

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

[Initial Configuration](#)

[NAS Manager](#)

[Advanced Disk and Volume Management](#)

[System Management](#)

[Backing Up the System](#)

[Recovering and Restoring the System](#)

[Dell ActiveArchive](#)

[Advanced Features](#)

[Troubleshooting](#)



NOTE: A NOTE indicates important information that helps you make better use of your computer.



NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

Information in this document is subject to change without notice.

© 2002 Dell Computer Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Computer Corporation is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *PowerVault*, *PowerEdge*, *Dell OpenManage*, and *Dell ActiveArchive* are trademarks of Dell Computer Corporation; *Microsoft*, *Windows*, and *Windows NT* are registered trademarks of Microsoft Corporation; *Novell* and *NetWare* are registered trademarks of Novell, Inc.; *VERITAS* and *Backup Exec* are registered trademarks of VERITAS Software; *UNIX* is a registered trademark of The Open Group of the United States and other countries; *Intel* is a registered trademark of Intel Corporation; *Computer Associates* is a registered trademark and *ARCserveIT* is a trademark of Computer Associates International.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

May 2002

Initial Configuration

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [Configuring Your NAS System for the First Time](#)
- [Configuring Your NAS System Automatically on a Network \(with DHCP\)](#)
- [Configuring Your System Using the Kick-Start Utility](#)
- [Configuring Your System Using a Keyboard, Monitor, and Mouse](#)
- [Configuring Your System Using a Serial Connection](#)
- [Other Documents You May Need](#)

This section provides information necessary to perform the initial configuration of the system.

The NAS system is a "headless" system that is managed through the network; it can be operated without a keyboard, monitor, or mouse. The NAS system is configured and managed using the browser-based Dell™ PowerVault™ NAS Manager, which can be accessed from a client system on the same network. See "[NAS Manager](#)" for more information. For certain configuration tasks and for troubleshooting, you can connect a keyboard, monitor, and mouse. You can also connect a client system directly to the NAS system using the serial cable provided with the NAS system.

Configuring Your NAS System for the First Time

You must set the NAS system's basic configuration from another system on the network that has a keyboard, monitor, and mouse. This system is referred to as the client system. After you set the basic configuration, you can use the NAS Manager from any system on the network to set passwords, local users, shares, and so on. See "[NAS Manager](#)."

You can configure your system in several ways, depending on whether Dynamic Host Configuration Protocol (DHCP) is installed on your network:

- If DHCP is installed on your network, your system automatically configures the network settings. If you are unsure whether your network uses DHCP, contact your network administrator. See "[Configuring Your NAS System Automatically on a Network \(with DHCP\)](#)."
 - If DHCP is not installed on your network, you can configure your system using the Dell OpenManage™ Kick-Start utility. See "[Configuring Your System Using the Kick-Start Utility](#)."
 - You can use a keyboard, monitor, and mouse connected directly to the NAS system. See "[Configuring Your System Using a Keyboard, Monitor, and Mouse](#)."
 - You can use a client system directly connected to the NAS system through a serial cable. See "[Configuring Your System Using a Serial Connection](#)."
-

Configuring Your NAS System Automatically on a Network (with DHCP)

1. Connect one end of the power cable to the NAS system and the other end to a power source.
2. Connect one end of an Ethernet cable into one of the two 10/100/1000 NIC connectors (see [Figure 1-1](#)) on the back of your NAS system.

For more information on the location of system connectors, see the *User's Guide*.



NOTE: There are three RJ-45 NIC connectors on the back panel of your system. However, only the two NIC connectors located in the center of the system's back panel can be used for NAS system network connections.

The third RJ-45 connector, located in the lower right corner of the system's back panel, is an embedded remote access connector and should only be used for remote access functions.

3. Connect the other end of the Ethernet cable to a functioning Ethernet jack.
4. Push the power button to turn on the NAS system.

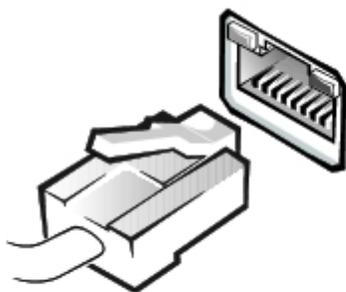
The NAS system retrieves the information it needs (the IP address, gateway subnet mask, and DNS server address) from a DHCP server on the network.

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system.

5. Verify that the link LED on the NIC connector is illuminated. See [Figure 1-1](#).

If the LED is not illuminated, check to make sure that each end of the Ethernet cable is seated properly in the NIC connector and the Ethernet jack.

Figure 1-1. NIC Connector



6. From a client system on the same network, open Microsoft® Internet Explorer 5.5 or later (or for Red Hat Linux only, open Netscape Navigator 6.2.2 or later), type the default system name in the Web address field, and press <Enter>.

The default system name is `DELLxxxxxxx`, where `xxxxxxx` is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`.

 **NOTE:** If you cannot connect to the system through a Web browser, you must use another method to configure the IP address, gateway subnet mask, and DNS server. See "[Configuring Your NAS System for the First Time](#)."

7. Enter the default administrative user name and password for your system when prompted, and then click **OK**.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

 **NOTICE:** If you are not using the Kick-Start utility to configure your system, you must disable it immediately. If the Kick-Start utility is enabled, the system automatically logs in as administrator, which creates a security risk. The Kick-Start utility also takes up system resources by constantly checking for configuration information. For more information, see "[Disabling the Kick-Start Utility](#)."

8. Use the NAS Manager to begin setting up shares and volumes on the NAS system.

See "[NAS Manager](#)."

Configuring Your System Using the Kick-Start Utility

 **NOTE:** Perform the procedures in this section only if you cannot configure your NAS system using a DHCP server on

the network. See "[Configuring Your NAS System Automatically on a Network \(with DHCP\)](#)."

1. Connect one end of the power cable to the NAS system and the other end to a power source.
2. Connect one end of an Ethernet cable into one of the two 10/100/1000 NIC connectors (see [Figure 1-1](#)) on the back of your NAS system.

For more information on the location of system connectors, see the *User's Guide*.

 **NOTE:** There are three RJ-45 NIC connectors on the back panel of your system. However, only the two NIC connectors located in the center of the system's back panel can be used for NAS system network connections. The third RJ-45 connector, located in the lower right corner of the system's back panel, is an embedded remote access connector and should only be used for remote access functions.

3. Connect the other end of the Ethernet cable to a functioning Ethernet jack.
4. From a client system on the same network, enable the Dell OpenManage Kick-Start utility and create your DHCP settings:

 **NOTE:** The client system should be on the same subnet as the NAS system. Because the NAS system is assigned an address on the 10.40.10.x subnet, the client system IP address must also be statically assigned to the 10.40.10.x subnet.

- a. Insert the *Resource* CD into the CD drive of the client system.
 - b. When the *Resource* CD window displays, click **Dell OpenManage Kick-Start**.
 - c. Click **Run Dell OpenManage Kick-Start**.
 - d. If a security warning appears, click **Yes**.
 - e. When asked if you want to run the program, click **Yes**.
 - f. At the bottom of the **Dell OpenManage Kick-Start** window, click **Setup**.
 - g. Click **Add**.
 - h. In the **Add Scope** window, type the following information and click **OK**:
 - **Starting IP Address:** 10.40.10.10
 - **Ending IP Address:** 10.40.10.20
 - **Subnet:** 255.255.255.0
 - **Gateway IP Address:** 10.40.10.1
 - i. Click **OK** to close the **Add Scope** window.
 - j. Click **Interfaces for DHCP Server** so that it is checked.
 - k. Click **OK** to close the **DHCP Server Setup** window.
5. Click **Enabled** at the bottom of the **Dell OpenManage Kick-Start** window to start the integrated DHCP server.
 6. Push the power button to turn on the NAS system.

After the system boots, it is displayed in the **Discovered Systems** list of the **Dell OpenManage Kick-Start** window.

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system.

7. Click the NAS system in the **Discovered Systems** list.

8. Click **Launch Configuration Tool** to launch the NAS Manager.

The **Configuring** icon is displayed for 5 minutes after you click **Launch Configuration Tool**. If the agent is still running after 5 minutes, the icon displays "Ready."

9. Use the NAS Manager to configure the NAS system's IP address.

See "[Configuring the Network Address for the NAS System](#)" in "NAS Manager."

Disabling the Kick-Start Utility

-  **NOTICE:** If you are not using the Kick-Start utility to configure your system, you must disable it immediately. If the Kick-Start utility is enabled, the system automatically logs in as administrator, which creates a security risk. The Kick-Start utility also takes up system resources by constantly checking for configuration information.

To disable the Kick-Start utility, perform the following steps:

1. From the NAS Manager primary menu, click **Maintenance**.
2. Click **Terminal Services**.
3. Log in to the system as an administrator.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

When asked if you want to disable the Kick-Start Agent, click **Yes** to disable the Kick-Start Agent and prevent it from running again, or click **No** if you want the Kick-Start Agent to continue running and also run when the system reboots.

Configuring Your System Using a Keyboard, Monitor, and Mouse

1. Connect one end of the power cable to the NAS system and the other end to a power source.
2. Connect a keyboard, monitor, and mouse to the NAS system.

For information about system connectors, see your *User's Guide*.

3. Push the power button to turn on the NAS system.
4. Log in to the NAS Manager.

For more information, see "[Logging in to the NAS Manager](#)."

5. Configure the IP address.

For more information, see "[Configuring the Network Address for the NAS System](#)" or your Windows online help.

6. Disable Kick-Start.

For more information, see "[Disabling the Kick-Start Utility](#)."

Configuring Your System Using a Serial Connection

If DHCP is not installed on your network, you can configure your NAS system using a serial connection. You can connect to the NAS system from a client system running one of the following operating systems:

- Windows® 2000
- Windows XP
- Microsoft Windows NT®

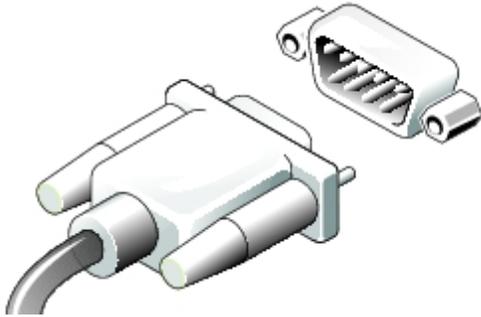
Configuring Your System Using a Serial Connection From a Windows 2000 Client

 **NOTE:** Perform this procedure only if you cannot configure your NAS system using a DHCP server on the network. See "[Configuring Your NAS System Automatically on a Network \(with DHCP\)](#)."

Setting Up the Windows 2000 Client to Connect to the NAS System

1. Connect one end of the serial cable provided with your NAS system (see [Figure 1-2](#)) to the serial port on the NAS system, and connect the other end to an available serial port (typically COM1 or COM2) on a client system running Windows 2000.

Figure 1-2. Serial Cable



2. Connect one end of the power cable to the NAS system and the other end to a power source.
3. Push the power button to turn on the NAS system.

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system. After the system boots, it may take several minutes for the direct serial connection to initialize.

4. On the client system's desktop, right-click **My Network Places**, and click **Properties**.

The **Network and Dial-up Connections** window appears.

5. Double-click **Make New Connection**.

The Network Connection Wizard is displayed.

6. Click **Next**.
7. Select **Connect directly to another computer**, and then click **Next**.
8. Select **Guest**, and then click **Next**.
9. From the **Select a Device** menu, select the COM port on your client system to which you connected the serial cable, and then click **Next**.

The COM port is the communication port on the client system to which the serial cable connects. The COM port used on

your client system is typically labeled COM1 or COM2.

10. Click **Only for myself**, and then click **Next**.
11. Type a name for the connection in the text box, and then click **Finish**.

Do *not* click **Connect** yet. The connection must first be configured before connecting to the NAS system.

12. Click **Properties**.
13. In the next window that appears, click the **General** tab, and then select **Communication cable between two computers** from the **Select a Device** drop-down menu.
14. Click **Configure**.

The **Modem Configuration** window appears.

15. Select the **Maximum Speed (bps)** menu, and then click **115200**.
16. Verify that only **Enable hardware flow control** is selected.
17. Click **OK** to close the **Modem Configuration** window.
18. Click **OK** to close the connection window.

The **Connect** box prompts you for a user name and password.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

19. Ensure that your NAS system is on and that it has sufficient time to boot into the Windows operating system.
20. Start a Web browser on the client system where you will configure the NAS system.
21. Type `https://192.168.192.1:1279` in the browser and press <Enter>.

192.168.192.1 is the IP address used by your NAS system for this serial cable connection.

22. Click **Yes** to accept the security certificate.

If a message appears that states that the name on the security certificate is invalid or does not match the name of the site, ignore the message and click **Yes**.

23. Enter the administrative user name and password for your system when prompted, and then click **OK**.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The NAS Manager is displayed.

After the NAS Manager is displayed, you can configure your system through the NAS Manager or through the Terminal Service Client. See "[Configuring the Network Address for the NAS System](#)" in "NAS Manager."

Connecting to the NAS System From a Windows 2000 Client

This section assumes that you have already configured your client system to connect to the NAS system. If you have not configured the client system, see "[Setting Up the Windows 2000 Client to Connect to the NAS System](#)."

1. Ensure that your NAS system is on and that it has had sufficient time to boot into the Windows operating system.

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system.

2. On the client system, right-click **My Network Places** on the desktop, and click **Properties**.

The **Network and Dial-up Connections** window appears.

3. Double-click the connection you created in "[Setting Up the Windows 2000 Client to Connect to the NAS System](#)."
4. Enter the administrative user name and password for your NAS system.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

5. Click **Connect**.

This action connects the client system to the NAS system through the serial cable.

6. Start a Web browser on the client system where you will configure the NAS system.

 **NOTE:** The NAS Manager supports clients running Microsoft Internet Explorer 5.5 or later (or Netscape Navigator 6.2.2 or later for Red Hat Linux).

7. Type `https://192.168.192.1:1279` in the browser and press <Enter>.

192.168.192.1 is the IP address used by your NAS system for this serial cable connection.

8. Click **Yes** to accept the security certificate.

If a message appears that states that the name on the security certificate is invalid or does not match the name of the site, ignore the message and click **Yes**.

9. Enter the administrative user name and password for your system when prompted, and then click **OK**.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The NAS Manager is displayed.

After the NAS Manager is displayed, you can configure your system through the NAS Manager or through the Terminal Service Client. See "[Configuring the Network Address for the NAS System](#)" in "NAS Manager."

Configuring Your System Using a Serial Connection From a Windows XP Client

 **NOTE:** Perform this procedure only if you cannot configure your NAS system using a DHCP server on the network. See "[Configuring Your NAS System Automatically on a Network \(with DHCP\)](#)."

Setting Up the Windows XP Client to Connect to the NAS System

1. Connect one end of the serial cable provided with your NAS system (see [Figure 1-2](#)) to the serial port on the NAS system, and connect the other end to an available serial port (typically COM1 or COM2) on a client system running Windows XP.
2. Connect one end of the power cable to the NAS system and the other end to a power source.
3. Push the power button to turn on the NAS system.

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system. After the system boots, it may take several minutes for the direct

serial connection to initialize.

4. On the client system's desktop, click the **Start** button and click **Control Panel**.
5. Click **Network and Internet Connections**.



NOTE: If you are prompted to set up phone and modem options here, enter all the appropriate information for your location.

6. Click **Network Connections**.
 7. Click **Create a new connection** in the left pane.
 8. In the **New Connection** window, click **Next**.
 9. Click **Set up an advanced connection**, and then click **Next**.
 10. Select **Connect directly to another computer**, and then click **Next**.
 11. Select **Guest**, and then click **Next**.
 12. Type a name for the connection to the NAS system in the **Computer Name** field.
 13. From the **Select a Device** menu, select the COM port on your client system to which you connected the serial cable, and then click **Next**.
- The COM port is the communication port on the client system to which the serial cable connects. The COM port used on your client system is typically labeled COM1 or COM2.
14. Click **Add a shortcut to this connection to my desktop**, and click **Finish**.

Connecting to the NAS System From a Windows XP Client

This section assumes that you have already configured your client system to connect to the NAS system. If you have not configured the client system, see "[Setting Up the Windows XP Client to Connect to the NAS System](#)."

1. Ensure that your NAS system is on and that it has had sufficient time to boot into the Windows operating system.



NOTE: It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system.

2. From the desktop of the client system, double-click the icon for the connection to the NAS system.
3. In the **Connect** window, click **Properties**.
4. In the **Properties** window, click **Configure**.
5. In the **Modem Configuration** window, select **115,200** for **Maximum speed (bps)** and click **OK**.
6. Click **OK** again to close the **Properties** window.
7. Enter the administrative user name and password for your NAS system.



NOTE: The default administrative user name is `administrator` and the default password is `powervault`.

8. Click **Connect**.

This action connects the client system to the NAS system through the serial cable.

9. Start a Web browser on the client system where you will configure the NAS system.

 **NOTE:** The NAS Manager supports clients running Microsoft Internet Explorer 5.5 or later (or Netscape Navigator 6.2.2 or later for Red Hat Linux).

10. Type `https://192.168.192.1:1279` in the browser and press <Enter>.

192.168.192.1 is the IP address used by your NAS system for this serial cable connection.

11. Click **Yes** to accept the security certificate.

12. Enter the administrative user name and password for your system when prompted, and then click **OK**.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The NAS Manager is displayed.

After the NAS Manager is displayed, you can configure your system through the NAS Manager or through the Terminal Service Client. See "[Configuring the Network Address for the NAS System](#)" in "NAS Manager."

Configuring Your System Using a Serial Connection From a Windows NT Client

 **NOTE:** Perform this procedure only if you cannot configure your NAS system using a DHCP server on the network. See "[Configuring Your NAS System Automatically on a Network \(with DHCP\)](#)."

Setting Up the Windows NT Client to Connect to the NAS System

1. Connect one end of the serial cable provided with your NAS system (see [Figure 1-2](#)) to the serial port on the NAS system, and connect the other end to an available serial port (typically COM1 or COM2) on a client system running Windows NT.
2. Connect one end of the power cable to the NAS system and the other end to a power source.
3. Push the power button to turn on the NAS system.

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system. After the system boots, it may take several minutes for the direct serial connection to initialize.

4. Log in to the client system as an administrator.
5. Install the modem on the client system:
 - a. Insert the Microsoft Windows NT 4.0 operating system CD into the CD drive of the client system.
 - b. Close the **Windows CD-ROM** menu when it displays.
 - c. From the desktop, double-click **My Computer**.
 - d. In the **My Computer** window, double-click **Dial-Up Networking**.
 - e. Click **Install**.
 - f. When asked if you want to be able to add a modem, click **Yes**.
 - g. In the **Install New Modem** window, select **Don't detect my modem; I will select it from a list** and click **Next**.
 - h. Click **(Standard Modem Types)**, and then click **Dial-Up Networking Serial Cable between 2 PCs**.

- i. Click **Next**.
 - j. Select the port to which you want to install the modem, and then click **Next**.
 - k. Enter the area code in the **Localization Information** window, and then click **Next**.
 - l. Click **Finish** to complete the modem installation.
 - m. In the **Add RAS Device** window, click **COMx - Dial-Up Networking Serial Cable Between 2 PCs**, and click **OK**.
 - n. In the **Remote Access Setup** window, select **Dial-Up Networking Serial Cable between 2 PCs**, and click **Continue**.
 - o. Click **Dial out only** and click **OK**.
 - p. In the **Remote Access Setup** window, select **Dial-Up Networking Serial Cable between 2 PCs**, and click **Network**.
 - q. Deselect NetBEUI and IPX as dial-out protocols, make sure that TCP/IP is selected, and click **Configure**.
 - r. Click **Continue**.
 - s. Remove the Windows NT CD from the CD drive.
 - t. Click **Restart**.
6. Log in to the client system as an administrator.
 7. Configure the modem properties:
 - a. From the client desktop, double-click **My Computer**.
 - b. Double-click **Control Panel**.
 - c. In the **Control Panel** window, double-click **Modems**.
 - d. For **Modem Properties**, select **Dial-Up Networking Serial Cable Between 2 PCs**.
 - e. Click **Properties**.
 - f. Select **115,200** for **Maximum speed** and click **OK**.
 - g. Click **Close**.
 8. Create the dial-up connection to the NAS system:
 - a. In the **My Computer** window, double-click **Dial-Up Networking**.
 - b. When a message states that your phonebook is empty, click **OK** to create a new phone book entry.
 - c. In the New Phonebook Entry Wizard, type a name for the connection to the NAS system.
 - d. Click **I know all about phonebook entries and would rather edit the properties directly**, and then click **Finish**.
 - e. Click **Configure**.
 - f. Select **115,200** for the **Initial Speed** and click **OK**.
 - g. Click the **Server** tab, and deselect **NetBEUI** and **IPX**.

TCP/IP should be the only protocol selected.
 - h. Click **OK**.

Connecting to the NAS System From a Windows NT Client

This section assumes that you have already configured your client system to connect to the NAS system. If you have not configured the client system, see "[Setting Up the Windows NT Client to Connect to the NAS System.](#)"

1. Ensure that your NAS system is on and that it has had sufficient time to boot into the Windows operating system.

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system.

2. From the desktop of the client system, double-click the icon for the connection to the NAS system.
3. Dial into the NAS system:
 - a. In the **Dial-Up Networking** window, click **Dial**.
 - b. Type the administrative user name, password, and domain for your NAS system when prompted, and then click **OK**.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`. For domain, enter the NAS system's name. The default system name is `DELLxxxxxxx`, where `xxxxxxx` is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`.

- c. Start a Web browser on the client system where you will configure the NAS system.

 **NOTE:** The NAS Manager supports clients running Microsoft Internet Explorer 5.5 or later (or Netscape Navigator 6.2.2 or later for Red Hat Linux).

- d. Type `https://192.168.192.1:1279` in the browser and press <Enter>.

192.168.192.1 is the IP address used by your NAS system for this serial cable connection.

- e. Click **Yes** to accept the security certificate.
- f. Enter the administrative user name and password for your system when prompted, and then click **OK**.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The NAS Manager is displayed.

After the NAS Manager is displayed, you can configure your system through the NAS Manager or through the Terminal Service Client. See "[Configuring the Network Address for the NAS System](#)" in "NAS Manager."

Other Documents You May Need

[Table 1-1](#) lists the additional documentation included with your system.

Table 1-1. Other Documents

Document	Type of Information
<i>Setting Up Your System</i>	General overview of system setup.
<i>User's Guide</i>	System features, technical specifications, and device drivers.
<i>Installation and</i>	Instructions for installing system hardware, as well as troubleshooting and diagnostic procedures for

<i>Troubleshooting Guide</i>	testing your system.
System Information	Basic information about your system, including safety and regulatory information. Warranty information may be in this document or in a separate document.
<i>Resource CD</i>	Contains electronic copies of your system documentation.
Online Help	Online help is available for the NAS Manager and the Windows Powered operating system. In addition, online help is provided with some of the system management and storage management software components. For more information on accessing online help, see " How to Find Online Help ."
Readmes and Release Notes	Last-minute updates about technical changes to the system or advanced technical reference material intended for experienced users or technicians. These documents are located on the <i>Resource CD</i> .
Information Updates	Documents that are sometimes included with the system to describe changes to the system or software documentation. Always read the updates before consulting any other documentation. The updates often contain information that supersedes information in the other documents.

[Back to Contents Page](#)

NAS Manager

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [Logging in to the NAS Manager](#)
- [Basic Navigation](#)
- [Changing the NAS Manager Language](#)
- [How to Find Online Help](#)
- [Configuring Network Properties](#)
- [Creating Users](#)
- [Using Shares](#)
- [Disk Quotas](#)
- [Using Logs](#)
- [Multiple Device Management](#)
- [Configuring MDM on Your NAS System](#)
- [Viewing MDM Device Status](#)
- [Using the MDM Controller to Administer NAS Devices](#)
- [Shutting Down the NAS System](#)
- [Managing Disks](#)
- [Managing Volumes](#)
- [Using the PowerVault Advanced Administration Menu](#)

The Dell™ PowerVault™ NAS Manager is a Web-based user interface that is the primary tool for configuring NAS systems. This section provides basic information on using the NAS Manager, including how to log on and navigate the interface, configuring network properties and IP addresses, creating users, using shares and disk quotas, and managing disks and volumes.

Logging in to the NAS Manager

To use the NAS Manager, you must be logged in as an administrator. You can log in only if the NAS system is on the network or if you are connected directly to the NAS system with a serial cable.

To log in to the NAS Manager, perform the following steps:

1. Open a Web browser from a client system.

The NAS Manager supports clients running Microsoft® Internet Explorer 5.5 or later (or Netscape Navigator 6.2.2 or later for Red Hat Linux).

2. Type in the name of the NAS system in the Web address field, and then press <Enter>.

The default system name is Dellxxxxxxx, where xxxxxxx is the system's service tag number. For example, if your service tag number is 1234567, enter `http://DELL1234567`.

The NAS Manager is served on port 1279 and is accessed using the following Web address: **`https://systemname:1279`** or **`https://system_ipaddress:1279`**, where *systemname* is Dellxxxxxxx (xxxxxxx is the system's service tag number). For example, if your service tag number is 1234567, you would enter `https://DELL1234567:1279`. Port 1279 uses secure socket layer (SSL) to encrypt data going to and coming from the NAS system to provide data security.

- ➡ **NOTICE:** Although port 1278 can be used, it uses plain text authentication, which can be a significant security risk. Therefore, using port 1278 is not recommended.

3. When the **Enter Network Password** window displays, type a user name and password and then click **OK** to log in as the administrator.



NOTE: The NAS Manager default administrator user name is `administrator` and the default password is `powervault`.

4. Click **Administer this server appliance**.
5. When the **Enter Network Password** window appears again, enter the same user name and password that you entered in step 3, and then click **OK**.

You are now logged in to the NAS Manager.

Default Administrator User Name and Password

When logging into the NAS system for the first time, you must enter an administrator user name and password. The default administrator user name for your NAS system is `administrator` and the default password is `powervault`.

Basic Navigation

When navigating the NAS Manager, use the buttons within the program to go backward and forward.

The top of each page of the Web user interface (UI) displays a status area, as well as primary and secondary menu bars, and the body of each page displays specific content related to each functional area.

Status Area

The following information is displayed from left to right in the top band of the NAS Manager Web UI:

- System host name
- System status, which displays the following status conditions:
 - Normal (green text)
 - Informational (grey text)
 - Warning (yellow text)
 - Critical (red text)

Clicking **Status:** `<status_type>` takes you to the **Status® Information** page.

- Microsoft Windows® Powered logo

Primary Menu

The primary menu bar below the status area allows you to choose from the following menu items:

- **Welcome** — Allows you to take a tour and set the administrator password, NAS system name, and default page.
- **Status** — Provides information about alerts and other status.
- **Network** — Provides access to basic network setup tasks such as setting the NAS system name, configuring properties of network interfaces, configuring global network settings, setting IP addresses and ports for the administration website, configuring Telnet, and changing passwords.

