspx.

Planning considerations for print services

Before configuring the print server or File Print Appliance, the following checklist of items should be followed:

1. **Determine the operating system version of the clients that will send jobs to this printer**. This information is used to select the correct client printer drivers for the client and server computers using

the printer. Enabling this role on the print server allows the automatic distribution of these drivers to the clients. Additionally, the set of client operating systems determines which of these drivers need to be installed on the server during the print server role installation.

2. **At the printer, print a configuration or test page that includes manufacturer, model, language, and installed options**. This information is needed to choose the correct printer driver. The manufacturer and model are usually enough to uniquely identify the printer and its language. However, some printers support multiple languages, and the configuration printout usually lists them. Also, the configuration printout often lists installed options, such as extra memory, paper trays, envelope feeders, and duplex units.
3. **Choose a printer name**. Users running Windows-based client computers choose a printer by using the printer name. The wizard that you will use to configure your print server provides a default name, consisting of the printer manufacturer and model. The printer name is usually fewer than 31 characters in length.
4. **Choose a share name**. A user can connect to a shared printer by entering this name, or by selecting it from a list of share names. The share name is usually fewer than 8 characters for compatibility with MS-DOS and Windows 3.x clients.
5. (Optional) **Choose a location description and a comment**. These can help identify the location of the printer and provide additional information. For example, the location could be "Second floor, copy room" and the comment could be "Additional toner cartridges are available in the supply room on floor 1."
6. **Enable management features for Active Directory and Workgroup Environments**. If the print server is part of an Active Directory domain rather than Workgroup, the print server enables the following management features:
   - Restrict access to printer-based domain user accounts.
   - Publish shared printers to Active Directory to aid in search for the resource.
7. **Deploy printers using group policy**. Print management can be used with Group Policy to automatically add printer connections to a server's Printers and Faxes folder. For more information, see the Microsoft article at http://technet2.microsoft.com/WindowsServer/en/Library/ab8d75f8-9b35-4e3e-a344-90d7799927231033.mspx.
8. **Determine whether printer spooling be enabled**. Two or more identical printers that are connected to one print server can act as a single printer. As a means to load-balance print queues when you print a document, the print job is sent to the first available printer in the pool. See "Setting Printer Properties" in the Windows online help for additional information.

Print queue creation

In addition to Windows Printer and Faxes, Add Printer Wizard, the HP Install Network Printer Wizard (INPW) utility discovers HP Jetdirect network printers on the local network and allows print queues to be created on the print server. The utility is located on the storage server or File Print Appliance in the `C:\hpnas\Components\Install Network Printer Wizard` folder.

Sustaining print administration tasks

Tasks that need to be performed regularly to support the print services include:

- Monitoring print server performance using the built-in performance monitoring tool in the Windows Server operating system.
- Supporting printers that include adding, moving, and removing printers as requirements change.
- Installing new printer drivers.
- Recording information about the printer's name, share names, printer features, and the location where the printers are physically installed. This information should be kept in an easily accessible place.

For process suggestions for recurring tasks, see the Microsoft Print Service Product Operations Guide at http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/pspog/pspog3/mspx.

Driver updates

Print drivers

The latest print drivers for many HP network printers are supplied on the Service Release DVD. If selected as part of the service release installation process, updated print drivers are copied to the print drivers folder `C:\hpnas\PRINTERS` on the storage server or File Print Appliance. Print drivers are also available for download on the HP Support web site for individual network printers.

User-mode vs. kernel-mode drivers

Drivers can be written in either user mode (also called version 3 drivers) or kernel mode (also called version 2 drivers). Native drivers on Windows 2000 and later run in user mode. Windows Server 2003 and Windows Storage Server 2003 can run kernel-mode drivers, although this is not recommended for stability reasons.

Kernel-mode driver installation blocked by default

In Windows Server 2003 and Windows Storage Server 2003, installation of kernel-mode drivers is blocked by default.

To allow kernal-mode drivers to be installed, perform the following steps:

1. Open Group Policy, click **Start > Run**, then type **gpedit.msc**, and press **Enter**.
2. Under **Local Computer Policy**, double-click **Computer Configuration**.
3. Right-click **Disallow installation of printers using kernel-mode drivers** and then click **Properties**.
4. On the **Setting** tab, click either **Not Configured** or **Disabled**, and then click **OK**.

HP Jetdirect firmware

The HP Download Manager (DLM) utility for Jetdirect printers provides upgrades of HP Jetdirect print server firmware on HP network printers. The utility is located on the storage server or File Print Appliance in the `C:\hpnas\Components\Download Manager for Jetdirect` folder. A connection to the Internet is required, or the utility can be pointed to a local location where the firmware images are stored. For more information on upgrading HP Jetdirect print server firmware, see http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06917.

Printer server scalability and sizing

A Microsoft technical paper overviews several key factors that influence the capacity of a given print server configuration. While this paper cannot provide a predictive formula to determine the printing throughput of a given configuration, it does describe several reference systems and their capacity. This paper also presents the information necessary to help the system administrator or capacity planner estimate, and later monitor, their server workload. The current version of this paper is maintained at http://www.microsoft.com/printserver.

Backup

It is recommended that you back up the print server configuration whenever a new printer is added to the network and the print server configuration is modified. For details on implementing the backup solution, refer to the *Medium Business Guide for Backup and Recovery*. The guide can be viewed or downloaded from Microsoft at http://www.microsoft.com/technet/itsolutions/smbiz/mits/br/mit_br.mspx.

The Print Migrator utility is recommended as a print-specific alternative to backing up print configuration settings on the print server or File Print Appliance. The Print Migrator utility is located in the `C:\hpnas\Components\PrintMigrator` folder on the storage server or File Print Appliance.

For more information about the Print Migrator utility, visit http://www.microsoft.com/WindowsServer2003/techinfo/overview/printmigrator3.1.mspx.

Best practices

The following is practical advice for managing print devices:

- Printers and print servers should be published in Active Directory.
- Locate printers in common areas, such as near conference rooms.
- Protect print servers using antivirus software.
- Ensure the print server is included in the backup configuration.
- Use Microsoft Printer Migrator to back up a print server configuration and restore settings on a new print server. This eliminates the need to manually re-create print queues and printer ports, install drivers, and change the IP configuration.
- Use Microsoft Printer Migrator to backup new printers configured on the print server.
- Use Microsoft Printer Migrator when migrating to new print servers.
- Perform a full backup of the print server, including the state information, before releasing the system to the users in the production environment.
- Whenever a new configuration is made or existing configuration is modified, a backup should be performed.
- To optimize performance, move the print spooler to another disk, separate from the disk supporting the operating system. To move the print spooler to another disk:
  - Start Printer and Faxes.
  - On the File menu, click **Server Properties**, and then click the **Advanced** tab.
  - In the Spool folder window, enter the path and the name of the new default spool folder for the print server or File Print Appliance, and then click **Apply** or **OK**.
  - Stop and restart the spooler service, or restart the print server or File Print Appliance.

Troubleshooting

The online help or Help and Support Center feature should be used to troubleshoot general and common print-related problems. Printing help can be accessed by selecting **Start > Help and Support**, then the **Printers and Faxes** selection under **Help Contents**.

The same print troubleshooting information can be accessed at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/2048a7ba-ec57-429c-95a3-226eea32d126.mspx

Specific print server related problems as well as other system related known issues and workarounds are addressed in release notes. To view the latest version, visit http://www.hp.com/go/support. Select **See support and troubleshooting information** and enter a product name/number. Under **self-help resources**, select the **manuals (guides, supplements, addendums, etc)** link.

Additional references for print services

The following Web sites provide detailed information for using print services with Windows Server 2003, which also applies to Windows Storage Server 2003.

- Windows Server 2003 print services home page at http://www.microsoft.com/windowsserver2003/technologies/print/default.mspx
- Medium Business Solution for Print Services at http://www.microsoft.com/technet/itsolutions/smbiz/mits/ps/mit_ps.mspx.

5 Microsoft Services for Network File System (MSNFS)

This chapter discusses networking features in Microsoft Services for Network File System (MSNFS).

MSNFS Features

MSNFS is an update to the NFS components that were previously available in Services for UNIX 3.5.

MSNFS includes the following new features:

- Updated administration snap-in—MSNFS Administration
- Active Directory Lookup—The Identity Management for UNIX Active Directory schema extension, available in Microsoft Windows Server 2003 R2, includes UNIX user identifier (UID) and group identifier (GID) fields, which enables Server for NFS and Client for NFS to look up Windows-to-UNIX user account mappings directly from Active Directory. Identity Management for UNIX simplifies Windows-to-UNIX user account mapping management in Active Directory.
- Enhanced server performance—Microsoft Services for NFS includes a file filter driver, which significantly reduces common server file access latencies.
- UNIX special device support—Microsoft Services for NFS supports UNIX special devices (mknod).
- Enhanced UNIX support—Microsoft Services for NFS now supports the following versions of UNIX:
  - Hewlett Packard HP-UX version 11i
  - IBM AIX version 5L 5.2
  - Red Hat Linux version 9
  - Sun Microsystems Solaris version 9

The following features that were previously available in Services for UNIX 3.5 are not included in MSNFS:

- Gateway for NFS
- Server for PCNFS
- All PCNFS components of Client for NFS

UNIX Identity Management

Identity Management for UNIX makes it easy to integrate users of Windows operating systems into existing UNIX environments. It provides manageability components that simplify network administration and account management across both platforms.

With Identity Management for UNIX, the administrator can:

- Manage user accounts and passwords on Windows and UNIX systems using Network Information Service (NIS).
- Automatically synchronize passwords between Windows and UNIX operating systems.

UNIX Identity Management consists of the following components:

- Administration components
- Password synchronization
- Server for NIS

The UNIX Identity Management component is not enabled by default on the storage server. To install this component:

1. Access **Add/Remove Programs**.
2. Select **Add/Remove Windows Components > Active Directory Services > Details**.
3. Install **Identity Management for Windows**.

MSNFS use scenarios

The following use scenarios are supported by MSNFS file services:

- Allow UNIX clients to access resources on computers running Windows Server 2003 R2.

  Your company may have UNIX clients accessing resources, such as files, on UNIX file servers. To take advantage of new Windows Server 2003 features, such as Shadow Copies for Shared Folders, you can move resources from your UNIX servers to computers running Windows Server 2003 R2. You can then set up MSNFS to enable access by UNIX clients that are running NFS software. All of your UNIX clients will be able to access the resources using the NFS protocol with no changes required.

- Allow computers running Windows Server 2003 R2 to access resources on UNIX file servers.

  Your company may have a mixed Windows and UNIX environment with resources, such as files, stored on UNIX file servers. You can use MSNFS to enable computers running Windows Server 2003 R2 to access these resources when the file servers are running NFS software.

