Dell™ PowerVault™ 750N and 755N NAS Appliances

SYSTEM ADMINISTRATOR'S GUIDE

DELL™

Contents

3   Advanced Disk and Volume Management Using Array Manager

4   System Management

5   System Recovery, Backup, and Restore

6   Dell ActiveArchive™

7 Advanced Features

8 Online Server Diagnostics

9 Troubleshooting

Tables

Preface

This guide provides system administrators, IT professionals, and those responsible for the installation of network attached storage (NAS) devices, with the information necessary to install, configure, and operate the Dell™ PowerVault™ 750N and 755N NAS appliances. Chapters include the following information:

- Chapter 1 — "Introduction" provides an overview of the system features, as well as the information necessary to perform the initial configuration of the system.

- Chapter 2 — "NAS Manager" provides a high-level introduction to the NAS Manager and how to find help.

- Chapter 3 — "Advanced Disk and Volume Management Using Array Manager" provides a comprehensive solution to storage management in an integrated graphical view.

- Chapter 4 — "System Management" provides directions for installing and configuring a Dell OpenManage™ Remote Assistant Card (DRAC) and information about Dell OpenManage Server Assistant.

- Chapter 5 — "System Recovery, Backup, and Restore" provides information on recovering from system failure, and how to back up and restore the system state.

- Chapter 6 — "Dell ActiveArchive™" provides information on the creation and preservation of persistent images of the PowerVault NAS appliance system data volumes using Dell ActiveArchive.

- Chapter 7 — "Advanced Features" provides information on network adapter teaming, network services for UNIX®, Macintosh, and Novell® NetWare®, language support, and other advanced features.

- Chapter 8 — "Online Server Diagnostics" describes how to install and run the Online Server Diagnostics on your NAS appliance.

- Chapter 9 — "Troubleshooting" lists potential issues with probable causes and possible solutions.

Warranty and Return Policy Information

Dell Computer Corporation ("Dell") manufactures its hardware products from parts and components that are new or equivalent to new in accordance with industry-standard practices. For information about the Dell warranty for your system, see your *System Information* document.

Safety, Regulatory, and Warranty Information

For safety, regulatory, and warranty information for your system, see the *System Information* document included with your system.

Other Documents You May Need

In addition to this *System Administrator's Guide*, the following documentation is included with your system:

- The NAS appliance *User's Guide*, which describes system features, technical specifications, and device drivers.

- The NAS appliance *Installation and Troubleshooting Guide* provides instructions for installing system hardware and includes troubleshooting and diagnostic procedures for testing your system.

- Supporting system documentation on the NAS appliance *Resource* CD, that includes information about all the option cards and software installed.

- The NAS appliance *Localization* CD that contains the Microsoft® Windows® Multilanguage User Interface (MUI) and language locales.

- Your *System Information* document, which provides basic information about your system.

- The *Dell OpenManage Array Manager User's Guide* provides instructions for using the Dell OpenManage™ Array Manager common interface for configuring and managing local and remote storage.

- The *Dell OpenManage Remote Assistant Card (DRAC) User's Guide* provides instructions for using the DRAC to manage and use a server through a modem or network connection, even when the server itself is down.

- The *Dell OpenManage Server Agent Messages Reference Guide* describes the event messages logged by the Dell OpenManage Server Agent 4.0 or later.

You may also have one or more of the following documents:

- Documentation that is included with options you purchase separately from the system. This documentation includes information that you need to configure and install these options in your system.

- Technical information files—sometimes called "readme" files—that might be installed on the hard-disk drive to provide last-minute updates about technical changes to the system or advanced technical reference material intended for experienced users or technicians.

- Documentation updates that are sometimes included with the system to describe changes to the system or software. Always read these updates before consulting any other documentation. These updates often contain information that supersedes the information in the other documents.

Notational Conventions

The following subsections describe notational conventions used in this document.

Notes, Notices, Cautions, and Warnings

 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 potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

 WARNING: A WARNING indicates a potentially hazardous situation which, if not avoided, may result in severe injury.

Some warnings may appear in alternate formats and may be unaccompanied by an icon. In such cases, the specific presentation of the warning is mandated by regulatory authority.

Typographical Conventions

The following list defines (where appropriate) and illustrates typographical conventions used as visual cues for specific elements of text throughout this document:

- *Keycaps*, the labeling that appears on the keys on a keyboard, are enclosed in angle brackets.

  Example: <Enter>

- *Key combinations* are series of keys to be pressed simultaneously (unless otherwise indicated) to perform a single function.

- Example: <Ctrl><Alt><Enter>

- *Commands* presented in lowercase bold are for reference purposes only and are not intended to be typed when referenced.

  Example: "Use the **format** command to..."

  In contrast, commands presented in the Courier New font are part of an instruction and intended to be typed.

  Example: "Type format a: to format the diskette in drive A."

- *Filenames* and *directory names* are presented in lowercase bold.

  Examples: **autoexec.bat** and **c:\windows**

- *Syntax lines* consist of a command and all its possible parameters. Commands are displayed in lowercase bold; variable parameters (those for which you substitute a value) are displayed in lowercase italics; constant parameters are displayed in lowercase bold. The brackets indicate items that are optional.

  Example: **del** [*drive:*] [*path*] *filename* [**/p**]

- *Command lines* consist of a command and may include one or more of the command's possible parameters. Command lines are presented in the Courier New font.

  Example: del c:\myfile.doc

- *Screen text* is text that appears on the screen of your monitor or display. It can be a system message, for example, or it can be text that you are instructed to type as part of a command (referred to as a *command line*). Screen text is presented in the Courier New font.

  Example: The following message appears on your screen:

  No boot device available

  Example: "Type md c:\programs and press <Enter>."

- *Variables* are placeholders for which you substitute a value. They are presented in italics.

  Example: DIMM*x* (where *x* represents the DIMM socket designation).

SECTION 1

Introduction

This chapter provides an overview of the Dell™ PowerVault™ 750N and 755N network attached storage (NAS) appliances features, as well as the information necessary to perform the initial configuration of the system.

These systems are "headless" systems that are managed through the onboard Ethernet connection; they operate without a keyboard, monitor, or mouse. While it is possible to connect these peripherals to a system, it is generally not necessary unless you are troubleshooting the system. These systems are managed and monitored via a Web-based user interface, the NAS Manager. You can also manage these systems remotely from a client computer attached to the network.

The Boot Process

The internal drives in your NAS appliance are logical small computer system interface (SCSI) drives that are controlled by a hardware redundant array of independent disks (RAID) controller. The Microsoft® Windows® Powered operating system and boot sectors are installed on two RAID 1 (mirrored) hard-disk drives.

The PowerVault 755N NAS appliance, which is a rack mounted system, uses a split bus and has five drives. One drive is in the drive media bay and four drives are in the standard bay. The operating system is installed on two mirrored RAID 1 drives. Data is stored on the remaining three drives that are configured as RAID 5 drives.

The PowerVault 750N NAS appliance, which can be a tower or rack mounted system, uses a split bus and has eight drives. Two drives are in the drive media bay and six drives are in the drive internal bay. The operating system is installed on the two drives in the media bay, which are configured as mirrored RAID 1 drives. Data is stored on the remaining six drives that are configured as RAID 5 drives.

The boot sequence is as follows:

- CD-ROM drive
- Diskette drive
- Operating system hard-disk drive

System Configuration

You can perform most configuration tasks through the NAS Manager, which is a web browser interface to the NAS appliance. The NAS Manager menus consist of common management tasks grouped under tabs on a menu bar. Each tab on the main menu bar has an associated secondary menu bar associated with it. The secondary menu bar lists the tasks you can perform from that page. The NAS Manager allows you to perform routine administrative tasks such as shutdown, restart, new share creation, and set user configuration. The NAS Manager home page displays a status indicator and provides a link to the **Messages** page, which contains details about logged events.