- **Disks** — Allows you to configure disks and volumes, set disk quotas, and create snapshots (or persistent images).
 - **Users** — Enables you to create, edit, and delete local users and groups.
 - **Shares** — Enables you to manage local folders and create or modify file shares.
 - **Maintenance** — Allows you to perform maintenance tasks such as backup and restore, apply software updates, check logs, change the language of the NAS Manager, and access the Terminal Services Advanced Client.
 - **MDM** — Allows you to configure multiple device management (MDM) settings.
 - **Help** — Provides access to online Help for network attached storage.
-

Changing the NAS Manager Language

The NAS Manager is available in different languages. To change the NAS Manager language, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Language**.
4. Click the radio button next to the language you want to use.
5. Click **OK**.
6. Reboot the system when prompted.

The NAS system reboots, and the changes are complete after the reboot.

How to Find Online Help

The NAS Manager provides two kinds of help. The NAS Manager online help provides information on NAS Manager functionality and procedures. The Windows Powered operating system online help, which you can access through the Terminal Services on the **Maintenance** page, documents the functionality of the Windows Powered operating system.

To access NAS Manager Help, use one of the following methods:

- Click **Help** on the primary menu; the NAS Manager screen is replaced by a split **Help** screen that displays a table of contents on the left and topics on the right.
- Click the question mark icon at the far right of the primary menu to access the context-sensitive help topic related to the current page.

To start Windows Powered help, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**.
4. Log in to the NAS system.



NOTE: The default administrative user name is `administrator` and the default password is `powervault`.

5. Perform one of the following procedures:
 - From the **Start** menu, click **Help**.

- On the Advanced Administration Menu, click **Administrative Tools**, and then click **Windows Powered Help**.
-

Configuring Network Properties

Use the **Network** tab in the NAS Manager to configure the NAS system for the network. This section provides information for setting up your NAS system on the network, including naming the system, defining the IP address, and configuring the NIC.

Naming the NAS System

By default, the NAS system uses your service tag number as the system name. To change the name of the NAS system, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Network**.
3. Click **Identification**.
4. Type a new name for the NAS system in the **Server appliance name** field.
5. Click **OK**.
6. Click **OK** to reboot, or click **Cancel**.

Until you reboot the system, the new name will not take effect. Use the new name when you connect to the NAS Manager.

Configuring the Network Address for the NAS System

If you have a DHCP server on your network, you do not need to configure your NAS system's IP address because DHCP automatically assigns an address to the NAS system. If you do not have a DHCP server on your network, you must set the address for the NAS system through the NAS Manager.

 **NOTE:** To configure an IP address for another interface such as DNS, WINS, or AppleTalk, see your NAS Manager online help.

 **NOTE:** Before you configure the IP address, make sure that the NAS system is connected to the network.

To configure the IP address, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Network**, and then click **Interfaces**.
3. Select the radio button beside the network connection that you want to configure.

 **NOTE:** If some of the text is missing due to column width, pass your cursor over the text in the column to see a pop-up window with a full description.

4. Click **IP**, and select **Use the following IP settings**.
5. Enter the desired IP address, subnet mask, and default gateway.

If you do not have this information, contact your system administrator.

6. Click **OK**.

The network address setup is complete.

 **NOTE:** When you change the IP address, you may be unable to access the NAS Manager until you reboot the NAS system, or for approximately 15 minutes until the network recognizes the new IP address. You can also try to access the NAS system by typing `https://new_ip_address:1279` in the NAS Manager.

Creating Users

A user is a person or group that has access to the shares on the NAS system. You create users after you configure the network properties of your NAS system.

Creating a Single Local User

 **NOTE:** In a domain environment, you cannot create domain users.

1. Log in to the NAS Manager.
2. Click **Users**.
3. Click **Local Users**.
4. On the **Local Users on Server Appliance** page, click **New**.
5. Complete the information on the **Create New User** page.

 **NOTE:** In a domain environment, do not create local users that have the same user name as domain users unless the local user and domain user have identical passwords.

The **Home Directory** text box specifies a new directory that will be created and to which the user will have exclusive access permission. The directory name is the same as the user name and is located in the path specified.

6. Click **OK**.

Creating a Group of Local Users

 **NOTE:** In a domain environment, you cannot create domain groups. However, you can add domain users to your local groups.

1. Log in to the NAS Manager.
2. Click **Users**.
3. Click **Local Groups**.
4. On the **Local Groups on Server Appliance** page, click **New**.
5. On the **Create New Group** page, enter the name and description of the group.
6. Click **Members**.
7. Select the members of the group by performing one of the following:
 - In the **Add user or group** box, select a local user or group from the list, and then click **Add**.
 - Type the domain and group name (`domain\group_name`) of a domain group or of a domain user account (`domain\user_name`) and then click **Add**.

NOTE: If you are adding a domain group, you must also enter the user name and password that will allow you to



add from that domain.

8. Click **OK**.

Using Shares

A share is a folder on the NAS system that is shared with other systems on the network, whether those systems are running a Windows, Novell® NetWare®, Macintosh, or UNIX® operating system.

A NAS system supports the following methods of sharing folders:

- CIFS — The Common Internet File System protocol is used by clients running a Windows operating system.
- NFS — The Network File System protocol is used by clients running UNIX.
- FTP — The File Transfer Protocol is an alternative way of accessing a file share from any operating system.
- HTTP — The Hypertext Transfer Protocol is the protocol for accessing a file share from Web browsers.
- AppleTalk — The AppleTalk protocol is used by clients running a Macintosh operating system.
- NCP (Novell NetWare) — The NCP protocol is used by NetWare clients.



NOTE: The AppleTalk and NetWare NCP protocols are disabled by default on the NAS system. See "[Advanced Features](#)" for information about enabling these protocols.

Adding a Share

To create a share, you must supply a share name that is different from all other shares on the system. This is the name that the client system uses to access the share. Some protocols also support the inclusion of a comment or brief description of the share. Additionally, you must enable at least one of the available protocols.



NOTICE: To make the shares more fault-tolerant, create your data shares on the data drives.

To add a share, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. On the **Shares** page, click **Shares**.
4. In the **Tasks** list on the **Shared Folders** page, click **New**.
5. Type the share name and share path.



NOTE: Do not share the root directory of your system. Share only folders in the root directory. For example, do not share **d:**; instead, share **d:\foldername**, where *foldername* is the name of the folder in the root directory.

6. If you entered a nonexistent folder in the **Share path**, click **Create folder if it does not already exist**.



NOTE: The **Comment** field is ignored for NFS, FTP, and HTTP shares.

7. Check the appropriate box(es) to specify the types of protocols to enable.

If you want to use a protocol that is grayed out, you must first enable it on the NAS system. See "[Advanced Features](#)"

for information about enabling the AppleTalk and NCP protocols.

8. Use the protocol tabs to configure the specific properties of each type of share.



NOTE: Services for NetWare (SFN) are compatible with the Novell NetWare Bindery service for authentication and file access using the Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) network protocol. You must perform a NetWare logon to the NAS system using a NetWare client before you can connect to the NetWare shares.

9. Click **OK**.

Modifying Share Properties

1. Log in to the NAS Manager.
2. Click **Shares**.
3. On the **Shares** page, click **Shares**.
4. In the **Shared Folders** table, click the share you want to modify.
5. Click **Properties**.

The **Share Properties** page displays. Use this page to change the description of the share. You can also select the type of client from which the share is accessible.

6. Click **OK**.

Removing a Share

When you remove a share, access to the share is removed; however, the actual files remain on the NAS system.

To remove a share, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. On the **Shares** page, click **Shares**.
4. In the **Shared Folders** table, click the share that you want to delete.
5. Click **Delete**.

A confirmation dialog appears.

6. Click **OK** to confirm the deletion, or click **Cancel** to keep the share.

Removing a Protocol From the Share

Because a share may have more than one protocol assigned, it is possible to remove a protocol from a share without removing the remaining protocols.

To remove one or more specific protocols from a share, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.

3. On the **Shares** page, click **Shares**.
 4. In the **Shared Folders** table, click the share for which you want to remove a protocol.
 5. Click **Properties**.
 6. Uncheck the protocol(s) to remove it from the share.
 7. Click **OK** to confirm the protocol removal, or click **Cancel** to keep the protocol(s) for the share.
-

Disk Quotas

Disk quotas track and control the use of disk space for volumes. You can configure the volumes on your NAS system to:

- Prevent further use of disk space 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 you enable disk quotas, you can 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 allocated within a specific volume.
- The warning level specifies the point at which the event log displays that a user is nearing the quota limit within a specific volume.

For example, you can set a user's disk quota limit to 50 MB and the disk quota warning level to 45 MB. With these settings, the user can store no more than 50 MB on the volume. If the user stores more than 45 MB on the volume, you can set the disk quota system to log a system event to the event log.

In addition, you can specify a quota limit for users but allow the users to exceed that quota limit. When you enable quotas without limiting disk space, you can track disk-space use on a per-user basis without denying users access to a volume when they exceed that limit. It is also possible to specify whether the system logs an event when a user exceeds the quota warning level and quota limit.

Enabling or Disabling Disk Quotas

To enable or disable quota management on a volume, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Disk Quota**.
4. On the **Volumes and Quotas** page, click the volume to manage.
5. Click **Quota**.
6. On the **Default Quota for volume** page, click the appropriate check box to enable or disable quota management.
7. Select the quota size and settings for this volume.
8. Click **OK**.

Adding Disk Quota Entries

The **Quota Entries** page allows you to add, delete, or configure disk quotas for any NAS system user.

When you enable disk quotas for an existing volume, volume usage is automatically tracked for new users from that point forward. However, existing volume users have no disk quotas applied to them. You can apply disk quotas to existing volume

users by adding new quota entries in the **Quota Entries** window.

To add a new quota entry, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Disk Quota**.
4. On the **Disk Quota** page, click the volume to manage.
5. Click **Quota Entries**.
6. Click **New**.
7. Select a local user from the list box, or type the name of a domain account in the text box (in the format *domain_name\user_name*).
8. To allow unlimited disk space usage, click the **Do not limit disk usage** radio button, and then go to step 10. Otherwise, go to step 9.
9. To limit disk space, perform the following steps:
 - a. Click the **Limit disk space to** radio button.
 - b. In the text box, enter a numerical value to specify the amount of disk space to assign to a particular user or group. Use the drop-down box to select kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).
 - c. Enter the amount of disk space that, when filled, triggers a warning to the user or group member that the used disk space is near the disk-capacity limit. Use the drop-down box to select KB, MB, GB, TB, PB, or EB.
10. Click **OK**.

Modifying Quota Properties

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Disk Quota**.
4. On the **Volumes and Quotas** page, click the volume to manage.
5. Click **Quota Entries**.
6. In the **Logon** list on the **Quota Entries** page for the selected volume, select a user account.
7. Click **Properties**.
8. On the **Quota entry for user** page, click the **Do not limit disk usage** radio button to allow unlimited disk use, or perform the following procedure to limit disk space:
 - a. Click the **Limit disk space to** radio button.
 - b. In the text box, enter a numerical value to specify the amount of disk space to assign to a particular user or group. Use the drop-down box to select **KB, MB, GB, TB, PB, or EB**.
 - c. Enter the amount of disk space that, when filled, triggers a warning to the user or group member that the used disk space is near the disk-capacity limit. Use the drop-down box to select **KB, MB, GB, TB, PB, or EB**.



NOTE: Any previously entered warning level does not appear in the text box. However, the warning level is still set on the NAS system.

9. Click **OK**.

Removing Disk Quota Entries

1. Log in to the NAS Manager.
 2. Click **Disks**.
 3. Click **Disk Quota**.
 4. On the **Volumes and Quotas** page, select the volume to manage.
 5. From the **Tasks** list, select **Quota Entries**.
 6. On the **Quota Entries** page, select the **Logon name** from which you want to remove the quota entry.
 7. On the **Tasks** list, select **Delete**.
 8. Click **OK**.
-

Using Logs

A log file stores messages, which are sometimes called events or event log entries, generated by an application, service, or operating system. The messages are used to track the operations performed by the system. Log files are usually plain text (ASCII) files with the **.log** file extension.

The NAS system provides access to the following logs:

- Application log
- FTP log
- NFS log
- Security log
- System log
- Web (HTTP) shares log
- Web administration log

Viewing Log Entry Details

You can view details from specific log files such as the date, time, source, event ID, description, and data.

To view log entry details, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Logs**.
4. On the **Logs** page, select the type of log you want to view.
5. Click the radio button next to the log entry you want to view.
6. In the **Tasks** list, click **Event Details** or **View Log** depending on the selected log type.
7. On the **Log Details** page, click **Up** and **Down** to scroll through the log files.

8. Click **Back** to close the **Log Details** page and return to the log entry list on the **Logs** page.

Modifying Log Properties

For system, security, and application logs, you can specify the maximum log size and determine how the system handles log entries when the maximum capacity of the NAS system is reached.

To modify the properties of a log file, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Logs**.
4. On the **Logs** page, select the type of log you want to configure.
5. In the **Tasks** list, click **Log Properties**.
6. In the **Maximum log size** text box on the **Log Properties** page, enter the maximum size (in kilobytes) of the log.
7. Determine how you want the system to handle log file entries after the maximum log file size has been reached, and then click one of the following choices:
 - **Overwrite events as needed** — The system writes over older events with new events as they occur.
 - **Overwrite events older than _____ days** — The system retains the event entries for the specified number of days before the events can be written over by current event entries.
 - **Do not overwrite events** — The system retains all events in the log and appends new events to the end of the file.
8. Click **OK**.

Downloading Log Files

The NAS Manager allows you to download specific log files from your NAS system.

To download log files, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Logs**.
4. On the **Logs** page, select the type of log you want to download.
5. In the **Tasks** list on the *Log Type Log* page, click **Download Log**.
6. On the **Download Log Type Log** page, if available, select the file type that you want to download, and then click **Download Log**.
7. In the **File Download** dialog window, select **Save this file to disk**.
8. Specify a directory where the log will be saved, and then click **Save**.
9. Click **Close** to close the **File Download** dialog window after the download is complete.

Viewing Downloaded Log Files

After downloading the log files, it is possible to view them in the following ways:

- **.log** files — With a text editor such as Microsoft Notepad.
- **.csv** files — With a text editor or with Microsoft Excel.
- **.evt** files — With the Event Viewer. The Event Viewer can usually be found under **Administrative Tools** from the **Start** menu of a Windows 2000 system. In the **Event Viewer** window, click **Action** and then click **Open Log File**. Browse to the location of your log file, choose the log type of your file, and then click **Open**.

Clearing Log Files

1. Log in to the NAS Manager.
 2. Click **Maintenance**.
 3. Click **Logs**.
 4. On the **Logs** page, select the type of log you want to clear.
 5. Select the specific log you want to clear, and then click **Clear** in the **Tasks** list.
 6. On the **Clear Log Confirmation** page, click **OK** to clear the log.
-

Multiple Device Management

Multiple Device Management (MDM) is a part of the NAS Manager functionality that allows you to run jobs on one or more NAS systems simultaneously. You can use MDM to perform tasks such as adding a user or retrieving system status information on multiple NAS systems from a single system.

 **NOTE:** MDM is disabled by default in your NAS system.

MDM is composed of two components: a device and a controller. A device is a system that executes jobs received from a controller and returns the job results to the controller. Jobs can be applied to individual devices or to a group of devices called *sets*. The purpose of the controller is to discover other MDM-enabled devices, manage ownership of devices, and manage jobs. To use MDM services, one of your NAS systems must be designated as a controller.

Configuring MDM on Your NAS System

From the **MDM** tab in the NAS Manager, use the **Multiple Device Management Settings** option to configure controllers and devices and to disable MDM services.

Configuring an MDM Controller

When you configure your NAS system as an MDM controller, it becomes both a device and a controller for other MDM devices.

1. Log in to the NAS Manager.
2. Click **MDM**.
3. Click **Configure MDM**.

The **Multiple Device Management Settings** page displays and the **Configure MDM Type** tab is active.

4. Select **MDM Controller**.
5. Click **OK**.

The system automatically reboots.

Configuring an MDM Device

Your NAS system can be configured as a device that can be controlled by any controller (*trust mode*) or as a device controlled only by a controller with a specific certificate (*certificate mode*). If you choose trust mode, the first controller that attempts to control the device becomes the device's controller. In certificate mode, only the system with the uploaded certificate can control the device.

To configure your NAS system as a device, perform the following steps:

1. Log in to the NAS Manager.
2. Click **MDM**.
3. Click **Configure MDM**.

The **Multiple Device Management Settings** page displays and the **Configure MDM Type** tab is active.

4. Select **MDM Device**.
5. Select one of the following **MDM Device** options:
 - **Any controller** — Allows the system to be controlled by any MDM controller. Choosing this option puts the system in *trust mode*.
 - **Only the controller with the following certificate** — Allows the system to be controlled only by an MDM controller with a specific certificate. Choosing this option puts the system in *certificate mode*. If you choose this option, you must first copy the required certificate from the MDM controller to your local system (client), and then upload the required certificate from your local system (client) to the NAS system (MDM device).

To upload the certificate, perform the following steps:

- a. Click **Upload Certificate**.
- b. In the **Upload Certificate File** window, type the name of the certificate file or choose **Browse** to navigate to it.
- c. Click **Upload Certificate**.

The MDM controller certificate file is uploaded to the intended MDM device.

6. Click **OK**.

The system automatically reboots.

Resetting MDM

Resetting MDM will disable the MDM feature and remove the MDM designation from your NAS system. After MDM has been reset, your system will no longer be designated as a device or controller.

To reset MDM on your NAS system, perform the following steps:

1. Log in to the NAS Manager.
2. If the system is configured as a device, click **MDM**. If the system is figured as a controller, click **Controller**.
3. Click **Reset MDM**.
4. Click **OK**.

The system automatically reboots.

Viewing MDM Device Status

When your NAS system is configured as an MDM device, you can use the NAS Manager to track the status of the system.

To view the status of an MDM device, perform the following steps:

1. Log in to the NAS Manager.
2. Click **MDM**.

The **MDM Agent Status** page displays the following information:

- o **Require Certificate** — **Yes** indicates that the system is operating in *certificate mode*. **No** indicates that the system is operating in *trust mode*.
 - o **Certificate** — Indicates whether the certificate is installed.
 - o **Controller** — Displays the host name of the last controller to take control of the system.
-

Using the MDM Controller to Administer NAS Devices

The NAS Manager's MDM feature allows you to collectively administer several NAS devices in a data center. MDM also allows you to automate routine processes such as adding users and querying systems for status information.

From the NAS Manager **Controller** tab, you can run a job, view alerts and job history, take or release control of individual devices, group individual devices into sets, and administer multiple devices.

Creating and Using MDM Sets

Use the **Create Sets** option from the NAS Manager **Controller** tab to create and manage sets and to administer individual devices contained in sets. The **Create Sets** option displays an Object/Task Selector that simultaneously lists up to 100 sets that can be sorted by selecting a column heading. You can also create or delete sets, modify set properties, or run a job on one or more sets.

To create a new set, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Controller**.
3. Click **Create Sets**.
4. In the **Tasks** list, click **New**.
5. Type a name and description for the new set.
6. Select the members for the new set from the **Devices** or **Existing sets** list.
7. Click **OK**.

Controlling MDM Devices

Use the **Control Devices** option from the NAS Manager **Controller** tab to create or delete device records, group devices into sets, take or release control of devices, modify device properties, or run jobs on one or more devices.

Creating a New MDM Device Record

1. Log in to the NAS Manager.

2. Click **Controller**.
3. Click **Control Devices**.
4. In the **Tasks** list, click **Add Device**.
5. Type the name, optional description, and optional MAC addresses for the device you are adding.
6. Click **OK**.

Grouping Devices into a Set

1. Log in to the NAS Manager.
2. Click **Controller**.
3. Click **Control Devices**.
4. In the **Name** column of the Object/Task Selector on the **Devices** page, select one or more devices to group into a set.
5. In the **Tasks** list, click **Create Set**.
6. On the **Create Set** page, enter a name and description for the new set.
7. From the **Devices** or **Existing sets** lists, add any additional members for the new set.
8. Click **OK**.

Taking Control of a Device

1. Log in to the NAS Manager.
2. Click **Controller**.
3. Click **Control Devices**.
4. In the **Device Name** column of the Object/Task Selector on the **Control Devices** page, select the device you want to control.
5. In the **Tasks** list, click **Take Control**.

If the operation completes successfully, the Object/Task Selector on the **Devices** page is redisplayed, and the status of the device chosen shows as **Active** (or **Missing** if the device did not respond to a heartbeat request).

If the operation did not complete successfully, an error page is displayed, giving you the option to retry or terminate the operation.

Running an MDM Job

A job is an administration task executed on a single device or on all controlled devices in a set. Jobs can take many forms; they can be scripts executed on devices by the controller, or they can be special operations such as shutting down or rebooting a NAS system.

To run a job, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Controller**.
3. Click **Run Jobs**.

4. In the **Tasks** list, click **Run**.
5. Follow the instructions in the Run Job Wizard.

Using MDM Job Templates

In addition to sample job scripts provided with the NAS Manager MDM services, you can create custom scripts that can be run remotely on one or more devices. These custom scripts are then incorporated into job templates that can be used later for running jobs.

Creating a New Job Template

1. Log in to the NAS Manager.
2. Click **Controller**.
3. Click **Run Jobs**.
4. In the **Tasks** list, click **New**.
5. Follow the instructions in the Job Template Wizard.

When the Job Template Wizard completes, the **Run Jobs** page displays.

Running a New Job Template

1. Create a new job template as described in "[Creating a New Job Template](#)."

When the Job Template Wizard completes, the **Run Job** page displays.

2. In the Object/Task Selector of the **Run Job** page, select the new job template.
3. Click **Run**.
4. Follow the instructions in the Run Job Wizard.

Using Sample MDM Scripts

Sample scripts are located in the **c:\MDMScripts** directory on your NAS system. They include scripts that join systems to a domain or workgroup, create users, verify a Microsoft QFE installation, or change user passwords. You can either run these scripts or make them part of a job template.

 **NOTE:** To see an example of how each script is used, type '?' in the parameter field and then run the job. The output shows script usage.

 **NOTE:** When script parameters include a password, the password must be entered for each job run. If a password is included in a template, the password will be replaced by a '*'. The script will not run until the '*' is replaced with a valid password.

JoinDomain.vbs

The **JoinDomain.vbs** script will join a specific NAS system or device set to a domain.

The parameters of the **JoinDomain.vbs** script to join a domain are:

```
-join <domainname> <username> -password <password>
```

Where *domainname* is the name of the domain, *username* is the name of a user on the domain, and *password* is the domain user's password.

The parameters of the **JoinDomain.vbs** script to join a workgroup are:

```
-workgroup <workgroupname>
```

Where *workgroupname* is the name of the workgroup.

CreateUser.vbs

The **CreateUser.vbs** script will add a user to a specific NAS system or device set.

The parameters of the **CreateUser.vbs** script are:

```
[-group <group>] <username> -password <password>
```

Where *group* (optional) is the group to which the user is being added, *username* is the name of the new user, and *password* is the new user's password.

IsQFEInstalled.vbs

The **IsQFEInstalled.vbs** script uses a QFE number for a parameter to validate the installation of QFE on a specific NAS system or on each system in a device set.

The parameters of the **IsQFEInstalled.vbs** script are:

```
<qfenum>
```

Where *qfenum* is the "Q" number of a Microsoft QFE, such as Q111111.

SetUserPassword.vbs

The **SetUserPassword.vbs** script sets or changes a user password.

The parameters of the **SetUserPassword.vbs** script are:

```
<username> -password <password>
```

Where *username* is the name of the user whose password is being changed, and *password* is the new password.

Viewing MDM Job Histories

Use the **View Job History** option to view summary information about jobs that have been run previously by the controller. From the **View Job History** page, you can view summary results from a specific job or summary information about alerts that have been generated on devices where alerts are enabled.

Viewing Job Results

1. Log in to the NAS Manager.
2. Click **Controller**.
3. Click **View Job History**.
4. In the Object/Task Selector of the **View Job History** page, select the job you want to view.
5. In the **Tasks** list, click **View Results**.

If the job was performed on a device set, the **View Results** page displays an Object/Task Selector list for each device in the set.

6. In the Object/Task Selector of the **View Results** page, select the device you want to view.
7. In the **Tasks** list, click **Properties**.

Viewing Alerts

1. Log in to the NAS Manager.
 2. Click **Controller**.
 3. Click **View Alerts**.
 4. Select the check box next to the alert you want to view.
 5. In the **Tasks** list, choose **Alert Details**.
 6. On the **Alert Details** page, you can view information about the condition(s) that caused the alert, and then follow the instructions.
 7. Click **Clear Message** to delete the alert.
-

Shutting Down the NAS System

To shut down, restart, or schedule a shutdown of the NAS system using the NAS Manager, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Shutdown**.
4. Click **Shut Down**, **Restart**, or **Scheduled Shutdown**.
5. If you select **Scheduled Shutdown**, specify when the shutdown should occur, and then click **OK**.
6. On the **Confirmation** page, click **OK** to confirm the action.

If you choose to restart the NAS system, the **Restarting** page displays. When the NAS Manager detects that the NAS system has come back online, the NAS Manager automatically returns to the home page.



NOTE: Do not refresh or perform any function in the NAS Manager until it comes back online. If you click **Refresh**, the NAS Manager might not automatically refresh.

Managing Disks

The NAS Manager allows you to list available disks, rescan for a disk, create a hot spare, free a hot spare, force a disk online, and view disk properties.



NOTE: For more information on disk management procedures not included in this section, see your NAS Manager online help.

Listing Available Disks and Viewing Properties

1. Log in to the NAS Manager.
2. Click **Disks**.
3. On the **Disks** page, click **Disks**.
4. Select the adapter that contains the disks you want to list by clicking the adjacent radio button.
5. Click **Select** in the **Tasks** column.

A list of available disks is displayed along with the status of each disk.

6. Click the disk whose properties you want to view, and then click **Properties**.

The **Properties** page displays information such as disk status, capacity, device type, and vendor.

Rescanning for Disks

1. Log in to the NAS Manager.
2. Click **Disks**.
3. On the **Disks** page, click **Disks**.
4. Select the adapter that contains the disk you want to rescan by clicking the adjacent radio button.
5. Click **Select** in the **Tasks** column.

A list of available disks is displayed along with the status of each disk.

6. In the **Physical Disks** column on the **Disks** page, select the disk to rescan.
7. In the **Tasks** list, click **Rescan**.
8. On the **Rescan** page, click **OK** to start the rescan.