NOTE:

Services for NFS can be implemented in both clustered and non-clustered environments using select storage servers. This chapter discusses Services for NFS in a non-clustered deployment. If your storage server is capable of using clusters, see the Cluster administration chapter for more information. (This chapter is not in manuals for those models that cannot use clusters.)

MSNFS components

MSNFS comprises the following three main components:

- Username Mapping Server

  Username Mapping Server maps user names between Windows and UNIX user accounts. In a heterogeneous network, users have separate Windows and UNIX security accounts. Users must provide a different set of credentials to access files and other resources, depending on whether they are stored on a Windows or UNIX file server. To address this issue, Username Mapping Server maps the Windows and UNIX user names so that users can log on with either their Windows or UNIX credentials and access resources regardless of whether they are stored on a Windows or UNIX file server.

- Server for NFS

  Normally, a UNIX computer cannot access files on a Windows-based computer. A computer running Windows Server 2003 R2 and Server for NFS, however, can act as a file server for both Windows and UNIX computers.

- Client for NFS

  Normally, a Windows-based computer cannot access files on a UNIX computer. A computer running Windows Server 2003 R2 and Client for NFS, however, can access files stored on a UNIX-based NFS server.

The Client for NFS feature of the Microsoft Services for NFS component is not preinstalled on the storage server although information about this feature appears in the online help. To enable Client for NFS:

1. Go to **Add/Remove Programs**.
2. Select **Add/Remove Windows Components > Other Network File and Print Services > Microsoft Services for NFS > Details**.

3. Install Client for NFS.

Administering MSNFS

To access Microsoft Services for Network File System from the Start menu:

1. Select **Start > Programs > Administrative Tools**.
2. Click **Microsoft Services for Network File System**.

To access Microsoft Services for Network File System from the HP Storage Server Management console:

1. Access the HP Storage Server Management console by clicking on the shortcut icon on the desktop.
2. In the left pane of the console, select the **Share Folder Management** listing.
3. In the center pane, under **Share Utilities**, select **Microsoft Services for NFS** (see Figure 21).

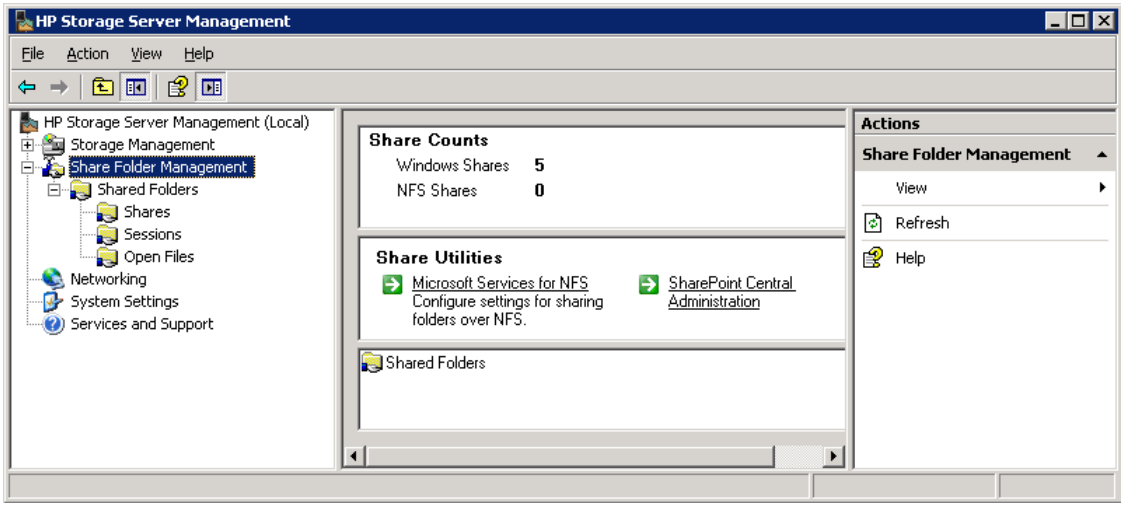


Figure 21 Accessing MSNFS from HP Storage Server Management console

Server for NFS

With Server for NFS, a computer running the Microsoft Windows Server 2003 R2 operating system can act as a Network File System (NFS) server. Users can then share files in a mixed environment of computers, operating systems, and networks. Users on computers running NFS client software can gain access to directories (called shares) on the NFS server by connecting (mounting) those directories to their computers. From the viewpoint of the user on a client computer, the mounted files are indistinguishable from local files.

UNIX computers follow advisory locking for all lock requests. This means that the operating system does not enforce lock semantics on a file, and applications that check for the existence of locks can use these locks effectively. However, Server for NFS implements mandatory locks even for those locking requests that are received through NFS. This ensures that locks acquired through NFS are visible through the server message block (SMB) protocol and to applications accessing the files locally. Mandatory locks are enforced by the operating system.

Server for NFS Authentication DLL vs. Service for User for Active Directory domain controllers

On a Windows Storage Server 2003 R2 storage server, Server for NFS depends on a domain controller feature called Service for User (S4U) to authenticate UNIX users as their corresponding Windows users. Windows Server operating systems prior to Windows Server 2003 and Windows Storage Server 2003 do not support S4U. Also, in mixed domain environments, legacy Services for UNIX (SFU), Services for NFS and Windows Storage Server 2003 NFS deployments do not use the S4U feature and still depend on the Server for NFS Authentication DLL being installed on domain controllers.

Therefore, the administrator needs to install the Server for NFS Authentication DLL on Windows 2000 domain controllers when:

- The NFS file serving environment uses previous NFS releases (NAS, SFU, and so on).
- The Windows domain environment uses pre-2003 domain controllers.

Refer to Table 7 for guidance as to when to use NFS Authentication DLL instead of S4U legacy NFS and R2 MSNFS.

Table 7 Authentication table

Domain controller type	Legacy NFS (pre-WSS2003 R2)	MSNFS (WSS2003 R2)
Legacy domain controller (pre-WSS2003)	Requires NFS Authentication DLL on domain controller	Requires NFS Authentication DLL on domain controller
Recent domain controllers (WSS2003 and later)	Requires NFS Authentication DLL on domain controller	Uses the built-in S4U (on the domain controller). It is unaffected by the NFS Authentication DLL on the domain controller.

The S4U set of extensions to the Kerberos protocol consists of the Service-for-User-to-Proxy (S4U2Proxy) extension and the Service-for-User-to-Self (S4U2Self) extension. For more information about the S4U2 extensions, see the Kerberos articles at the following URLs: http://searchwindowssecurity.techtarget.com/originalContent/0,289142,sid45_gci1013484,00.html (intended for IT professionals) and http://msdn.microsoft.com/msdnmag/issues/03/04/SecurityBriefs/default.aspx (intended for developers).

Installing NFS Authentication DLL on domain controllers

NOTE:

If the authentication software is not installed on all domain controllers that have user name mappings, including primary domain controllers, backup domain controllers, and Active Directory domains, then domain user name mappings will not work correctly.

You need to install the version of NFS Authentication included with Services for UNIX 3.5. You can download Services for UNIX 3.5 at no charge from http://go.microsoft.com/fwlink/?LinkId=44501.

To install the Authentication software on the domain controllers:

1. From the SFU 3.5 files, locate the directory named `SFU35SEL_EN`.
2. On the domain controller where the Authentication software is being installed use Windows Explorer to:
   a. Open the shared directory containing `setup.exe`.
   b. Double-click the file to open it. Windows Installer is opened.

NOTE:

If the domain controller used does not have Windows Installer installed, locate the file `InstMSI.exe` on the SFU 3.5 directory and run it. After this installation, the Windows Installer program starts when opening `setup.exe`.

3. In the Microsoft Windows Services for UNIX Setup Wizard dialog box, click **Next**.
4. In the User name box, enter your name. If the name of your organization does not appear in the Organization box, enter the name of your organization there.
5. Read the End User License Agreement carefully. If you accept the terms of the agreement, click **I accept the terms in the License Agreement**, and then click **Next** to continue installation. If you click **I do not accept the License Agreement** (Exit Setup), the installation procedure terminates.

6. Click Custom Installation, and then click **Next**.
7. In the Components pane, click the down arrow next to Windows Services for UNIX, and then click **Entire component will not be available**.
8. Click the plus sign (+) next to Authentication Tools.
9. In the Components pane, click the plus sign (+) next to Authentication Tools.
10. Click **Server for NFS Authentication**, click **Will be installed on local hard drive**, and then click **Next**.
11. Follow the remaining instructions in the Wizard.

NOTE:

NFS users can be authenticated using either Windows domain accounts or local accounts on the Windows server. Server for NFS Authentication must be installed on all domain controllers in the domain if NFS users will be authenticated using domain accounts. Server for NFS Authentication is always installed on the computer running Server for NFS.

Elevate S4U2 functionality on Windows Server 2003 domain controllers

NOTE:

The S4U2 functionality does not work until the domain functional level is elevated to Windows Server 2003.

To elevate the functional level to Windows Server 2003:

1. On the Windows 2003 domain controller, open Active Directory Domains and Trusts.
2. In the console tree, right-click the domain for which you want to raise functionality, and then click **Raise Domain Functional Level**.
3. In Select an available domain functional level, click **Windows Server 2003**.
4. Click **Raise**.

Server for NFS administration

The Server for NFS administration online help contains information for the following topics:

- Understanding the Server for NFS component
- Starting and stopping Server for NFS
- Configuring Server for NFS
- Securing Server for NFS
- Optimizing Server for NFS performance
- Using file systems with NFS
- Managing NFS shares
- Managing NFS client groups
- Using Microsoft Services for NFS with server clusters
- Server for NFS Authentication

Accessing NFS resources for Windows users and groups

Server for NFS allows Windows clients to access NFS resources on the storage server without separately logging on to Server for NFS. The first time users attempt to access an NFS resource, the Server for NFS looks up the user's UNIX UID and GID information in either Windows Active Directory or the User Name Mapping function on the storage server. If the UNIX UID and GID information is mapped to a Windows user and group accounts, the Windows names are returned to Server for NFS, which then uses

the Windows user and group names to grant file access. If the UNIX UID and GID information is not mapped, then Server for NFS will deny file access.

There are two ways to specify how Server for NFS on the storage server obtains Windows user and group information:

- Using the Windows interface
- Using a command line (`nfsadmin.exe`)

IMPORTANT:

- Before using Active Directory Lookup, administrators must install and populate the Identity Management for UNIX Active Directory schema extension, included in Windows Server 2003 R2, or have an equivalent schema which includes UNIX UID and GID fields.
- The IP address of the User Name Mapping server can be specified instead of the name of the server.
- Before using User Name Mapping, the computer running Server for NFS must be listed in the .maphosts file on the computer running User Name Mapping. For more information, see "Securing access to the User Name Mapping server."