You can access the **Terminal Services Advanced Client** from the NAS Manager to perform tasks not available directly through the NAS Manager. See "Advanced Features" for more information.

Administrator User Name and Password

To log on to the NAS Manager, you must enter the administrator user name and password. The default administrator user name is `administrator` and the default password is `powervault`. To change the user name and password, click **Set Administrator Password** in the **Welcome** window.

Basic Configuration

This section includes information to enable you get your system up and running. You will set the basic configuration from another system that has a keyboard, monitor, and mouse. After you set the basic configuration, you can use the NAS Manager to set passwords, local users, shares, and so on.

> **NOTICE:** If you do not use Kick-Start to configure your system, you must disable Kick-Start immediately. If Kick-Start is enabled, the system logs in automatically as administrator, which creates a security risk. Kick-Start also takes up system resources by constantly checking for configuration information. For additional information, see "Disabling the Kick-Start Utility."

There are several ways to configure your system, depending on whether or not you are using Dynamic Host Configuration Protocol (DHCP):

- If DHCP is installed on your network, your system automatically configures the network settings.

- If DHCP is not installed on your network, you can configure your system using a serial connection or the Dell OpenManage™ Kick-Start utility.

Configuring Your System With DHCP

⊃ **NOTICE:** If you do not use Kick-Start to configure your system, you must disable Kick-Start immediately. If Kick-Start is enabled, the system logs in automatically as administrator, which creates a security risk. Kick-Start also takes up system resources by constantly checking for configuration information. For additional information, see "Disabling the Kick-Start Utility."

When the system is powered on for the first time, it invokes the DHCP client to get parameters (the Internet protocol (IP) address, gateway subnet mask, and domain naming system (DNS) server address) from a DHCP system. The default system name ("Dell*xxxxxx*", where *xxxxxx* is the system's service tag number) is entered as the DNS server name. Connect to the system using Microsoft Internet Explorer 5.0 or later (or for Red Hat Linux only, use Netscape Navigator 6.0 or later) by entering the system name in the Web browser.

✏ **NOTE:** Microsoft Internet Explorer 4.0 may be used only with Windows NT® 4.0 with Service Pack 4 or later. All other browsers are not supported.

If DHCP fails, you need to set the IP address, gateway subnet mask, and DNS server using either a serial connection or the Kick-Start utility.

You can configure the system using the NAS Manager. The NAS Manager is served on port 1279 and is accessed by the URL,https://< *systemname | system_ipaddress*>:1279, where *systemname* is the DELL< *service_tag*>. Port 1279 uses secured socket layers (SSL) to encrypt data going to and coming from the NAS appliance to provide some 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.

In a system without a DNS server, you can use Internet Explorer (or for Linux only, use Netscape 6.0 or later) to search for the default hostname of the system ("Dell*xxxxxx*", where *xxxxxx* is the system's service tag number).

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

Configuring Your System Using a Serial Connection

⊃ **NOTICE:** If you do not use Kick-Start to configure your system, you must disable Kick-Start immediately. If Kick-Start is enabled, the system logs in automatically as administrator, which creates a security risk. Kick-Start also takes up system resources by constantly checking for configuration information. For additional information, see "Disabling the Kick-Start Utility."

✏ **NOTE:** You must be logged in as Administrator to perform these steps.

On a system running Windows 2000, perform the following steps to connect to the NAS Manager through the Administration port:

1   Connect the serial cable included with your system from the system you are using for configuration to the administration port (serial port 1) on your system.

2   Click the **Start** button, point to **Settings**, and then click **Control Panel**.

3   In the **Control Panel**, click **Phone and Modem Options**.

4   On the **Modems** tab, click **Add** for the **Add/Remove Hardware Wizard**.

5   Click the **Don't detect my modem; I will select it from a list** checkbox and then click **Next**.

6   In the drop-down menu for **Manufacturers**, click **(Standard Modem Types)**.

7   In the drop-down menu for **Models**, click **Communications cable between two computers**, and then click **Next**.

8   Click the **Selected ports** radio button, select the appropriate communication port from the list, and then click **Next**.

9   Click **Finish** to close the **Add/Remove Hardware Wizard**, and then click **OK** to close the **Phone and Modem Options** dialog box.

10 On the desktop, right-click **My Network Places** and click **Properties**.

11 In the **Properties** window, double-click **Make New Connection**.

    The **Network Connection Wizard** displays.

12 Click **Next**.

13 Select the radio button for **Connect Directly To Another Computer** and click **Next**.

14 Select the radio button for **Guest** and click **Next**.

15 In the drop-down menu, click the COM port that you are using and then click **Next**.

16 Click **Only for myself** and then click **Next**.

17 Enter the name of the connection and then click **Finish**.

    After you configure your direct serial connection, the **Connect Direct Connection** window displays.

18 Click **Properties**.

19 Click the **General** tab.

20 Under **Select a Device**, click **Communication cable between two computers**.

21 Click **Configure**.

This selection opens the **Modem Configuration** window.

22 In the **Maximum Speed (bps)** drop-down menu, click **115200**.

23 Click **OK** to close the **Modem Configuration** window.

24 Click **OK** to close the **Direct Connection** window.

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

25 Enter the user name and password for your system.

26 Click **Connect**.

This action connects the system you are using for configuration.

27 Start the Web browser on the system you are using to configure the NAS appliance.

28 Type in the name of the PowerVault 750N or 755N system.

The **PowerVault NAS Manager** displays.

Configuring Your System Using the Kick-Start Utility

The Kick-Start utility is software shipped with your system. This utility is used to define the initial network configuration of a system, which makes the system available on the network for complete configuration using the NAS Manager. This utility is intended for customers who have one or more systems to configure but do not want to use the default DHCP assigned address and system name.

A NAS appliance requires configuration information before it can function on the web. You can specify this information locally using the Kick-Start utility installed on the NAS appliance.

You can also supply configuration information using the Remote Kick-Start utility (a browser-based Java applet) to save the configuration information on a diskette or send it to one or more systems across an IP network from another system on the same IP subnet.

 NOTE: The system you use to create configuration files must be running Windows 2000 and have one of the following browsers installed: Microsoft Internet Explorer 5.0 or higher or Netscape 6.0 or higher. If you use a Netscape browser, you must install the Java plug-in, which is available at **http://java.sun.com/**.

 NOTE: The Remote Kick-Start utility provides an integrated DHCP service that can supply a temporary IP address to discovered NAS appliances that you add to your network before configuring them. If your network already provides DHCP services, the Remote Kick-Start utility detects this and does not turn on the integrated DHCP service.