Creating a Hot Spare

1. Log in to the NAS Manager.
2. Click **Disks**.
3. On the **Disks** page, click **Disks**.
4. Select the adapter that contains the disk you want to make a hot spare by clicking the adjacent radio button.
5. Click **Select** in the **Tasks** column.

A list of available disks is displayed along with the status of each disk.

6. In the **Physical Disks** column on the **Disks** page, select the disk to make a hot spare.
7. In the **Tasks** list, click **Make Hotspare**.

Freeing a Hot Spare

1. Log in to the NAS Manager.
2. Click **Disks**.
3. On the **Disks** page, click **Disks**.
4. Select the adapter that contains the hot spare you want to free by clicking the adjacent radio button.
5. Click **Select** in the **Tasks** column.

A list of available disks is displayed along with the status of each disk.

6. In the **Physical Disks** column on the **Disks** page, select the disk to free.
7. In the **Tasks** list, click **Free Hotspare**.

Forcing a Disk Online

1. Log in to the NAS Manager.
2. Click **Disks**.
3. On the **Disks** page, click **Disks**.
4. Select the adapter that contains the disk you want to force online by clicking the adjacent radio button.
5. Click **Select** in the **Tasks** column.

A list of available disks is displayed along with the status of each disk.

6. In the **Physical Disks** column on the **Disks** page, select the disk to force online.
 7. In the **Tasks** list, click **Force Online**.
-

Managing Volumes

A volume is an allocation of usable space on one or more physical disks. The NAS Manager allows you to create, delete, expand, reconfigure, repair, or view the properties of a volume.

 **NOTE:** You can also create volumes using Array Manager. See "[Creating a Dynamic Volume](#)" in "Advanced Disk and Volume Management."

 **NOTE:** For more information on volume management procedures not included in this section, see your NAS Manager online help.

Creating a Volume

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volumes**.
4. On the **Tasks** list, click **New**.
5. Select the adapter where you want to create a volume by clicking the adjacent radio button.
6. Click **Select** in the **Tasks** column.
7. Select the disks to be used for the new volume.
8. Click **OK**.

Preparing for Volume Expansion

 **NOTE:** You cannot expand an internal RAID group.

The NAS Manager allows you to expand volumes, while retaining the same fault tolerance level. However, a volume must be prepared before it is expanded. During preparation, the original volume is still accessible.

 **NOTE:** See "[Advanced Disk and Volume Management](#)" for advanced operations on all RAID controllers.

To prepare a volume for expansion, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volumes**.
4. In the **Volumes** column, select the volume to prepare for expansion by clicking the adjacent radio button.
5. On the **Tasks** list, click **Prep Expand**.
6. Select the disks you want to add to this volume.
7. Click **OK**.

The RAID status changes to show the preparation is in progress. When completed, the volume is ready to expand.

 **NOTE:** This process may take several hours to complete.

Expanding a Volume

 **NOTE:** You cannot expand an internal RAID group.

After a volume has been prepared for expansion, the RAID status is marked as **Ready to Expand**.

 **NOTE:** See "[Advanced Disk and Volume Management](#)" for advanced operations on all RAID controllers.

To expand a volume, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volumes**.
4. In the **Volumes** column, select the volume to expand by clicking the adjacent radio button.
5. On the **Tasks** list, click **Expand**.
6. Click **OK**.

Deleting a Volume

 **NOTICE:** You must delete all shares and persistent images from your volume before deleting it. If a volume is removed before all shares of that volume have been removed, the NAS Manager may display shares incorrectly.

When you delete a volume, the operation cannot be undone. All the data in the volume will be lost.

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volumes**.
4. In the **Volumes** column, select the volume to delete by clicking the adjacent radio button.

5. In the **Tasks** list, click **Delete**.
6. Click **OK**.

Reconfiguring a Volume

 **NOTICE:** When you reconfigure a data volume, all data on the existing volume is deleted. Therefore, it is important to back up your data before reconfiguring a volume.

1. Manually remove all shares and persistent images before reconfiguring the volume.

 **NOTE:** If the volume is in use or contains shares or persistent images, you cannot reconfigure the volume. The message `Use Array Manager` is displayed. The administrator can use Array Manager to force deletion of the volume. See "[Using the Array Manager to Manage Your Disks and Volumes](#)" in "Advanced Disk and Volume Management."

2. If a message is displayed during the deletion process indicating that the deletion cannot be completed, use Array Manager to perform this task.

See "[Using the Array Manager to Manage Your Disks and Volumes](#)" in "Advanced Disk and Volume Management."

3. Log in to the NAS Manager.
4. Click **Disks**.
5. Click **Volumes**.
6. In the **Volumes** column, select the volume whose properties you want to view by clicking the adjacent radio button.
7. On the **Tasks** list, click **Reconfigure**.

If **Repair** appears instead of **Reconfigure**, your volume is damaged and needs to be repaired. See "[Repairing a Volume](#)."

8. Select the **New Layout**, which is either **Single RAID-5** or **Single RAID-0**.

 **NOTE:** RAID-0 volumes are not fault-tolerant and do not provide data protection if a drive fails.

9. Click **OK** to delete and reconfigure the volume.

 **NOTE:** If the volume is in use—for example, if the volume is open in a browser window, the volume contains shares or snapshots, or another application is using the volume—a message displays indicating that the operation has failed and you need to use Array Manager. See "[Advanced Disk and Volume Management](#)" for more information.

Repairing a Volume

The operating system is loaded on a fault-tolerant RAID-1 mirrored volume, and data drives are originally configured as RAID-5 volumes. If an operating system drive or a data drive fails, use the NAS Manager to repair the volume and restore its fault tolerance.

 **NOTE:** RAID 0 volumes are not fault-tolerant and cannot be repaired.

1. Shut down the NAS system.

See "[Shutting Down the NAS System](#)."

2. Remove the failed hard drive.
3. Insert a new hard drive ordered from Dell that is the same size as or larger than the failed drive.

 **NOTE:** The repair feature will not work if you insert a hard drive that is smaller than the failed drive.

4. Power on the NAS system.
5. Log in to the NAS Manager.
6. Click **Disks**.
7. Click **Volumes**.
8. Click **Repair**.

If the repair button does not appear, then you do not have a drive that is the same size as or larger than the failed drive, or you did not have the drive in the system when the system booted.

9. Click **OK**.

 **NOTE:** The process of fully rebuilding the RAID volumes may take several hours.

 **NOTE:** If the volume is in use—for example, the volume is open in a browser window, the volume contains shares or snapshots, or another application is using the volume—a message displays stating that the operation has failed and that you need to use Dell OpenManage Array Manager. See "[Advanced Disk and Volume Management](#)" for more information.

Viewing Volume Properties

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volumes**.
4. In the **Volume** column, select the volume whose properties you want to view by clicking on the adjacent radio button.
5. On the **Tasks** list, click **Properties**.
6. Click **OK** to return to the **Volumes** window.

Using the PowerVault Advanced Administration Menu

The Advanced Administration Menu is a software application that provides links to advanced functionality in your NAS system. The menu runs automatically when you access your NAS system through Terminal Services.

To access the Advanced Administration Menu, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**, and then log in to the NAS system as an administrator.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The Advanced Administration Menu displays. If it does not display, double-click the **Advanced Administration Menu**

icon on the desktop of the NAS system.

4. Click **Administrative Tools** or **System Management** to display the list of selectable options.
5. Click the tool or setting you want.
6. When you are finished using the Advanced Administration Menu, log off by clicking **Logoff** at the bottom of the Advanced Administration Menu.

The following tools are available through the Advanced Administration Menu:

- **Broadcom Network Teaming** — Launches Broadcom Advanced Server Control Suite, which allows you to perform advanced functions on Broadcom NICs, such as setting up teaming and virtual LANs.
- **Distributed File System** — Allows management of multiple network shares.
- **Event Viewer** — Allows you to view events in your application log, security log, and system log.
- **Intel Network Teaming** — Launches Intel® PROSet II, which allows you to perform advanced functions on Intel NICs, such as setting up teaming and virtual LANs.
- **Network Tools** — Displays the **Network Tools Interface Utility**, which allows you to perform operations such as nslookup, ping, and tracer.
- **Performance Monitor** — Displays the Performance Monitor.
- **Perform System State Backup** — Enables you to back up your system-state data.
- **Retrieve Dell Service Tag** — Provides the Dell service tag number for your NAS system.
- **Windows Powered Help** — Displays help for the Windows Powered operating system.
- **Windows QFEs** — Displays the QFEs installed on the NAS system.
- **Windows 2000 Backup/Recovery** —Launches Windows 2000 Backup and Recovery Tools.
- **Computer Management** — Provides management for local or remote computers.
- **Dell Remote Assistant Setup** — Configures the remote access IP address, user name and password.
- **Disk Management** — Launches Dell OpenManage Array Manager, which provides comprehensive storage management for your disks and volumes.
- **Internet Information Services** — Provides management for Internet Information Services on the system.
- **Local Security Settings** — Enables you to manually set security settings.
- **Network Properties** — Displays the **Network and Dial-up Connections** window.
- **NFS Cache** — Enables and disables the NFS write-back cache.
- **Removable Storage** — Enables you to track or manage storage media and devices.
- **Set Date/Time** — Allows you to set the date and time.
- **Set Regional Options** — Displays the **Regional Options** window, which allows you to change the locale and language settings for the system.
- **Task Manager** — Provides applications, processes, and performance information.
- **Terminal Services Config** — Enables you to configure Terminal Services.

Click the **Language** link to change the language of the Advanced Administration Menu to Chinese, English, French, German, Japanese, or Spanish.

Advanced Disk and Volume Management

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [Using the Array Manager to Manage Your Disks and Volumes](#)
- [Array Manager Common Tasks](#)
- [Managing Disk Arrays](#)
- [Array Disk Commands](#)
- [General Controller Commands](#)
- [Disk Management](#)
- [Volume Management](#)
- [Working With Dynamic Volumes](#)
- [Enclosure Management](#)

This section provides information about using Dell OpenManage™ Array Manager to manage your disks, volumes, and physical hard drives.

Using the Array Manager to Manage Your Disks and Volumes

Although Dell OpenManage Array Manager provides a comprehensive solution to storage management, you should use it for *advanced features* that cannot be performed from the **Disks** tab in the NAS Manager.

Array Manager allows you to configure your storage devices and logical volumes contained in your system. Array Manager displays storage configuration in both a physical and a logical view. The physical view shows the physical connections between the storage devices. The logical view shows a logical representation of your storage as logical volumes.

Array Manager provides a single console for array and volume configuration, from which you can do the following:

- Manage the hardware redundant array of independent disks (RAID) solution
- Manage external storage subsystems
- Display all of your storage information in a graphical environment

Launching Array Manager From the NAS Manager

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**.
4. Log in to the **Terminal Services** session as an administrator.

 **NOTE:** The NAS Manager default administrator user name is `administrator` and the default password is `powervault`.

5. From the **Advanced Administration Menu**, click **Disk Management** under **System Management**.

 **NOTE:** If the **Advanced Administration Menu** does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

6. If a Dell OpenManage Array Manager window with buttons such as **Create Volume** or **Create Virtual Disk** displays, click the task you want to perform, or close the window to view the Array Manager console.

 **NOTE:** To automatically launch Array Manager into the console window, ensure that **Show this window at start-up** is *not* selected.

Array Manager Console

The Array Manager console display uses a tree view to display storage objects in the left pane of the window and tabbed views in the right pane to display additional information about storage objects. The following subsections provide more information about the left and right panes.

Left Pane

The left pane shows objects that the Array Manager software detects. The major storage objects are the local system object, arrays, disks, and volumes. By clicking the plus sign (+) in front of a storage object, you can see the subordinate storage objects under that object.

- Arrays represent the physical and logical storage subsystems connected to RAID controllers.
- Disks represent the disks recognized by the Microsoft® Windows® Powered operating system.
- Volumes include dynamic RAID volumes created in Array Manager, primary and extended partitions, and logical drives associated with extended partitions.
- **My Network Places**, **History**, and **Favorites** provides remote connection functionality not supported by the NAS system and should be ignored.

Right Pane

The right pane identifies the various objects and their status and displays any error conditions that might exist. The four tabbed views in the right pane include the following:

- The **General** tab displays parameters based on the objects you select in the console's tree view.

The parameters for **Disks** are as follows:

- **Name** is the name of the object.
- **Status** can vary, depending on the object. Common status conditions are **Online**, **Healthy**, and **Resynching**.
- **Type** identifies the object, such as **Basic Disk**.
- **Disk Group** shows an entry for disks in a basic or dynamic group.
- **Capacity** is the maximum size of the disk.
- **Unallocated Space** is the amount of free hard-drive space still available.
- **Graphical Layout** is a graphical representation of how much of the disk is being used.
- **Progress** shows the current progress (percentage of completion) for tasks.
- **Device** is the type of disk: All of the drives on the NAS system are SCSI drives.
- **Port** identifies the controller card. A SCSI port has zero or more target IDs, and a target ID has one or more logical unit numbers (LUNs).
- **LUN** is the logical unit number.
- **Target** is the SCSI ID that uniquely identifies the disk on the controller card.

- **Vendor** identifies the vendor on hardware objects.

The parameters for **Volumes** are as follows:

- **Name** is the name of the object.
 - **Status** can vary, depending on the object. Common status conditions are **Online**, **Healthy**, and **Resynching**.
 - **Layout** identifies the object, such as **Basic Primary Partition**.
 - **Disk Group** shows an entry for disks in a basic or dynamic group.
 - **Capacity** is the maximum size of the disk.
 - **Free Space** is the amount of free hard-drive space still available.
 - **Progress** shows the current progress (percentage of completion) for tasks.
 - **File System** shows the type of file system.
 - **Graphical Layout** is a graphical representation of how much of the disk is being used.
-
- The **Events** tab displays event log messages associated with storage objects.
 - The **Disk View** tab displays a graphical layout of the disks on your system, including CDs or other removable media.
 - The **DM View** tab is grayed-out on the Array Manager console.

Array Manager Common Tasks

This section provides a high-level description of the most common procedures performed using Array Manager. For more information, see your Array Manager documentation.

Creating a New Volume

1. Create a RAID 5 virtual disk from the available pool of physical drives.
2. Write a signature to the disk created.
3. Upgrade the disk to dynamic.
4. Create a new volume on the upgraded disk.
5. Assign the next available drive letter, and then format the volume as an NT File System (NTFS).



NOTE: Your NAS system supports only NTFS partitions. Formatting all partitions as NTFS allows for advanced features only available under that file system.

Deleting an Existing Volume

1. Select and delete the appropriate volume.
2. Revert the disk that contained the volume to a basic disk.
3. Determine the virtual disk that corresponds to the basic disk.
4. Delete that virtual disk.

Expanding an Existing Volume

1. Find the virtual disk that corresponds to the volume you are going to expand.
2. Add a member to that virtual disk.



NOTE: After adding a member to a virtual disk, the virtual disk is reconstructed by the adapter. This operation will take several hours.

3. After the virtual disk has completed the reconstruction process, perform a **rescan operation**.
4. Extend the specified volume with the new space available to the virtual disk.

Managing Disk Arrays

This section describes how to use Array Manager to configure and manage arrays with the Dell™ PowerEdge™ Expandable RAID Controller 3/Dual Channel (PERC 3/DC) and PERC 3/QC controllers that are included with your NAS system. The PERC 3/DC and PERC 3/QC controllers are high-performance, intelligent, PCI-to-SCSI host adapters with RAID capabilities which allow you to create up to 40 virtual disks per controller.

The following topics are discussed:

- Recommended virtual disk configuration
- Creating virtual disks
- Deleting virtual disks
- Reconfiguring and managing virtual disks

Creating Virtual Disks

The first step in configuring your system for improved system management is creating virtual disks.



NOTE: Virtual disks created using a supported PERC controller card cannot be created from array disks with an aggregate size greater than 2 terabytes (TB). For example, you cannot select more than 30 array disks that contain 73 gigabytes (GB) regardless of the size of the resulting virtual disk. When you attempt to select more than 30 disks of this size, a message displays that indicates that the 2-TB limit has been reached and that you should select a smaller number of array disks. This is a standard SCSI limitation.



NOTE: To take advantage of all the system features such as **Defrag** and **Encryption**, use the default value of 64 KB for the stripe size when creating a virtual disk.

To create a virtual disk, perform the following steps:

1. Right-click an array group.
2. Click **Create Virtual Disk** to launch the **Create Virtual Disk Wizard**.
3. Read the **Welcome** screen, and then click **Next** to continue.

The **Select Creation Mode** dialog box displays. You can cancel the operation at any time by clicking **Cancel**.

4. Select **Custom Mode**, and then click **Next** to continue.

The **Select Disks and Virtual Disk Attributes** screen displays.

5. Select the disks and confirm information presented in the wizard.

 **NOTE:** Your NAS system supports only NTFS partitions. Formatting all partitions as NTFS allows for advanced features only available under that file system.

6. Click **Next** to continue.

The **Completing the Create Virtual Disk Wizard** dialog box displays.

7. Click **Finish** to create a virtual disk or **Back** to return to the previous screen.

Array Manager confirms the creation of the virtual disk.

The **Rescan Disk Layout** checkbox is selected by default. **Rescan Disk Layout** allows the Microsoft Windows Powered operating system to recognize the new virtual disk. You can perform a **Rescan Disk Layout** later if the box is not checked when you create the virtual disk.

Deleting Virtual Disks

 **NOTICE:** Deleting a virtual disk permanently deletes all information contained on that disk.

1. Right-click the virtual disk.
2. Click **Delete**.

A confirmation dialog box appears.

3. Click **OK** to continue.

The virtual disk disappears from the left pane.

Reboot your system after deleting a virtual disk and before creating new virtual disks.

Reconfiguring and Managing Virtual Disks

This section summarizes how you can change the virtual disk configuration through the NAS Manager. The following topics are discussed:

- Using Add Member
- Using Transform Type
- Using Change Policy
- Using Check Consistency
- Initializing disks
- Properties
- Blink Virtual Disk
- Unblink Virtual Disk

 **NOTE:** Because of hardware restrictions, the PERC 3/DC and PERC 3/QC controllers will not detect a drive status change until you attempt to read from or write to the drive. For example, when an unconfigured drive is removed, the controller will not detect the change until a you perform a manual rescan or read/write to the drive.

Using Add Member

Perform the following steps to add array disks to a virtual disk or to change the virtual disk's RAID level:

1. Right-click a virtual disk.
2. Click **Add Member**.

A **Virtual Disk Add Member** dialog box appears. The available disks are listed in the left pane. You can choose appropriate disks to add by selecting them and using **Add Disk** to move them to the right pane.

3. Choose the RAID level in the **Virtual Disk Type** pull-down menu.
4. Click **OK** to continue or **Cancel** to cancel the operation.

Add Member shows progress information in the right pane.

5. To view your progress, click the parent of the virtual disk.

The status of the virtual disk will be **Reconstructing**, and progress information displays until the **Add Member** operation is finished. At the end of the operation, the **Type** category shows the changed RAID level.

Using Transform Type

The following is a list of supported RAID level migrations:

- RAID 1 to RAID 0
- RAID 5 to RAID 0

To change a RAID level of a virtual disk without adding or removing disks, perform the following steps:

1. Right-click the virtual disk whose type you want to transform.

The **Virtual Disk Transform Type** dialog box appears.

2. Select **RAID Type** or **Stripe Size** from the available choices.
3. Click **OK** to continue or **Cancel** to quit the operation.

A warning dialog box appears asking if you want to continue.

4. Click **Yes**.

Transform Type displays progress information in the right pane.

5. To view progress, click the parent of the virtual disk.

The status of the virtual disk will be **Reconstructing**, and progress information displays until the operation is finished. At the end of the operation, the **Type** category shows the changed RAID level.

Using Change Policy

To change the cache policies of a virtual disk, perform the following steps:

1. Right-click a virtual disk.
2. Click **Change Policy**.

The **Virtual Disk Change Policy** dialog box displays.

3. From the pull-down menu, choose the policies you want.

You can enable or disable the write-cache or enable or disable the read-cache.

4. Click **OK** to continue or **Cancel** to quit the operation.

When you are finished, click **Properties** to verify if the policy changes occurred.

Using Check Consistency

If your disk is in a degraded state, using **Check Consistency** might enable you to restore your disk to **Ready** status.

To check mirror synchronization and rebuild parity if necessary, perform the following steps:

1. Right-click the virtual disk to be checked.
2. Click **Check Consistency**.

The **Check Consistency** operation displays progress information in the right pane.

3. To view progress, click the parent of the virtual disk.

The status of the virtual disk is **Resynching**, and progress information displays until the operation is finished.

Initializing Virtual Disks

Initialize any virtual disk before you use it.

Perform the following procedure on any virtual disk on a PERC 3/DC or PERC 3/QC controller system.

 **NOTICE:** All data on the virtual disk is lost when the disk is initialized.

1. Right-click the virtual disk that you want to initialize.
2. Click **Initialize**.

The status of the disk displays **Initializing** in the right pane until the operation is finished.

Properties

This command displays a window that shows the properties associated with the virtual disk.

Blink Virtual Disk

This command allows you to locate the array disks included in a virtual disk by blinking the LEDs on the array disks. This command automatically cancels after a short duration such as 30 or 60 seconds.

Unblink Virtual Disk

This command allows you to cancel the **Blink Virtual Disk** command before the 30- or 60-second time limit has been reached.

Array Disk Commands

This section describes the following commands for working with array disks:

- Format
- Rebuild
- Assign global hot spare
- Unassign global hot spare
- Online array disk
- Offline array disk
- Prepare to remove
- Properties

Format

The **Format** command performs a low-level formatting of the array disk. To format the array disk, perform the following steps:

1. Right-click the disk that you want to format.
2. Click **Format**.

The right pane shows the status of the format. The status displays **Formatting** until the operation is finished.

Rebuild

The **Rebuild** command is enabled only when a disk has failed. You can rebuild only on failed disks in redundant arrays (RAID 1 or RAID 5) by performing the following steps:

1. Right-click the failed disk that you want to rebuild.
2. Click **Rebuild**.

In the right pane, the status of the disk is **Rebuilding** and a progress bar shows the percentage of completion.

 **NOTE:** This process may take several hours.

Assign Global Hot Spare

A hot spare is an unused backup disk that is part of the array group. Hot spares remain in standby mode. When an array disk in a virtual disk fails, the assigned hot spare will be activated to replace the failed array disk without interrupting the system or requiring your intervention.

You can change the hot-spare disk assignment by unassigning a disk and choosing another disk to assign, as needed.

To assign a global hot spare, perform the following steps:

1. Right-click the array disk that you want to use as a hot spare.
2. Click **Assign Global Hot Spare**.

The **Assign Hot Spare** dialog box appears.

3. Confirm the successful completion of the operation by checking the properties displayed in the right pane.

The status of the array disk must be **Ready** and the type must be **Spare Array Disk**.

Unassign Global Hot Spare

The **Unassign Global Hot Spare** command unassigns the hot-spare disk. To unassign the hot-spare disk, perform the following steps:

1. Right-click the disk that is assigned as a hot spare.
2. Click **Unassign Global Hot Spare**.
3. Confirm the successful completion of the operation by checking the properties displayed in the right pane.

The status of the array disk must be **Ready** and the type must be **Array Disk**.

Online Array Disk

You can only set to **Online** an array disk that is part of a virtual disk that has been set to **Offline**.

1. Right-click the disk that you want to set to **Online**.
2. Click **Online**.

In the right pane, the status of the disk is changed from **Offline** to **Online**.

Offline Array Disk

You can only set to **Offline** an array disk that is part of a virtual disk that has been set to **Online**.

1. Right-click the disk that you want to set to **Offline**.
2. Click **Offline**.

A confirmation dialog box appears.

3. Click **OK** to continue.

In the right pane, the status of the disk will be changed from **Online** to **Failed**.

Prepare to Remove

Use this procedure to prepare for removing an array disk from a PERC 3/DC or PERC 3/QC controller.

 **NOTICE:** To prevent data loss, Dell recommends that you perform this operation before you remove any physical disk from an enclosure.

1. Right-click the disk that you want to remove.
2. Click **Prepare to Remove**, and then click **OK** to continue.

When the lights on the disk you have prepared to remove stop blinking, the disk is ready to be physically removed. The disk will not be listed in the array group.

Properties

Use this command to display the array disk properties.

General Controller Commands

This section describes the general controller operations:

- Rescan controller
- Flush cache
- Enable alarm
- Disable alarm
- Rebuild rate
- Properties

Rescan Controller

The **Rescan Controller** command can be used to check whether any new disks were attached after a configuration was set. To rescan the controller, perform the following steps:

1. Right-click the controller you want to rescan.
2. Click **Rescan Controller**.

After the operation is finished, the console is refreshed and the newly attached disks (if there are any) will appear under the **Array Disk Group** object and under the controller object.

Flush Cache

The **Flush Cache** command forces the PERC 3/DC and PERC 3/QC controllers to write the contents of cache memory onto the virtual disks. You might want to use this option if you find your application or disks in an unstable condition.

Enable Alarm

The **Enable Alarm** command enables the controller alarm setting. When enabled, the alarm sounds in the event of a device failure.

To enable the alarm sound, perform the following steps:

1. Right-click a controller.
2. Click **Enable Alarm**.

Disable Alarm

The **Disable Alarm** command disables the alarm. If disabled, the alarm does not sound in the event of a device failure.

To disable the alarm sound, perform the following steps:

1. Right-click a controller.
2. Click **Disable Alarm**.

Rebuild Rate

The **Rebuild Rate** command changes the rebuild rate settings. The rebuild rate is the fraction of the compute cycles dedicated to rebuilding failed drives. A rebuild rate of 100 percent means the system is totally dedicated to rebuilding the

failed drive.

During a rebuild, the complete contents of an array disk are reconstructed. A rebuild operation can occur during normal operation; however, it will degrade performance. You can reduce the rebuild rate to maintain system performance during the rebuild operation; however, a reduced rebuild rate extends the rebuild time.

 **NOTICE:** The default rebuild rate is 30 percent. System performance might be degraded if you change the rebuild rate to a higher value than the default.

The PERC 3 rebuild rate can be configured between 0 percent and 100 percent. At 0 percent, the rebuild is only done if the system is idle. At 100 percent, the rebuild rate has a higher priority than any other system activity.

Properties

The **Properties** command displays controller attributes.

To view properties, perform the following steps:

1. Right-click the appropriate controller.
2. Click **Properties**.

A **Controller Properties** dialog box appears displaying **Name**, **Vendor**, **Status**, **Type**, **Firmware Version**, and **Cache Size** of the controller.

Disk Management

This section describes conceptual and procedural information about how Array Manager implements basic and dynamic disks.