For additional information about accessing NFS resources, see the MSNFS online help. For additional information about Identity Management for UNIX, see the UNIX Identify Management online help

Managing access using the .maphosts file

The User Name Mapping component of MSNFS acts as an intermediary between NFS servers and NFS clients on a network containing UNIX hosts and Windows-based computers. To maintain the implicit trust relationship between NFS client and host computers, administrators can control which computers can access User Name Mapping by editing the .maphosts in the %windir%\msnfs directory of the storage server. Conditions to allow or deny access include:

- If the .maphosts file is present but not empty, then only those computers allowed access by entries in the file can access User Name mapping.
- If the .maphosts file is present but empty (the default), no computers except the computer running User Name Mapping itself can access User Name Mapping.
- If the .maphosts file is not present, no computers (including the computer running User Name Mapping) can access User Name Mapping.

The ordering of entries is important as User Name Mapping searches the .maphosts file from the top down until it finds a match.

For additional information about the .maphosts file, see the MSNFS online help.

Allowing anonymous access to resources by NFS clients

It may be desirable to add anonymous access to a share. An instance would be when it is not desirable or possible to create and map a UNIX account for every Windows user. A UNIX user whose account is not mapped to a Windows account is treated by Server for NFS as an anonymous user. By default, the user identifier (UID) and group identifier (GID) is -2.

For example, if files are created on an NFS Share by UNIX users who are not mapped to Windows users, the owner of those files are listed as anonymous user and anonymous group, (-2,-2).

By default, Server for NFS does not allow anonymous users to access a shared directory. When an NFS share is created, the anonymous access option can be added to the NFS share. The values can be changed from the default anonymous UID and GID values to the UID and GID of any valid UNIX user and group accounts.

NOTE:

In Windows Server 2003, the Everyone group does not include anonymous users by default.

When allowing anonymous access to an NFS Share, the following must be performed by a user with administrative privileges due to Windows Storage Server 2003 security with anonymous users and the Everyone group.

1. Click **Remote Desktop**. Log on to the storage server.
2. Click **Start** >**Control Panel** > **Administrative Tools**, and then click **Local Security Policy**.
3. In Security Settings, double-click **Local Policies**, and then click **Security Options**.
4. Right-click **Network access: Let Everyone permissions apply to anonymous users**, and then click **Properties**.
5. To allow permissions applied to the Everyone group to apply to anonymous users, click **Enabled**. The default is **Disabled**.
6. Restart the NFS server service. From a command prompt, enter `net stop nfssvc`. Then enter `net start nfssvc`. Notify users before restarting the NFS service.
7. Assign the Everyone group the appropriate permissions on the NFS Share.
8. Enable anonymous access to the share.

To enable anonymous access to an NFS share, do the following:

1. Open Windows Explorer by clicking **Start** > **Run**, and entering Explorer.
2. Navigate to the NFS share.
3. Right-click the NFS Share, and then click **Properties**.
4. Click **NFS Sharing**.
5. Select the **Allow Anonymous Access** checkbox.
6. Change from the default of -2,-2, if desired.
7. Click **Apply**.
8. Click **OK**.

Best practices for running Server for NFS

- Provide user-level security
- Secure files
- Secure new drives
- Allow users to disconnect before stopping the Server for NFS service
- Use naming conventions to identify shares with EUC encoding
- Protect configuration files

For further details, see the online help for Microsoft Services for Network File System.

User Name Mapping

The User Name Mapping component provides centralized user mapping services for Server for NFS and Client for NFS. User Name Mapping lets you create maps between Windows and UNIX user and group accounts even though the user and group names in both environments may not be identical. User Name Mapping lets you maintain a single mapping database making it easier to configure account mapping for multiple computers running MSNFS.

In addition to one-to-one mapping between Windows and UNIX user and group accounts, User Name Mapping permits one-to-many mapping. This lets you associate multiple Windows accounts with a single UNIX account. This can be useful, for example, when you do not need to maintain separate UNIX accounts for individuals and would rather use a few accounts to provide different classes of access permission.

You can use simple maps, which map Windows and UNIX accounts with identical names. You can also create advanced maps to associate Windows and UNIX accounts with different names, which you can use in conjunction with simple maps.

User Name Mapping can obtain UNIX user, password, and group information from one or more Network Information Service (NIS) servers or from password and group files located on a local hard drive. The password and group files can be copied from a UNIX host or from a NIS server.

User Name Mapping periodically refreshes its mapping database from the source databases, ensuring that it is always kept up-to-date as changes occur in the Windows and UNIX name spaces. You can also refresh the database anytime you know the source databases have changed.

You can back up and restore User Name Mapping data at any time. Because the database is backed up to a file, you can use that file to copy the mapping database to another server. This provides redundancy for the sake of fault tolerance.

NOTE:

If you obtain information from multiple NIS domains, it is assumed that each domain has unique users and user identifiers (UIDs). User Name Mapping does not perform any checks.

User Name Mapping associates Windows and UNIX user names for Client for NFS and Server for NFS. This allows users to connect to Network File System (NFS) resources without having to log on to UNIX and Windows systems separately.

NOTE:

Most of the functionality of User Name Mapping has been replaced by Active Directory Lookup. Active Directory Lookup enables Client for NFS and Server for NFS to obtain user identifier (UID) and group identifier (GID) information directly from Active Directory. For information about storing UNIX user data in Active Directory, see documentation for Identity Management for UNIX. For information about enabling Active Directory Lookup, see "Specifying how Server for NFS obtains Windows user and group information" available in online help.

User Name Mapping Administration

The User Name Mapping administration online help contains information for the following topics:

- Understanding the User Name Mapping component
- Starting and stopping User Name Mapping
- Configuring User Name Mapping
- Securing access to the User Name Mapping server
- Managing maps
- Managing groups

Best practices for User Name Mapping

- Install User Name Mapping on a domain controller.
- Create a User Name Mapping server pool.
- Configure User Name Mapping on a server cluster.
- Make sure User Name Mapping can download users from all domains.
- Refresh data whenever a user is added or changed.
- Place password and group files on the User Name Mapping server.
- Use appropriate permissions to protect password and group files.
- Ensure consistency of group mapping.
- Specify the computers that can access User Name Mapping.

For further details, see the online help for Microsoft Services for Network File System.

Microsoft Services for NFS troubleshooting

The following information on how to troubleshoot issues with Microsoft Services for NFS is available using the online help:

- General issues
- Troubleshooting Server for NFS
- Troubleshooting User Name Mapping

For further details, see the online help for Microsoft Services for Network File System.

Microsoft Services for NFS command-line tools

Table 8 provides a listing of Windows command-line administration tools.

Table 8 MSNFS command-line administration tools

Command	Function
mapadmin	Adds, lists, deletes, or changes user name mappings
mount	Mounts NFS network exports (shares)
nfsadmin	Manages Server for NFS and Client for NFS
nfsshare	Displays, adds, and removes exported NFS shares
nfsstat	Views statistics by NFS operation type
showmount –a	Views users who are connected and what the user currently has mounted
showmount –e	Views exports from the server and their export permissions
unmount	Removes NFS-mounted drives

For further details, see the online help for Microsoft Services for Network File System.

Optimizing Server for NFS performance

The following sources provide useful information on how to optimize performance for Microsoft Services for NFS.

The MSNFS online help covers the following topic areas:

- Adding performance counters
- Monitoring and tuning performance
- Changing the directory cache memory setting

For further details, see the online help for Microsoft Services for Network File System.

A technical paper titled *Performance Tuning Guidelines for Microsoft Services for Network File System* is available at http://www.microsoft.com/technet/interopmigration/unix/sfu/perfnfs.mspx.

Print services for UNIX

Network clients with UNIX-based operating systems that use the client program line printer remote (LPR) can send printing jobs to the line printer daemon (LPD) on the storage server. LPR clients must comply with Request for Comments (RFC) 1179. The combination of the LPR and LPD are included in print services for UNIX. Print services for UNIX is not pre-installed on the print server or the File Print Appliance.

To install print services for UNIX:

1. Log on as administrator or as a member of the Administrators group.
2. Select **Start** > **Control Panel**, and then click **Add or Remove Programs**.

3. Click **Add/Remove Windows Components**.
4. In the Components list, click **Other Network File and Print Services** (but do not select or clear the check box), and then click **Details**.
5. In the Subcomponents of Other Network File and Print Services list, select **Print Services for UNIX**, if appropriate to the print services that you want to install:

   Print Services for UNIX: This option permits UNIX clients to print to any printer that is available to the print server.

> **NOTE:**
>
> When installing Print Services for UNIX, this automatically installs the LPR port and the TCP/IP Print Server service.

6. Click **OK**, and then click **Next**.
7. Click **Finish**.

Point and print from UNIX to Windows Server 2003

Point-and-Print behavior from UNIX clients to Windows Server 2003 and Windows Storage Server 2003 is similar to the behavior for Windows 95, Windows 98, and Windows Millennium Edition clients, because all these clients create SMB connections. However, the non–Windows operating systems maintain their own driver model, so these clients do not automatically get the driver during Point and Print—they must install the driver locally. Like the Windows 95, Windows 98, and Windows Millennium clients, these non–Windows clients do not receive driver updates from the print server after a driver is initially downloaded. The same connection methods are available: drag and drop, the Add Printer Wizard, referencing a UNC path, or double-clicking the shared printer icon.

Additional resources

Consult the following resources for more information about using and configuring Print Services for UNIX:

- *How To: Install and Configure Print Services for UNIX*

  http://support.microsoft.com/kb/324078
- *How To: Install Print Services for UNIX in Windows Server 2003*

  http://support.microsoft.com/?scid=kb;en-us;323421

6 Other network file and print services

This chapter discusses file and print services for NetWare and Macintosh.

File and Print Services for NetWare (FPNW)

File and Print Services for NetWare (FPNW) is one part of the Microsoft software package called Services for NetWare. The most common use of the NetWare network operating system is as a file and print server. FPNW eases the addition of the storage server into a mixed infrastructure by providing a NetWare user interface (UI) to a Windows Storage Server 2003-based server; administrators and users see their same, familiar NetWare UI. Additionally, the same logon for clients is maintained without a need for any client configuration changes.

This service also provides the ability to create Novell volumes, which are actually NTFS shares, from which users can map drives and access resources. Novell Login scripts are supported on the storage server or through an existing NDS (Novell Directory Services) account. This requires no changes or additions to the software on the NetWare client computers.

NOTE:

FPNW is not a clusterable protocol. With FPNW on both nodes of a cluster, the shares do not fail over because the protocol is not cluster-aware.

NOTE:

IPX/SPX protocol is required on the Novell servers.