Table 1-1.   Kick-Start Configuration Overview

Step 1	Step 2 Record the following information:	
Use this guide and the *Resource CD* included with your system.	NIC 0: IP Address	_ _ _ · _ _ _ · _ _ _ · _ _ _
	NIC 0: Subnet Mask	_ _ _ · _ _ _ · _ _ _ · _ _ _
	NIC 0: Gateway	_ _ _ · _ _ _ · _ _ _ · _ _ _
	NIC 1: IP Address	_ _ _ · _ _ _ · _ _ _ · _ _ _
	NIC 1: Subnet Mask	_ _ _ · _ _ _ · _ _ _ · _ _ _
	NIC 1: Gateway	_ _ _ · _ _ _ · _ _ _ · _ _ _
	Host Name	_____
	DNS Server	_____
	Administrator/Root Password	_____
	Additional User/Password (if any)	_____

Step 3 Perform one of the following methods of configuration:		
Appliance does not have a monitor and keyboard attached but is connected to an IP network	Appliance does not have a monitor and keyboard attached and is not connected to an IP network	Appliance has a monitor and keyboard attached
Remote IP Network	**Remote Diskette**	**Local**
a Go to a workstation on your network, insert the *Resource* CD, and run Remote Kick-Start.	a Go to a workstation on your network, insert a diskette, and then insert the *Resource* CD. Run Remote Kick-Start to copy configuration settings to the diskette.	a Turn on the NAS appliance. The Kick-Start utility appears.
b Enter information collected in step 2 and save the configuration.	b Enter information collected in step 2 and save the configuration to the diskette.	b Follow the screen instructions and enter data you collected in step 2. When you finish, the system restarts.
c Select a NAS appliance, select the configuration, and click **Apply**.	c Insert the diskette into the NAS appliance diskette drive.	c Start the NAS Manager in a browser from a remote workstation using this address: https**://***myappliance***:1279**, where *myappliance* is your system name.
d Start the NAS Manager in a browser from a remote workstation using this address: https://*myappliance*:1279, where *myappliance* is your system name.	d Start the NAS Manager in a browser from a remote workstation using this address: https**://***myappliance***:1279**, where *myappliance* is your system name.	

Configuration Methods

You can specify configuration information using the following methods:

- **Method 1: Remote Configuration** — Use the Remote Kick-Start utility located on the *Resource* CD to enter configuration information. This method does not require you to attach a mouse, keyboard, or monitor to the NAS appliance (a system without input devices is sometimes called a *headless system*). You can remotely configure a NAS appliance in one of the following ways:

  – Preparing the configuration information for one or more NAS appliances on a diskette that you create on another system. You can save one configuration or an ordered set of configuration files on a diskette.

  – Sending the configuration information to the NAS appliance over an IP network. The system you use must be on the same IP subnet as the NAS appliance.

- **Method 2: Local Server Configuration** — Use the Kick-Start utility provided on the NAS appliance to specify configuration information directly on the system, which requires you to attach a monitor, keyboard, and mouse to the NAS appliance. This native version of the Kick-Start utility starts when you turn on the system.

Method 1: Configuring NAS Appliances Remotely

This method allows you to remotely configure one or more NAS appliance, providing the information to the NAS appliance either on a Kick-Start diskette or sent from another system on the same network IP subnet.

This method is probably the easiest if you are configuring multiple systems. For more information about the multiple configuration feature, see "Notes on NAS Appliance Multiple Configuration Files."

Starting the Remote Kick-Start Utility

The first step in configuring one or more NAS appliances remotely is to start the Remote Kick-Start utility on another system. On a system running Microsoft Internet Explorer 5.0 or higher or Netscape 6.0 or higher, perform the following steps:

1 Insert the *Resource* CD into the CD drive.

  The *Resource* CD main menu should appear automatically. If it does not, double-click **My Computer** on the desktop, right-click the CD drive, and click **Autoplay**.

2 On the main menu, click **Dell OpenManage Kick-Start** or click the **Kick-Start** tab.

3   Click **Dell OpenManage Kick-Start 2.1**.

A confirmation message that asks whether you want to grant permission for a Java applet from Dell to access your system.

4   Click **Yes** or **Grant**, depending on your browser, to grant permission so you can complete the remaining configuration tasks.

The **Kick-Start** window appears where you can create, view, and save configurations by name. You can then apply them to selected NAS appliances that have been discovered on the network or save the configurations on a diskette or on your local hard-disk drive. The following procedures explain how to perform these tasks.

Creating Configurations

After you start the Kick-Start utility, you are ready to prepare the configuration information that you will apply to one or more NAS appliances. This process works the same way, whether you apply this data using a diskette or using an IP network.

You can save configurations by name and assign them an order within a named set, such as **config001**, **config002**, and so on. Also, you can view or edit configurations.

To prepare configuration information, perform the following steps:

1   Double-click **Defined Configurations**.

2   Click **PowerVault NAS Appliance**.

3   Click **New** in the **Remote Kick-Start** window. The **Configurations List** changes to display the **Configuration Form**.

4   Select or type the following configuration information:

- **Configuration Name** — Each configuration file you create must have a name. Using the + (plus) and – (minus) buttons beside the name, you can change the three-digit number that is appended to this name. This number lets you create an *ordered set* of configuration files on a diskette. An ordered set of configuration files on the diskette can be used to apply configurations in sequence to a group of NAS appliances.

- **Time Zone** — You can change the time zone by selecting an entry from this list. This is a required field.

- **Language** — You can change the default system language and locale by selecting a language in the drop-down list. This is a required field.

   NOTE: This change does not install the Multilanguage User Interface (MUI). To install the MUI or other languages than those that are listed in the Kick-Start menu, use the *Localization* CD.

✍ NOTE: The Kick-Start utility Ethernet 0 matches Windows Local Area Connection, and Ethernet 1 matches Local Area Connection 2.

- **Ethernet Port 0** — This port is the built-in Ethernet port on your system closest to the outside edge of the system. You can optionally enter the IP address information for this port. Enter the IP address, subnet mask, and the default gateway IP address. Kick-Start ensures that you have entered all portions of an IP address and checks for a valid IP subnet mask. (Optional field — If you do not complete this field, the system will use DHCP to try to obtain an IP address.)

- **Ethernet Port 1** — This port is the built-in Ethernet port on your system farthest from the outside edge of the system. You can optionally enter the IP address information for this port. Enter the IP address and subnet mask. The gateway IP address is optional. Kick-Start ensures that you have entered all portions of an IP address and checks for a valid IP subnet mask. (Optional field — If you do not fill in this field, the system will use DHCP to try to obtain an IP address.)

- **DNS IP Addresses** — You can optionally enter one or two DNS IP addresses. Kick-Start ensures that you have entered all portions of an IP address.

- **Host/Machine Name and Domain** — The host/machine name is required. It is composed of a base host name and a DNS Domain name. Domain indicates a DNS domain (for example, dell.com) and does not indicate a Windows domain. The domain name is optional.

- **Administrator Password** — This field is required. You must enter the administrator password twice, and it must be at least six characters long. For security purposes, the password does not appear on the screen, but each character of the password shows an asterisk (*) placeholder.

- **User Name and Password** — You can optionally enter a user login name and password (enter the password twice). For security purposes, the password will not be seen on the screen, but each character of the password will display as an asterisk (*). Passwords of less than six characters will not be accepted.

5 Click **Save** when you finish.

6 Repeat this process to create and save another configuration if you want to configure more than one NAS appliance. Click the + or – buttons to increment or decrement the series number at the right of the configuration name to create an ordered set that use the *same name*.

You are ready to apply the configuration to the NAS appliance either using an IP network connection or by saving the configurations on a diskette.

Configuring NAS Appliances Over an IP Network

If you are configuring multiple NAS appliances on the same IP subnet as the system you use to run Remote Kick-Start, this is probably the fastest configuration method. After starting the Remote Kick-Start utility and creating configurations, perform the following steps:

1   Select the NAS appliance you want to configure from the **Discovered Dell Systems List**. If it does not appear, scroll down and click the Integrated **DHCP Server** check box and wait a few seconds for the system to be assigned a temporary IP address and discovered by Remote Kick-Start.

    NOTE: You must configure the DHCP scope before using the embedded DHCP server. See "Using the Integrated DHCP Server" in the Kick-Start online help for more information about configuring the DHCP scope.

2   Select an existing configuration file from the list.

3   Click a NAS appliance in the **Discovered Dell Systems List**, and click **Apply**. If the configuration was successful, the status of the NAS appliance in the **Remote Kick-Start** window changes to **Configured** (a check mark icon).