The following topics are discussed:

- Writing a disk signature
- Upgrading a basic disk to a dynamic disk
- Reactivating dynamic disks
- Merging foreign disks
- Monitoring disk reliability

Writing a Disk Signature

When you create a virtual disk and perform a rescan, the newly created virtual disk appears under the **Disks** node. The unsigned disk displays an error bitmap on the icon. The **Disk Type** is **Unsigned Disk**. The unsigned disk cannot be used until it has a signature on it.

To write a disk signature, right-click the unsigned disk. A menu displays showing the **Write Signature** command. (The **Write Signature** command appears only if a disk does not have a signature on it.) Select this command to write a signature on the disk.

After a signature is written on a disk, the disk displays as a **Basic Disk**. You can create partitions on the basic disk, or you can upgrade the disk to dynamic to create volumes on it.

 **NOTE:** Upgrade all data disks on the system to dynamic before creating any volumes. This allows the system to support online volume extension. Even though it is possible to upgrade disks with existing volumes to dynamic, those volumes cannot be extended. Only volumes created on disks that are already dynamic can be extended.

 **NOTICE:** Because of system recovery limitations, the operating system disk must remain a basic disk. All other disks should be upgraded to dynamic during creation.

Upgrading a Basic Disk to a Dynamic Disk

Because only dynamic disks can be used for online volume extension, it is recommended that you use Array Manager to upgrade all data disks on your system to dynamic. The upgrade includes new disks, which are added to the system as basic disks.

-  **NOTICE:** Because of system recovery limitations, the operating system disk must remain a basic disk. Do not upgrade your operating system disk to dynamic.

To upgrade a basic disk to a dynamic disk, perform the following steps:

1. Right-click the disk you want to upgrade, and then click **Upgrade Dynamic Disk**.

The **Upgrade Disk Wizard** provides information about upgrading.

2. Click **Next** to continue.

You are asked to select the disks to upgrade.

3. Add the basic disks you want to upgrade to the list of dynamic disks, and then click **Next**.
4. Click **Finish**.

-  **NOTE:** After a disk is upgraded to dynamic it cannot be reverted back to basic unless all volumes on that disk are removed. Dell strongly recommends that you do not revert a disk back to basic after data volumes are present.

Reactivating Dynamic Disks

A dynamic disk might appear as a missing disk when it is corrupted, powered down, or disconnected. You can reactivate a dynamic disk to bring it back online by performing the following steps:

1. Right-click the disk marked **Missing** or **Offline dynamic disk**.
2. Click **Reactivate Disk** on the menu.

The disk should be marked **Online** after the disk is reactivated.

Merging Foreign Disks

Dynamic disks with a foreign status are disks that have been moved from another system. You cannot reactivate a foreign disk; you must merge the disk to the system. To change the status of a foreign disk and enable it to be seen as a part of the current system, use the command **Merge Foreign Disk**.

Perform the following steps to merge foreign disks:

1. From the NAS Manager, log on to the **Terminal Services Advanced Client**.

-  **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

2. Launch the Dell OpenManage Array Manager by clicking the **System Management** in the **Advanced Administration Menu**, and then clicking **Computer Management**.

Foreign disks will appear in the disk list and graphical views as **Foreign**.

3. Right-click a foreign disk, and then click **Merge Foreign Disks**.

The **Merge Foreign Disk Wizard** displays.

4. Select the foreign disks that you would like to merge to the system.

By default all foreign disks are selected to be merged.

5. Click **Next**.
6. Click **Next** again to validate the volume status of each foreign disk.
7. Click **Finish**.

Monitoring Disk Reliability

Array Manager supports Self-Monitoring Analysis and Reporting Technology (SMART) on array disks that are SMART enabled.

SMART performs predictive failure analysis on each hard drive and sends an alert if a hard disk failure is predicted. The RAID controllers check the array disks for failure predictions. If the RAID controller predicts a failure, it passes the information to the Array Manager. Array Manager immediately displays an alert icon for the hard drive, raises an alert under the **Events** tab, and puts an alert message in the Windows Powered Event Log.



NOTE: The supported PERC controllers do not report SMART alerts for unassigned or hot-spare hard drives. Also, when you pause controller I/O, the controller does not send SMART alerts or events.

Volume Management

This section describes conceptual and procedural information about how Array Manager implements basic and dynamic volumes.

The following topics are discussed:

- Volume overview
- Checking partition or volume properties
- Formatting a partition or volume
- Deleting a partition or volume

Volume Overview

A volume is a logical entity that consists of portions of one or more physical disks. A volume can be formatted with a file system and can be accessed by a drive letter.

Like disks, volumes can be basic or dynamic. In Array Manager, basic volumes refer to all volumes that are not on dynamic disks. Dynamic volumes are logical volumes created from dynamic disks with Array Manager.

In your system, create all data volumes and dynamic volumes on dynamic disks. Only the operating system drive should remain basic because of system recovery limitations.

Checking Partition or Volume Properties

1. Right-click the partition or volume to be checked.
2. Choose **Properties** from the context menu.

The **Properties** window displays.

3. Check the properties for your volume.

Formatting a Partition or Volume

1. Right-click the volume or partition you want to format, and then click **Format**.
2. Choose **NTFS** as the file system type.

 **NOTE:** Your NAS system supports only NTFS partitions. Formatting all partitions as NTFS allows for advanced features only available under that file system.

3. Enter a label for the volume.

The label appears on the Array Manager console. If a name has been selected, this name appears in the **Name** field. You can change the name by typing a different name.

4. Enter an allocation size or use the default, which is automatically selected.
5. Select the file system type and formatting options:
 - **Quick format** — This option formats the volume or partition without scanning for bad sectors in the volume or partition. Check this box to use this format method.
 - **Enable file and folder compression** — This option can be used only if you selected NTFS format. Check this box to use this format method.
6. Click **OK** to begin formatting.

A progress bar displays in the list view.

Deleting a Partition or Volume

 **NOTICE:** You must delete all shares and persistent images from your volume before deleting it. If a volume is removed before all shares of that volume have been removed, the NAS Manager might not display shares correctly.

1. Right-click the designated volume, and then click **Delete Volume**.
2. Click **Yes** to delete or **No** to cancel.

The volume is removed immediately if you click **Yes**.

Working With Dynamic Volumes

Dynamic volumes are volumes created on dynamic disks with Array Manager. This section discusses how to create and extend dynamic volumes.

Creating a Dynamic Volume

 **NOTE:** To take advantage of all the system features such as *defrag* and *encryption*, it is recommended that you use the default value of 64 KB for the allocation unit size when creating a virtual disk.

 **NOTE:** The maximum supported volume size is 2 TB.

1. From the toolbar, click the **Create Volume** icon.

The **Create Volume Wizard** appears.

2. Click **Next**.

You are prompted to select whether to create a partition or a volume. Ensure that the **Dynamic** volume button is highlighted.

The dynamic group to which the volume will belong is automatically created and appears selected.

3. Click **Next**.

You are prompted for the volume layout and size of the volume to create.

4. Select the concatenated dynamic volume types.



NOTE: Software mirroring, striping, and software RAID are not recommended because of performance degradation.

5. Provide a size in MB or GB.

6. Click **Next**.

When you create the volume, you will see a **Query Max Size** button. **Query Max Size** works differently depending on whether you have one disk or multiple disks selected.

- If you have no disks selected and you click **Query Max Size**, the size shown in the **Total volume size** entry field will be the maximum for all available disks.
- If a disk or disks are selected and you click **Query Max Size**, the size indicated will be the maximum size for the selected disk(s). However, if you click **Query Max Size** a second time, the size will be the maximum for all available disks.

7. After all selections are made, verify your settings, and then click **Next**.

You can choose a different disk for the volume you are creating.

8. Click **Modify** to display the **Modify Disks** dialog box.

9. Click the disk you want to change, and then click the arrow to select a disk from the drop-down menu.

10. Choose a drive letter.

11. Click **Next**.

12. Format the volume using **NTFS** as the volume type.

13. Select an allocation unit size, if you chose to use a size other than the default.

14. Choose the file system type and, if wanted, a formatting option.



NOTE: **Quick format** formats the disk without checking for bad sectors.

15. Click **Next**, and then click **Finish**.

Extending a Dynamic Simple or Spanned Volume

You can extend a volume only if the following are true:

- The volume is formatted as NTFS.
- The volume was originally created on a dynamic disk.
- Unallocated space exists on a dynamic disk onto which the volume will be extended.

You cannot extend a volume if any of the following are true:

- The volume is formatted as FAT or FAT32.
- The volume is using software RAID (striped, mirrored, or RAID 5 volume).
- Unallocated space is not available on a dynamic disk.

You can extend simple and spanned volumes on dynamic disks onto a maximum of 32 dynamic disks. After a volume is extended, it cannot be mirrored or striped using software RAID. No portion of a spanned volume can be deleted without deleting the entire spanned volume.

1. Right-click the simple or spanned volume you want to extend, and then click **Extend Volume**.

The selected volume appears in the dialog box along with its current size.

2. Enter the amount to extend the volume, and then click **OK**.

Ignore any system messages that you might see while the volume extends. You do not have to run any special utilities.

3. Click **OK**.

The volume now shows the size of the extended volume.

Enclosure Management

The PERC 3/DC and PERC 3/QC controllers support enclosure management. Array Manager displays the properties of the enclosure's fans, power supply, and temperature probes. Array Manager also notifies you of enclosure status changes through events that are displayed on the **Events** tab and logged in the **Windows Powered Event Log**.

Enclosure Components in the Tree View

When you expand a storage subsystem in the Array Manager tree view in the left pane, you see the controllers that are attached to the storage subsystem. You can expand the controller to display the controller's channels. Expanding an enclosure channel displays the enclosure's fans, power supply, and temperature probes. Each of these objects expands to display the individual fans, power supplies, and temperature probes within the enclosure.

Thermal Shutdown

Enclosure management provides a feature which automatically shuts down the operating system, the server, and the enclosure when the enclosure's temperature reaches dangerous temperature extremes. The temperature when shutdown occurs is determined by the enclosure temperature probe's **Minimum Error Threshold** and the **Maximum Error Threshold**. These thresholds are default settings that cannot be changed.

Enclosure Fans

The fans that are installed in the enclosure are displayed under **Fans** in the tree view in the left pane. You can select and expand **Fans** to display the individual fans and their status information in the right pane. You can also expand **Fans** to display the individual fans in the left page.

If you right-click the **Fans** object or an individual fan, a context menu is displayed with a **Properties** option.

Enclosure Power Supplies

The power supplies that are installed in the enclosure are displayed under **Power Supplies** in the tree view. Select **Power Supplies** in the left pane to display the individual power supplies and their status information in the right pane. You can also

expand **Power Supplies** to display the individual power supplies in the left pane.

If you right-click **Power Supplies** or an individual power supply, a context menu displays with a **Properties** option.

Enclosure Temperature Probes

The temperature probes that are installed in the enclosure are displayed under **Temperature Probes** in the tree view. You can select **Temperature Probes** to display the individual temperature probes and their status information in the right pane. The status information includes the current temperature in Celsius and the warning and error thresholds for the temperature probe. The error threshold has a default value that cannot be changed. However, you can set the warning threshold. See the **Set Thresholds for Temperature** command in "[Enclosure Commands](#)" for information on setting the warning threshold.

Right-clicking **Temperature Probes** in the left pane displays a context menu with a **Properties** option. You can also expand **Temperature Probe** to display the individual temperature probes in the tree view. Right-clicking an individual temperature probe also displays a context menu with a **Properties** option. This option enables you to set the minimum and maximum warning threshold for the selected temperature probe.

Enclosure Commands

This section describes the commands associated with the enclosure and its fans, power supplies, and temperature probes. For the commands associated with the array disks in an enclosure, see "[Array Disk Commands](#)."

Right-clicking an enclosure object in the tree view displays a context menu with the enclosure commands. Right-clicking the enclosure's fans, power supplies, and temperature probes also displays a context menu for each of these components.

The enclosure's context menu items can vary depending on the model of the enclosure. The enclosure context menu might include any of the following commands:

- **Rescan** — Checks whether any new array disks and other components such as fans or temperature probes have been added to the enclosure.
- **Enable Alarm** — Enables an audible alarm that sounds whenever the fault LED lights.
- **Disable Alarm** — Turns off the audible alarm settings. If the alarm is already sounding, you can turn it off with this command.
- **Set Tag Data** — Allows you to enter or change asset information for the enclosure.
- **Download Firmware** — Allows you to download firmware to the enclosure.



NOTE: The **Download Firmware** command is only available on the Dell PowerVault™ 220S and PowerVault 221S enclosures.

- **Enclosure Properties** — Displays enclosure properties.
- **Set Thresholds for Temperature** — Sets the minimum and maximum values for the temperature warning threshold. This command is located on the context menu for the individual temperature probes, not on the main context menu.

System Management

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [Dell OpenManage Server Administrator](#)
- [Using Remote Access Controllers](#)
- [Alert Log Messages From Dell OpenManage Server Agent](#)
- [Configuring SNMP Properties](#)

This section provides information about system management for your NAS system, including an overview of Dell OpenManage™ Server Administrator, using Embedded Remote Access (ERA), and configuring SNMP properties.

Dell OpenManage Server Administrator

Dell OpenManage Server Administrator provides a comprehensive, one-to-one system management solution in two ways: from an integrated, Web browser-based GUI (the Server Administrator home page) and from a command line interface (CLI) through the operating system. Server Administrator allows you to manage NAS systems on a network locally and remotely and to focus on managing the entire network with comprehensive, one-to-one system management.

Server Administrator provides information about:

- Systems that are operating properly and systems that have problems
- Systems that require updates
- Systems that require remote recovery operations

Integrated Features

Server Administrator provides easy-to-use management and administration of local and remote systems through a comprehensive set of integrated management services. Server Administrator resides solely on the managed system and is accessible both locally and remotely from the Server Administrator home page. Server Administrator ensures the security of its management connections through role-based access control (RBAC), authentication, and industry-standard secure socket layer (SSL) encryption.

Server Administrator Home Page

The Server Administrator home page provides easy-to-set-up and easy-to-use Web browser-based system management from the managed node system or from a remote host through a LAN, dial-up service, or wireless network. When the NAS system is installed and configured on the managed node system, you can perform remote management functions from any system that has a supported Web browser and connection. Additionally, the Server Administrator home page provides extensive, context-sensitive online help.

Instrumentation Service

The Instrumentation Service provides rapid access to detailed fault and performance information gathered by industry-standard systems management agents and allows remote administration of monitored systems, including shut down, start up, and security.

Remote Access Service

The Remote Access Service provides a complete remote system management solution for systems equipped with remote access controllers such as the Dell™ Remote Access Card III (DRAC III) and Embedded Remote Access (ERA). For more

information on the Remote Access Service, see "[Using Remote Access Controllers.](#)"

Storage Management Service

The Storage Management Service provides storage management information in an integrated graphical view. The Storage Management Service enables you to view the status of local and remote storage attached to a monitored system. The Storage Management Service obtains logical and physical information about attached storage devices from the Dell OpenManage Array Manager managed node.

Diagnostic Service

The Diagnostic Service provides a suite of diagnostic programs that run locally on your system or remotely on a system connected to the network. The Diagnostic Service is engineered to diagnose problems on individual systems and to run concurrently with all other applications running on the system under test.

Update Service

The Update Service provides up-to-date version control and valuable change management tools for performing BIOS and firmware version updates on your local system.

Logs

Server Administrator displays logs of commands issued to or by the system, monitored hardware events, POST events, and system alerts. You can view logs on the home page, print or save them as reports, and send them by e-mail to a designated service contact.

Accessing Server Administrator

Server Administrator can be accessed through a Web browser directly or by using the NAS Manager.

To access the Server Administrator using the NAS Manager, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Server Administrator**.

To access Server Administrator directly from a client system on the same network, open Microsoft® Internet Explorer 5.5 or later. Connect to the secure port, 1311, of your NAS System. For example, type `https://DELL1234567:1311`; where DELL1234567 is the name of your NAS system.

Additional Information About Server Administrator

Please refer to the Dell OpenManage documentation provided on the *Resource* CD for more information on the Dell OpenManage Server Administrator.

Using Remote Access Controllers

The Server Administrator Remote Access Service provides a complete remote system management solution for SNMP- and CIM-instrumented systems equipped with a Dell ERA controller, a DRAC III, or a Dell Embedded Remote Access Option (ERA/O) card. These hardware and software solutions are collectively known as remote access controllers (RACs).

The Remote Access Service provides remote access to an inoperable system, allowing you to get the system up and running as quickly as possible. The Remote Access Service also provides alert notification when a system is down and allows you to remotely restart a system. Additionally, the Remote Access Service logs the probable cause of system crashes and saves the most recent crash screen.

You can log in to the Remote Access Service through the Server Administrator home page or by directly accessing the controller's IP address using a supported browser.

See the *Server Administrator Command Line Interface User's Guide* for information about running the Remote Access Service from the command line.

When using the Remote Access Service, you can click **Help** on the global navigation bar for more detailed information about the specific window you are viewing. Remote Access Service help is available for all windows accessible to the user based on user privilege level and the specific hardware and software groups that Server Administrator discovers on the managed node system.

Accessing a RAC From the NAS Manager

From the NAS Manager **Advanced Administration** menu, you can display or change the IP address or create or change the user name and password of the RAC administrator.

To access a RAC from the NAS Manager, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**.
4. Click **System Management**.
5. Click **Dell Remote Assistant Setup**.

Additional Information About RACs

See the *Dell Remote Access Controller Installation and Setup Guide* for complete information about installing and configuring RAC software.



NOTE: The default user name and password for a RAC on the NAS system are `administrator` and `powervault` respectively, which differs from the user name and password in the RAC documentation.

Alert Log Messages From Dell OpenManage Server Agent

Server Administrator generates alert messages that appear in the SNMP event log file. Alert log messages contain information, status, warning, and failure messages for drive, temperature, fan, and power conditions.

To see the trap logs, perform the following steps:

1. Click **Maintenance**.
 2. Click **Logs** or **Terminal Services** to log on to your system.
 3. From the **Advanced Administration** menu, click **Administrative Tools**.
 4. Click **Event Viewer** to view logged events.
-

Configuring SNMP Properties

Configuring SNMP Community Properties

1. Click **Maintenance**.
2. Click **Terminal Services**.

3. Log on to the **Terminal Services Advanced Client** session.



NOTE: The default administrator user name is `administrator` and the default password is `powervault`.

4. Click the **Advanced Administration Tool** icon to access the **PowerVault Advanced Administration Menu**.
5. From the **PowerVault Advanced Administration Menu**, select **System Management**, and then click **Computer Management**.
6. From the **Computer Management** console tree, click **Services and Applications**.
7. Click **Services**.
8. In the details pane, right-click **SNMP Service**.
9. From the **Action** menu, click **Properties**.
10. From the **Security** tab, click **Send authentication trap**.

Select this option if you want a trap message sent when authentication fails.

11. Select **Accepted community names**, and then click **Add**.
12. Select **Community Rights**, and then select a permission level for this host to process SNMP requests from the selected community.
13. To view a description of a dialog box item, right-click the item, and then click **What's This?**
14. In **Community Name**, type a case-sensitive community name, and then click **Add**.
15. In **SNMP Service Properties**, specify whether or not to accept SNMP packets from a host:
 - To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
 - To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate host name, Internet protocol (IP) or Internetwork Packet eXchange (IPX) address, and then click **Add** again.



NOTE: You can make changes to an entry by clicking the entry, and then clicking **Edit**. You can delete a selected entry by clicking **Remove**.



NOTE: If you remove all the community names, including the default name `Public`, SNMP does not respond to any community names presented. You can add additional community and host names as necessary.



NOTE: If you change existing SNMP settings, your changes take effect immediately. You do not need to restart the SNMP service for your settings to take effect. If you are configuring SNMP for the first time, you must restart SNMP before these settings take effect.

Configuring SNMP Agent Properties

1. Click **Maintenance**.
2. Click **Terminal Services**.
3. Log on to the **Terminal Services Advanced Client** session.



NOTE: The default administrator user name is `administrator` and the default password is `powervault`.

4. Click **Advanced Administration Menu**.

5. At the **Advanced Administration Menu**, select **System Management**, and then click **Computer Management**.
6. Click **Services and Applications**.
7. Click **Services**.
8. In the details pane, right-click **SNMP Service**.
9. From the **Action** menu, click **Properties**.
10. Select the **Agent** tab, select **Contact**, and then type the name of the user or system administrator.
11. Select **Location**, and then type the physical location of the system or the contact.
12. In the **Service** panel, select the appropriate check boxes for this system, and then click **OK**.
13. To view a description of a dialog box item, right-click the item, and then click **What's This?**



NOTE: If you change existing SNMP settings, your changes take effect immediately. You do not need to restart the SNMP service for your settings to take effect. If you are configuring SNMP for the first time, you must restart SNMP before these settings take effect.

[Back to Contents Page](#)

Backing Up the System

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [System-State Backup](#)
 - [Backing Up Data Volumes](#)
 - [Windows 2000 Backup and Recovery Tools](#)
 - [Third-Party Backup Software](#)
 - [Installing Tape Device Drivers for Windows 2000 Backup and Recovery Tools](#)
 - [Backing Up Dell ActiveArchive™ Persistent Images](#)
 - [Using Tape Backups on a SAN](#)
-

This section provides instructions on how to back up files on your system. The following topics are included:

- Backing up system-state files
 - Backing up data volumes
 - Using the Microsoft® Windows® 2000 Backup and Recovery Tools
 - Using third-party software for local and network backups
 - Installing tape device drivers for Windows 2000
-

System-State Backup

System-state files contain configuration information about the NAS system. Backing up the system state allows you to recover the system if an operating system reinstallation is required. Restoring your system state restores customized settings such as user and share information.

The integrated Windows 2000 Backup and Recovery Tools allows administrators to back up and restore system-state data, which includes the following:

- Registry
- COM+ class registration database
- System boot files
- Users and groups information
- CIFS/NFS/Novell® NetWare®/Macintosh share data

For more information, see the online help for Windows 2000 Backup and Recovery Tools. For information on restoring a system-state backup, see "[Restoring System State Data](#)."

Backing Up System-State Data

Dell recommends that you regularly back up your system state.

To back up system-state data, perform the following steps:

1. Log in to the NAS Manager as an administrator.
2. Click **Maintenance**.

3. Click **Backup**.
4. In the **Log on to Windows** window, enter the administrator user name and password and click **OK**.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The **Welcome to Windows 2000 Backup and Recovery Tools** window displays.

 **NOTE:** If the **Windows 2000 Backup and Recovery Tools** window does not display, click **Maintenance**, and then click **Terminal Services**. On the Advanced Administration Menu, click **Administrative Tools** and then click **Windows 2000 Backup/Recovery**.

5. Click **Backup Wizard**.
6. In the **Backup Wizard** window, click **Next**.
7. In the **What to Back Up** window, click **Only back up the System State data**, and then click **Next**.
8. In the **Where to Store the Backup** window, click **Browse**.
9. In the **Open** window, select the location to store your system-state backup file, enter the filename, and then click **Open**.

For fault tolerance, you should select a location that is not on the NAS system.

10. Click **Next** and then click **Finish**.

The backup begins and progress displays in the **Backup Progress** window.

11. When the backup is complete, click **Close**.

Backing Up Data Volumes

To back up your volumes, you can use direct-attached local backups or network backups. In a direct-attached backup, the NAS system is backed up to an external tape device connected directly to the system. In a network backup, the NAS system is backed up to LAN-attached backup servers.

The following software is supported for direct-attached local backups:

- Windows 2000 Backup and Recovery Tools
- VERITAS® Backup Exec® Server Professional 8.6 for Windows NT® and Windows 2000
- Computer Associates® ARCserve/IT™ 2000 for Windows NT and Windows 2000

The following software is supported for remote network backups:

- VERITAS Backup Exec Server Professional 8.6 for Windows NT and Windows 2000
- Computer Associates ARCserveIT
 - ARCserveIT 2000 for Windows NT and Windows 2000
 - ARCserveIT 7.0 for Red Hat Linux 7.0 and 7.1

Windows 2000 Backup and Recovery Tools

Windows 2000 Backup and Recovery Tools allow you to back up your data volumes to a locally attached tape drive or to a file.

 **NOTE:** You must have a supported SCSI card and a tape drive installed to back up your data volumes to tape.

You can access the Windows 2000 Backup and Recovery Tools by clicking the **Maintenance** tab on the NAS Manager primary menu and clicking **Backup** or by clicking **Windows 2000 Backup/Recovery Tools** on the Advanced Administration Menu under **Administrative Tools**.

For more information, see the online help for Windows 2000 Backup and Recovery Tools.

Third-Party Backup Software

You can back up your data volumes locally or over the network to LAN-attached backup servers.

Using Third-Party Backup Software for Network Backups

For network backups, you must already have a backup server installed on the network. It is also recommended that you use the network accelerator agents provided by your backup software to improve network backup performance.

Installing Network Accelerator Agents

VERITAS Backup Exec network accelerator agent can be installed remotely on the NAS system from a remote system on the network.

See your backup software documentation for more information on installing the network accelerator agents.

Installing and Using Third-Party Backup Software for Local Backups

The following information explains how to install and use the VERITAS Backup Exec and ARCserve 2000 software for local backups.

VERITAS Backup Exec

 **NOTE:** Before installing the backup software, check the Dell | Support website at support.dell.com for the latest driver and software updates. You might need to install the updates after completing the procedures that follow.

Installing VERITAS Backup Exec on the NAS System

 **NOTE:** VERITAS Backup Exec supports installation using Terminal Services and management using VERITAS Remote Administrator.

1. Insert the VERITAS Backup Exec installation CD in the NAS system's CD drive.
2. Log in to the NAS Manager.
3. Click **Maintenance**.
4. Click **Terminal Services**.
5. Log in to the NAS system.
6. Follow the instructions in the documentation that came with your backup software to complete the installation.

 **NOTE:** If the installation CD does not autorun, from the Windows Control Panel click **Start** ® **Run**. Browse to the executable file on the CD drive. Click **Open**, and then click **OK**.

Installing VERITAS Backup Exec Remote Administrator on a Client System

1. Insert the *VERITAS Backup Exec* CD in the CD drive of the client system.

The CD starts the software automatically.

2. If the CD does not start the software automatically, open Windows Explorer, right-click the CD drive that contains the VERITAS software, and select **Autoplay** from the menu.
3. Follow the instructions in the documentation that came with your backup software to complete the installation.

Using VERITAS Backup Exec Remote Administrator

1. On the remote system, click the **Start** button, and then point to **Programs® VERITAS Backup Exec**.

The **Connect to Server** window displays.

2. Type the name of the NAS system in the **Server** field.
3. Type login information in the **Login Information** field, and then click **OK**.

The **Backup Exec Assistant** window, which displays in front of the **Backup Exec** window, provides wizards for many common backup tasks. You can also use the **Tools** menu on the **Backup Exec** window to display the **Backup Exec Assistant**.