Installing Services for NetWare

The installation of FPNW on the storage server allows for a smooth integration with existing Novell servers. FPNW allows a Windows Storage Server 2003 based server to emulate a NetWare file and print server to users, clients, and administrators. This emulation allows authentication from Novell clients, the use of Novel logon scripts, the creation of Novell volumes (shares), the use of Novell file attributes, and many other Novell features.

Information on Microsoft Directory Synchronization Services and the File Migration Utility can be found at

http://www.microsoft.com/WINDOWS2003/guide/server/solutions/NetWare.asp

To install Services for NetWare:

1. From the desktop of the storage server, select **Start** > **Settings** > **Network Connections > Local Area Connection**, and then right-click **Properties**.
2. Click **Install**.

   The **Select Network Component Type** dialog box is displayed.
3. Click **Service**, and then click **Add**.
4. Click the **Have Disk** icon, and then navigate to the location of **Services for NetWare**.

   Services for NetWare is located in the path: *c:\hpnas\components/SFN5.02/fpnw/netsfn.inf*.

5. Select the NETSFNTSRV file, and then click **OK**.

   File and Print Services for NetWare should now be displayed as an option to install.

6. Select **File and Print Services for NetWare**, and then click **OK**.

Managing File and Print Services for NetWare

FPNW resources are managed through Server Manager. Server Manager can be used to modify FPNW properties and manager shared volumes.

Use File and Print Services for NetWare to:

- Access files, modify file settings and permissions from Computer Management, and use third party tools that can be used with NetWare servers.
- Create and manage user accounts by using Active Directory Users and Computers.
- Perform secured log-ons.
- Support packet burst and Large Internet Packet (LIP).
- Support NetWare locking and synchronization primitives that are used by some NetWare-specific applications.
- Support long file names, compatible with OS/2 long file name (LFN) support.

File and Print Services for NetWare does not support the following NetWare groups and functions:

- Workgroup Managers
- Accounting
- User disk volume restrictions
- Setting Inherited Rights Masks (IRMs)
- NetWare loadable modules
- Transaction Tracking System (TTS)

To access File and Print Services:

To access FPNW:

1. From the desktop of the storage server, select **Start** > **Settings** > **Control Panel > Administrative Tools > Server Manager**.
2. Select **FPNW**, and then click **Properties**.

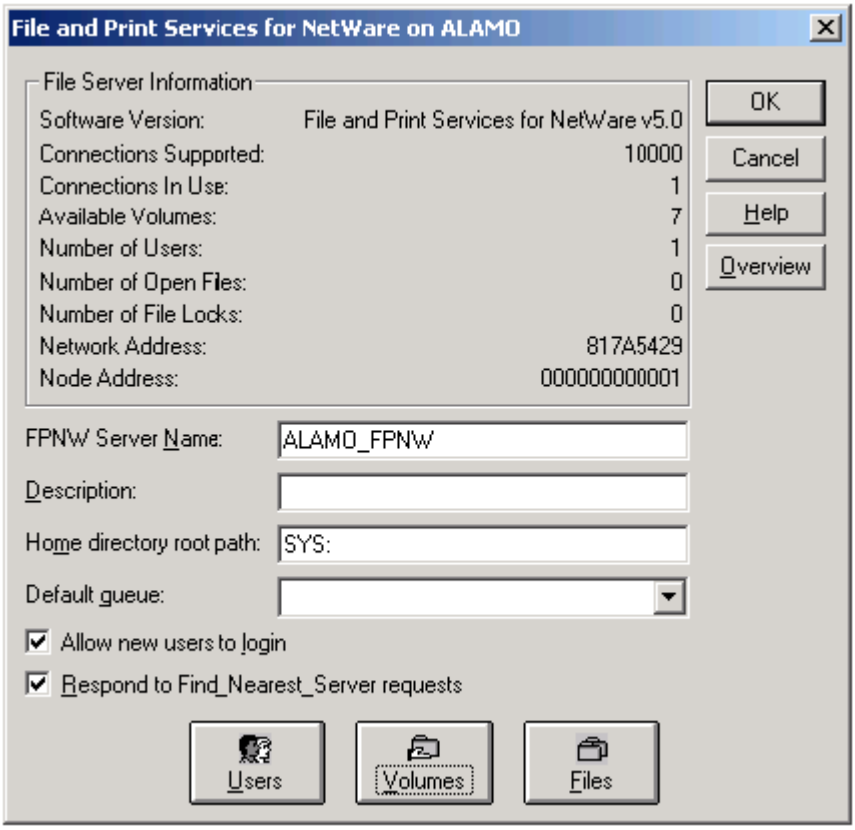


Figure 22 File and Print Services for NetWare dialog box

3. Enter an FPNW Server Name and Description.

   This server name must be different from the server name used by Windows or LAN Manager-based clients. If changing an existing name, the new name is not effective until stopping and restarting FPNW. For example, in Figure 22 the Windows server name is Alamo and the FPNW server name is Alamo_FPNW.

4. Indicate a Home directory root path.

   This path is relative to where the Sysvol volume is installed. This is the root location for the individual home directories. If the directory specified does not already exist, it must first be created.

5. Click **Users** to:

   See connected users, disconnect users, send broadcast messages to all users connected to the server, and to send a message to a specific user.

6. Click **Volumes** to:

   See users connected to specific volume and to disconnect users from a specific volume.

7. Click **Files** to:

   View open files and close open files.

Creating and managing NetWare users

To use Services for NetWare, the Novell clients must be entered as local users on the storage server.

Adding local NetWare users

1. From the storage server desktop, click the **Management Console** icon, click **Core Operating System**, and then click **Local Users and Groups**.

2. Right-click the **Users** folder, and then click **New User**.

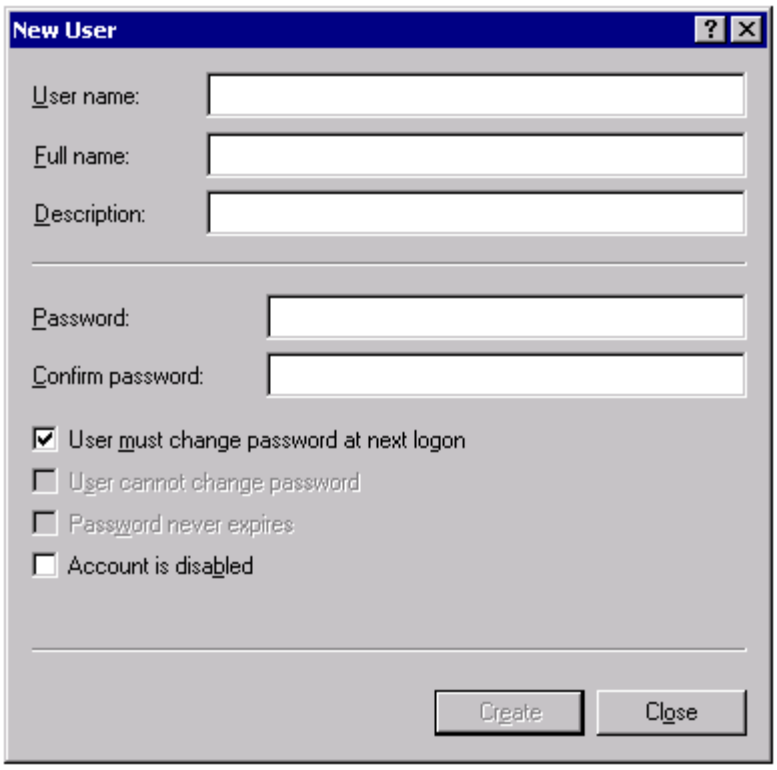


Figure 23 New User dialog box

3. Enter the user information, including the user's User name, Full name, Description, and Password.
4. Click **Create**.
5. Repeat these steps until all NetWare users have been entered.

Enabling local NetWare user accounts

1. In the **Users** folder (MC, Core Operating System, Local Users and Groups), right-click an NCP client listed in the right pane of the screen, and then click **Properties**.
2. Click the **NetWare Services** tab.

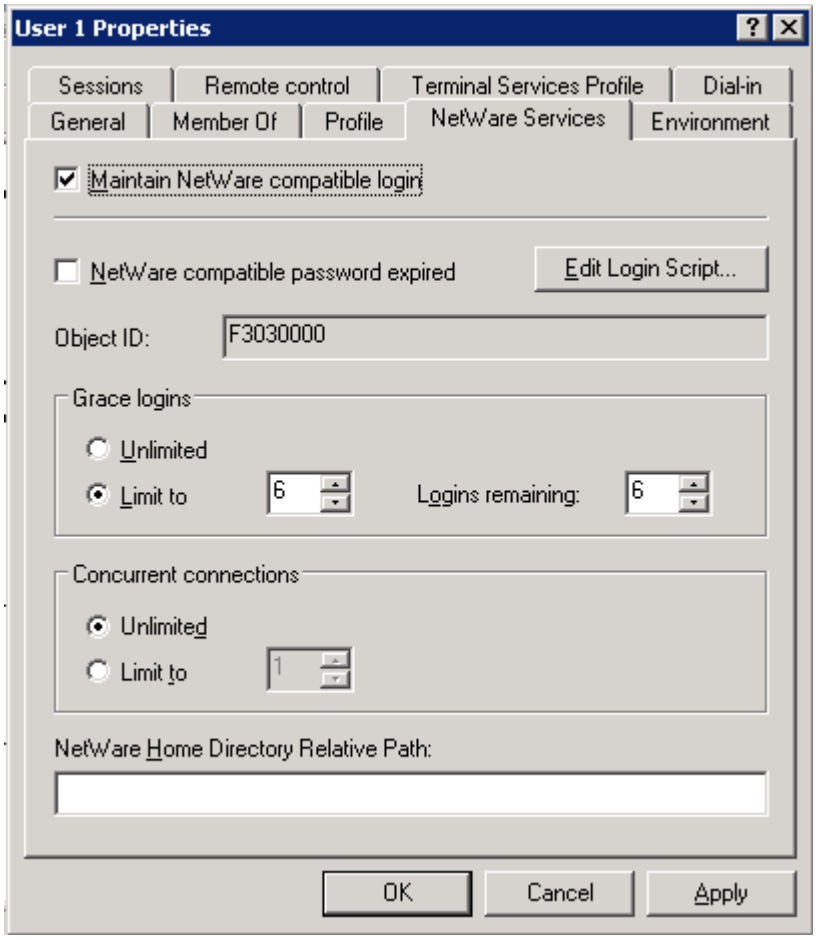


Figure 24 NetWare Services tab

3. Select **Maintain NetWare compatible login**.
4. Set other NetWare options for the user, and then click **OK**.

NOTE:

The installation of File and Print Services for NetWare also creates a supervisor account, which is used to manage FPNW. The supervisor account is required if the storage server was added as a bindery object into NDS.

Managing NCP volumes (shares)

NCP file shares are created the same way as other file shares; however, there are some unique settings. NCP shares can be created and managed using Server Manager.