    NOTE: If more than one Remote Kick-Start utility runs on your network, you can reserve the right to configure a system by locking it first. To do this, select the system in the **Discovered List** and click **Lock**.

Configuring NAS Appliances Using a Kick-Start Diskette

If the NAS appliance is not on an IP network, you might prefer to create the configuration on a diskette. If you want to configure several NAS appliances with a single diskette, create an ordered set of configuration files on the diskette, then you can use that diskette locally at each system to configure it.

After starting the Remote Kick-Start utility and creating configurations, perform the following steps on the system where you have been running Remote Kick-Start:

1   Insert your Kick-Start diskette into the diskette drive of the system where you created your configurations.

2   Select the configurations you created and saved in the **Configurations List** and click **Write Diskette**.

Applying Configuration Information Using a Kick-Start Diskette

After you have created configuration files on a Kick-Start diskette, you can use the diskette to set up one or more NAS appliances. The Kick-Start utility uses an automatic reading and loading sequence that is especially useful for setting up headless NAS appliances.

When you insert the configuration diskette into a NAS appliance diskette drive, Kick-Start looks for configuration files on the Kick-Start diskette. If a configuration file is found, a 20-second countdown timer begins. If the keyboard or mouse are inactive during the 20-second interval, Kick-Start applies the configuration settings found in that file.

Kick-Start looks for the configuration files on the diskette. If found, it selects and applies a configuration to the NAS appliance, AND then marks the file as having been *applied*. Configuration files for NAS appliances have a **.nas** file extension. For more information about the multiple configuration feature, see "Notes on NAS Appliance Multiple Configuration Files."

The Kick-Start utility skips files marked **Applied** the next time you use the diskette to configure a system and advances to the next nonapplied file in the list.

To set up one or more NAS appliances, perform the following steps:

1   Turn on your NAS appliance.

2   Insert the configured Kick-Start diskette into the diskette drive of the first NAS appliance you want to set up.

   For the first 30 seconds, the diskette drive light turns on and indicates that the diskette drive is active while Kick-Start reads and loads a configuration file for the NAS appliance. When the drive light turns off for more than 30 seconds, Kick-Start has finished applying the configuration.

   The NAS appliance automatically reboots.

3   If you customized the Kick-Start diskette to contain multiple configurations, go to the next NAS appliance and repeat steps 1 and 2.

Method 2: Configuring a NAS Appliance Locally

This section describes how to enter configuration information locally on a NAS appliance. You do not need a Kick-Start diskette for this method.

Ⓩ NOTE: Configuring the NAS appliance locally requires a keyboard and monitor. A mouse is optional, but it can be used in this procedure for simplicity.

Connect a monitor, keyboard, and mouse to your NAS appliance, and then perform the following steps:

1   Start your NAS appliance.

   The **Kick-Start** window appears, prompting you to either insert a configuration diskette or click **Enter Configuration Information** to directly configure the server. On the left side of the screen you may select from the available languages.

2 Click **Enter Configuration Information**.

3 Select the items you want to configure and click **Next**.

   Your choices are:

   • Ethernet port 0

   • Ethernet port 1

   ✎ NOTE: The Kick-Start utility Ethernet 0 matches Windows Local Area Connection, and Ethernet 1 matches Local Area Connection 2.

   • Domain name server (DNS)

   • Host/system name and domain (domain is a DNS Domain, not a Windows domain. For example, www.dell.com.)

   • Administrator password

   • User name and password

   ✎ NOTE: The user you set up in this step does not have administrator privileges.

4 Type your configuration information into the provided text boxes and click **Next**.

5 Click **Yes** when prompted to apply your configuration settings to this system.

   After a 10–15 second delay, your NAS appliance reboots when the configuration process is complete. At the prompt, you can log in as administrator with the password you specified in step 3.

Notes on NAS Appliance Multiple Configuration Files

Using Remote Kick-Start, you can create multiple configuration files on the Kick-Start diskette. At the top of each configuration form, a **Configuration Name** field appears. You can use this field to enter information that helps you identify a particular machine, such as, rack1-slot2, netserver-1, and so on.

Using the + (plus) and – (minus) buttons next to this field, you can change the three-digit number that Remote Kick-Start appends to the configuration name. The name of the configuration file is formed by appending this three-digit number at the end of the configuration name. Files with the same name but a different three-digit number are called an ordered set.

The configuration process uses the three-digit number at the end of the filename to determine which configuration to apply next. Because names of the configuration files are important to the configuration process, you *must not alter the configuration filenames* after they are written to the diskette.

Do not save more than one ordered set of configuration files on a single diskette, which creates more than one file with the same three-digit number. Kick-Start uses these three-digit numbers exclusively to decide which configuration to apply next. Thus, putting multiple configuration sets on a single diskette prevents you from knowing which configuration you are applying.

For example, if the **Aaaa#001.nas** and **Bbbb#001.nas** files are both stored on the same configuration diskette, there is no guarantee that **Aaaa#001.nas** will be applied first (even though it is alphabetically first).

Disabling the Kick-Start Utility

If you do not use Kick-Start to configure your system, you must disable Kick-Start immediately. If Kick-Start is enabled, the system logs in automatically as administrator, which creates a security risk. Kick-Start also takes up system resources by constantly checking for configuration information.

To disable Kick-Start, perform the following steps:

1   From the NAS Manager primary menu, click **Maintenance**.

2   Click **Terminal Services**.

3   Log onto the system as an administrator.

4   Click the **X** on the top, right-hand corner of the Kick-Start window.

    A **Warning** window displays that asks whether you want the Dell OpenManage Kick-Start configuration tool to run automatically each time the machine starts.

5   Click **No**. If you click **Yes**, Kick-Start closes; however, it will run again the next time the system is rebooted.

2

SECTION 2

NAS Manager

The Dell™ PowerVault™ NAS Manager is a Web-based user interface that is the primary way to configure NAS appliances. This chapter describes basic navigation of the NAS Manager. See "How To Find Online Help" for more information.

✐ NOTE: To use the NAS Manager you must be logged in as Administrator. The NAS Manager default administrator user name is `administrator` and the default password is `powervault.`

Basic Navigation

The NAS Manager displays when you access a PowerVault 750N or 755N system from a Microsoft® Internet Explorer 5.0 or later (or for Red Hat Linux only, Netscape Navigator 6.0 or later) Web browser.

✐ NOTE: Microsoft Internet Explorer 4.0 may be used only in Windows NT® 4.0 with Service Pack 4 or later. All other browsers are not supported.

When navigating the NAS Manager, use the browser buttons to go backward and forward. In addition, there are two associated menu bars.

The top of each page of the interface is composed of a status area, as well as primary and secondary menu bars. The body of each page of the Web user interface (UI) is composed of the content area.

Status Area

The following information displays from left to right:

- Logo
  - Clicking the logo sends you to **http://support.dell.com**.
- System host name
- System status

  The status might be:

  - Normal (green text)
  - Informational (grey text)
  - Warning (yellow text)
  - Critical (red text)

  Clicking **Status: <status type>** sends you to the **Messages** page.

- Microsoft Windows® Powered logo

Menu Bar

The main menu bar has the following tabs:

- **Home** — Provides links to the other tabs.
- **Network** — Provides access to basic network setup tasks such as changing passwords.
- **Disks** — Allows you to configure disks and volumes, set disk quotas, and take persistent images.
- **Services** — Enables you to manage services such as network file system (NFS) and file transfer protocol (FTP).
- **Users** — Enables you to manage 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, check logs, and access the Terminal Services Advanced Client.
- **Help** — Provides access to Windows Help for network attached storage.