Use Remote Administrator to manage all backup operations just as you would from the local application. See the VERITAS Backup Exec documentation for more information about how to use the software.

ARCserve 2000

 **NOTE:** Before installing the backup software, check the Dell | Support website at support.dell.com for the latest driver and software updates. You might need to install the updates after completing the procedures that follow.

To use ARCserve 2000 for system backups, you must first install ARCserve 2000 on the NAS system and then install ARCserve Manager on a client system.

Installing ARCserve 2000 on the NAS System

 **NOTE:** You must first attach a keyboard, mouse, and monitor to the system before installing ARCserve 2000. ARCserve 2000 cannot be installed or managed using Terminal Services.

1. Insert the *ARCserve 2000* CD into the CD drive of the NAS system.

The CD starts the installation automatically.

2. If the installation does not start automatically, open Windows Explorer, right-click the CD drive that contains the ARCserve 2000 software, and select **Autoplay** from the menu.

The **ARCserve 2000 Product Explorer** window displays.

3. Follow the instructions in the documentation that came with your backup software to complete the installation.

Installing ARCserve Manager on a Client System

1. Insert the *ARCserve 2000* CD in the CD drive of the client system.

The CD starts the installation automatically.

2. If the installation does not start automatically, open Windows Explorer, right-click the CD drive that contains the ARCserve 2000 software, and select **Autoplay** from the menu.

The **ARCserve 2000 Product Explorer** window displays.

3. Follow the instructions in the documentation that came with your backup software to complete the installation.

Using ARCserve 2000 Remote Manager

1. On the client system, click the **Start** button, and then point to **Programs** ® **ARCserve** ® **ARCserve Manager**.

The **ARCserve Quick Access** window displays.

The **ARCserve Quick Access** window provides wizards for many common backup tasks. You can use these wizards or go through the standard menus to perform your backup tasks.

2. Enter the name of the NAS system in the **Server** field at the top of the screen to manage the backup software on the NAS system.

You can manage all your backup operations from this application, just as you would manage them from the local application. See the ARCserve 2000 documentation for more information on using the software.

Installing Tape Device Drivers for Windows 2000 Backup and Recovery Tools

If you are using Windows 2000 Backup and Recovery Tools, you might need to install drivers for both tape drives and tape media changers.



NOTE: Most of the tape device drivers are located in the `c:\dell\drivers` directory. However, you should always check the Dell | Support website at support.dell.com for updated drivers and patches.

Installing Drivers for Dell™ PowerVault™ Tape Drives

1. Connect the PowerVault tape drive, and then restart the system.
2. Log in to the NAS Manager.
3. Click **Maintenance**.
4. Click **Terminal Services**.
5. Log in to a Terminal Services Client session.
6. On the Advanced Administration Menu under **System Management**, click **Computer Management**.



NOTE: If the Advanced Administration Menu does not display, double-click the Advanced Administration Menu icon on the desktop of the NAS system.

7. Click **Computer Management** in the left pane.
8. Click **System Tools** in the left pane.

9. Click **Device Manager** in the left pane.
10. Click **Unknown Devices** in the right pane.

 **NOTE:** The tape device may also appear under **Other Devices**.

11. Double-click the tape device.
12. Click the **Driver** tab.
13. Click **Update Driver**.

The Upgrade Device Driver Wizard displays.

14. Click the radio button next to **Search for a suitable driver for my device (recommended)**, and then click **Next**.
15. In **Optional search locations**, click the check box next to **Specify a location**, and deselect the other check boxes.
16. Click **Next**.
17. In the path for **Copy manufacturer's files from**, specify the folder name that contains the device drivers.
18. Click **OK**, and then click **Next**.

The Upgrade Device Driver Wizard searches the specified folder for the driver files.

19. Make sure that the wizard has selected the appropriate PowerVault tape device, and then click **Next**.
20. Click **Finish**.
21. Click **Close** to exit the driver properties dialog box.

Installing Drivers for PowerVault Tape Drive Media Changers

To install drivers for tape media changers when using Windows 2000 Backup and Recovery Tools, perform the following steps:

1. Connect the PowerVault tape device, and then restart the NAS system.
2. Log in to the NAS Manager.
3. Click **Maintenance**.
4. Click **Terminal Services**.
5. Log in to a **Terminal Services Client** session.
6. In the Advanced Administration Menu, click **System Management**, and then click **Computer Management**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the Advanced Administration Menu icon on the desktop of the NAS system.

7. Click **Computer Management** in the left pane, and then click **System Tools**.
8. Click **Device Manager** in the left pane.
9. Click **Medium Changers** in the right pane.
10. Double-click **Unknown Medium Changer**.
11. Click **Driver** tab in the **Properties** window.

12. Click **Update Driver**.

The Upgrade Device Driver Wizard displays.

13. Click **Next**.
14. Click the radio button next to **Search for a suitable driver for my device (recommended)**, and then click **Next**.
15. In **Optional search locations**, click the check box next to **Specify a location**, and deselect the other check box.
16. Click **Next**.

A dialog box displays with a field for you to enter the location of the device driver.

17. In the path for **Copy manufacturer's files from**, specify the folder name that contains the device drivers, and then click **OK**.
18. Click **Next**.

The Upgrade Device Driver Wizard searches the specified folder for the driver files.

19. Make sure that the Upgrade Device Driver Wizard has selected the appropriate PowerVault tape device, and then click **Next**.
20. Click **Finish**.
21. Click **Close**.

Backing Up Dell ActiveArchive™ Persistent Images

Backing up persistent images eliminates the possibility of files changing during backup. Persistent images always contain the data that existed when the persistent image was taken.

- ➡ **NOTICE:** Backing up persistent images is a complex procedure and should be performed only by advanced backup administrators. If you are not an advanced backup administrator, it is recommended that you use the available open file agents in VERITAS Backup Exec to back up your open files rather than backing up persistent images.
- ➡ **NOTICE:** Do not use Computer Associates ARCserve to back up persistent images.

Limitations on Backing Up Persistent Images

- You cannot do incremental or differential backups of persistent images.
- You cannot use GFS rotation schemes when backing up persistent images.
- You cannot schedule a backup of a persistent image.

You must perform a manual backup of persistent image files because each persistent image filename is unique in that it includes the date and time (hour-minute-second) that the persistent image was taken.

- When you restore a persistent image, you must redirect the restore to a location other than the original persistent image location. A restore to the original location is not successful.

To back up a persistent image, perform the following steps:

1. Use the NAS Manager to create a persistent image.

See "[Dell ActiveArchive](#)."

 **NOTE:** For increased performance, back up only read-only persistent images.

2. On the NAS Manager primary menu, click **Maintenance**.
3. Click **Terminal Services** and log in to the NAS system.
4. When the **PowerVault Advanced Administration** window displays, click **Exit**.
5. Double-click **My Appliance** and browse to the persistent image created in step 1.

Persistent images are located in the Dell ActiveArchive directory of the volume on which you created the persistent image in step 1.

6. Right-click the persistent image, and then click **Sharing**.
7. Click **Share this folder**.
8. Type the name of the share in the **Share name** field.
9. Click **Permissions**.
10. Set the required permissions in the **Permissions** window, and then click **OK**.
11. Click **OK** in the **Properties** window.
12. On the system that is running VERITAS Backup Exec, set up VERITAS Backup Exec so that it is able to back up user shares.

You can find this option in the **Tools® Options** menu on the **Network** tab.

13. In the VERITAS Backup Exec **Backup Selections** window, browse to your NAS system under **Entire Network**.
14. Select the share name that you created in step 8 for your persistent image.
15. Deselect the **Persistent Storage Manager State** directory when performing persistent image backups.

This directory contains files needed for persistent images. However, to save space on your backup media, backing up the files is not recommended.

16. Click **Backup**.
17. Select **Run Now** to run the backup now or **Schedule** to schedule your backup job to run at a later time.

 **NOTE:** Although you are backing up your persistent image from a network share, it does not create network traffic if you are backing up to a local backup device.

Restoring Persistent Images From Tape Backup

 **NOTICE:** Do not use Computer Associates ARCserve to restore persistent images.

To restore your persistent images from tape backup, perform the following steps:

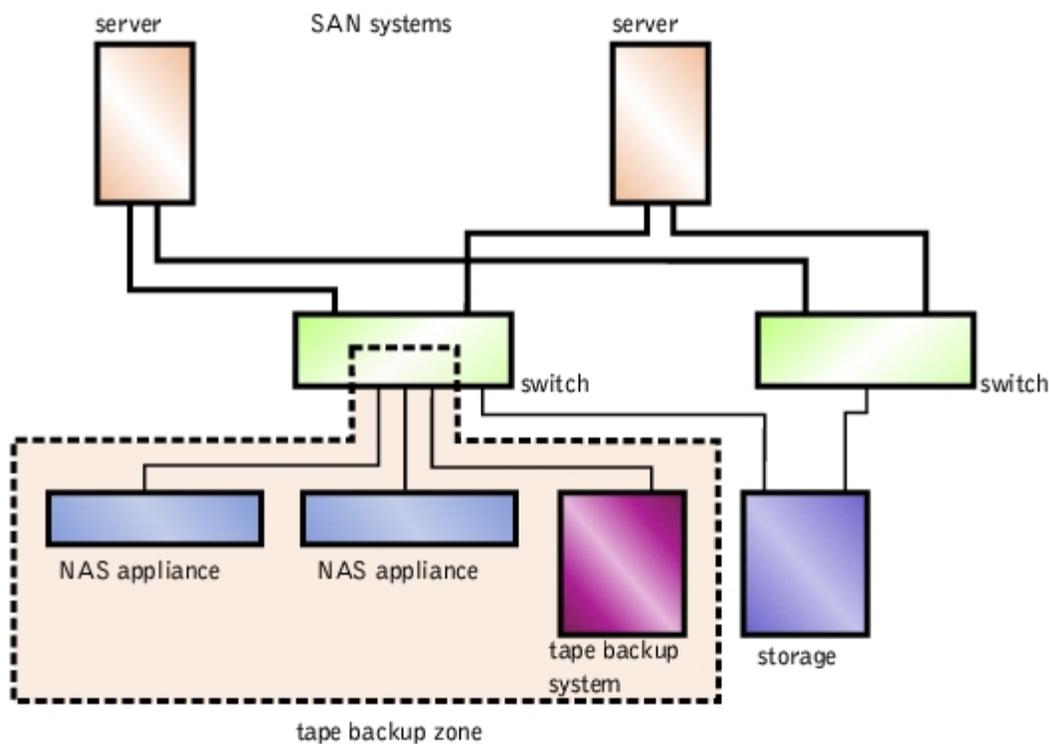
1. On the network system running VERITAS Backup Exec, click the **Restore Selections** tab to bring up the window that lists your previous backup files.
2. Browse to the backup of the persistent image you want restored, and then select it by clicking the check box next to it.
3. Click **Restore**.
4. Click the **Redirection** tab.

5. Click the check box next to **Redirect Files**.
 6. Enter the drive letter and path where you want the files to be restored. This path must be different from the original persistent image location.
 7. Click **Run Now** to run the restore immediately or click **Schedule** to schedule your restore job to run at a later time.
-

Using Tape Backups on a SAN

You can use one or more NAS systems to back up data to a tape backup device on a storage area network (SAN). To use this backup method, the NAS system(s), switch ports, and tape backup devices must be in separate zones. Because it is necessary for these components to be in separate zones, the NAS system cannot access other servers or storage systems on the SAN. For more information about SANs and creating zones in a SAN, see the documentation that came with your Fibre Channel switch and your *SAN Administrator's Guide*. [Figure 5-1](#) illustrates a typical configuration for backing up a NAS system on a SAN tape device.

Figure 5-1. NAS System and SAN Tape Backup Zone



Each NAS system supports one Fibre Channel HBA, which provides a single path to the Fibre Channel SAN switch.

 **NOTE:** The single HBA provides one data path, which does not support redundancy or failover capability.

[Back to Contents Page](#)

Recovering and Restoring the System

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [Solutions to Try Before Reinstalling](#)
- [Recovery From System Failure](#)
- [Restoring System State Data](#)
- [Restoring Initial System Setup](#)

This section provides instructions on how to recover the NAS system if the operating system fails. Additionally, this section provides information for possible solutions that do not require restoring the operating system.

Because your NAS system is designed with redundancy, it can recover from certain hardware and software failures. In some situations, it recovers automatically; in others, you must have administrator privileges and manually intervene to recover the NAS system.

Use the following methods in the order shown to restore your NAS system:

1. Work through the possible solutions listed in "[Solutions to Try Before Reinstalling](#)."
2. Reinstall the operating system as described in "[Recovery From System Failure](#)."

Solutions to Try Before Reinstalling

This section provides a list of possible solutions that you should try before you reinstall your operating system or replace a hard drive. Some of the checks require you to observe the LEDs on the front and back of the NAS system. For more information about the LEDs, see your *Installation and Troubleshooting Guide*.

- Does the power LED show that the NAS system is turned on? If not, is the power cable connected to the NAS system and a power source?
- Are the link LEDs on the NAS system, and any network switches to which it may be connected, illuminated?
- Are you are using a standard Ethernet cable to connect to the network?
- Has the Ethernet cable been connected inadvertently to the embedded remote access connector on the back of the system instead of one of the two standard 10/100/1000 NIC connectors? To locate the proper connectors, see your *User's Guide*.
- Have you allowed enough time for the NAS system to boot? Depending on your configuration and the amount of storage attached, the NAS system may take several minutes to boot.
- Does the NAS system boot completely? Use console redirection to connect to the NAS system, or connect a keyboard, monitor, and mouse directly to the system, and observe the boot process. See "[Console Redirection](#)" in "Troubleshooting."
- Can you connect using a serial connection? For more information on using a serial connection, see the procedures in "[Configuring Your NAS System for the First Time](#)" in "Initial Setup." If you are able to connect serially, the problem may be the network instead of the NAS system.
- Are the LEDs on all internal hard drives on the NAS system illuminated? If not, you have a failed hard drive.

Recovery From System Failure

If the Windows Powered operating system becomes inoperable, you can use the NAS system's Reinstallation CD to reinstall the operating system. After the operating system is reinstalled, the system state backup can be restored to recover system

configuration information.

To recover from a system failure, you must complete the following tasks:

- Reinstall the operating system using the *Reinstallation* CD
- Configure the system using the System Setup program
- Restore the system-state backup (see "[Restoring System State Data](#)" in "[Backing Up the System](#)" for more information)

Reinstalling the Operating System

 **NOTICE:** Using the *Reinstallation* CD will cause you to lose any data on the operating system drive.

1. Insert the *Reinstallation* CD into the CD drive.
2. Shut down the NAS system.
3. If one or both existing operating-system disk drives are operational, proceed to step 4.

If both existing operating system drives (SCSI drives 0 and 1) have been replaced with new, initialized drives, you must disconnect all the internal *data* drives by pulling them out of the system far enough so that they are disengaged from the backplane. This will leave only the two new operating-system disk drives installed in the internal drive bays.

4. Turn on the NAS system.

The *Reinstallation* CD automatically starts the reinstallation process if the first logical volume configured on the RAID controller is a drive that is part of a two-drive, RAID 1 group.

It takes approximately 30 minutes for the reinstallation to complete.

 **NOTE:** The CD automatically ejects several minutes after reinstallation begins. Even though the CD is no longer in the CD drive, the reinstallation is still in progress.

5. If you disconnected data drives in step 3, after the reinstallation CD ejects, reinsert all data drives. Otherwise, proceed to step 6.
6. Use a client's Web browser to connect to the NAS system.
7. Use the Dell OpenManage™ Array Manager to merge into the system any data containers that were previously defined.

See the "[Merging Foreign Disks](#)" section in "[Advanced Disk and Volume Management](#)" for more information about merging disks.

Restoring System State Data

 **NOTE:** To restore your system state, you must have previously backed up your system using the System State Backup Tool on the Advanced Administration Menu or using Windows 2000 Backup and Recovery Tools.

To use the NAS Manager to restore system state data, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Backup**.
4. Log on to the system as administrator.



NOTE: The default user name is administrator and the default password is powervault.

5. Click **Restore Wizard**.

The Restore Wizard window displays.

6. Click **Next**.

If you do not see the media that contains your restoration files, skip to step 7. Otherwise, perform the following steps:

- a. Click + next to **File**.
- b. Click + next to the media that contains the restoration files.
- c. Select **System State**.
- d. Click **Next**.
- e. Go to step 8.

7. If you do not see the media that contains your restoration files, you must import the files.

After a reinstallation, you must import the file because your system is not aware of previous backups.

- a. Click **Import File**.

The **Backup File Name** window displays.

- b. Click **Browse**.

The **Select file to catalog** window displays.

- c. After locating your file, click **Open**, and then click **OK**.

The **What to Restore** window displays.

- d. Click + next to **File**.
- e. Click + next to **Media Created on**.

You are prompted for your backup file location.

- f. If the location is correct, click **OK**. Otherwise, browse to the correct backup file location.

An icon labeled **System State** will appear in the **What to Restore** window.

- g. Click + next to **System State**.

You are asked to reconfirm your backup file location.

- h. If the location is correct, click **OK**. Otherwise, browse to the correct backup file location.
- i. Click the check box next to **System State**, and then click **Next**.
- j. Click **Advanced**.

The **Where to Restore** window displays.

k. In the **Restore files to** field, choose **Original location**, and then click **Next**.

The **How to Restore** window displays.

l. Select **Always replace the files on disk**, and then click **Next**.

The **Advanced Restore Options** window displays.

m. Leave all check boxes unchecked, and then click **Next**.

8. Click **Finish** to begin the restore process, and then click **OK**.

9. Restart your system after the restore process completes.



NOTE: Because Windows must replace all locked files on the system during restoration, it may take the system approximately 15 minutes to restart.

Restoring Initial System Setup

After the operating system is reinstalled on the NAS system, you must reconfigure the system to establish network communication. See "[Initial Configuration](#)" for information on configuring the system.

[Back to Contents Page](#)

Dell ActiveArchive

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [Introduction to Persistent Images](#)
- [Configuring the Persistent Image Global Settings](#)
- [Configuring Persistent Image Volume Settings](#)
- [Using Persistent Images](#)
- [Scheduling Persistent Images](#)
- [Accessing Stored Persistent Images](#)
- [Restoring Volumes From an Existing Persistent Image](#)
- [Reextending an Extended Volume](#)
- [Changing the Dell ActiveArchive Event Log Language](#)
- [Defragmenting a Volume Containing Persistent Images](#)

Dell ActiveArchive™ allows the creation and preservation of persistent images of your NAS system's data volumes. The Dell ActiveArchive software can be configured using the NAS Manager.

Introduction to Persistent Images

A persistent image is a point-in-time copy of a disk volume. A persistent image contains an exact copy of the file system at the time the persistent image was created. If you change a file on the active file system after taking a persistent image, the persistent image contains the old version of the file. If an active file gets corrupted or deleted, you can restore the old version by copying the file from the latest persistent image or restoring the entire volume. Also, because the persistent image contains the contents of the file system when the persistent image was taken, you can perform a backup from the persistent image without stopping all I/O to the NAS system, thus eliminating the backup window required by other types of backup.

-  **NOTICE:** Persistent images are temporary backups of your data that reside on the same volume as your data. If the volume becomes damaged and you lose your data, the persistent image is also lost. Therefore, persistent images do not replace regular backups of your volume.

Cache File

The Dell ActiveArchive software stores changed data in a cache file. A cache file resides on each volume of your system. By default, the persistent image cache file is 20 percent of each volume. You can use the NAS Manager to change the percentage of the volume that is dedicated to the cache file.

-  **NOTE:** You cannot take a persistent image of the operating system volume.

Cache Thresholds

The Dell ActiveArchive software has two thresholds that provide warnings when the cache file is approaching maximum capacity. The warning threshold logs an event in the event log and displays a warning in the NAS Manager status indicator when the cache file reaches the threshold (default is 80 percent full). The deletion threshold, which is labeled "Begin deleting images" in the NAS Manager, specifies the threshold at which the NAS Manager deletes the oldest persistent images with the lowest retention weights until the cache file is below the deletion threshold (default is 90 percent full). The NAS Manager indicates when it is necessary to delete persistent images to get below the threshold by displaying an error on the NAS Manager **Status** page.

Persistent Image Retention Weights

When the ActiveArchive cache file reaches the deletion threshold, the system begins deleting files, depending on the retention weight (the deletion priority of the file) and age of the persistent image. The system first looks for the persistent image with the lowest retention weight in the cache file. It then deletes the oldest persistent image with the lowest retention weight until the cache file is below the deletion threshold. After all persistent images with the lowest retention weight have been deleted, Dell ActiveArchive looks for and deletes the oldest files with the next lowest retention weight.

Persistent Image Considerations

When using persistent images, system performance might be degraded, depending on the rate your data is changing and the number of persistent images kept for each virtual disk. Read performance of the virtual disk remains constant, regardless of the presence of persistent images. Read performance of the persistent image is identical to that of the virtual disk. Write performance, however, might vary. Each initial write to a virtual disk area causes the Dell ActiveArchive software to rewrite the data to the persistent image cache file, and the initial write is slower if the data is being protected by a persistent image. Changes to data that is not protected by a persistent image does not cause a performance degradation.

Storing Persistent Images

You can configure the NAS system to store a maximum of 250 persistent images per volume; however, if you exceed the maximum, the oldest persistent image with the lowest retention weight is overwritten. This number of persistent images allows you to schedule multiple persistent images. (You should tailor your schedule depending on how the data is changing.) For example, you could implement a schedule similar to the following schedule:

- Seven daily persistent images with a high priority
- Two weekly persistent images with a medium priority
- Two monthly persistent images with a low priority

This type of schedule gives you good snapshot coverage and ensures that your most recent data has the highest priority.

Multivolume Persistent Images in a Cluster Environment

You can take persistent images of more than one volume in a cluster environment. If you frequently move volumes from one cluster node to another, you should make persistent images of individual volumes only. Multivolume persistent images may become inaccessible if one or more of the volumes in a multivolume persistent image fail over to another node in the cluster. It is recommended that you do not make multivolume persistent images of a cluster-protected volume and a noncluster-protected volume. If the cluster node fails for any reason, cluster-protected volumes fail over to another cluster node and the multivolume persistent images may become inaccessible.

Configuring the Persistent Image Global Settings

You can modify the various aspects of the persistent image environment by performing the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Global Settings**.
5. Configure the following options.



NOTE: Before changing the image directory name, you must delete all existing persistent images.

- **Maximum persistent images** — Specifies the maximum number of active persistent images per volume, up to a maximum of 250. When the volume has 250 persistent images stored, starting another persistent image overwrites the oldest persistent image with the lowest retention weight.

- **Inactive period** — Prior to starting a persistent image, the system waits for a period of relative inactivity on the volume being imaged. The default value for this period, which is 5 seconds, allows systems to start an image with a consistent file set and a minimal time-out. Experienced administrators may reduce or increase this value for system optimization. Reducing the inactive period allows persistent images to begin on systems where disk inactivity is rare, at the possible expense of synchronization problems within applications that are concurrently writing to multiple files.
- **Inactive time-out** — Specifies the amount of time the system continues to retry to create a persistent image (default time is 15 minutes). A persistent image cannot start until a period of relative inactivity, specified by **Inactive period**, occurs. If an interval longer than **Inactive time-out** passes before the persistent image can begin, the persistent image cannot be taken and an error is displayed in the NAS Manager status indicator and logged in the event log.
- **Image directory** — Specifies the directory name that is to be used for the persistent image mount point. Each persistent image appears as a subdirectory in the volume that is being imaged. The entire content of the volume, as it existed when the persistent image was created, appears under this directory.

6. If you need to reestablish the system defaults, click **Restore Defaults**.

7. Click **OK** to update the global settings.

Configuring Persistent Image Volume Settings

You can modify volume settings by performing the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Volume Settings**.
5. Select the volume that you want to reconfigure.
6. Click **Configure**.
7. Use the appropriate menus to configure the following options.



NOTE: Before changing the cache size, you must delete all persistent images on that volume.

- **Warning threshold reached when** — Defines the percentage of cache space used that triggers warning messages to the system event log.
- **Begin deleting images when** — Defines the percentage of cache space used that triggers automatic deletion of the oldest persistent images with the lowest retention weight on the system. Automatic persistent image deletions are recorded in the system log.
- **Cache size** — Specifies the percentage of the volume that is allocated to the cache file. Increasing this value allows more and larger persistent images to be maintained. Ensure that adequate space is available on the persistent image files' location drive.

8. If you need to reestablish the system defaults, click **Restore Defaults**.

9. Click **OK**.

Using Persistent Images

In addition to scheduling persistent images, you can take new persistent images on demand, delete existing persistent images, configure the persistent image environment, and set persistent image retention weights.

Taking a New Persistent Image on Demand

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Persistent Images**.
5. In the **Tasks** list on the **Persistent Images** page, click **New**.
6. In the menu that is displayed, select the **Volume(s)** to preserve.

Consider the following when selecting the volume(s):

- You can take persistent images only of volumes with drive letters, not volumes mounted to a directory (mount points).
- If volumes are not protected by RAID 1 or RAID 5, or if volumes are frequently being added and removed, it is recommended that you make persistent images of individual volumes. Because multivolume persistent images are linked to each other, a multivolume persistent image may become inaccessible if one volume in the multivolume persistent image fails or is removed from the system.



NOTE: To select multiple volumes, press and hold <Ctrl> and select all volumes that are to be included in the persistent image.



NOTE: It is recommended that you do not take multivolume persistent images of both a cluster-protected volume and a non-cluster-protected volume. For more information, see "[Multivolume Persistent Images in a Cluster Environment](#)."

7. Select the **Read Only** or **Read/Write** attribute.
8. Select the retention weight for the persistent image.
9. Confirm the persistent image name.

You can use patterns in the persistent image name to differentiate your persistent images. For example if you use a pattern of **Snapshot.%i** and you take two persistent images, you have **Snapshot.1** and **Snapshot.2**. The default persistent image name pattern is **Snapshot %M-%D-%Y %H.%m.%s**. Valid pattern macros are as follows:

- %M = Month
- %D = Day
- %Y = Year
- %h = Hours in 12-hour format
- %H = Hours in 24-hour format
- %m = Minute
- %s = Second
- %i = Instance, which increments once per instance
- %a = AM/PM
- %W = Day of the week
- %w = Three-letter day of the week

- %% = Percent sign

10. Click **OK** to create the persistent image.

Deleting a Persistent Image

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Persistent Images**.
5. Click the check box next to the persistent image that is to be deleted.
6. In the **Tasks** list, click **Delete**.
7. Click **OK** to delete the persistent image.

Undoing Writes to a Read/Write Persistent Image

To undo writes to a read/write persistent image, you must select an item from the **Persistent Images** list and then click **Undo** in the **Tasks** list.