NOTE:

NCP shares can be created only after FPNW is installed. See the previous section "Installing Services for Netware" for instructions on installing FPNW.

Creating a new NCP share

To create a new file share:

1. From the storage server desktop, select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Server Manager**.
2. Select **File and Print Service for NetWare**> **Shared Volumes**.
3. Click **Create Volume**.
4. Specify the volume name and path.
5. Click **Permissions** to set permissions.
6. Click **Add** to add additional users and groups, and to set their permissions.
7. Highlight the desired user or group, and then click **Add**.
8. Select the Type of Access in the drop down list.

   Type of Access can also be set from the Access Through Share Permissions dialog box.
9. Click **OK** when all users and groups have been added.
10. Click **OK** in the **Create Volume** dialog box.
11. Click **Close**.

Modifying NCP share properties

To modify a file share:

1. From the storage server desktop, select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Server Manager**.
2. Select **File and Print Services for NetWare** > **Shared Volumes**.
3. Highlight the volume to modify.
4. Click **Properties**.

Print Services for NetWare

With File and Print Services for NetWare installed, the print server or File Print Appliance appears to a NetWare client as a NetWare 3.x–compatible print server. Print services presents the same dialog boxes to the client as a NetWare-based server uses to process a print job from a client. A user can display and search for printers on the print server or File Print Appliance just like in a NetWare environment.

Installing Print Services for NetWare

Refer to the previous section "Installing Services for Netware" for information on installing Print Services for NetWare.

Point and Print from Novell to Windows Server 2003

Point-and-Print behavior from Novell clients to Windows Server 2003 and Windows Storage Server 2003 is similar to the behavior for Windows 95, Windows 98, and Windows Millennium Edition clients, because all these clients create SMB connections. However, the non–Windows operating systems maintain their own driver model, so these clients do not automatically get the driver during Point and Print—they must install the driver locally. Like the Windows 95, Windows 98, and Windows Millennium clients, these non–Windows clients do not receive driver updates from the print server after a driver is initially downloaded. The same connection methods are available: drag and drop, the Add Printer Wizard, referencing a UNC path, or double-clicking the shared printer icon.

Additional resources

For more information about using and configuring File and Print Services for NetWare, refer to the online help.

AppleTalk and file services for Macintosh

The AppleTalk network integration allows the storage server to share files and printers between your server and any Apple Macintosh clients that are connected to your network. After installing Microsoft Windows Services for Macintosh, the administrator can use the AppleTalk protocol to configure the storage server to act as an AppleTalk server. The AppleTalk protocol is the communications protocol used by clients running a Macintosh operating system. The Macintosh computers need only the Macintosh OS software to function as clients; no additional software is required.

AppleTalk network integration simplifies administration by maintaining just one set of user accounts instead of separate user accounts, for example, one on the Macintosh server and another on the computer running Windows server software.

Installing the AppleTalk protocol

1. From the desktop of the storage server, select **Start > Settings > Network Connections**. Right-click **Local Area Connection**, and then click **Properties**.
2. Click **Install**.
3. Select **Protocol**, and then click **Add**.
4. Select **AppleTalk Protocol**, and then click **OK**.

Installing File Services for Macintosh

To install File Services for Macintosh, perform the following steps:

1. Access the desktop on the storage server.
2. Open **Add or Remove Programs** from the Control Panel.
3. Click **Add or Remove Windows Components**.
4. Double-click **Other Network File and Print Services**.
5. Select **File Services for Macintosh**, and then click **OK**.
6. Click **Next**.
7. Click **Finish**.

Completing setup of AppleTalk protocol and shares

See the online help to complete the following set up and configurations tasks:

- To set up AppleTalk protocol properties

  AppleTalk shares can be set up only after AppleTalk Protocol and File Services for Macintosh have been installed on the storage server.

△ **CAUTION:**

AppleTalk shares should not be created on clustered resources because data loss can occur due to local memory use.

- To set up AppleTalk shares
- To configure AppleTalk sharing properties
- To allow client permission to an AppleTalk share

  If AppleTalk is enabled for your server configuration, specify which AppleTalk clients are granted access to each share. Access can be granted or denied on the basis of client host name. Access can also be granted or denied on the basis of client groups, where a client group contains one or more client host names.

Print services for Macintosh

Macintosh clients can send print jobs to a print server or File Print Appliance (FPA) when Print Server for Macintosh is installed on the server. To the Macintosh-based client, the print server or FPA appears to be an AppleTalk printer on the network, and no reconfiguration of the client is necessary.

Installing Print Services for Macintosh

Consult the following resource for information about installing Print Services for Macintosh:

- *How To: Install Print Services for Macintosh in Windows Server 2003*

  http://support.microsoft.com/?scid=kb;en-us;323421

Point and Print from Macintosh to Windows Server 2003

Point-and-Print behavior from Macintosh clients to Windows Server 2003 or Windows Storage Server 2003 is similar to the behavior for Windows 95, Windows 98, and Windows Millennium Edition clients, because all these clients create SMB connections. However, the non-Windows operating systems maintain their own driver model, so these clients do not automatically get the driver during Point and Print—they must install the driver locally. Like the Windows 95, Windows 98, and Windows Millennium clients, these non-Windows clients do not receive driver updates from the print server after a driver is initially downloaded. The same connection methods are available: drag and drop, the Add Printer Wizard, referencing a UNC path, or double-clicking the shared printer icon.

7 Troubleshooting, servicing, and maintenance

Troubleshooting the storage server

The "Support and troubleshooting" task at the HP Support & Drivers web site (http://www.hp.com/go/support) can be used to troubleshoot problems with the storage server. After entering the storage server name and designation (for example,ML310 storage server) or component information (for example, Array Configuration Utility), use the following links for troubleshooting information:

- Download drivers and software—This area provides drivers and software for your operating system.
- Troubleshoot a problem—This area provides a listing of customer notices, advisories and bulletins applicable for the product or component.
- Manuals—This area provides the latest user documentation applicable to the product or component. User guides can be a useful source for troubleshooting information. For most storage server hardware platforms, the following ProLiant server manuals may be useful for troubleshooting assistance:
  - **HP ProLiant <model> Server User Guide or HP ProLiant <model> Server Maintenance and Service Guide** (where <model> is the product model of the storage server, such as ML310).

    These guides contain specific troubleshooting information for the server. The guides are available by selecting the applicable ProLiant Server series model, then the Manuals (guides, supplements, addendums, etc) link.

    For example, instead of using "ML310 storage server", enter "ML310 server" for the product to search, then select the "HP ProLiant ML310 Server series" link, then the Manuals (guides, supplements, addendums, etc.) link to locate the guide.
  - **HP ProLiant Servers Troubleshooting Guide**

    The guide provides common procedures and solutions for many levels of troubleshooting with a ProLiant server. The guide is available at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00300504/c00300504.pdf.

IMPORTANT:

Not all troubleshooting procedures found in ProLiant server guides may apply to the ProLiant Storage Server. If necessary, check with your HP Support representative for further assistance.

For software related components and issues, online help or user guide documentation may offer troubleshooting assistance. The Release Notes for the storage server product line is updated frequently. The document contains issues and workarounds to a number of categories for the storage servers.

Known issues and workarounds for the storage server products and the service release are addressed in release notes. To view the latest release notes, go to http://www.hp.com/support/manuals. Under the storage section, click **NAS** and then select your product.

Maintenance and service

HP provides specific documentation for maintaining and servicing your storage server and offers a customer self-repair program.

Maintenance and service documentation

For specific documentation for the maintenance and servicing of HP ProLiant storage servers, refer to the *HP ProLiant <model> Server Maintenance and Service Guide* for your storage server model. This document can be obtained at http://www.hp.com/support/manuals. Under the servers section, select **ProLiant and tc series servers**, and then select your product.

Maintenance updates

Regular updates to the storage server or File Print Appliance are supplied on the HP ProLiant Storage Server Service Release DVD. The Service Release DVD can be obtained at http://www.software.hp.com.

Individual updates for each product are available for download from the HP Support web site at http://www.hp.com/go/support.

System updates

System updates to the hardware (BIOS, firmware, drivers), critical updates, and hotfixes for the operating system and other related software updates are bundled on the Service Release DVD.

NOTE:

For recommendations, instructions, and documentation to help manage the software update, hotfix, and security patches process on storage servers and File Print Appliances, see Microsoft Software Updates on HP ProLiant Storage Servers at http://h18006.www1.hp.com/storage/storageservers.htm.

Customer self repair

HP's customer self-repair program offers you the fastest service under either warranty or contract. It enables HP to ship replacement parts directly to you so that you can replace them. Using this program, you can replace parts at your own convenience.

This convenient, easy-to-use program:

- Lets an HP support specialist diagnose and access whether a replacement part is required to address a system problem. the specialist also determines whether you can replace the part.
- Provides replacement parts that are express-shipped. Most in-stock parts are shipped the very same day you contact HP. You may be required to send the defective part back to HP, unless otherwise instructed.
- Is available for most HP products currently under warranty or contract. For information on the warranty service, refer to the HP website http://h18004.www1.hp.com/products/servers/platforms/warranty/index.html.

For more information about HP's customer self-repair program, contact your local service provider. For the North American program, refer to the HP website http://www.hp.com.go/selfrepair.

Firmware updates

Firmware is software that is stored in Read-Only Memory (ROM). Firmware is responsible for the behavior of the system when it is first switched on and for passing control of the server to the operating system. When referring to the firmware on the system board of the server, it is called the System ROM or the BIOS. When referring to the firmware on another piece of hardware configured in the server, it is called Option ROM. ProLiant servers have hard drives, Smart Array Controllers, Remote Insight Lights-Out Edition (RILOE), Remote Insight Lights-Out Edition II (RILOE II) and Integrated Lights-Out options that have firmware that can be updated.

It is important to update the firmware (also called "flashing the ROM") as part of regular server maintenance. In addition, checking for specific firmware updates in between regular updates helps to

keep the server performing optimally. HP recommends checking for a firmware update before sending a part back to HP for replacement.

Certificate of Authenticity

The Certificate of Authenticity (COA) label is used to:

- Upgrade the factory-installed operating system using the Microsoft Upgrade program for license validation.
- Reinstall the operating system because of a failure that has permanently disabled it.

The COA label location varies by server model. On rack-mounted server models, the COA label is located either on the front section of the right panel or on the right front corner of the top panel. On tower models, the COA label is located toward the rear of the top panel of the server.

8 System installation and recovery

This chapter describes how to use the Installation and Recovery DVD that is provided with your storage server.

The Installation and Recovery DVD

The HP ProLiant Storage Server System Installation and Recovery DVD that is provided with your storage server allows you to install an image or recover from a catastrophic failure. The DVD is used initially to install and configure the operating system and applications provided with your storage server.