How To Find Online Help

There are two kinds of help available to you through NAS Manager. The NAS Manager Online Help documents NAS Manager content. The Windows 2000 Help, which you can access through the **Terminal Services** on the **Maintenance** page, documents Windows 2000 content.

To access help in the NAS Manager, select one of two methods:

- When you click **Help** on the primary menu, the NAS Manager screen is replaced by a split-screen **Help** screen that has the **Table of Contents** of help topics on the left, and the topic content on the right.
- Click the **?** icon at the far right of the primary menu to access the context-sensitive help topic related to the page you are on.

In addition to the Online Help for your system, you can also access help for Microsoft Windows 2000 through **Terminal Services**.

To start Windows 2000 Help, perform the following steps:

1 On the NAS Manager main menu, click **Maintenance**.
2 Click **Terminal Services**.
3 Log into the system.

4   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**.

Using Shares

A folder on your NAS appliance can be shared with other systems on the network, whether those systems are running a Microsoft Windows operating system or a Unix operating system.

A NAS appliance 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®.

- AppleTalk — The Appletalk protocol is used by clients running a Macintosh operating system.

- NCP (Novell® NetWare®) — The NCP protocol is used by NetWare clients.

- FTP — The File Transfer Protocol is an alternative way of accessing a file share from any operating system.

- HTTP — The Hyptertext Transfer Protocol is the protocol for accessing a file share from Web browsers.

When you create a share on the appliance, you can enable any or all of the listed protocols.

You can add and manage shares from the NAS Manager.

Managing Shares

The **Shares** page allows users to create, open, delete, or configure a variety of network folders. The **Shares** page displays a **Shared Folders** table that has the following columns:

- **Share Name** lists each shared folder by name.

  To create, open, delete, or configure the properties of a given share, click the radio button next to the name of the share you want to modify.

- **Share Path** displays the share path.

- **Type** indicates the share type:
    - W = Windows (CIFS)
    - U = UNIX (NFS)
    - F = FTP
    - H = HTTP
    - A = Apple (AppleTalk)
    - N = NetWare (NCP)
- **Comment** displays a brief description of the share, if one has been provided.
- **Tasks** lists the tasks that can be performed for each selected item.

Use this table to select a share, and then click the task you want to perform from the **Tasks** list (located to the right of the table).

Adding a Share

To create a share, you must supply a share name (the name of the directory on the NAS appliance that is to be shared) that is unique from all other shares on the system. 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.

Although a single user interface is provided for creating a share for all protocols, it actually creates a separate share for each protocol. You can remove a share for one protocol without removing the share for the other protocols; however, this process can be quite confusing. Therefore, it must be done carefully.

🔵 NOTICE: Do not create any data shares on the operating system hard-disk drive. Using the *Reinstallation* CD will destroy all data on the operating system hard-disk drive.

To add a share, perform the following steps:

1 On the NAS Manager primary menu, click **Shares**.

2 In the **Tasks** list on the **Shared Folders** page, click **New**.

3 On the **General** tab, enter the Share Name, Share Path, (and if desired) a brief description of the share in the **Comment** field.

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

4 Check the appropriate box(es) to specify which types of protocols to enable. The available options are: Microsoft Windows (CIFS), UNIX (NFS), Novell NetWare, Apple Macintosh, FTP or HTTP

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

> ✍ NOTE: 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. You must log into the NAS appliance using a Netware client before you can connect to the NetWare shares.

Modifying Share Properties

Use the **Shares** page to view and modify share properties.

To modify share properties, perform the following steps:

1   On the NAS Manager primary menu, click **Shares**.

2   On the **Shares** page, click **Shares**.

3   In the **Object/Task Selector**, select the share for which the properties will be modified.

4   On the **Shared Folders** page, in the **Tasks** list, click **Properties**.

The **General** property page is displayed. Use this page to change the name, path, and description of the share. You can also select the type of client from which the share is accessible.

Removing a Share

You can remove shares entirely, or you can disable one or more protocols. When you remove a share, access to the share is removed; however, the actual files remain on the NAS appliance.

To remove a share and all protocols for that share, perform the following steps:

1   On the NAS Manager primary menu, click **Shares**.

2   On the **Shares** page, click **Shares**.

3   In the **Shared Name** list on the **Shared Folders** page, select the share that is to be removed.

4   In the **Tasks** list on the **Shared Folders** page, click **Delete**.

A confirmation dialog appears.

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

Removing a Protocol From the Share

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

1   On the NAS Manager primary menu, click **Shares**.

2 On the **Shares** page, click **Shares**.

3 In the **Shared Name** list on the **Shared Folders** page, select the share for which you want to modify properties.

4 In the **Tasks** list on the **Shared Folders** page, click **Properties**.

The **General** property page is displayed.

5 Uncheck the protocol(s) to remove from the share.

6 Click **OK** to confirm the removal, or click **Cancel** to keep the protocol(s) for the share.

Using the PowerVault Advanced Administration Menu

The PowerVault Advanced Administration Menu is a software application that is installed on your NAS appliance. It provides links to common administrative tools for your appliance. This menu automatically runs when you access the Terminal Services Advanced Client.

The Advanced Administration Menu provides the following information:

- **Administrative Tools** — Provides a list of tools that you can use to monitor the status of and to perform administrative tasks on your NAS appliance.
- **System Management** — Provides a list of tools that you can use to manage your NAS appliance.
- **Logoff** — Ends the Terminal Services Advanced Client session
- **Exit** — Exits the PowerVault Advanced Administration Menu and returns you to the NAS Manager desktop.

To access the **Advanced Administration** menu, perform the following steps:

1 From the NAS Manager, click **Maintenance**.

2 Click **Terminal Services** and log on to the appropriate system. The **PowerVault Advanced Administration Menu** displays.

3 Click **Administrative Tools** or **System Management** to display the list of selectable options.

4 Click the desired tool or setting. (See "Retrieving Your Service Tag" for an example of a system setting you can obtain using this procedure.)

Retrieving Your Service Tag

1   On the **Advanced Administrative Menu**, click **Administrative Tools** to present the list of options.

2   Click **Retrieve Dell Service Tag** to display the service tag of the NAS appliance.

Disk Quotas

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

•   Prevent further disk space use and log an event when a user exceeds a specified disk space limit.

•   Log an event when a user exceeds a specified disk space warning level.

When 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 allowed to use.

•   The warning level specifies the point at which a user is nearing his or her quota limit.

For example, you can set a user's disk quota limit to 50 megabytes (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 the users but let the users exceed that quota limit. Enabling quotas and not limiting disk space use is useful when you want to track disk space use on a per-user basis, but do not want to deny users access to a volume when they exceed that limit. You can also specify whether or not the system should log an event when a user exceeds either their quota warning level or their quota limit.

Enabling Disk Quota Management

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

1   On the primary menu of the NAS Manager, click **Disks**.

2   Click **Disk Quota**.

3   On the **Volumes and Quotas** page, select the volume to manage.

4   On the **Tasks** list, select **Quota**.

5   On the **Default Quota for** *volume* page, click the appropriate check box to enable or disable quota management.

6   Select the desired quota size and settings for this volume.

Adding Disk Quota Entries

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

When you enable disk quotas for an existing volume, volume usage is automatically tracked for new users from that point on. However, existing volume users have no disk quotas applied to them. You can apply disk quotas to those existing volume users by adding new quota entries in the **Quota Entries** window.

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

1   On the NAS Manager primary menu, click **Disks**.

2   On the **Disks** page, select **Disk Quota**.

3   On the **Disk Quota** page, select the volume to manage.

4   From the **Tasks** list, select **Quota Entries.**

5   On the **Tasks** list, select **New…**.

6   Select a local user from the list box, or type the name of a domain account in the text box (using the < domain name\user name>).