To undo persistent image writes, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click the persistent image to be restored to its original state.
5. In the **Tasks** list, click **Undo**.
6. Click **OK** to restore the image or **Cancel** to leave it intact.

Setting Persistent Image Retention Weights and Read Only or Read/Write Attributes

To change the read only or read/write attribute or the retention weight (deletion priority) of an image, you must edit the persistent image properties by selecting an image from the **Persistent Image** list, and then clicking **Properties** in the **Tasks** list.

To edit the persistent image properties, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Persistent Images**.
5. Click the persistent image that you want to edit.
6. In the **Task** list, click **Properties**.
7. Select the **Read Only** or **Read/Write** attribute.

8. Select the retention weight.
 9. Click **OK** to update the persistent image.
-

Scheduling Persistent Images

When you click from the NAS Manager primary menu **Disks® ActiveArchive® Schedules**, the **Scheduled Persistent Image** page displays a list of all scheduled persistent images and associated tasks. Each scheduled persistent image is identified by the scheduled time, day, frequency, starting date, and target volume ID. Persistent images identified by time and date are located in the **ActiveArchive** directory. The **ActiveArchive** directory is located in the root of each ActiveArchive volume. Only the administrator can access the **ActiveArchive** directory. The files and folders in the persistent image directories have the same permissions as the files and folders on the original volume. Persistent image directories are used exactly the same way as conventional system volumes. Unlike conventional volumes, read-only persistent image images are static, recording the precise content of the originating volume at the time you created the persistent image.

 **NOTE:** In a cluster environment, persistent image schedules do not fail over. However, the schedule still attempts to take persistent images on the node where the schedule was set. As a result, you may receive errors indicating that the persistent images could not be taken.

Displaying the List of Persistent Images

The **Persistent Images** page displays all currently active persistent images. Each entry identifies the date and time that the persistent image was created and the volume it preserves. Select an individual persistent image by clicking the radio button to the left of the description.

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Persistent Images**.

Adding Persistent Images to the Schedule

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Schedules**.
5. In the **Tasks** list on the **Persistent Image Schedules** page, click **New**.
6. Use the menus to select the start time (**Start at**), the frequency at which to repeat the persistent image (**Repeat every**), the day to begin (**Begin**), the volume(s) to include, the image attributes (**Read-only** or **Read/Write**), the retention weight, number of images to save (per schedule), and the persistent image name.

 **NOTE:** To select multiple volumes, press and hold <Ctrl> and select all volumes that are to be included in the persistent image.

 **NOTE:** If volumes are not protected by RAID 1 or RAID 5, or if volumes are frequently being added and removed, it is recommended that you make persistent images of individual volumes. Because multivolume persistent images are linked to each other, a multivolume persistent image may become inaccessible if one volume in the multivolume persistent image fails or is removed from the system.

You can use patterns in the persistent image name to differentiate your persistent images. For example if you use a

pattern of **Snapshot.%i** and you take two persistent images, you have **Snapshot.1** and **Snapshot.2**. The default persistent image name pattern is **Snapshot %M-%D-%Y %H.%m.%s**. Valid pattern macros are as follows:

- %M = Month
- %D = Day
- %Y = Year
- %h = Hours in 12-hour format
- %H = Hours in 24-hour format
- %m = Minute
- %s = Second
- %i = Instance, which increments once per instance
- %a = AM/PM
- %W = Day of the week
- %w = Three-letter day of the week
- %% = Percent sign

7. Click **OK** to save the new scheduled persistent image.



NOTE: It is recommended that you do not take multivolume persistent images of both a cluster-protected volume and a non-cluster-protected volume. For more information, see "[Multivolume Persistent Images in a Cluster Environment.](#)"

Deleting a Persistent Image Schedule

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Schedules**.
5. On the **Persistent Image Schedules** page, click the check box next to the scheduled persistent image to be deleted.
6. In the **Tasks** list on the **Persistent Image Schedules** page, click **Delete**.
7. Click **OK** to delete the item or **Cancel** to leave the item intact.

Editing the Properties of a Persistent Image Schedule

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Schedules**.
5. Click the persistent image schedule you want to change.
6. In the **Tasks** list on the **Persistent Image Schedules** page, click **Properties**.
7. Use the appropriate menus to select or change the starting time, the frequency at which to repeat the persistent image

(**Repeat every**), the day to begin, the volume(s) to include, the image attributes (**Read-only** or **Read/Write**), retention weight, the number of images to save (per schedule), and the image name.

 **NOTE:** To select multiple volumes, press and hold <Ctrl> and select all volumes that are to be included in the persistent image.

 **NOTE:** If volumes are not protected by RAID 1 or RAID 5, or if volumes are frequently being added and removed, it is recommended that you make persistent images of individual volumes. Because multivolume persistent images are linked to each other, a multivolume persistent image may become inaccessible if one volume in the multivolume persistent image fails or is removed from the system.

8. Click **OK** to modify the schedule or **Cancel** to leave the schedule intact.

Accessing Stored Persistent Images

 **NOTE:** Only Windows clients (CIFS) can access Dell ActiveArchive persistent images.

 **NOTE:** The name of the utility that creates persistent images is Dell ActiveArchive. The name of the directory where Dell ActiveArchive persistent images are stored is **ActiveArchive**.

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**.
4. Log in to a **Terminal Services Advanced Client** session.
5. If the **PowerVault Advanced Administration Menu** window is displayed, click **Exit**, and then click **OK** to close it.
6. Use Microsoft® Windows® Explorer to navigate to the **ActiveArchive** directory on the volume root.

Accessing Directories, Folders, and Files

By default, administrators can access the **ActiveArchive** directory in the root of each volume. Each persistent image is displayed separately with a date and time stamp showing when the persistent image occurred. The administrator can browse the persistent image as if it were a standard volume. Each persistent image is mounted as a volume on the file system to allow access by clients. Persistent images are created as read-only or write-only.

Persistent image directories are used in the same way that conventional directories are used. The files and folders in the persistent image directories have the same permissions as the files and folders on the original volume. All persistent images are persistent and survive system power losses or reboots.

Allowing User Access to Persistent Images

The files and folders within a persistent image are identical to the permissions on the original files and folders. However, by default, the **ActiveArchive** directory is restricted to administrator access only. To allow users to access the persistent images, the system administrator must modify the permissions for the **ActiveArchive** directory.

Use the NAS Manager to change the **ActiveArchive** directory permissions by performing the following steps:

1. Log in to the NAS Manager as an administrator.
2. Click **Maintenance**.
3. Click **Terminal Services**.
4. Log in to a **Terminal Services Advanced Client** session.

5. Open Windows Explorer.
6. Select the drive on the left side.
7. Right-click the **ActiveArchive** directory, and then click **Properties**.
8. Click **Security**, and then click **Add**.
9. Click specific users or groups or type the individual users or group names to add individual users or groups, and then click **OK**.

 **NOTE:** To ensure that all persistent image files do not inherit the same permissions as the ActiveArchive directory, under **Permissions** ® **Security** ® **Advanced**, be sure the **Reset permissions on all child objects and enable propagation of inheritable permissions** is not checked.

10. Give the selected members **Read** and **List Folder Contents** permissions.
11. Click **OK**.

After setting the permissions for the **ActiveArchive** directory, perform the following procedure to allow the user access to a share on the directory:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. On the **Shares** page, click **Shares**.
4. In the **Tasks** list on the **Shared Folders** page, click **New**.
5. Type the share name `ActiveArchives` and path `volume_letter:\ActiveArchives`, where *volume_letter* is the volume of the persistent images.

 **NOTE:** Ignore the **Comment** field for NFS, FTP, and HTTP shares.

6. Check the **Microsoft Windows (CIFS)** box.
7. Click **CIFS Sharing** and add the users that you want to have access to persistent images.
8. Click **OK**.

Users can access persistent images from a Windows 2000 client by performing the following steps:

1. Right-click **My Appliance**, and select **Map Network Drive**.
2. Map to the ActiveArchives directory as a user that has permissions to the ActiveArchives share.
3. For **Folder**, type `\\Dellxxxxxxx\ActiveArchives`, where `Dellxxxxxxx` is the name of the NAS system.

The default system name is `Dellxxxxxxx`, where `xxxxxxx` is the system's service tag number. For example, if your service tag number is 1234567, enter `http://DELL1234567`.

4. Use Windows Explorer to navigate to the **ActiveArchive** directory on the newly mapped drive.

Naming Files in Microsoft Windows Explorer

Windows Explorer has a limitation of 255 characters in a filename, including the path. When you make a persistent image, the entire path and filename are stored in addition to the Dell ActiveArchives default path and persistent image name. The default Dell ActiveArchives naming convention would result in a name such as the following:

```
Drive_Letter:\ActiveArchives\Snapshot 01-01-2001 12.00.00\Path_and_Filename
```

The original path and filename and the Dell ActiveArchives default path might exceed the 255-character limit and become inaccessible through Windows Explorer.

If a file becomes inaccessible because of the 255-character limit, perform the following steps to ensure that you can access long path and file names in Windows Explorer:

1. Create a share for the desired snapshot folder. For example:

```
E:\ActiveArchives\Snapshot 01-01-2001 12.00.00\
```

2. Access that share through the desired client.

The path and filename no longer include the additional directory information, which shortens the path and filename to the original character length. You can now access the file through Windows Explorer.

Restoring Volumes From an Existing Persistent Image

To restore a volume(s) from a persistent image, you must select the persistent image to be restored. Ensure that you select the persistent image carefully because any activity that occurred after the persistent image was taken is lost.

-  **NOTICE:** Restoring a volume restores the volume back to its state at the time the persistent image was made. This restore destroys all data on the volume and replaces it with the data from the persistent image.
-  **NOTICE:** A volume is dismounted during a restore. All reads and writes to a volume that occur during the restore process are denied. Therefore, you must stop all I/O traffic to a volume while restoring it.
-  **NOTE:** In a cluster environment, you cannot restore an entire volume using the **Restore Persistent Images** function. To restore an entire volume in a cluster, copy the desired files and folders from the persistent image and paste them into the volume.

To restore volumes from a persistent image, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Restore Persistent Images**.
5. Click the persistent image that is to be restored.
6. Click **Restore**.
7. Click **OK** to restore the volumes protected by the persistent image, or click **Cancel** to leave the volume intact.

 **NOTE:** Restoring persistent images that contain multiple volumes restores all of the volumes in the persistent image. If you want the ability to restore a single volume, you must take single volume persistent images.

 **NOTE:** If you delete a share from a volume after a snapshot is taken, that share will not be accessible after you restore the snapshot. For example, if you create a persistent image of volume E, which has a share called "users," and you later delete "users," when you restore volume E, the "users" share will not be accessible, although the directory will still exist and contain the files.

Reextending an Extended Volume

The **reextend.exe** command allows you to take a persistent image of a volume, extend that volume, and restore the image without reducing the volume to the size it was when the persistent image was taken.

The following steps provide an example of how you can use the **reextend.exe** command:

1. Copy your files to a dynamic volume.
2. Take a persistent image of this dynamic volume.

For information about taking a persistent image, see "[Using Persistent Images](#)."

3. Extend the dynamic volume.

For information about extending a volume, see "[Extending a Dynamic Simple or Spanned Volume](#)."

4. Delete the files on the extended volume.
5. Take another persistent image of the dynamic volume.
6. Revert to (or restore) the original persistent image you took in step 2.

For information about restoring a persistent image, see "[Restoring Volumes From an Existing Persistent Image](#)."

7. Run **reextend.exe** with the drive letter that needs extension by using the syntax **reextend -L: <driveletter>**.

For example, type `reextend -L:g`, where *g* is the drive to be reextended.

The **reextend.exe** file is located in the **c:\WINNT\system32\ServerAppliance** directory.

8. Use the **Dir** command to prove that the total size and free space has expanded.
 9. Compare files from the reverted and reextended dynamic volume to the original persistent image of the volume.
-

Changing the Dell ActiveArchive Event Log Language

Applying a selected language changes the graphical user interface to that language, but it does not change the language in which the Dell ActiveArchive event log messages are generated. The messages are generated in English unless you run a batch file to change the language to one of the following supported languages:

- English
- French
- German
- Japanese
- Spanish

To change the language in which the event log messages are generated, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**.
4. Log in to the system as administrator.
5. If the Advanced Administration Menu is open, click **Exit**, and then **OK** to close it.
6. Open the Microsoft Windows Explorer, expand the hard drive C directory and the **Dell** directory.
7. Open the **AArchive_Langpatch** directory.
8. Double-click the appropriate batch file, such as the **english.bat** file for English or the **japanese.bat** file for Japanese.

9. After the batch file has run, reboot your system.
-

Defragmenting a Volume Containing Persistent Images

-  **NOTICE:** Defragmenting a volume containing persistent images without using the following procedure can corrupt your persistent images and degrade your system performance.
-  **NOTICE:** To defragment a volume, you must delete all persistent images on that volume.
-  **NOTE:** If you do not have persistent images on your volume, this procedure does not apply.

To defragment a volume containing persistent images, perform the following steps:

1. Log in to the NAS Manager.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

2. Click **Disks**.
3. Click **ActiveArchive**.
4. Click **Schedules**.
5. Select a scheduled persistent image, and then click **Delete**.
6. Repeat step 5 until all scheduled persistent images are deleted.
7. Click **Back**.
8. Click **Persistent Images**.
9. Select a persistent image, click **Delete**, click **OK**, and then click **OK**.
10. Repeat step 9 until all persistent images are deleted.
11. Click **Maintenance**.
12. Click **Terminal Services**.
13. Log in to the NAS system.
14. Click **Exit**, and then **OK** to close the Advanced Administration Menu.
15. Double-click **My Appliance**.
16. Right-click the drive that you want to defragment, and click **Properties**.
17. Click **Tools**.
18. Click **Defragment Now**.

The **Defragmentation** window displays.

19. Click **Defragment**.

You are notified when defragmentation is complete.

20. Exit **Terminal Services Client**.
21. Reschedule your persistent images for this volume.

[Back to Contents Page](#)

Advanced Features

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

- [Using the Redundant Memory Feature](#)
- [Installing Multilanguage User Interface \(MUI\) Support](#)
- [Installing and Configuring Support for Other Languages](#)
- [Network Adapter Teaming](#)
- [Services for UNIX®](#)
- [File Server for Macintosh](#)
- [Services for Novell® NetWare®](#)
- [Microsoft Directory Synchronization Services](#)
- [Using Secure Sockets Layers](#)

This section includes descriptions of advanced features that cannot be performed from the Dell™ PowerVault™ NAS Manager.

To perform the procedures in this section, you must use the Terminal Services Advanced Client. To access the Terminal Services Advanced Client, perform the following steps:

1. Log in to the NAS Manager.
2. From the NAS Manager, click **Maintenance**.
3. Click **Terminal Services**.
4. Log on as an administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

Using the Redundant Memory Feature

The NAS system's redundant memory feature (also known as "memory spare row") allows the system to identify a row of faulty RAM and to hot-swap the faulty memory with a reserved row of memory. The chip set reports a faulty row when the threshold of single-bit ECC errors in a single bank is exceeded. When a faulty row is reported, the system copies the faulty row to the spare row and then configures it for access.

System Requirements

To use the redundant memory feature, your NAS system must meet the following requirements:

- All three banks of system memory must use the same type of DIMM.
- The system must be operating in memory-interleaved mode.

Considerations for Using Redundant Memory

- When the redundant memory feature is enabled, only two-thirds of the installed memory is available to the system.
- The redundant memory feature is supported on a per-bank basis. The smallest unit of redundant memory is a bank.
- The spare bank can be used only once per boot. After a bank is swapped, the system has no more redundant memory until it is reset.

For information on enabling the your NAS system's redundant memory feature, see your system's *User's Guide*.

Installing Multilanguage User Interface (MUI) Support

 **NOTE:** Installing the MUI for your language automatically installs the appropriate language locale.

The NAS system allows you to change languages for its Microsoft Windows Powered operating system's user interface. The MUI allows the NAS system to display Windows Powered operating systems menus, dialogs, and help files in multiple languages. The supported MUI languages are simplified Chinese, traditional Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Spanish, and Swedish. You must install a language MUI from the *Multilingual Support* CD before it can be used on the system.

 **NOTE:** Installing and configuring the operating system MUI does not affect the language used by the NAS Manager.

1. Insert the *Multilingual Support* CD into the NAS system's CD drive.
2. From a client system, log in to the NAS Manager.
3. Click **Maintenance**, and then click **Terminal Services**.
4. Log in to the system as an administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

5. Close the Advanced Administration Menu by clicking **Exit** and then clicking **OK**.
6. Double-click **My Appliance** on the NAS desktop.
7. Browse to the CD drive and double-click **Dell PowerVault Multilingual Support CD** to launch the CD's web interface.
8. Click the **Install Multilanguage User Interface (MUI) Support** link to launch the **Multilanguage File Installation** installer program.
9. In the installer window, select the languages to be installed, and select the default MUI language from the menu.
10. Click **OK** to perform the installation.
11. If the **Insert Disk** window appears, you must perform the following steps:
 - a. Click **OK**.
 - b. In the **Files needed** window, click **Browse**, browse to the **i386** directory on the *Multilingual Support* CD, and then click **Open**.
 - c. If the **Insert Disk** window displays, click **OK** to allow the operating system to find the required files for installation.
12. After the installation is complete, you must reboot your system.

Applying the MUI Language

After a MUI language has been installed, you can apply it to any user by performing the following steps:

1. From a client system, log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**.

4. Log in to the system as an administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

5. On the **Advanced Administration Menu**, click **System Management**, and then click **Set Regional Options** to launch the **Regional Options** control panel.
 6. On the **General** tab, select the MUI language from the **Your locale (location)** drop-down menu, and then click **Apply**.
 7. Log off and log in to the system again for the new language MUI to take effect.
-

Installing and Configuring Support for Other Languages

 **NOTE:** Install additional language locales only if your preferred language is not available with MUI support or you need additional locale support.

The Windows Powered operating system that comes installed on your NAS system can be configured to support reading and writing documents in a number of languages. To install the software required to support a specific language, perform the following steps:

1. Insert the *Multilingual Support* CD into the NAS system's CD drive.
2. From a client system, log in to the NAS Manager.
3. Click **Maintenance**.
4. Click **Terminal Services**.
5. Log in to the system as an administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

6. Close the **Advanced Administration Menu** by clicking **Exit** and then clicking **OK**.
7. Double-click **My Appliance** on the NAS desktop.
8. Browse to the CD drive and double-click **Dell PowerVault Multilingual Support CD** to launch the CD's web interface.
9. Click the **Install Language Locales Not Supported by MUI** link to launch the **Regional Options** control panel.
10. From the **Language Settings for the System** panel, select the languages to be configured.
11. Set the default language for the system by clicking **Set default...** and selecting the appropriate language from the menu, and then click **OK**.
12. Click **Apply** to complete the operation.
13. If the **Insert Disk** window appears, you must perform the following steps:
 - a. Click **OK**.
 - b. In the **Files needed** window, click **Browse**, browse to the **i386** directory on the *Multilingual Support* CD, and then click **Open**.
 - c. Click **OK** from the **Insert Disk** window to allow the operating system to find the required files for installation.
14. After the installation is complete, you must reboot your system.

 **NOTE:** For more information, see the Microsoft Windows Powered operating system's online help.

Network Adapter Teaming

Network adapter teaming allows the system to use the combined throughput of multiple network ports in parallel to increase performance or to provide fault tolerance. Network adapter teaming on your NAS system supports the following technologies:

- Adaptive Load Balancing (ALB) from Intel®
- Adapter Fault Tolerance (AFT) from Intel
- Link Aggregation
- Fast EtherChannel (FEC)
- IEEE 802.3ad

 **NOTE:** When creating or removing network adapter teams, the IP address of the NAS system's LAN connections changes. To prevent disconnection from the NAS system during team configuration, use a serial connection (or connect a keyboard, monitor, and mouse to the NAS system) when creating or removing teams. See "[Configuring Your System Using a Serial Connection](#)" in "Initial Configuration" before configuring your teams.

Adaptive Load Balancing

Adaptive Load Balancing (ALB) is a simple and efficient method for increasing the NAS system's network transmission throughput. The ALB software continuously analyzes transmission loading on each adapter and balances the load across the teamed ports as needed. Adapter teams configured for ALB also provide the benefits of adapter fault tolerance. To use ALB, the Ethernet ports on the NAS system must be linked to the same Ethernet switch.

Adapter Fault Tolerance

Adapter Fault Tolerance (AFT) provides the safety of an additional backup link between the NAS system and the hub or switch. If a hub, switch port, cable, or Ethernet port fails, you can maintain uninterrupted network performance. AFT is implemented with a primary adapter and a backup, or secondary, adapter. If the link to the primary adapter fails, the link to the secondary adapter automatically takes over.

Link Aggregation

Link aggregation is a performance technology developed by Intel and others to increase a system's network throughput. Unlike ALB, link aggregation can be configured to increase both transmission and reception channels between your system and switch. Link aggregation works only with compatible Intel switches. To use link aggregation, the Ethernet ports of the NAS system must be linked to the same Intel Ethernet switch.

Fast EtherChannel

Fast EtherChannel (FEC) is a performance technology developed by Cisco Systems to increase a system's network throughput. Unlike ALB, FEC can be configured to increase both transmission and reception channels between your NAS system and switch. FEC works only with compatible Cisco switches. To use FEC, the Ethernet ports of the NAS system must be linked to the same Cisco FEC-compatible switch.

IEEE 802.3ad

IEEE 802.3ad is a performance technology standard that increases a system's network throughput. IEEE 802.3ad is similar to the FEC standard developed by Cisco. However, whereas FEC works only with FEC-compatible Cisco switches, IEEE 802.3ad works with all switches that support IEEE 802.3ad. To use IEEE 802.3ad, the Ethernet ports of the NAS system must be linked to the same IEEE 802.3ad switch.

Creating Intel PROSet II Network Teams

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the Terminal Services session as `administrator`.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

4. Under **Administrative Tools** on the Advanced Administration Menu, click **Intel Network Teaming**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

The Network Teaming utility, Intel PROSet II, displays.

5. Click **Action**, click **Add to Team**, and then click **Create New Team**.

The Teaming Wizard displays.

6. Select the type of team to create, and then click **Next**.

The types of team include **Adapter Fault Tolerance**, **Adaptive Load Balancing**, **Fast EtherChannel*/Link Aggregation**, and **IEEE 802.3ad**.

7. Select the Intel adapters to include with this team, and then click **Next**.

 **NOTE:** Broadcom NICs cannot be selected.

8. Verify that the team contains the appropriate members, and then click **Finish**.
9. If the team needs to be modified, click **Back**.

Removing Intel PROSet II Network Teams

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the Terminal Services session as `administrator`.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

4. Under **Administrative Tools** on the Advanced Administration Menu, click **Intel Network Teaming**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

The Network Teaming utility, Intel PROSet II, displays.

5. In the tree view, click the team that you want to remove.
6. Click **Action**, and then click **Remove**.

Removing an Intel PROSet II Adapter From a Network Team

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the Terminal Services session as administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

4. Under **Administrative Tools** on the Advanced Administration Menu, click **Intel Network Teaming**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

The Network Teaming utility, Intel PROSet II, displays.

5. In the tree view, click the adapter that you want to remove.
6. Click **Action**, and then click **Remove from Team**.

Changing the Intel PROSet II Network Team Mode

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the Terminal Services session as an administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

4. Under **Administrative Tools** on the Advanced Administration Menu, click **Intel Network Teaming**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

The Network Teaming utility, Intel PROSet II, displays.

5. In the tree view, click the team to modify.
6. Click **Action**, and then click **Change Team Mode**.
7. In the Teaming Wizard, select the type of team that you want to create, and then click **Next**.

The types of team include **Fault Tolerance**, **Load Balancing**, **Fast EtherChannel*/Link Aggregation**, and **IEEE 802.3ad**.

8. Click **OK** to close.

For more information, see your Intel PROSet II help.

Creating Network Teams Using the Broadcom Advanced Server Control Suite

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the Terminal Services session as administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

4. Under **Administrative Tools** on the Advanced Administration Menu, click **Broadcom Network Teaming**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

The **Broadcom Advanced Server Control Suite** window displays.

5. Click **Load Balance/Virtual LAN**.
6. Click **Create Team**.
7. Enter the team name and select the appropriate team mode.

The types of team include **Start Load Balance and Fail Over**, **FEC/GEC**, and **Link Aggregation (IEEE 802.3ad)**.

8. Click **OK**.
9. Select the team name in the **Configuration** box.
10. Select an unassigned adapter to add to the team, and then click the arrow adjacent to the **Team Members** list to add the adapter.
11. Repeat step 10 for the second adapter.
12. Click **OK**.

Removing Broadcom Adapter From a Network Team

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the Terminal Services session as administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

4. Under **Administrative Tools** on the Advanced Administration Menu, click **Broadcom Network Teaming**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

The **Broadcom Advanced Server Control Suite** window displays.

5. Click **Load Balance/Virtual LAN**.
6. Select the team name in the **Configuration** box.
7. Select an adapter in the **Team Members** list, and then click the arrow adjacent to **Load Balance Members** to remove the adapter.
8. Click **OK**.

Changing the Network Team Mode Using the Broadcom Advanced Server Control Suite

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the Terminal Services session as administrator.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

4. Under **Administrative Tools** on the Advanced Administration Menu, click **Broadcom Network Teaming**.

 **NOTE:** If the Advanced Administration Menu does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

The **Broadcom Advanced Server Control Suite** window displays.

5. Click **Load Balance/Virtual LAN**.
6. Right-click the team name in the **Configuration** box, and then click **Properties**.
7. Select the new type of team and click **OK** to apply the change.

The types of team include **Start Load Balance and Fail Over**, **FEC/GEC**, and **Link Aggregation (IEEE 802.3ad)**.

8. Click **OK** to complete the change.

For more information, see your Broadcom Advanced Server Control Suite help.

Services for UNIX®

Services for UNIX (SFU) provides the tools needed to integrate UNIX and Windows networks by leveraging existing UNIX network resources and expertise. SFU includes more than 60 of the most common UNIX command line utilities to provide a familiar environment for UNIX users and administrators.

Server for NFS (network file system) allows you to leverage your existing UNIX network resources for UNIX clients.

SFU provides important tools to enhance and simplify the administration of your network.

- Telnet Server enables character- and script-based remote administration of Windows 2000 and Windows NT®-based servers from a variety of clients.
- Microsoft Management Console (MMC) snap-in enables a consistent and central management point for all SFU functionality.
- ActivePerl enables existing and new scripts to use the Windows Management Interface (WMI) to automate network administration tasks.
- User Name Mapping associates Windows and UNIX user names, which allows users to connect to NFS resources without having to log in to UNIX systems separately.