At any later time, you may boot from the DVD and restore the server to the factory condition. This allows you to recover the system if all other means to boot the server fails.

While the recovery process makes every attempt to preserve the existing data volumes, you should have a backup of your data if at all possible before recovering the system.

To restore a factory image

1. Insert the System Installation and Recovery DVD. The main window appears.
2. Choose **Restore Factory Image**.

Systems with a DON'T ERASE partition

The DON'T ERASE logical disk supports the restoration process only and does not host a secondary operating system. Be sure to back up your user data, and then use the Recovery and Installation DVD to restore the server to the factory state.

Managing disks after a restoration

After a system has been restored, drive letters may be assigned to the wrong volume. Windows Storage Server 2003 assigns drive letters after the restoration in the order of discovery. To help maintain drive letter information, placing the drive letter into a volume label is recommended. To change the drive letters to the appropriate one, go into Disk Management and perform the following steps for each volume:

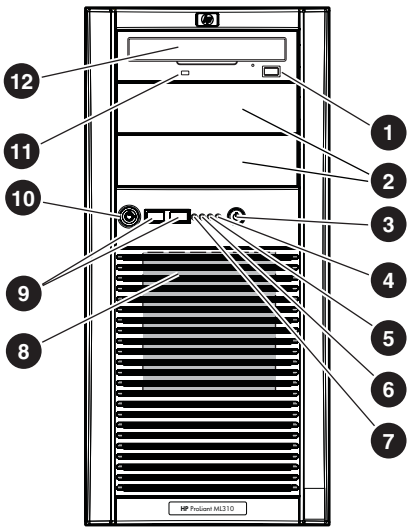
1. Right-click the volume that needs to be changed.
2. Select **Change drive Letter and Paths**.
3. In the **Change drive Letter and Paths** dialog box, select **Change**.
4. Select the appropriate drive letter an click **OK**.
5. Click **Yes** to confirm the drive letter change.
6. Click **Yes** to continue. If the old drive letter needs to be reused, reboot the server after clicking Yes.

A Server components

This appendix provides illustrations of the storage server hardware components.

ML310 hardware components

The following figures show components, controls, and indicators located on the front and rear panels of the ML310 storage server.

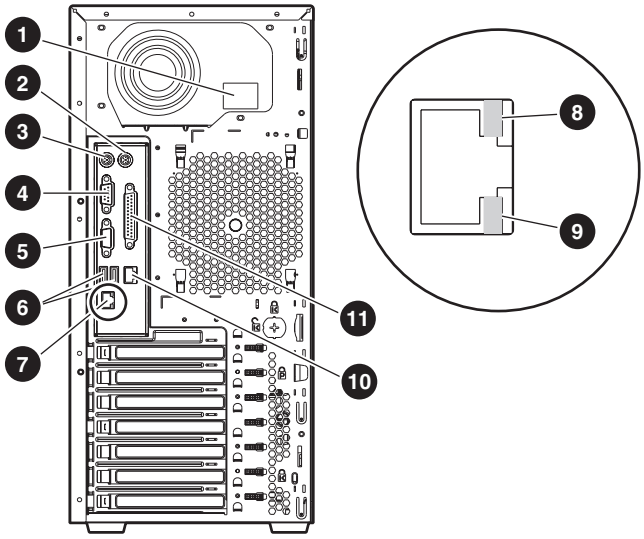


5081

Figure 25 Front panel

Table 9 Front panel components

Item	Description	Status
1	DVD-RW drive ejector button	N/A
2	Media bays (bezel blanks)	N/A
3	Power On/Standby button	N/A
4	System power LED	Amber = System has AC power and is in standby mode Green = System has AC power and is functioning Off = System has no AC power
5	Hard drive activity LED	Green = Hard drives are properly connected and functioning Off = No hard drive activity
6	NIC link/activity LED	Green = Linked to network Flashing green = Linked with activity on the network Off = No network connection
7	Internal system health LED	Green = Normal (system on) Amber = System health is degraded Red = System health is critical Off = Normal (system off)
8	Hard drive bays	N/A
9	USB connectors (2)	N/A
10	Bezel lock	N/A
11	DVD-RW drive indicator LED	On = Activity Off = No activity
12	DVD-RW drive	N/A



5082

Figure 26 Rear panel

Table 10 Rear panel components

Item	Description
1	Power supply connector
2	Mouse connector
3	Keyboard connector
4	Serial connector
5	Video connector
6	USB connectors (2)
7	RJ-45 Ethernet connector
8	NIC activity LED (Flashing = Activity, Off = No activity)
9	NIC link LED (On = Link, Off = No link)
10	RJ-45 connector (iLO 2)
11	Parallel connector

NOTE:

Connecting the power cord illuminates the LEDs on the front of the bezel, the Systems Insight Display LED, and the LEDs on the NIC connector (rear panel). The iLO 2 NIC LED (rear panel) illuminates if the iLO 2 port is connected. Connecting the power cord also restores the storage server to whatever previous powered state it was last in. This could result in the server powering up, the fans operating, and the power indicator coming on.

NOTE:

The keyboard, mouse, and monitor are used only for the "Direct attach method" on page 19. They are not provided with your storage server.

B Configuring storage server for Web access (optional)

Setting up an Internet connection

Before running Windows 2003 R2 operating system updates, you must set up an Internet connection for the storage server. There are two methods for configuring an Internet connection:

- Internet Explorer to use automatic configuration
- Internet Explorer to use a proxy server

To configure Internet Explorer to use automatic configuration

1. On the **Tools** menu in Internet Explorer, click **Internet Options**, click the **Connections** tab, and then click **LAN Settings**.
2. Under **Automatic Configuration**, click either the **Automatically detect settings** or **Use automatic configuration script** check box.

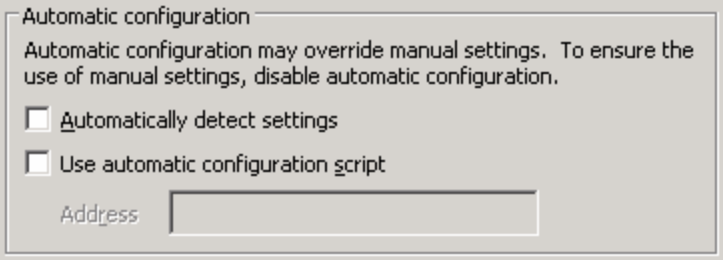


Figure 27 Automatic configuration settings

3. Click **OK** to close the **LAN Settings** dialog box.
4. Click **OK** again to close the **Internet Options** dialog box.

To configure Internet Explorer to use a proxy server

1. On the **Tools** menu in Internet Explorer, click **Internet Options**, click the **Connections** tab, and then click **LAN Settings**.
2. Under **Proxy server**, click the **Use a proxy server for your LAN** check box.



Figure 28 Proxy server settings

3. In the **Address** box, type the network name or IP address of the proxy server.
4. In the **Port** box, type the port number that is used by the proxy server for client connections (for example, 8080).

5. Click the **Bypass proxy server for local addresses** check box if you do not want the proxy server computer to be used when you connect to a computer on the local network.
6. Click **OK** to close the **LAN Settings** dialog box.
7. Click **OK** again to close the **Internet Options** dialog box.

C Regulatory compliance and safety

Federal Communications Commission notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (personal computers, for example). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows which class (A or B) the equipment falls into. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. Once the class of the device is determined, refer to the following corresponding statement.

Class A equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Declaration of conformity for products marked with the FCC logo, United States only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact:

Hewlett-Packard Company

P. O. Box 692000, Mail Stop 530113

Houston, Texas 77269-2000

Or, call

1-800- 652-6672

For questions regarding this FCC declaration, contact:

Hewlett-Packard Company

P. O. Box 692000, Mail Stop 510101

Houston, Texas 77269-2000

Or, call

(281) 514-3333

To identify this product, refer to the Part, Series, or Model number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Laser compliance

This product may be provided with an optical storage device (that is, CD or DVD drive) and/or fiber optic transceiver. Each of these devices contains a laser that is classified as a Class 1 Laser Product in accordance with US FDA regulations and the IEC 60825–1. The product does not emit hazardous laser radiation.

⚠ **WARNING!**

Use of controls or adjustments or performance of procedures other than those specified herein or in the installation guide of the laser product may result in hazardous radiation exposure. To reduce the risk of exposure to hazardous radiation:

- Do not try to open the module enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP authorized service technicians to repair the unit.

The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

International notices and statements

Canadian notice (Avis Canadien)

Class A equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union notice

CE Products bearing the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community and if this product has telecommunication functionality, the R&TTE Directive (1999/5/EC).

Compliance with these directives implies conformity to the following European Norms (in parentheses are the equivalent international standards and regulations):

- EN 55022 (CISPR 22) - Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11) - Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2) - Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3) - Power Line Flicker
- EN 60950 (IEC 60950) - Product Safety

BSMI notice

警告使用者:

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japanese notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean notice A&B

Class A equipment

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Class B equipment

B급 기기 (가정용 정보통신기기)

이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든지역에서 사용할 수 있습니다.

Safety

Battery replacement notice

⚠ **WARNING!**

The computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. A risk of fire and burns exists if the battery pack is not properly handled. To reduce the risk of personal injury:

- Do not attempt to recharge the battery.
- Do not expose the battery to temperatures higher than 60°C (140°F).
- Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.



Batteries, battery packs, and accumulators should not be disposed of together with the general household waste. To forward them to recycling or proper disposal, please use the public collection system or return them to HP, an authorized HP Partner, or their agents.

For more information about battery replacement or proper disposal, contact an authorized reseller or an authorized service provider.

Taiwan battery recycling notice



The Taiwan EPA requires dry battery manufacturing or importing firms in accordance with Article 15 of the Waste Disposal Act to indicate the recovery marks on the batteries used in sales, giveaway or promotion. Contact a qualified Taiwanese recycler for proper battery disposal.

Power cords

The power cord set must meet the requirements for use in the country where the product was purchased. If the product is to be used in another country, purchase a power cord that is approved for use in that country.

The power cord must be rated for the product and for the voltage and current marked on the product electrical rating label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product. In addition, the diameter of the wire must be a minimum of 1.00 mm^2 or 18 AWG, and the length of the cord must be between 1.8 m (6 ft) and 3.6 m (12 ft). If you have questions about the type of power cord to use, contact an HP authorized service provider.

NOTE:

Route power cords so that they will not be walked on and cannot be pinched by items placed upon or against them. Pay particular attention to the plug, electrical outlet, and the point where the cords exit from the product.

Japanese power cord notice

製品には、同梱された電源コードをお使い下さい。
同梱された電源コードは、他の製品では使用出来ません。

Electrostatic discharge

To prevent damage to the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

Preventing electrostatic discharge

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper grounding, wear the strap snug against the skin.

- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

NOTE:

For more information on static electricity, or for assistance with product installation, contact your authorized reseller.

Waste Electrical and Electronic Equipment (WEEE) directive

Czechoslovakian notice

Likvidace zařízení soukromými domácími uživateli v Evropské unii



Tento symbol na produktu nebo balení označuje výrobek, který nesmí být vyhozen spolu s ostatním domácím odpadem. Povinností uživatele je předat takto označený odpad na předem určené sběrné místo pro recyklaci elektrických a elektronických zařízení. Okamžité třídění a recyklace odpadu pomůže uchovat přírodní prostředí a zajistí takový způsob recyklace, který ochrání zdraví a životní prostředí člověka. Další informace o možnostech odevzdání odpadu k recyklaci získáte na příslušném obecním nebo městském úřadě, od firmy zabývající se sběrem a svozem odpadu nebo v obchodě, kde jste produkt zakoupili.

Danish notice

Bortskaffelse af affald fra husstande i den Europæiske Union



Hvis produktet eller dets emballage er forsynet med dette symbol, angiver det, at produktet ikke må bortskaffes med andet almindeligt husholdningsaffald. I stedet er det dit ansvar at bortskaffe kasseret udstyr ved at aflevere det på den kommunale genbrugsstation, der forestår genvinding af kasseret elektrisk og elektronisk udstyr. Den centrale modtagelse og genvinding af kasseret udstyr i forbindelse med bortskaffelsen bidrager til bevarelse af naturlige ressourcer og sikrer, at udstyret genvindes på en måde, der beskytter både mennesker og miljø. Yderligere oplysninger om, hvor du kan aflevere kasseret udstyr til genvinding, kan du få hos kommunen, den lokale genbrugsstation eller i den butik, hvor du købte produktet.

Dutch notice

Verwijdering van afgedankte apparatuur door privé-gebruikers in de Europese Unie



Dit symbool op het product of de verpakking geeft aan dat dit product niet mag worden gedeponeerd bij het normale huishoudelijke afval. U bent zelf verantwoordelijk voor het inleveren van uw afgedankte apparatuur bij een inzamelingspunt voor het recyclen van oude elektrische en elektronische apparatuur. Door uw oude apparatuur apart aan te bieden en te recyclen, kunnen natuurlijke bronnen worden behouden en kan het materiaal worden hergebruikt op een manier waarmee de volksgezondheid en het milieu worden beschermd. Neem contact op met uw gemeente, het afvalinzamelingsbedrijf of

de winkel waar u het product hebt gekocht voor meer informatie over inzamelingspunten waar u oude apparatuur kunt aanbieden voor recycling.

English notice

Disposal of waste equipment by users in private household in the European Union



This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service, or the shop where you purchased the product.

Estonian notice

Seadmete jäätmete kõrvaldamine eramajapidamistes Euroopa Liidus



See tootel või selle pakendil olev sümbol näitab, et kõnealust toodet ei tohi koos teiste majapidamisjäätmetega kõrvaldada. Teie kohus on oma seadmete jäätmed kõrvaldada, viies need elektri- ja elektroonikaseadmete jäätmete ringlussevõtmiseks selleks ettenähtud kogumispunkti. Seadmete jäätmete eraldi kogumine ja ringlussevõtmine kõrvaldamise ajal aitab kaitsta loodusvarasid ning tagada, et ringlussevõtmine toimub viisil, mis kaitseb inimeste tervist ning keskkonda. Lisateabe saamiseks selle kohta, kuhu oma seadmete jäätmed ringlussevõtmiseks viia, võtke palun ühendust oma kohaliku linnakantselei, majapidamisjäätmete kõrvaldamise teenistuse või kauplusega, kust Te toote ostsite.

Finnish notice

Laitteiden hävittäminen kotitalouksissa Euroopan unionin alueella



Jos tuotteessa tai sen pakkauksessa on tämä merkki, tuotetta ei saa hävittää kotitalousjätteiden mukana. Tällöin hävitettävä laite on toimitettava sähkölaitteiden ja elektronisten laitteiden kierrätyspisteeseen. Hävitettävien laitteiden erillinen käsittely ja kierrätys auttavat säästämään luonnonvaroja ja varmistamaan, että laite kierrätetään tavalla, joka estää terveyshaitat ja suojelee luontoa. Lisätietoja paikoista, joihin hävitettävät laitteet voi toimittaa kierrätettäväksi, saa ottamalla yhteyttä jätehuoltoon tai liikkeeseen, josta tuote on ostettu.

French notice

Élimination des appareils mis au rebut par les ménages dans l'Union européenne



Le symbole apposé sur ce produit ou sur son emballage indique que ce produit ne doit pas être jeté avec les déchets ménagers ordinaires. Il est de votre responsabilité de mettre au rebut vos appareils en les déposant dans les centres de collecte publique désignés pour le recyclage des équipements électriques et électroniques. La collecte et le recyclage de vos appareils mis au rebut indépendamment du reste des déchets contribue à la préservation des ressources naturelles et garantit que ces appareils seront recyclés dans le respect de la santé humaine et de l'environnement. Pour obtenir plus d'informations sur les centres de collecte et de recyclage des appareils mis au rebut, veuillez contacter les autorités

locales de votre région, les services de collecte des ordures ménagères ou le magasin dans lequel vous avez acheté ce produit.

German notice

Entsorgung von Altgeräten aus privaten Haushalten in der EU



Das Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass das Produkt nicht über den normalen Hausmüll entsorgt werden darf. Benutzer sind verpflichtet, die Altgeräte an einer Rücknahmestelle für Elektro- und Elektronik-Altgeräte abzugeben. Die getrennte Sammlung und ordnungsgemäße Entsorgung Ihrer Altgeräte trägt zur Erhaltung der natürlichen Ressourcen bei und garantiert eine Wiederverwertung, die die Gesundheit des Menschen und die Umwelt schützt. Informationen dazu, wo Sie Rücknahmestellen für Ihre Altgeräte finden, erhalten Sie bei Ihrer Stadtverwaltung, den örtlichen Müllentsorgungsbetrieben oder im Geschäft, in dem Sie das Gerät erworben haben.

Greek notice

Απόρριψη άχρηστου εξοπλισμού από χρήστες σε ιδιωτικά νοικοκυριά στην Ευρωπαϊκή Ένωση



Το σύμβολο αυτό στο προϊόν ή τη συσκευασία του υποδεικνύει ότι το συγκεκριμένο προϊόν δεν πρέπει να διατίθεται μαζί με τα άλλα οικιακά σας απορρίμματα. Αντίθετα, είναι δική σας ευθύνη να απορρίψετε τον άχρηστο εξοπλισμό σας παραδίδοντάς τον σε καθορισμένο σημείο συλλογής για την ανακύκλωση άχρηστου ηλεκτρικού και ηλεκτρονικού εξοπλισμού. Η ξεχωριστή συλλογή και ανακύκλωση του άχρηστου εξοπλισμού σας κατά την απόρριψη θα συμβάλει στη διατήρηση των φυσικών πόρων και θα διασφαλίσει ότι η ανακύκλωση γίνεται με τρόπο που προστατεύει την ανθρώπινη υγεία και το περιβάλλον. Για περισσότερες πληροφορίες σχετικά με το πού μπορείτε να παραδώσετε τον άχρηστο εξοπλισμό σας για ανακύκλωση, επικοινωνήστε με το αρμόδιο τοπικό γραφείο, την τοπική υπηρεσία διάθεσης οικιακών απορριμμάτων ή το κατάστημα όπου αγοράσατε το προϊόν.

Hungarian notice

Készülékek magánháztartásban történő selejtezése az Európai Unió területén



A készüléken, illetve a készülék csomagolásán látható azonos szimbólum annak jelzésére szolgál, hogy a készülék a selejtezés során az egyéb háztartási hulladéktól eltérő módon kezelendő. A vásárló a hulladékká vált készüléket köteles a kijelölt gyűjtőhelyre szállítani az elektromos és elektronikai készülékek újrahasznosítása céljából. A hulladékká vált készülékek selejtezéskori begyűjtése és újrahasznosítása hozzájárul a természeti erőforrások megőrzéséhez, valamint biztosítja a selejtezett termékek környezetre és emberi egészségre nézve biztonságos feldolgozását. A begyűjtés pontos helyéről bővebb tájékoztatást a lakhelye szerint illetékes önkormányzattól, az illetékes szemételtakarító vállalattól, illetve a terméket elárusító helyen kaphat.

Italian notice

Smaltimento delle apparecchiature da parte di privati nel territorio dell'Unione Europea



Questo simbolo presente sul prodotto o sulla sua confezione indica che il prodotto non può essere smaltito insieme ai rifiuti domestici. È responsabilità dell'utente smaltire le apparecchiature consegnandole presso un punto di raccolta designato al riciclo e allo smaltimento di apparecchiature

elettriche ed elettroniche. La raccolta differenziata e il corretto riciclo delle apparecchiature da smaltire permette di proteggere la salute degli individui e l'ecosistema. Per ulteriori informazioni relative ai punti di raccolta delle apparecchiature, contattare l'ente locale per lo smaltimento dei rifiuti, oppure il negozio presso il quale è stato acquistato il prodotto.

Latvian notice

Nolietotu iekārtu iznīcināšanas noteikumi lietotājiem Eiropas Savienības privātajās mājsaimniecībās



Šāds simbols uz izstrādājuma vai uz tā iesaiņojuma norāda, ka šo izstrādājumu nedrīkst izmest kopā ar citiem sadzīves atkritumiem. Jūs atbildat par to, lai nolietotās iekārtas tiktu nodotas speciāli iekārtotos punktos, kas paredzēti izmantoto elektrisko un elektronisko iekārtu savākšanai otrreizējai pārstrādei. Atsevišķa nolietoto iekārtu savākšana un otrreizējā pārstrāde palīdzēs saglabāt dabas resursus un garantēs, ka šīs iekārtas tiks otrreizēji pārstrādātas tādā veidā, lai pasargātu vidi un cilvēku veselību. Lai uzzinātu, kur nolietotās iekārtas var izmest otrreizējai pārstrādei, jāvēršas savas dzīves vietas pašvaldībā, sadzīves atkritumu savākšanas dienestā vai veikalā, kurā izstrādājums tika nopirkts.

Lithuanian notice

Vartotojų iš privačių namų ūkių įrangos atliekų šalinimas Europos Sąjungoje



Šis simbolis ant gaminio arba jo pakuotės rodo, kad šio gaminio šalinti kartu su kitomis namų ūkio atliekomis negalima. Šalintinas įrangos atliekas privalote pristatyti į specialią surinkimo vietą elektros ir elektroninės įrangos atliekoms perdirbti. Atskirai surenkamos ir perdirbamos šalintinos įrangos atliekos padės saugoti gamtinius išteklius ir užtikrinti, kad jos bus perdirbtos tokiu būdu, kuris nekenkia žmonių sveikatai ir aplinkai. Jeigu norite sužinoti daugiau apie tai, kur galima pristatyti perdirbtinas įrangos atliekas, kreipkitės į savo seniūniją, namų ūkio atliekų šalinimo tarnybą arba parduotuvę, kurioje įsigijote gaminį.