7   To allow unlimited disk space usage, click the **Do not limit disk usage** radio button. Otherwise, go to step **8**.

8   To limit disk space, perform the following procedure:

   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 indicate kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).

   c   Enter the amount of disk space which, when filled, will trigger 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 indicate KB, MB, GB, TB, PB, or EB.

9   Click **OK**.

Modifying Quota Properties

1   On the NAS Manager primary menu, click **Disks**.

2   On the **Disks** page, select **Disk Quota**.

3   On the **Disk Quota** page, select the volume to manage.

4   From the **Tasks** list, select **Quota Entries.**

5   On the **Quota Entries** page for the selected volume, select a user account from the **Logon name** field of the **Object/Task Selector**.

6   On the **Tasks** list, click **Properties**.

7   On the **Quota entry for user** page, perform one of the following procedures:

  •   To allow unlimited disk use, click the **Do not limit disk usage** radio button.

  •   To limit disk space, perform the following procedure:

  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 indicate KB, MB, GB, TB, PB, or EB.

  c   Enter the amount of disk space which, when filled, will trigger 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 indicate KB, MB, GB, TB, PB, or EB.

8   Click **OK**.

Removing Disk Quota Entries

1   On the NAS Manager primary menu, click **Disks**.

2   On the **Disks** page, select **Disk Quota**.

3   On the **Disk Quota** page, select the volume to manage.

4   From the **Tasks** list, select **Quota Entries.**

5   On the **Quota Entries** page, select the **Logon name** from which you want to remove the quota entry.

6   On the **Tasks** list, select **Delete**.

7   Click **OK**.

Using Logs

A log file is a file that stores messages, which are sometimes called events or event log entries, generated by an application, service, or operating system. These messages are used to track the operations performed by the system. Log files are usually plain text (ASCII) files and usually have **.log** extensions.

You can use the PowerVault NAS Manager to access these log files to monitor the operation of your system.

Managing Logs

You can use the **Logs** feature to download, view, clear, and configure several types of event logs that are provided by the system. The available logs are as follows:

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

Downloading Log Files

The **Download Log Files** page on the NAS Manager allows you to download specific log files to your NAS appliance.

1   On the PowerVault NAS Manager primary menu, click **Maintenance**.
2   On the **Maintenance** page, click **Logs**.
3   On the **Logs** page, select the type of log you want to download.
4   In the **Tasks** list on the **Log Type Log** page, click **Download**.
5   In the **File Download** dialog window, select **Save this file to disk**.
6   Click **OK** to download the log file.

Viewing Downloaded Log Files

1 On the NAS Manager primary menu, click **Maintenance**.

2 On the **Maintenance** page, click **Terminal Services**.

3 Log in to a **Terminal Services Advanced Client** session.

4 On the **Terminal Services** desktop, right-click **My Computer** and select the **Manage** pop-up menu item.

 The **Computer Management** window opens.

5 In the left column of the **Computer Management** window, select **Event Viewer**.

6 In the right column of the **Computer Management** window, select the log you want to view.

Viewing Log Entry Details

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

1 On the NAS Manager primary menu, click the **Maintenance** tab.

2 On the **Maintenance** page, select **Logs**.

3 On the **Logs** page, select the type of log you want to view.

4 Click the radio button next to the log entry you want to view.

5 In the **Tasks** list, click **Event Details**.

6 On the **Log Details** page, click the **Up** and **Down** buttons to scroll through the log files.

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

Modifying Log Properties

You can specify the maximum log size and determine how the system will handle log entries when the maximum capacity of the server appliance is reached. To modify the properties of a log file, perform the following steps:

1 On the PowerVault NAS Manager primary menu, click **Maintenance**.

2 On the **Maintenance** page, click **Logs**.

3 On the **Logs** page, select the type of log you want to configure.

4   In the **Tasks** list, click **Log Properties**.

5   In the **Maximum log size** text box on the **Log Properties** page, enter the maximum
    size (in kilobytes) of the log.

6   Determine how you want the system to handle log file entries after the maximum log
    file size has been reached, and 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.

Clearing Log Files

You can clear specific log files by performing the following steps:

1   On the NAS Manager primary menu, select **Maintenance**.

2   On the **Maintenance** page, select **Logs**.

3   On the **Logs** page, select the type of log you want to clear.

4   In the **Tasks** list, click **Clear Log**.

5   On the **Clear Log** page, click **OK** to clear the log.

Using Other Languages

The NAS Manager is available in English and Japanese. To change the NAS Manager
language, perform the following steps:

1   On the NAS Manager primary menu, select **Maintenance**.

2   On the **Maintenance** page, click **Language**.

3   Click the radio button next to the desired language. (For example, click the radio
    button for Japanese if you want to use Japanese.)

4   Click **OK**.

Shutting Down the NAS Appliance

You can shut down, shut down and restart, or schedule a shut down of the NAS appliance from the NAS Manager by performing the following steps:

1 On the NAS Manager primary menu, select **Maintenance**.

2 On the **Maintenance** page, click **Shutdown**.

3 Click the action you want to perform.

4 For **Shut Down** and **Restart**, proceed to step 5. For **Scheduled Shutdown**, specify when the shut down should occur and click **OK**.

5 On the **Confirmation** page, click **OK** to confirm the action.

   If you selected to restart the NAS appliance, the **Restarting** page displays.

   ✍ NOTE: While the **Restarting Page** is displayed, the NAS Manager checks periodically to determine whether the appliance is back online. If the NAS Manager detects that the appliance has come back online, it automatically returns the NAS Manager to the home page.

Managing Volumes

The NAS Manager allows you to perform the most often used volume management tasks on the external disk arrays. With the NAS Manager, you can create, delete, and expand external volumes.

✍ NOTE: For managing internal hard-disk drives and to perform advanced tasks on your external disk arrays, see "Advanced Disk and Volume Management Using Array Manager."

Creating a Volume

When you create a new volume, you must select a minimum of three disks. The new volume is created with RAID 5 fault tolerance.

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

To create a new volume, perform the following steps:

1 On the NAS Manager primary menu, select **Disks**.

2 On the **Disks** page, select **Volumes**.

3 In the **Tasks** list, click **New...**.

4   In the **Adapter** column of the **Configure, create, or delete volumes** page, select the adapter you wish to create the volume on by clicking the appropriate radio button.

5   In the **Tasks** list, click **Select...**.

6   Select the disks to be used for the new volume and then click **OK**.

Preparing a Volume for Expansion

✍ NOTE: You cannot expand an internal RAID group.

This option prepares a volume to be expanded. The new volume retains the same fault tolerance level. During reconstruction, the original volume is still accessible. This option is not available after the volume has been prepared for expansion.

✍ NOTE: See "Advanced Disk and Volume Management Using Array Manager" for advance operations on all RAID controllers.

To prepare a volume to expand, perform the following steps:

1   On the NAS Manager primary menu, select **Disks**.

2   On the **Disks** page, select **Volumes**.

3   In the **Volumes** column of the **Configure, create, or delete volumes**, select the volume to prepare for expansion by clicking on the adjacent radio button.

4   On the **Tasks** list, click **Prep Expand...**.

5   Select the disks you want to add to this volume.

6   Click **OK**.

The RAID status changes to show the process is occurring. 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 to expand, the RAID status is marked as **Ready to Expand**.

✍ NOTE: See "Advanced Disk and Volume Management Using Array Manager" for advanced operations on all RAID controllers.

To expand a volume, perform the following steps:

1   On the PowerVault NAS Manager primary menu, select **Disks**.

2   On the **Disks** page, select **Volumes**.

3   In the **Volumes** column of the **Configure, create, or delete volumes**, select the volume to expand.

4   On the **Tasks** list, click **Expand...**.

5   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 might not display shares correctly.