Server for Network File System (NFS)

SFU provides a robust Server for NFS that can be used to provide disk resources from systems running Windows NT and

Windows 2000 to any system on your network that supports NFS. To administer Server for NFS, set the following options from the SFU MMC console:

- **User Mapping** is the name of the mapping server to use.
- **Auditing** is the size and location of the logging file and the operations to audit.
- **Locking** is the grace period for locks and a list of current locks.
- **Client Groups** is used to group client systems for easier setting of permissions.

See [Table 8-1](#) for information on the utilities provided with SFU.

UNIX Utilities

Table 8-1. UNIX Utilities Provided with SFU

Category	Utility
File and directory utilities	basename, cp, diff, dirname, dos2unix, find, ln, ls, mkdir, mount, mv, paste, pwd, rm, rmdir, sdiff, split, tee, touch, uniq, uudecode, uuencode, umount
Text utilities	cat, cut, grep, egrep, fgrep, head, more, printf, sed, sort, tail, tr, vi, wc
Programming utilities	perl, od, sh, strings
Security utilities	chmod, chown, su
Process and general utilities	cron, crontab, date, du, kill, nice, printenv, ps, rcmd, renice, sleep, atr, top, uname, wait, which, xargs

Telnet Server

The Telnet server works optimally for most installations. It accepts logins from a variety of clients, including the Telnet clients shipped with Windows 2000, Windows NT, Windows 95, and Windows 98, as well as a variety of character mode terminal clients from virtually any operating system. In addition, it can be configured to meet specific site requirements such as improving security, simplifying logins, and supporting stream or console mode.

Authentication

The SFU Telnet server supports Windows NT LAN Manager (NTLM) for authentication of client logins. NTLM allows users to be automatically authenticated to the Telnet server based on their Windows NT login. This makes using Telnet completely transparent to users, while ensuring that clear text passwords do not pass over the network. However, NTLM must be supported on the client side of the login as well.

When users are logged in to a system that is using NTLM login, they are restricted to local drives on that system. If they need to map network resources, they can do so by explicitly mapping with full credentials.

Administration

The Telnet server is administered using the SFU MMC snap-in or the **tnadmin** program.

The following options are available:

- **Authentication** gives you the choice of **NTLM** or **Username/Password**.
- **Auditing** allows you to set event logging to a separate log file or to the event log and to specify what events to log.
- **Server Settings** allows you to set the following options:
 - Maximum number of simultaneous connections.
 - Maximum number of failed login attempts.

- o Map <Alt> key to <Ctrl><A>.
 - o Telnet port.
 - o **Console** or **Stream** for mode of operation.
 - o **Default Domain Name** is the domain name that is automatically added to the login username. The default is ".", which disables this feature.
 - o **Idle Session Timeout** is the time until an idle session is forcibly disconnected.
 - o **Terminate all programs when disconnecting** or **Continue to run programs started with the command bgjob**.
- **Sessions** allows you to see data about the currently active sessions (such as user, domain, system, and logon date/time) and to either send a message to the session or terminate it.

Services for UNIX MMC Console

SFU includes a single MMC for managing all of SFU. The MMC provides a cohesive management interface that allows you to administer all systems on the network from any console. Further, since SFU supports the WMI, management can be scripted from the command line.

You can access the MMC Console by selecting **Computer Management** under **System Management** on the Advanced Administration Menu. See "[Using the PowerVault Advanced Administration Menu](#)" in "NAS Manager."

ActiveState ActivePerl 5.6

SFU includes ActiveState's ActivePerl 5.6, a full-featured port of Perl 5.6 and Perl Script to Windows Powered operating systems. Among other improvements, ActivePerl 5.6 includes support for `fork()` emulation at the interpreter level, improving the portability of scripts and modules. ActivePerl also provides full support for the Windows Script Host, making ActivePerl an excellent tool for system administration tasks.

User Name Mapping

User Name Mapping provides mapping of names between the UNIX and Windows environments. You can configure User Name Mapping from the SFU MMC Console or by using the NAS Manager to configure properties for the NFS Sharing Protocol. With User Name Mapping, you can create simple maps between Windows Powered user accounts and corresponding UNIX accounts. You can also use the Advanced Map feature to map accounts with dissimilar names. Because UNIX user names are case-sensitive, and Windows Powered operating system names are not, the use of User Name Mapping can greatly simplify maintaining and managing accounts in the two environments. User Name Mapping uses Network Information Service (NIS) or local Personal Computer Network File System (PCNFS) user and group files to authenticate users. Also, User Name Mapping supports bidirectional one-to-many mapping, allowing you to map a single UNIX or Windows Powered operating system account to multiple accounts in the other environment. For example, you can map more than one administrative account in a Windows Powered operating system to the UNIX root account.

Special Mappings

By default, the root user for the UNIX client is mapped to an unmapped user. This setting is commonly known as "root squashing." When an NFS authentication request is made for a user name mapped to an unmapped user, the result is an anonymous UID and GID (typically -2 and -1, respectively). Any files created by such a user will show file ownership as an anonymous Windows user.



NOTE: To prevent SFU from performing root squashing for specific NFS shares, the UNIX root user and group must be mapped to the Windows administrator user and group. The "access type" for the NFS share's permissions must also be set to root for each applicable client or client group.

To create user and group name maps, perform the following steps:

1. Log in to the NAS Manager.

2. From the NAS Manager, click **Shares**.
3. Click **Sharing Protocols**.
4. Click **NFS Protocol**, and then click **Properties**.
5. Click **User and Group Mappings**.
6. Use the **User and Group Mappings** window to define your user and group maps.

Configuration

To configure the type of server to be used to access UNIX user and group names, perform the following steps:

1. On the **User and Group Mappings** window, click **General**.
 2. Click **Use NIS server**, or click **Use password and group files** to select the server type.
 3. Depending on whether you use an NIS server or password and group files, perform one of the following steps:
 - For password and group files, specify the location and filename of the UNIX password file and UNIX group file.
-  **NOTE:** The UNIX password file and group file formats must conform to the UNIX standard for these files.
- For NIS server, type the NIS domain and, optionally, the name of the NIS server.
4. Click **OK** to apply the configuration.

Defining Maps

To define simple maps in SFU, perform the following steps:

1. In the **User and Group Mappings** window menu, click **Simple Mappings**.
2. Click **Enable Simple Mapping**.
3. Specify the **Windows Domain**.
4. Click **OK** to create the maps.

If you are defining explicit maps, you create user and group maps individually. To create explicit maps, perform the following steps:

1. On the **User and Group Mappings** window menu, click **Explicit User Mapping** to create user maps, or click **Explicit Group Mapping** to create group maps.
2. Specify the **Windows Domain**. If the server is configured as **PCNFS**, go to step 4.
3. Click **List UNIX Users** or **List UNIX Groups**.

This action refreshes your UNIX users or groups selection.

4. Create map entries by selecting a Windows user or group and a UNIX user (UID) or group (GID) from the list and clicking **Add**.
5. Click **OK** to create the maps.

Basic Scenarios

For UNIX and Windows NT User Name Mapping, an NIS Server must already exist in the UNIX environment, or UNIX user and group files must exist on the PowerVault NAS system. User Name Mapping associates UNIX users and groups to Windows NT users and groups. You can use two types of maps, simple and explicit. Simple maps define a one-to-one relationship between the same user names and groups. Explicit maps define a relationship between dissimilar user names and groups.

Workgroup

In the workgroup scenario, you configure User Name Mapping locally on the NAS system. All maps are contained on this system.

Domain

In the domain scenario, you configure NFS Authentication on all domain controllers. The NT Authentication Service installation program must be installed on the domain controller and available in the **DomainUtils** share on the NAS system.

To install the NT Authentication Service on a domain controller, perform the following steps:

1. Log in to the domain controller as an administrator.
2. Map the NAS system's **DomainUtils** share.
3. Run **sfucustom.msi**, which is located in the **Services for Unix** directory.

Filename Character Translation

Although Windows and UNIX file systems do not allow certain characters in filenames, the characters that are prohibited by each operating system are not the same. For example, a valid Windows filename can not contain a colon (:), but a UNIX filename can. If a UNIX user attempts to create a file in an NFS share and that file contains an illegal character in its name, the attempt will fail.

You can use filename character translation to replace characters that are not allowed in a file system by mapping them to characters that are valid. To enable filename character translation, create a text file that maps Windows to UNIX characters, and then modify the registry entry that specifies the path and name of the translation file.

The filename character translation text file is a list of mapped characters in the following format, such as the following:

```
0xnn : 0xnn [ ; comment ]
```

where *nn* is the hexadecimal value of the character

The entry for a map from the UNIX character ":" to the Windows character "-" in the filename character translation text is as follows:

```
0x3a : 0x2d ; Map ':' (0x3a) to '-' (0x2d)
```

To map the character combination "()" to the character "^", add the following entry:

```
0x28 0x29 : 0x5e ; Map '()' to '^'
```

To specify the path and name of the filename character translation text file for Server for NFS to use, modify the following registry key to contain the path and filename of the character translation file:

```
HKLM\SOFTWARE\Microsoft\Server for NFS\CurrentVersion\Mapping\CharacterTranslation
```

File Server for Macintosh

File Server for Macintosh (FSM) provides the tools needed to integrate Macintosh and Windows networks by leveraging existing Macintosh network resource and expertise. FSM is disabled by default on the NAS system. See "[Enabling the AppleTalk Protocol](#)" for information about enabling FSM.

Enabling the AppleTalk Protocol

The AppleTalk protocol is disabled on the NAS system by default. You must enable the AppleTalk protocol for Macintosh clients to access the NAS system.

To enable the AppleTalk protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **AppleTalk Protocol**, and then click **Enable**.

Disabling the AppleTalk Protocol

To disable the AppleTalk protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **AppleTalk Protocol**, and then click **Disable**.

Configuring the AppleTalk Protocol

To configure the AppleTalk protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **AppleTalk Protocol**, and then click **Properties**.
5. In the **AppleTalk Service Properties** window, type the logon message the users will see at logon, click the **Security** check box if you allow workstations to save passwords and select the type of authentication to be used, and specify the number of concurrent sessions that are allowed.
6. Click **OK** to complete the configuration.

Adapter Bindings

FSM can bind to only one network adapter. By default, it is bound to the embedded 10/100TX Network Adapter. To change the binding in systems with multiple network adapters, the AppleTalk protocol properties for the network adapter to be used by AppleTalk must be modified to accept inbound connections.

AppleTalk Protocol Adapter Binding

To modify the AppleTalk protocol adapter binding for systems with multiple network adapters, perform the following steps from the NAS Manager:

1. Log in to the NAS Manager.
2. Click **Network**.
3. Click **Interfaces**.
4. Click the radio button next to an enabled adapter to bind the AppleTalk protocol.

 **NOTE:** The AppleTalk protocol must bind to an adapter that is enabled, regardless of whether the File Server for Macintosh is disabled.

5. On the **Tasks** menu, click **AppleTalk**.
6. Click the check box next to **Enable inbound AppleTalk connections on this adapter**.
7. Optionally, if you use AppleTalk zones, select the appropriate zone in the drop-down box.
8. Click **OK**.

Microsoft UAM Volume

A user authentication map (UAM) is a software program that prompts users for an account name and password before they log in to a server. The Macintosh Chooser has a standard UAM built in that uses the clear-text password or Apple's RandNum Exchange method of security.

Microsoft Authentication offers an additional level of security because the password is used as a key to encrypt a random number. If the system administrator has determined that encryption is an important security measure, you may be asked to use Microsoft Authentication in addition to Microsoft UAM authentication.

Requirements

To use Microsoft UAM 5.01, you must have a Macintosh client running AppleShare Client 3.8 or later or Macintosh 8.5 or later operating system. If you do not meet the minimum requirements, the Microsoft UAM Installer installs the old Microsoft UAM 1.0 module. If you upgrade your system software, you need to run the Microsoft UAM Installer again.

Installing User Authentication

Log in to the Microsoft UAM Volume on the system to access the **MS UAM** file, and then drag this file to the **AppleShare Folder** in your **System** folder.

To access the Microsoft Authentication files on the system, perform the following steps:

1. Create a user with a password of less than eight characters.
 - a. Log in to the NAS Manager.
 - b. Click **Users**.
 - c. Click **Local Users**.
 - d. Click **New**.
 - e. Complete the information in the **Create New User** window and click **OK**.

 **NOTE:** The password can be no longer than eight characters. Passwords longer than eight characters cannot be used when mapping an Apple share without a UAM.

2. Click **Chooser** on the **Macintosh Apple** menu.
3. Double-click the **AppleShare** icon, and then click the **AppleTalk** zone in which the system with Services for Macintosh resides.

Ask your system administrator if you are not sure of the zone.

4. Select the system from the list of file servers, and click **OK**.
5. Click **Registered User**.

6. Enter the user name and password you created in step 1, and then click **OK**.
7. Select the **Microsoft UAM Volume**, and then click **OK**.
8. Close the **Chooser** dialog box.

To install the authentication files on the Macintosh workstation, perform the following steps:

1. Double-click **Microsoft UAM Volume** on the Macintosh desktop.
2. Double-click the **Microsoft UAM Installer** file on the Microsoft UAM volume.
3. Click **Continue** in the **Installer Welcome** screen.

The installer reports whether the installation succeeds.

If the installation succeeds, Macintosh users of this workstation are offered Microsoft Authentication when they connect to the system.

Restarting Workstation Services

If File Services for Macintosh cannot establish communications to the local RPC service, you may need to restart the Workstation Service.

To restart the Workstation Service, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the NAS system as an administrator.



NOTE: The default administrative user name is `administrator` and the default password is `powervault`.

The Advanced Administration Menu displays. If it does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

4. Click **System Management**, and then click **Computer Management**.
5. Click **Services and Application**.
6. Double-click **Services**.
7. Right-click **Workstation** in the **Services** window, and select **Restart**.
8. Confirm that you want to restart the Workstation Services.

Services for Novell® NetWare®

Services for NetWare (SFN) are compatible with Novell NetWare Bindery service for authentication and file access using the internetwork packet exchange/sequenced packet exchange (IPX/SPX) network protocol. Services for NetWare are disabled by default. See "[Enabling Services for NetWare](#)."

Enabling Services for NetWare

The NetWare protocol is disabled on the NAS system by default. You must enable the NetWare protocol for NetWare clients to access the NAS system.

To enable the NetWare protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **NetWare Protocol**, and then click **Enable**.

 **NOTE:** For the NAS system, the default NetWare supervisor user name is `supervisor`, and the password is `powervault`.

Disabling Services for NetWare

To disable the NetWare protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **NetWare Protocol**, and then click **Disable**.

Configuring the NWLink IPX/SPX Compatible Protocol

To configure this protocol, you need the internal network number, frame type, and network number.

Internal Network Number

Internal network numbers are used for internal routing and are generally needed only for servers. You should not need to change this option on your system.

Frame Type and Network Number

Frame types define the packet formats that are used by different networks. It is important that all systems in a network have the same frame type so that they can communicate with the rest of the network.

When you are configuring your system, it attempts to automatically detect the frame type for the client. In most cases, this is successful. However, the automatic detection feature occasionally selects an inappropriate frame type, usually because more than one frame type exists on the network. If this happens, you should manually set the frame type to match the one specified on your NetWare server.

 **NOTE:** If more than one frame type exists, you should select the one that is detected first. For example, if the frame types Ethernet 802.2 and Ethernet 802.3 are bound to the same segment, configure frame type Ethernet 802.2. The order of detection is Ethernet 802.2, Ethernet 802.3, Ethernet II, and then Ethernet SNAP.

Configuring the IPX Protocol

By default, the IPX protocol is configured on the NAS system to automatically detect frame types. To use the IPX protocol, you must change your NAS system's IPX properties to manually detect frame types.

To configure the IPX protocol to manually detect frame types, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the NAS system as an administrator.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The Advanced Administration Menu displays. If it does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

4. Click **System Management**, and then click **Network Properties**.
5. In the **Network and Dial-up Connections** window, right-click the network adapter used by the NAS system and select **Properties**.
6. In the **Local Area Connection Properties** window, click **NWLink/IPX/NetBIOS Compatible Transport Protocol**, and click **Properties**.
7. In the **NWLink/IPX/NetBIOS Compatible Transport Protocol** window, select **Manual Frame type detection**.
8. Click **Add**.
9. In the **Manual Frame Detection** window, select a frame type, enter a network number for the IPX network, and then click **OK**.
10. Click **OK**.
11. Click **OK** to close the **Local Area Connection** window.
12. Close the **Network and Dial-Up Connections** window.

The IPX protocol is now configured on the NAS system to manually detect frame types.

Microsoft Directory Synchronization Services

Microsoft Directory Synchronization Services (MSDSS) allows you to synchronize a wide variety of data stored in the Active Directory service with Novell Directory Service (NDS) and NetWare 3.x binderies.

MSDSS is a highly flexible service that helps Novell users to perform the following tasks:

- Adopt Windows 2000 Server and the Active Directory service
- Reduce directory management through two-way synchronization
- Migrate NDS and bindery information to Windows 2000 Server

MSDSS supports two-way synchronization with NDS and one-way synchronization with NetWare 3.x binderies to provide a complete directory interoperability solution. MSDSS also supports password synchronization and provides a directory migration service.

MSDSS allows NetWare users to deploy Active Directory without having to replace existing directories or bear the cost of managing two separate directories. As a result, users have the flexibility to:

- Consolidate directory management when multiple directories are required
- Manage accounts from either directory
- Use directory-enabled applications, devices, and services based on the Windows 2000 Active Directory service

MSDSS is easy to use and makes synchronization and Active Directory setup easy through its management interface. It is fully featured to allow users a choice of management, synchronization, and migration options.

MSDSS supports all major NetWare platforms and most Novell directories and binderies, and it includes support for IPX/SPX and TCP/IP network protocols.

Windows 2000 MSDSS Domain Controller

To implement MSDSS, you must install the Windows 2000 Server operating system and the MSDSS software (available on the *Microsoft Services for NetWare Version 5 CD*) on at least one system. In Windows 2000, when you promote a system running Windows 2000 Server to an Active Directory server, it becomes a domain controller. You use this domain controller to configure Active Directory, install MSDSS, and then import information from the existing NetWare environment.

The larger the environment, the more new servers you need. If you are planning to have more than one domain, then you need new hardware for the first domain controller in each domain.

You must also install Novell Client Access software on the MSDSS server or servers. MSDSS uses Novell Client Access to authenticate and to access NDS. While accessing NDS, it authenticates, but does not use a license. MSDSS also uses Novell Client Access to map one directory's contents to another, taking into account the fact that the object classes in Novell's NDS or bindery directories are different from Active Directory object classes. Novell Client Access is also required to use the File Migration utility to migrate files.

You can install Novell Client Access in four modes: **IP only**, **IPX only**, **IP and IPX combined**, and **IP with IPX Compatibility Mode**. Most NetWare environments still use IPX. MSDSS works in all the modes because it uses Novell Client Access to access the lower layers.

If you are migrating NDS, you can import the user and group information from one NDS server to the MSDSS server because you have one user database per tree. You can then migrate the file system. Remember that each Novell server has its own file system, which is not replicated to other servers (whereas NDS is replicated to other servers). After the files are migrated, you can uninstall NDS from the server to provide more space for the Windows 2000 Server operating system.

Outline of the MSDSS Deployment Procedure

The next two sections describe the procedures for implementing MSDSS in a smaller (local area network [LAN] only) or larger (wide area network [WAN]) network. You should adapt the guidelines to suit your environment and goals.

Small Environment

A small company with a LAN-based, simple network is often a likely candidate for a quick migration. After doing all the preparations described in the previous section, perform the following steps (adjusted, if necessary, to your situation):

1. Back up your NetWare system and user data.
2. Install and configure a Windows 2000 domain controller (see the documentation that came with your operating system software).
3. Install the Novell Client for Windows 2000 from the Novell website at www.novell.com/download.
4. Replace services or applications that require NDS with software that is compatible with Active Directory. (Remove NDS applications before you begin using MSDSS, except for ZENworks, which can be replaced by IntelliMirror at any time.)
5. Install MSDSS from the system **DomainUtils** share.

 **NOTE:** To access MSDSS software, map a network drive to `\\Dellxxxxxxx\DomainUtils`, where `xxxxxxx` is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`.

6. Log in to the NDS tree or bindery server as `administrator`.
7. Log in to the appropriate Windows 2000 domain as a member of the Domain Admins group.
8. On the MSDSS server, open the Help files, and then print out the procedures "To perform a one-time migration" and "To migrate files."
9. Click the **Start** button, and then point to **Programs® Administrative Tools® Directory Synchronization** to start MSDSS.
10. Follow the instructions as described in the Help printout, "To perform a one-time migration." The prompts guide you through the following steps:
 - a. Right-click **MSDSS** in the console tree, and then click **New Session** to start the New Session Wizard.
 - b. Specify whether objects are to be copied from NDS or Bindery.

- c. Click **Migration**.
- d. If you plan to migrate files as well as directory objects, click the **Migrate Files** check box.

You must also run the File Migration utility.

- e. Specify the path to the Active Directory container in which you want to copy items.
- f. Accept the default domain controller in which to store the migration log.
- g. Specify the NDS Container or Bindery Container from which to copy items.
- h. Provide the name and password of the Novell administrative account.
- i. On the **Initial Reverse Synchronization** page, specify the password options (such as **Set passwords to the user name**.)

When you are performing a migration, this page does not include the option to actually perform an initial reverse synchronization, but it is the page where you specify which password option you want to use.

- j. Set **synchronization mode** to **default object mapping** or to **custom object mapping**.
- k. If you selected **custom object mapping**, you are prompted to manually establish one-to-one relationships between pairs of objects.
- l. Click **Finish**.

After the user accounts are migrated, you can migrate the file system (migrating the users before the files allows you to migrate file-system permissions). Follow the instructions in the Help printout, "To migrate files." The prompts guide you through the following steps:

- To start the File Migration Utility, click the **Start** button and point to **Programs® Administrative Tools® File Migration Utility**.
- To view mapping relationships, click **View Maps**.
- To view mapped access rights for the users, groups, organization units, and organizations to be migrated, click **Access Rights**.

The **NDS Modify** option converts, by default, to **Read** because it does not have an equivalent NDFS right. You might want to click the **Write** check box to allow read/write access.

- On the **Step 2 — Security Accounts** tab, verify that you are logged on with the correct Active Directory, NDS, or Bindery credentials.
- On the **Step 3 — Source and Target** tab under **Source (NDS/Bindery)**, click the volume or directories from which you want to migrate files. Under **Target (Active Directory)**, click the shares or directories to which you want to migrate files, click the **Map** button, and then click **Next**.

If the NDS or Bindery volume you selected in the source tree displays **Unavailable**, then you are not currently logged in to that tree or Bindery server. Log in, and then press <F5> after reselecting the volume to view the directories within the displayed volume.

- On the **Step 4 — Log File** tab, select your logging options, and then click **Next**.
- On the **Step 5 — Scan** tab, click **Scan**, and then click **Next**.

The utility scans all source volumes and counts and displays the number of directories and files in each. It ensures that proper access has been given to each source volume, directory, and file. If any errors occur, the utility displays them under **NetWare scan logs** and **Windows scan logs**, respectively. You can select a number of acceptable errors; if this number is exceeded, the process aborts, allowing you to return to previous steps to correct the errors.

- On the **Step 6 — Migrate** tab, click **Migrate**.

Manually migrate (or use third-party utilities to migrate) object security permissions and system accounts, printer objects, application objects, and other objects that MSDSS does not migrate from Bindery or NDS to Active Directory. (MSDSS migrates NetWare user accounts, groups, and distribution lists for Bindery and NDS, and, for NDS only, MSDSS also migrates NDS organizational units and organizations.)

1. Upgrade your NetWare server(s) to the Windows 2000 Server or Professional operating system.
2. On each Windows desktop in your NetWare network, uninstall Novell Client Access.

You must configure the desktops to join the Windows 2000 domain.

3. Optionally, upgrade NetWare clients (workstations) to the Windows 2000 Professional operating system.
4. Configure all client systems (both Windows and non-Windows), to join the Windows 2000 domain.

Be sure that the users know how to handle their password the first time they log in (for possible password options, see "MSDSS Password Management" in "MSDSS Deployment: Understanding Synchronization and Migration)" at www.microsoft.com.

Medium-Sized or Large Environment

An organization large enough to have WAN links probably selects to synchronize its networks temporarily while performing a gradual migration over time (up to 3 months for a large network), or it prefers to use synchronization to establish a mixed Novell/Windows 2000 network on a long-term basis. If you plan a staged migration, one-way synchronization is often the appropriate choice.

After doing all the preparation described above, perform the following steps (adjusted, if necessary, to your situation):

1. Back up your NetWare user and system data.
2. Install and configure a Windows 2000 domain controller (see the documentation that came with your operating system software).
3. Install the Novell Client for Windows 2000 from the Novell website at www.novell.com/download.
4. Install MSDSS from the NAS system **DomainUtils** share.



NOTE: To access MSDSS software, map a network drive to `\\Dellxxxxxxx\DomainUtils`, where xxxxxxxx is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`.

5. Log in to the NDS tree or Bindery server with administrative credentials.
6. Log in to the appropriate Windows 2000 domain as a member of the **Domain Admins** group.
7. On the MSDSS server, open the Help files, and then print out the steps (briefly summarized below) for "To perform a one-way synchronization" or "To perform a two-way synchronization."
8. Click the **Start** button, point to **Programs® Administrative Tools® Directory Synchronization** to start MSDSS, and then allow the prompts to guide you through the following tasks:
 - a. Start the New Session Wizard (right-click **MSDSS** in the console tree).
 - b. Select **Novell Bindery** or **Novell Directory Services (NDS)** for one-way synchronization, or select **Novell Directory Services (NDS)** for two-way synchronization.
 - c. Select **One-way synchronization (from Active Directory to NDS or Bindery)** or select **Two-way synchronization (from Active Directory to NDS and back)**.
 - d. Specify the path to the **Active Directory** container into which you want to copy items.
 - e. Accept the default domain controller in which to store the session database.
 - f. Specify the NDS Container or Bindery Container from which to copy items.

- g. Provide the name and password of the Novell administrative account.
 - h. On the **Initial Reverse Synchronization** page, select **Perform an initial reverse synchronization**.
 - i. Still on the **Initial Reverse Synchronization** page, specify the password options (such as **Set passwords to the user name**).
 - j. On the **Object Mapping Scheme** page, click **Default** (to accept the default mapping for each source and target directory pair) or **Custom** (for NDS only), and then click **Object Mapping Table** (to specify objects for which you want to establish a one-to-one relationship, regardless of the object location in either directory tree).