Polish notice

Pozbywanie się zużytego sprzętu przez użytkowników w prywatnych gospodarstwach domowych w Unii Europejskiej



Ten symbol na produkcie lub jego opakowaniu oznacza, że produktu nie wolno wyrzucać do zwykłych pojemników na śmieci. Obowiązkiem użytkownika jest przekazanie zużytego sprzętu do wyznaczonego punktu zbiórki w celu recyklingu odpadów powstałych ze sprzętu elektrycznego i elektronicznego. Osobna zbiórka oraz recykling zużytego sprzętu pomogą w ochronie zasobów naturalnych i zapewnią ponowne wprowadzenie go do obiegu w sposób chroniący zdrowie człowieka i środowisko. Aby uzyskać więcej informacji o tym, gdzie można przekazać zużyty sprzęt do recyklingu, należy się skontaktować z urzędem miasta, zakładem gospodarki odpadami lub sklepem, w którym zakupiono produkt.

Portuguese notice

Descarte de Lixo Elétrico na Comunidade Européia



Este símbolo encontrado no produto ou na embalagem indica que o produto não deve ser descartado no lixo doméstico comum. É responsabilidade do cliente descartar o material usado (lixo

elétrico), encaminhando-o para um ponto de coleta para reciclagem. A coleta e a reciclagem seletivas desse tipo de lixo ajudarão a conservar as reservas naturais; sendo assim, a reciclagem será feita de uma forma segura, protegendo o ambiente e a saúde das pessoas. Para obter mais informações sobre locais que reciclam esse tipo de material, entre em contato com o escritório da HP em sua cidade, com o serviço de coleta de lixo ou com a loja em que o produto foi adquirido.

Slovakian notice

Likvidácia vyradených zariadení v domácnostiach v Európskej únii



Symbol na výrobku alebo jeho balení označuje, že daný výrobok sa nesmie likvidovať s domovým odpadom. Povinnosťou spotrebiteľa je odovzdať vyradené zariadenie v zbernom mieste, ktoré je určené na recykláciu vyradených elektrických a elektronických zariadení. Separovaný zber a recyklácia vyradených zariadení prispieva k ochrane prírodných zdrojov a zabezpečuje, že recyklácia sa vykonáva spôsobom chrániacim ľudské zdravie a životné prostredie. Informácie o zberných miestach na recykláciu vyradených zariadení vám poskytne miestne zastupiteľstvo, spoločnosť zabezpečujúca odvoz domového odpadu alebo obchod, v ktorom ste si výrobok zakúpili.

Slovenian notice

Odstranjevanje odslužene opreme uporabnikov v zasebnih gospodinjstvih v Evropski uniji



Ta znak na izdelku ali njegovi embalaži pomeni, da izdelka ne smete odvreči med gospodinjske odpadke. Nasprotno, odsluženo opremo morate predati na zbirališče, pooblaščeno za recikliranje odslužene električne in elektronske opreme. Ločeno zbiranje in recikliranje odslužene opreme prispeva k ohranjanju naravnih virov in zagotavlja recikliranje te opreme na zdravju in okolju neškodljiv način. Za podrobnejše informacije o tem, kam lahko odpeljete odsluženo opremo na recikliranje, se obrnite na pristojni organ, komunalno službo ali trgovino, kjer ste izdelek kupili.

Spanish notice

Eliminación de residuos de equipos eléctricos y electrónicos por parte de usuarios particulares en la Unión Europea



Este símbolo en el producto o en su envase indica que no debe eliminarse junto con los desperdicios generales de la casa. Es responsabilidad del usuario eliminar los residuos de este tipo depositándolos en un "punto limpio" para el reciclado de residuos eléctricos y electrónicos. La recogida y el reciclado selectivos de los residuos de aparatos eléctricos en el momento de su eliminación contribuirá a conservar los recursos naturales y a garantizar el reciclado de estos residuos de forma que se proteja el medio ambiente y la salud. Para obtener más información sobre los puntos de recogida de residuos eléctricos y electrónicos para reciclado, póngase en contacto con su ayuntamiento, con el servicio de eliminación de residuos domésticos o con el establecimiento en el que adquirió el producto.

Swedish notice

Bortskaffande av avfallsprodukter från användare i privathushåll inom Europeiska Unionen



Om den här symbolen visas på produkten eller förpackningen betyder det att produkten inte får slängas på samma ställe som hushållssopor. I stället är det ditt ansvar att bortskaffa avfallet genom att överlämna det till ett uppsamlingsställe avsett för återvinning av avfall från elektriska och elektroniska

produkter. Separat insamling och återvinning av avfallet hjälper till att spara på våra naturresurser och gör att avfallet återvinns på ett sätt som skyddar människors hälsa och miljön. Kontakta ditt lokala kommunkontor, din närmsta återvinningsstation för hushållsavfall eller affären där du köpte produkten för att få mer information om var du kan lämna ditt avfall för återvinning.

A

accessing
  HP Storage Server Management console, 18
ACL, defining, 64
Active Directory Lookup, 75
ActiveX
  enabling, 20
AppleTalk, 35
Array Configuration Utility, 40
array controller, purpose, 31
arrays, defined, 31
audience, 11
authorized reseller
  HP, 13

B

backup, printer, 72
backup, with shadow copies, 56
basic disks, 33, 33, 34
battery replacement notice, 108
boot sequence, 18

C

cables, 106
cache file, shadow copies, 48
CIFS, share support, 64
Class A equipment, 105
Class B equipment, 105
clustered server elements, 34
Command View EVA
  expanding storage, 44
configuration
  Internet, 103
  network, 16
  server, 25
  worksheet, 25
conventions
  document, 12
  text symbols, 12

D

data blocks, 31
data striping, 31
default login, 19
DHCP, 25
Disk Management
  extending volumes, 43
document
  conventions, 12
  related documentation, 11
dynamic disks
  clustering, 34
  spanning multiple LUNs, 33

E

electrostatic discharge, 109
European Union notice, 107
expanding storage
  Array Configuration Utility, 44
  Command View EVA, 44
extending volumes
  Disk Management, 43

F

factory image, 17
fault tolerance, 31
FCC notice, 105
File and Print Services for NetWare.
  See FPNW
file level permissions, 57
file recovery, 54
file screening management, 65
File Server Resource Manager, 37, 65
file services management, 38
file system elements, 34
file-sharing protocols, 34
files, ownership, 62
folder management, 57
folder recovery, 54
folders
  auditing access, 60
  managing, 57
FPNW
  accessing, 86
  described, 85
  installing, 85

G

grounding methods, 109
groups, adding to permissions list, 58

H

hardware support services, 13
help, obtaining, 11
host configuration protocols, DHCP and non-DHCP, 25

HP
Array Configuration Utility, 39
authorized reseller, 13
hardware support services, 13
Storage Manager, 40
Storage Server Management Console, 38, 65, 77
storage web site, 13
Subscriber's choice web site, 13
technical support, 12
Web Jetadmin, 70
HP Storage Server Management console
iLO 2 method, 24
direct attach method, 19
remote browser method, 24
remote desktop method, 24
remote server access, 18

I

iLO 2
See Integrated Lights-Out 2
iLO 2 method
connecting to network, 24
installation
planning, 15
server, 16
Integrated Lights-Out 2, described, 23
international notices and statements, 107
Internet
automatic configuration, 103
proxy server, 103
set up, 103
ISSE
See hardware support services

K

kernel-mode drivers
check for, 72
installation blocked, 72
kit contents, 17

L

laser compliance, 106
logical storage elements, 32, 34
LUNs
described, 32

M

Microsoft Disk Manager, 18
Microsoft Print Management Console, 70
Microsoft Printer Migrator, 72
mount points
creating, 33
not supported with NFS, 33
mounted drives and shadow copies, 47

N

NCP, creating new share, 89, 90
NetWare
adding local users, 87
enabling user accounts, 88
installing services for, 85
supervisor account, 89

O

online spares, 32

P

partitions
extended, 33
primary, 33
permissions
file level, 57
list
adding users and groups, 58
removing users and groups, 58
modifying, 58
resetting, 59
physical configuration, 17
physical storage elements, 30
planning
configuration checklist, 16
installation, 15
network access method, 15
network configuration, 16
power cords, 109
power on
server, 17
print services for UNIX, 83
printer backup, 72

Q

quota management, 65

R

RAID
data striping, 31
LUNs in volumes, 33
summary of methods, 32
Rapid Setup Wizard, 26
regulatory compliance, 105
related documentation, 11
remote access
Telnet Server, 23
remote browser method
connecting to network, 20
remote desktop method
connecting to network, 22

S

safety, 108

SAN Connection and Management white paper, 38
SAN environment, 38
Search enhancements, 37
security
  auditing, 60
  file level permissions, 57
  ownership of files, 62
serial number, 16
server
  installation, 16
  ML310 hardware components, 99
  power on, 17
Server for NFS
  Authentication DLL, 77
  described, 77
Service for User
  for Active Domain controllers, 77
services for AppleTalk, installing, 91
Services for UNIX, 33, 34
set up
  Internet, 103
setting up
  overview, 15
setup completion, 26
shadow copies, 34
  backups, 56
  cache file, 48
  defragmentation, 46
  described, 44
  disabling, 51
  file or folder recovery, 54
  managing, 47
  mounted drives, 47
  on NFS shares, 53
  on SMB shares, 52
  planning, 45
  redirecting, 50
  scheduling, 50
  uses, 44
  viewing list, 50
Shadow Copies for Shared Folders, 52
share management, 63
shares
  administrative, 64
  creating new NCP, 89, 90
  managing, 63
  NCP, 89
  standard, 64
Single Instance Storage, 37
startup
  collecting information, 25
storage configurations, 17
storage management
  elements, 29
  overview, 29
  process, 30
Storage Manager for SANs, 37
storage reports, 65
Subscriber's choice
  HP, 13
symbols in text, 12
system updates, 94

T

technical support
  HP, 12
Telnet Server, 23
  enabling, 23
  sessions information, 23
text symbols, 12
troubleshooting, 93

U

UNIX, print services, 83
user-mode drivers, 72
users
  adding to permission list, 58
  NetWare
    adding, 87
    enabling, 88

V

Volume Shadow Copy Service, 44
volumes
  creating Novell, 85
  NCP, 89
  planning, 33
vssadmin tool, 47

W

web sites
  HP documentation, 13
  HP storage, 13
  HP Subscriber's choice, 13
WEEE directive, 110