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

1   On the NAS Manager primary menu, select **Disks**.

2   On the **Disks** page, select **Volumes**.

3   In the Volume column of the **Configure, create, or delete** page, select the volume to be deleted by clicking the adjacent radio button.

4   In the **Tasks** list, click **Delete...**.

5   Click **OK**.

6   On the confirmation page, click **OK** to continue or **Cancel** to abort the operation.

Viewing Volume Properties

1   On the NAS Manager primary menu, select **Disks**.

2   On the **Disks** page, select **Volumes**.

3   In the **Volumes** column of the **Configure, create, or delete volumes**, select the volume for which you want to view properties.

4   On the **Tasks** list, click **Properties...**.

5   Click **OK** to return to the **Volume** list.

Managing Disks

The NAS Manager allows you to perform the most often used disk management tasks on the external disk arrays. With the NAS Manager, you can list available disks, rescan for disks, create a hot spare, free a hot spare, and force a disk online.

NOTE: See "Advanced Disk and Volume Management Using Array Manager" for advance operations on all RAID controllers.

Listing Available Disks

1 On the NAS Manager primary menu, select **Disks**.

2 On the **Disks** page, select the **Disks**.

3 In the **Adapter** column on the **Configure, create, or delete volumes** page, select the adapter to list disks for by clicking the adjacent radio button.

4 On the **Tasks** list, click **Select...**.

A page titled with the adapter name that contains a list of disk drives displays.

Rescanning for Disks

1 On the NAS Manager primary menu, select **Disks**.

2 On the **Disks** page, select the **Disks**.

3 In the **Adapter** column on the **Configure, create, or delete volumes** page, select the adapter to list disks for by clicking the adjacent radio button.

4 In the **Tasks** list, click **Select...**.

5 In the **Tasks** list on the adapter page, click **Rescan...**.

Creating a Hotspare

1 On the NAS Manager primary menu, select **Disks**.

2 On the **Disks** page, select the **Disks**.

3 In the **Adapter** column on the **Configure, create, or delete volumes** page, select the adapter to list disks for by clicking the adjacent radio button.

4 In the **Tasks** list, click **Select...**.

5 In the **Physical Disks** column of the adapter page, select the disk to use to create a hotspare.

6 In the **Tasks** list on the adapter page, click **Make Hotspare....**

Freeing a Hotspare

1 On the NAS Manager primary menu, select **Disks**.

2 On the **Disks** page, select the **Disks**.

3 In the **Adapter** column on the **Configure, create, or delete volumes** page, select the adapter to list disks for by clicking the adjacent radio button.

4 In the **Tasks** list, click **Select...**.

5 In the **Physical Disks** column of the adapter page, select the hotspare disk to free.

6 In the **Tasks** list on the adapter page, click **Free Hotspare...**.

Forcing a Disk Online

1 On the NAS Manager primary menu, select **Disks**.

2 On the **Disks** page, select the **Disks**.

3 In the **Adapter** column on the **Configure, create, or delete volumes** page, select the adapter to list disks for by clicking the adjacent radio button.

4 In the **Tasks** list, click **Select...**.

5 In the **Physical Disks** column of the adapter page, select the disk to force online.

6 In the **Tasks** list on the adapter page, click **Force Online...**.

Viewing Disk Properties

1 On the NAS Manager primary menu, select **Disks**.

2 On the **Disks** page, select the **Disks**.

3 In the **Adapter** column on the **Configure, create, or delete volumes** page, select the adapter to list disks for by clicking the adjacent radio button.

4 In the **Tasks** list, click **Select...**.

5 In the **Physical Disks** column of the adapter page, select the disk to force online.

6 In the **Tasks** list on the adapter page, click **Properties**....

3

Advanced Disk and Volume Management Using Array Manager

www.dell.com | support.dell.com

Although the Dell OpenManage™ Array Manager provides a comprehensive solution to storage management, you should use it only for *advanced features* that cannot be performed from the **Disks** tab in the NAS Manager. You can access the Array Manager through the Terminal Services Advanced Client in the NAS Manager.

Array Manager allows you to configure your storage devices and the 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
- Display all of your storage information in a graphical environment

Array Manager Common Tasks

This section provides a high-level description of the most common procedures performed under Array Manager.

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 format the volume NT File System (NTFS).

   ✍ NOTE: The PowerVault 750N and 755N only support NTFS partitions. Formatting all partitions as NTFS allow for advanced features only available under that file system.

Deleting an Existing Volume

1 Select and delete the desired 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.

4 Extend the specified volume with the new space available to the virtual disk.

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 on
storage objects. The following sections provide more information about the left and right
panes.

Left Pane

The left pane shows the objects detected by the Array Manager software. The major storage
objects are the local computer 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, logical drives associated with extended partitions.

- **My Network Places**, **History**, and **Favorites** provide remote connection functionality
  not supported by the PowerVault 750N and 755N systems 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 system's right pane console view include the following:

- The **General** tab displays parameters based on the objects you select in the console's tree view. The parameters 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 Array 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-disk 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: small computer system interface (SCSI), integrated drive electronics (IDE), and so on.
    - **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, which uniquely identifies the disk on the controller card.
    - **Vendor** identifies the vendor on hardware objects.

- 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 CD or other removable media.

- The **DM View** tab is grayed-out on the Array Manager console.

Launching Array Manager From the NAS Manager

📝 NOTE: To use the NAS Manager you must be logged in as Administrator. The NAS Manager default administrator user name is administrator and the default password is powervault.

You can launch the Array Manager from the NAS Manager

1 On the NAS Manager primary menu, click **Maintenance**.

2 Click **Terminal Services**.

3 Log into the **Terminal Services** session.

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

Managing Disk Arrays

This section describes how 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 the PowerVault 750N or 755N NAS appliance. The PERC 3/DC and PERC 3/QC controllers are high-performance intelligent PCI-to-SCSI host adapters with RAID capabilities. Each channel supports SCSI data transfer rates of up to 160 megabytes (MB) per second per channel. You can create a maximum of 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

Recommended Virtual Disk Configuration

It is recommended that each virtual disk created on your system's external SCSI enclosures contain 11 physical drives and be configured as a RAID-5 virtual disk. Virtual disks configured in this manner are optimized by the PERC 3/DC or PERC 3/QC adapter to provide the best performance. You are also recommended to assign a global hotspare within the same enclosure for each virtual disk.

Creating Virtual Disks

📝 NOTE: The maximum supported volume size is 2 terabytes (TB).

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

✍ NOTE: When you create virtual disks, you might want to consider how virtual disks will be deleted. Virtual disks created on the PERC 3/DC or PERC 3/QC controller must be deleted in reverse order of their creation. In other words, you must delete the most recently created virtual disk first and continue to delete in reverse order.

✍ NOTE: To take advantage of all the system features such as **Defrag** and **Encryption**, you are recommended to 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 on an array group.

2 Click **Create Virtual Disk** to launch the **Create Virtual Disk Wizard**.

3 Read the **Welcome** screen and 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 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: The PowerVault 750N and 755N only supports NTFS partitions. Formatting all partitions 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

Deleting a virtual disk permanently deletes all information contained on that disk. Virtual disks created on the PERC 3/DC or PERC 3/QC controller must be deleted in the reverse order that they were created. In other words, the last disk that you created must be deleted first.

● NOTICE: All data on the virtual disk is lost when the disk is deleted.

1 Right-click the last virtual disk that was created.

2 Click **Delete**.

   A confirmation dialog box appears.

3 Click **OK** to continue.

   The virtual disk disappears from the left pane. If the disk was not the last one created, the delete option is grayed out.

   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

✍ 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.

5 **Add Member** shows progress information in the right pane.