MSDSS does not support custom object mapping for Bindery.
 - k. Still on the **Object Mapping Scheme** page, click **Filters** if you want to configure a filter for this synchronization session.
 - l. On the **Session Name** page, accept the default session name or specify a new name.
 - m. Click **Finish**.
9. If you selected one-way synchronization, you should now perform all user, group, and NDS organizational unit (OU) object management from Active Directory. If you established two-way synchronization, you can now manage user, group, and OU objects from either Active Directory or NDS.
 10. If you plan long-term coexistence between Active Directory and NetWare, you are now finished, unless you want to migrate a subset of users, systems, and/or files. If you plan to continue by migrating in stages from NetWare to Active Directory, perform the following tasks in the time-frame that is convenient for you:
 - Install and configure File and Print Services for NetWare (to allow NetWare clients access to files and printers on Windows 2000 servers) and Gateway Services for NetWare (to allow Windows clients access files and printers on NetWare servers).
 - Replace services or applications that require NDS with commensurate software compatible with Active Directory. Perform large conversions (such as GroupWise to Exchange) as separate projects.
 - Migrate the pilot group of users and their files (adapt instructions from the migration steps provided in the "[Small Environment](#)" section). Get the pilot group's feedback, and then set a schedule to migrate additional groups of users, according to the priorities you have established.
 - Migrate the rest of the users as appropriate (for example, if you migrate the set of applications they use, it is time to migrate them as well).

For more information, see the Novell website at support.novell.com/servlet/Knowledgebase and the Windows 2000 website at www.microsoft.com/windows2000.

Using Secure Sockets Layers

This section explains how secure sockets layers (SSL) are used in the NAS system. It also explains how to use your own certificate, if you have one, and how to regenerate your certificate.

Introduction to SSL Certificates

Certificates contain information used to establish system identities over a network. This identification process is called authentication. Although authentication is similar to conventional forms of identification, certificates enable Web servers and users to authenticate each other before establishing a connection to create more secure communications. Certificates also contain encryption values, or keys, that are used in establishing an SSL connection between the client and server. Information, such as a credit card number, sent over this connection is encrypted so that it cannot be intercepted and used by unauthorized parties.

Two types of certificates are used in SSL. Each type has its own format and purpose. *Client certificates* contain personal information about the clients requesting access to your site, which allows you to positively identify them before allowing them access to the site. *Server certificates* contain information about the server, which allows the client to positively identify the

server before sharing sensitive information.

Server Certificates

To activate your Web server's SSL 3.0 security features, you must obtain and install a valid server certificate. Server certificates are digital identifications containing information about your Web server and the organization sponsoring the server's Web content. A server certificate enables users to authenticate your server, check the validity of Web content, and establish a secure connection. The server certificate also contains a *public key*, which is used in creating a secure connection between the client and server.

The success of a server certificate as a means of identification depends on whether the user trusts the validity of information contained in the certificate. For example, a user logging on to your company's website might be hesitant to provide credit card information, despite having viewed the contents of your company's server certificate. This might be especially true if your company is new and not well known.

For this reason, certificates are sometimes issued and endorsed by a mutually trusted, third-party organization, called a certification authority. The certification authority's primary responsibility is confirming the identity of those seeking a certificate, thus ensuring the validity of the identification information contained in the certificate.

Alternatively, depending on your organization's relationship with its website users, you can issue your own server certificates. For example, in the case of a large corporate intranet handling employee payroll and benefits information, corporate management might decide to maintain a certificate server and assume responsibility for validating identification information and issuing server certificates. For more information, see "[Obtaining a Server Certificate From a Certification Authority](#)."

PowerVault 77 xN Certificate

By default, your NAS system has a self-generated and self-signed certificate. The configured SSL port is 1279.

 **NOTE:** For non-SSL communication, use port 1278. This port is not a secure port and all text is sent in plain text over the network.

Using a Custom Certificate

If a certification authority is present in the network, the administrator can choose to change the default certificate for your NAS system. The administrator must use the wizards to first request a certificate and then apply it to the NAS system.

Obtaining a Server Certificate From a Certification Authority

 **NOTE:** If you are replacing your current server certificate, the Internet Information Server (IIS) continues to use the old certificate until the new request has been completed.

Find a certification authority that provides services that meet your business needs, and then request a server certificate.

 **NOTE:** For the latest list of certification authorities supporting IIS, see the Microsoft Security website. In the **By Category** list, select **Certification Authority Services**.

To obtain a server certificate, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Terminal Services**.
3. Log in to the NAS system as an administrator.

 **NOTE:** The default administrative user name is `administrator` and the default password is `powervault`.

The Advanced Administration Menu displays. If it does not display, double-click the **Advanced Administration Menu** icon on the desktop of the NAS system.

4. Click **System Management**, and then from the list, click **Internet Information Services**.

5. Navigate to and right-click the **Administration** folder, and then select **Properties**.
6. Under **Secure Communications** on the **Directory Security** property sheet, click **Server Certificate** to access the Web Server Certificate Wizard.
7. Use the Web Server Certificate Wizard to create a certificate request.
8. Send the certificate request to the certification authority.

The certification authority processes the request and sends you the certificate.



NOTE: Some certification authorities require you to prove your identity before processing your request or issuing you a certificate.

9. Use the Web Server Certificate Wizard to install your certificate.

For more information about SSL, see the Internet Information Server online help.

[Back to Contents Page](#)

Troubleshooting

Dell™ PowerVault™ 77xN NAS Systems Administrator's Guide

• [Tools and Techniques](#)

• [Troubleshooting](#)

Tools and Techniques

Because your NAS system is a "headless" system that does not have a keyboard, mouse, or monitor, you must use other methods for troubleshooting issues and conditions. This section provides suggestions for and information about alternative troubleshooting tools and techniques.

Console Redirection

Console redirection allows you to directly attach a client system to the NAS system for local management and troubleshooting. For more information about console redirection, see "[Console Redirection](#)" in "Advanced Features."

Serial Connection

You can directly attach a client system to your NAS system using a serial cable and the administration port to configure or troubleshoot your NAS system. For more information about using a serial connection, see the serial connection information for your operating system in "[Configuring Your NAS System for the First Time](#)" in "Initial Configuration."

Ping Your NAS System

If you are unable to connect to the NAS system using the NAS Manager, try to ping the NAS system. From a client system, click the **Start** button, click **Run**, and then type `cmd`. At the command prompt in the **cmd.exe** window, type `ping system_name`, and then press <Enter>.

 **NOTE:** The default system name is `DELLxxxxxxx`, where `xxxxxxx` is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`.

If you can ping the NAS system but cannot access it through the NAS Manager, your NAS system might still be booting into Microsoft® Windows® and might not have started the Microsoft Internet Information Services (IIS).

 **NOTE:** It may take several minutes for the NAS system to boot, depending on your configuration and the amount of storage attached to the system.

My Network Places

If you have a Windows 2000 client system on the same subnet as the NAS system, double-click **My Network Places**. Browse through the network and locate your NAS system.

System LEDs and Beep Codes

If your NAS system is not booting or responding properly, you can diagnose some problems using the system's LEDs and beep codes. For more information about the LEDs and beep codes, see your system's *Installation and Troubleshooting Guide*.

Terminal Services

You can use the Terminal Services Advanced Client to connect to your NAS system from a client system. You can access Terminal Services Client through the NAS Manager or the **Start** menu.

To access Terminal Services from the NAS Manager, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Terminal Services**.
4. Enter the administrator user name and password and click **OK**.

 **NOTE:** The default administrator user name is `administrator` and the default password is `powervault`.

Troubleshooting

Use the following tables to help you troubleshoot various conditions that might occur on your NAS system:

- [Table 9-1](#), "General Troubleshooting"
- [Table 9-2](#), "NAS Manager"
- [Table 9-3](#), "Dell ActiveArchive"
- [Table 9-4](#), "Dell OpenManager Array Manager"
- [Table 9-5](#), "UNIX and Red Hat Linux"
- [Table 9-6](#), "Macintosh and AppleTalk"
- [Table 9-7](#), "Netscape Navigator"

Table 9-1. General Troubleshooting

Issue	Possible Cause	Resolution
I just created a new volume on my system but cannot see the volume on Windows Explorer through Terminal Services.	Terminal Services cannot update to show a new volume during the session in which it was created.	Log off Terminal Services. When you reconnect to Terminal Services, the volume should be visible.
I see the following error message in the event log: WMI ADAP was unable to load the winspool.drv performance library due to an unknown problem within the library: 0x0	This is an issue with the WDAP Performance library and is documented on Microsoft's website.	Connect to the system via Terminal Services Advanced Client, and then open a local command prompt. Type the following command: <code>WINMGMT/CLEARADAP</code> . When the prompt returns, type <code>WINMGMT/RESYNCPERF winmgmt service PID</code> .
I have just brought up my new NAS system on the network, but I am unable to upload files using FTP even though I am the administrator.	By default, no user has write privileges on the default FTP site.	The FTP permissions must be configured using the Microsoft Management Console (MMC). To access the MMC, click Computer Management on the Advanced Administration Menu, which is available through Terminal Services. See the online help for specific information about configuring this service.
I have deleted an FTP share and folder from my NAS system. However, when I use Terminal Services to confirm the removal, I can still see the shared folder in the FTP section of the MMC.	By default, this folder is not deleted by the NAS Manager.	Manually remove this listing from the listed shared folders in the FTP section of the MMC.

The BIOS does not see hard drive 0.	The hard drive has failed or the operating system files or boot record is missing or corrupt.	No immediate action is required. The NAS system can automatically boot from hard drive 1.
I cannot connect to or ping the NAS system after turning it on.	The NAS system has not finished booting.	Wait at least 5 minutes for the NAS system to finish booting. If you still cannot connect, attempt the procedures in " Solutions to Try Before Reinstalling " in "Recovering and Restoring the System."
My network connection seems slow.	You are using a Broadcom NetXtreme Gigabit Ethernet Server Adapter without the correct drivers, and you have enabled the wake-on-LAN (WOL) feature through the System Setup program.	Your system's network connection will operate at a speed of 10/100 until the operating system loads the correct drivers. When the correct drivers are installed, the connection speed will increase to 10/100/1000.
After using Terminal Services to connect to my NAS system, I am unable to type using my native language.	The NAS system is set to English, the default language.	You can install your native language character set from the <i>Multilingual Support</i> CD that was shipped with your system. For installation instructions, see " Advanced Features ."
I cannot get console redirection to work correctly. Only a few keys work on the keyboard, and none of the keys work when trying to configure the BIOS.	<Scroll Lock>, <Caps Lock>, or <Num Lock> might be set on your keyboard. Also, your operating system may not support all of the keys on your keyboard.	Ensure that the <Scroll Lock>, <Caps Lock>, and <Num Lock> lights are turned off on the keyboard. If these lights are not on and the problem persists, see " Console Redirection " in "Advanced Features."
During a Terminal Services session to the NAS system, I mapped a network share from the NAS system. Now the system does not reboot correctly and hangs during shutdown.	Having a share mapped from the NAS system causes the system to hang during shutdown.	Make sure that when you map a share, you do not select Reconnect at logon . To disconnect the drive, right-click My Appliance on the NAS system desktop, and select Disconnect Network Drive . Click the CD share in the Disconnect Network Drive window, and then click OK . If you cannot log in to the NAS system, reboot the system. Then connect using Terminal Services and disconnecting the drive. If Terminal Services does not work, try connecting using a serial connection. See " Configuring Your System Using a Serial Connection " in "Initial Configuration."
The Telnet option in the NAS Manager does not allow me to enable Telnet on the NAS system, even though I have selected the check box next to Enable Telnet access to this NAS system on the Telnet Administration Configuration page.	This option is not enabled.	To enable Telnet on your NAS system, perform the following steps: <ol style="list-style-type: none"> 1. From the NAS Manager primary menu, click Maintenance® Terminal Services. 2. Log in to the NAS system as an administrator. 3. If the Advanced Administration Menu is displayed, click Exit to close it. 4. Right-click My Appliance. 5. Click Manage. 6. Double-click Services and Applications® Services. 7. Locate and right-click Telnet, and then click Start. Telnet starts on the NAS system.
I cannot connect to the NAS system using the IPX protocol.	IPX networks require that you assign an IPX network number to all clients. By default, the NAS system does not assign an IPX number to the	Change the IPX protocol on the NAS system to manually detect frame types. See " Configuring the IPX Protocol " in "Advanced Features."

	network.	
I am trying to install the CA ARCserve Remote Agent on the NAS system by mounting the CD share that contains the CA ARCserve CD. However, I am having trouble installing the program.	The CA installer does not work properly when installing from a CD share mounted on your NAS system.	To install the CA ARCserve Remote Agent, copy the CD contents to drive C of your NAS system. Then run the installer from the NAS system. Or, connect a keyboard, monitor, and mouse to the NAS system and use the CD from the local CD drive.
After restoring files from a backup, the modified dates of folders are inconsistent.	The modified dates of folders reflect either the date you performed the restore or the date the folder was modified.	Take no action. This is a design issue that occurs only with folders; the files' modified dates are consistent.
The Advanced Administration Menu does not display anymore.	You were not logged off of Terminal Services before you closed the NAS Manager.	Log off Terminal Services by clicking the Start button on the NAS system and logging off.
The device "Communication cable between two computers" shows changed in the online diagnostics.	Online diagnostics has improperly identified this device as an external modem.	Because the "Communication cable between two computers" device is allocated to the Routing and Remote Access services, do not attempt to run diagnostics on this device.
The system summary and the task manager show twice as many processors as are actually installed in the system.	The NAS system provides a hyperthreading option, which allows one physical processor to appear to the operating system and other applications as two logical processors.	Take no action. Your NAS system is operating correctly.

Table 9-2. NAS Manager

Issue	Possible Cause	Resolution
I am trying to select the Administer My Appliance link on the opening page of the NAS Manager, but the link does not function properly.	The user account that you used to log in to the domain does not have administrator privileges. The link does not work for users without administrator privileges.	Type the address of the NAS Manager in your browser. For SSL connections, type: <code>https://servername:1279</code> or <code>https://IPaddress:1279</code> For non-SSL connections, type: <code>http://servername:1278</code> or <code>http://IPaddress:1278</code>
I have just deleted a volume, and now I am unable to view my shares in the NAS Manager.	In the event that a volume with shares is deleted, the NAS Manager cannot display any shares until the shares that were directed to the deleted volume are removed.	Use Terminal Services Advanced Client to remove the shares for the deleted volume. Exit the NAS Manager, and restart the system. The shares should now be visible.
I have just added an HTTP share but cannot see it from the NAS Manager.	For security purposes, directory browsing is not enabled by default on an HTTP share directed to the same folder or volume as another share.	To enable directory sharing for an HTTP share, from the NAS Manager Maintenance page, click Terminal Services Advanced Client , and then modify the Web sharing properties of the folder.
I have just changed the IP address of my system, and now I cannot administer it through the NAS Manager.	Although the IP address changed, your local host is still trying to communicate with the system using the old IP address. It takes approximately 15 minutes for the IP address to automatically update on most networks.	Close Microsoft Internet Explorer (or for Red Hat Linux only, Netscape Navigator 6.2.2 or later). Reconnect using the newly created IP address. Type: <code>https://IPaddress:1279</code> . It takes approximately 15 minutes for the DNS server to recognize the new IP address.
I can only see the first 100 items in the NAS Manager Web user interface.	The NAS Manager will only display 100 items per page.	To display the next 100 items, click the down-arrow icon at the top of the list.
In the NAS Manager, if I click OK and then click Cancel , it doesn't seem to	Cancel does not dynamically stop an update to the system after you click OK .	If an operation has been performed in error, the system administrator must change the setting back manually.

cancel the operation.		
When I select the Check All box and then deselect one or more choices on some screens in the NAS Manager, the Check All box remains selected.	The Check All box is not automatically deselected. However, this does not mean that all items in the list are selected.	This behavior does not affect functionality. The Check All box does not indicate what has specifically been selected or deselected.
I have changed the password for the administrator account; however, several minutes have passed and I have not been queried for the new password.	The NAS Manager does not automatically refresh the account information for the administrator while in the NAS Manager. Instead, it performs the refresh as a timed function.	The password was successfully changed. If you want to confirm that the new password is in effect, close the browser, and then reconnect. The new password should work, but the old one should not.
I am looking for a topic on the context-sensitive online help in the NAS Manager, but it says No Topic Available.	Some sections of the NAS Manager do not have context-sensitive help.	For information on a specific function, see the Windows Powered Help, which is available through Terminal Services by clicking Windows Powered Help on the Advanced Administration Menu, or see the appropriate section in this <i>Administrator's Guide</i> .
I tried to clear the FTP log or the Web (HTTP) Shares log in the Maintenance section of the NAS Manager, but I received an error message and the log was not cleared.	The logs are currently locked by the NAS system for the FTP service and to support the NAS Manager. The logs cannot be cleared in the NAS Manager.	Connect to the NAS system using Terminal Services and clear these logs by using MMC. You can access MMC by clicking Computer Management on the Advanced Administration Menu, which is available through Terminal Services.
While viewing the properties of a user, I selected the General tab. The fields for this user are now all blank.	You were already on the General tab and the page did not refresh properly.	Select Cancel or click Back on your browser. Then reselect the user for whom you wanted to view properties.
I added members to a local group using the NAS Manager, but when I click OK , the screen only refreshes.	You might have removed and then added the same member to the local group. This may cause the screen to refresh instead of update correctly.	Reselect the Local Groups tab in the NAS Manager primary menu. Then add or remove the appropriate members to or from the local group.
I cannot change the WINS addresses when I click Network on the NAS Manager primary menu, click Network Interfaces , and then click WINS in the Tasks list.	The NAS Manager grays out the WINS Servers Configuration page unless you set the IP Address Configuration page to Use the following IP settings .	To set the WINS addresses from the NAS Manager, click Network on the primary menu, click Interfaces , and click IP in the Tasks list. On the IP Address Configuration page, click the radio button for Use the following IP settings , and then type the IP address, Subnet mask, and the default gateway in the appropriate text boxes.

Table 9-3. Dell ActiveArchive™

Issue	Possible cause	Resolution
I cannot access my Dell ActiveArchive persistent images from a UNIX® Network File System (NFS) or Macintosh client.	Only Microsoft Windows (CIFS) clients can access the persistent images stored in the ActiveArchive folders for each volume.	Access the ActiveArchive folders through the Windows client to perform data recovery.
The XCOPY command does not copy my persistent images.	XCOPY cannot read the persistent images on a volume.	Do not use XCOPY to copy persistent images. Copy the files manually in Windows Explorer.
After I take a new persistent image, the definition of the persistent image is blank, or	The NAS Manager must complete a refresh cycle before it can correctly show the persistent image.	If this is the first persistent image, wait several minutes and check again.

the persistent image does not show at all in the persistent images list.		If this is a subsequent persistent image, wait for the NAS Manager to complete a refresh or press <F5>.
When I click Restore Defaults on the Global Settings page in Dell ActiveArchive after taking a persistent image, it changes my cache file size and the area is grayed out.	After you take a persistent image, you cannot change the cache file size; therefore, clicking Restore Defaults does not change the cache file size. To verify the cache file size, look at the cache file size on the Volume Settings page. You should see that it has reverted back to the original cache file size that you set before taking a persistent image.	Take no action. Dell ActiveArchive is functioning as designed.
I get a permission error when I try to access my persistent images from an HTTP or FTP share.	Accessing the persistent image directory through HTTP or FTP is not supported.	If you need to access your persistent image directory, connect to the system through a Terminal Services Advanced Client session and use Windows Explorer in the NAS system to access them.
When the maximum number of persistent images (250 by default) has been reached and I continue to take more of them, lower-priority persistent images are overwriting the existing higher-priority persistent images.	If a persistent image is taken manually or by schedule, ActiveArchive takes the persistent image even if the maximum number of persistent images has been reached. Therefore, the new persistent image must overwrite an existing persistent image. By design, the new persistent image writes over the oldest, lowest-priority persistent image available, even if it is a higher-priority persistent image than the one currently being taken.	Take no action. ActiveArchive is functioning as designed.
I noticed that the date and time for the ActiveArchive directory changes every time I reboot my NAS system.	The ActiveArchive directory date and time are reset at each reboot. The new dates and times do not change the dates and times of your persistent images.	Take no action. This is the normal functionality of ActiveArchive.
I have deleted a persistent image, but when the Persistent Images page redisplay I can still see the persistent image. If I try to delete it again, I get a blank page.	In some environments, the Persistent Images page in the NAS Manager refreshes too quickly.	Wait a few seconds and refresh the page. You should see that the persistent image you deleted is no longer listed.
When I try to take a persistent image, a critical error message states that the snapshot could not be taken.	ActiveArchive may still be deleting or restoring a volume or taking another snapshot.	Wait a few minutes for the previous process to complete and then try again.
In the event log or on the Status page, a message states: An exception has occurred. The data contains the exception record.	This is a known issue.	Ignore this message. The NAS system is functioning normally.
After restoring a volume from a persistent image, I cannot mount to a share on that volume from a Linux client.	During the restore, the volume is dismounted.	From the NAS Manager, restart NFS, and then remount to a share on the volume.
The % symbol does not show in the ActiveArchive event logs.	ActiveArchive event log messages that tell you how full the cache file is and how close the system is to the maximum allowed snapshots are generated messages. These messages do not include the % symbol.	Take no action. The NAS system is functioning as designed.

Table 9-4. Dell OpenManage Array Manager

Issue	Possible cause	Resolution
-------	----------------	------------

After repairing a volume in the NAS Manager, one or more disks show as "missing" in Array Manager.	The repair does not actually delete the disks, although the disks are displayed as missing.	Take no action. Your NAS system is still operating correctly.
--	---	---

Table 9-5. UNIX and Red Hat Linux

Issue	Possible cause	Resolution
I cannot access the Terminal Services Advanced Client through the NAS Manager from my Linux client system using the Netscape browser.	The Terminal Services Advanced Client is not supported by the Linux operating system and does not work with the NAS Manager.	Use a Windows client system to manage the NAS system through a Terminal Services Advanced Client session.
While updating client access to an NFS share, the No Access option is displayed, but the Root option is not.	Only the All Machines category options are displayed during this update.	Add the appropriate clients, and then select OK . After you have added the client, navigate back to the NFS tab for this share and select the correct options for the individual Client Machines .
Every time I try to obtain a directory listing from an NFS client on the root of a system volume, I get an error message, such as <i>Permission Denied</i> .	The problem you are experiencing involves a System Volume Information directory created by Microsoft Index Server. The NFS service does not have access to this directory and returns an error message to the client when trying to list its properties. This issue only occurs when sharing the root of a drive letter.	Ignore this error. The System Volume Information directory is not used by NFS clients or your system by default.
Sometimes I am unable to delete folders that have been used and that are shared to an NFS client.	This is a situation that occurs with NFS discretionary access lists (DACLS) and inheritance. When the folder to be shared is created, the only access control entry (ACE) created by default is Everyone with Full Control . When an NFS client creates a directory or a file in this directory (mounted share), Services for UNIX (SFU) creates a new DACL that replaces the inherited Everyone with Full Control ACE. This DACL contains an Everyone ACE with the appropriate UNIX file creation access and may contain two other ACEs for the mapped user and group. If this happens, the administrator of the Windows client cannot delete the file or directory unless that administrator takes ownership through the Windows system and changes the access.	As the administrator, use a Windows client system to take ownership and change the access to allow yourself to delete the share folders. When you delete the NFS share folders, ensure that there are no open file handles for the share. If you are unsure, delete the share, and then restart NFS.
When updating client access to an NFS share, the All Machines	The NAS Manager might reset the All Machines client group to Read-Write when there are no clients that have read-only or read-write access.	Add a client that has read-write or read-only access, and then set the All Machines client

client group is reset from the No Access access type to Read-Write access.		group to No Access .
My NAS system is experiencing low NFS performance.	NFS write-back cache is disabled.	If your system is not part of a cluster, you can enable NFS write-back cache to improve performance. See "Advanced Features" for more information.
The BIG5, EUC-KR, EUC-TW, GB2312-80, KSC5601, and Shift-JIS character encoding schemes for NFS shares cannot be specified in the NAS Manager.	The NAS Manager user interface supports only EUC-JP and ANSI character encoding for NFS shares.	Access the NAS system's desktop and modify the NFS share properties of the folder directly.
The NFS client group All Machines is reset to No Access when another client group is set with the same access permissions and root.	Setting a client group to use the same permissions as All Machines causes All Machines to be reset to No Access .	Access the NAS system's desktop and modify the NFS share properties of the folder directly.
I am getting inconsistent map definitions when I use the NAS Manager and the SFU MMC to create user name maps.	Modifications to user name maps are cached and may not take effect immediately.	Use only one tool to administer user name maps.

Table 9-6. Macintosh and AppleTalk

Issue	Possible cause	Resolution
I am getting event errors for Services for Macintosh.	Services for Macintosh are bound to the onboard network interface controller (NIC) by default. If this NIC has been disabled, binding errors occur.	Bind the AppleTalk protocol to an enabled NIC. See "AppleTalk Protocol Adapter Binding" in "Advanced Features."
From a Macintosh client, users cannot modify or delete a file that a Windows client has accessed.	The time between clients and the system is not properly synchronized.	Make sure that clients have their time synchronized to within 10 minutes of the time zone.
I have rebooted my NAS system from	The most likely cause is that the NAS system has	Close Internet Explorer, and

a Macintosh client. Several minutes have passed and my NAS system has not rebooted or the page has not refreshed.	come back online, but the client screen has not refreshed because the NAS Manager does not automatically refresh the screen when the NAS system has finished rebooting.	then reconnect to the NAS Manager. The NAS system should behave normally.
From a Macintosh client, I cannot connect to the administration part of the NAS Manager by using the Administer This Appliance link on the HTTP Shares page.	The internally generated certificate is not supported by Internet Explorer for Macintosh.	You can administer the NAS system by using the address <code>http://servername:1278;</code> however, this is a nonsecure link.
After modifying properties of the AppleTalk protocol, File Services for Macintosh does not restart.	File Services for Macintosh can not establish communication to the local RPC service.	Restart the workstation service. See " Restarting Workstation Services " in "Advanced Features."

Table 9-7. Netscape Navigator

Issue	Possible cause	Resolution
I cannot use the Back button in Netscape Navigator for the online help in the NAS Manager.	This feature is not supported.	Use the Previous Topic link to navigate back to earlier topics.
I get a password prompt when navigating through Local Groups in the NAS Manager using Netscape Navigator on Linux.	The password prompt is generated by Netscape and does not require re-authentication. The administrator is being asked whether the password that was used to access this screen should be saved.	Select Do not Prompt Me Again , and this message will not display in the future.
I am using Netscape Navigator to administer my NAS system through the NAS manager. A long gray bar at the bottom of the screen is covering the OK and Cancel buttons.	The page has not finished loading.	Use one of the following resolutions: <ul style="list-style-type: none"> • Wait for the page to finish loading. • Refresh the page several times.

[Back to Contents Page](#)