6 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 on 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.

Array Disk Commands

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

- Format
- Rebuild
- Assign a global hot spare
- Unassign a 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 is 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 on 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 on 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 on 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, it is recommended that you perform this operation before you remove any physical disk from an enclosure.

1   Right-click on 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 sound

• Disable sound

• Rebuild rate

• Properties

Rescan Controller

The **Rescan Controller** command can be used to check whether there are any new disks that 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 Sound

The **Enable Sound** 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 Sound**.

Disable Sound

The **Disable Sound** 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 Sound**.

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.

🔵 NOTICE: The default rebuild rate is 30%. 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% and 100%. At 0%, the rebuild is only done if the system is not doing anything else. At 100%, 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 on 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

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 cannot be used until it has a signature on it.

To write a disk signature, right-click on 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, you are recommended to 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 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 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. You are strongly recommended not to 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 PowerVault NAS Manager, log on to the **Terminal Services Advanced Client**.

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 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**.

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 volume properties
- Formatting a partition or volume
- Deleting a partition or volume

Volume Overview

A volume is a logical entity that is made up 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: The PowerVault 750N and 755N only supports NTFS partitions. Formatting all partitions as NTFS allow 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 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.

Delete 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 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 asked to select whether to create a partition or a volume. Make sure 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 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 desired, 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.

- There is unallocated space on a dynamic disk onto which volume can 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).

- There is no unallocated space 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 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.

4

SECTION 4

System Management

This chapter provides information about system management for your PowerVault™ 750N or 755N NAS appliance. The following topics are discussed:

- Dell OpenManage™ Remote Assistant Card (DRAC)
- Alert log messages from Dell OpenManage Server Agent
- Configuring Simple Network Management Protocol (SNMP) community properties
- Configuring SNMP agent properties

Dell OpenManage Remote Assistant Card

The DRAC is an optional server management card designed to provide remote manage capabilities. With the addition of the DRAC, system administrators can manage and monitor a system through a modem or network connection, even when the system itself is down.

If you purchased a DRAC with your PowerVault 750N or 755N system, you will need to install the DRAC software as outlined in this chapter.

After the server software has been installed, you will need to install the DRAC Web Client software on the system that you plan to use as the DRAC client. This software is included on the *Resource* CD. See the DRAC documentation on the *Resource* CD for more information on how to install the DRAC Web Client software.

The DRAC must already be installed in your system. See the *Dell OpenManage Remote Assistant Card User's Guide* on the *Resource* CD for instructions on installing this card in your system.

To install and configure the DRAC software on your PowerVault 750N or 755N system using the **Terminal Services Advanced Administration Menu**, perform the following steps:

1 Connect to the system through NAS Manager.

✎ NOTE: To use the NAS Manager you must be logged in as Administrator. The NAS Manager default administrator user name is `administrator` and the default password is `powervault`.

2 Click **Maintenance** and then click **Terminal Services**.

3 If required in the **Terminal Services Client** window, log in to the **Terminal Services Client** by entering your user name and password.

4 Click the **Advanced Administration Tool** icon to access the **Advanced Administration Menu**.

5   At the **System Management** menu, click **Dell Remote Assistant Setup**.

    The **Dell Remote Assistant Card Setup and Configuration** window displays.

6   Click **Install DRAC Software**.

    The **Setup/Install Wizard** starts. You can install the management software. Ensure that you use the default install directory (C:\Program Files\DRAC\Host).

7   Reboot your system.

    ![note icon] NOTE: Rebooting disconnects the NAS Manager.

8   Repeat steps 1 through 4 after the system has rebooted.

9   Click **Configure DRAC Card**.

    The **Advanced Administration Window** displays. You can edit the configuration file, apply the configuration, and reset the DRAC. DRAC uses the RacConf utility as described in the *Dell OpenManage Remote Assistant Card User's Guide*.

10 Click **Edit Config File**.

    Edit the configuration file and customize the DRAC.

    The following is an example of setting information for both user and Internet protocol (IP) address:

    [AdminEntry0]
    Administrator Alias = drac
    Password = password

    [NetConfig]
    IpAddr = 10.4.1.200
    SubnetMask = 255.255.0.0
    GatewayAddr = 0.0.0.0

    ![note icon] NOTE: When you create the username and password, ensure there are no spaces before or after the username or password.

11 Click **Configure**.

    You can load the configuration file information into the DRAC after the file has been edited and saved.

    After the configuration file has loaded, the user name and password will be automatically removed from the configuration file as a security precaution.

12 Click **Soft Reset**.

For more information about your DRAC, see the *Dell OpenManage Remote Assistant Card User's Guide* on the *Resource* CD.

Alert Log Messages From Dell OpenManage Server Agent

Server Agent server management software generates alert messages that appear in the SNMP event log file. Alert log messages consist of information, status, warning, and failure messages for drive, temperature, fan, and power conditions. To see the trap logs, from the NAS Manager **Maintenance** page, go to the **Logs** page or go to **Terminal Services** to log onto your server and click the **Event Viewer** link under **Administrative Tools** in the **Advanced Administration Menu** to view logged events.

Configuring SNMP Community Properties

1   Click **Maintenance**.

2   Click **Terminal Services**.

3   Log in to the **Terminal Services** session.

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 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 click **Add**.

12 Select **Community Rights**, and 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 in to the **Terminal Services** session.

4 Click **Advanced Administration Menu**.

5 At the **Advanced Administration Menu**, select **System Management**, and 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, then select **Contact**, and 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.

SECTION 5

System Recovery, Backup, and Restore

This section provides instructions on how to recover from a system failure, and how to back up and restore the system state. The following topics are discussed:

• Recovery from system failure

• System state backup and restore

• Microsoft® Windows® 2000 backup and recovery tools

• Third-party backup software for network backups

• Installing device drivers for Windows 2000

Recovery From System Failure

If the Windows Powered operating system becomes inoperable, you can use the *Reinstallation* CD for your system to reinstall the operating system. After the operating system is reinstalled, the system state backup can be restored to recover system configuration information.

Operating system reinstallation includes the following procedures:

• Reinstalling the operating system using the *Reinstallation* CD.

• Performing system setup

• Restoring the system state backup (see "Restoring System State Data" for more information)

Reinstalling the Operating System

● NOTICE: When using the *Reinstallation* CD, you will lose all data on the operating system drive.

1 Insert the *Reinstallation* CD into the CD drive.

2 Shutdown the system.

3 If one or both existing operating system disks are operational, proceed to step 4.

If both operating system mirrored drives (small computer system interface [SCSI] drives 0 and 1) have been replaced with new, initialized drives, you must remove all of the internal *data* drives. You do not need to completely remove the internal data drives from the enclosure. You only need to pull the internal data drives out far enough to ensure that they are disconnected from the backplane. Ensure that you leave only the two new operating system drives installed in the internal drive bays.

4   Turn on the system.

The *Reinstallation* CD automatically starts the installation process if the system is a PowerVault 750N or 755N NAS appliance and if the first logical volume configured on the RAID controller is a drive in a two drive RAID 1 group.

It takes up to 30 minutes for the system to reinstall.

> ✎ NOTE: The CD ejects approximately 7 minutes into the installation time. The ejection of the CD does not indicate an error or that the process is finished.

5   If you had two new, initialized drives in step 3, reinsert any internal data drives that were removed prior to the operating system reinstallation after the CD has ejected. Otherwise, proceed to step 6.

6   Use a Web browser to connect to the 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 "System Recovery, Backup, and Restore" for more information about merging disks.)

Initial System Setup

After the operating system is reinstalled on the system, you should configure the system again to establish network communication. If Kick-Start is used for configuration, insert your Kick-Start diskette after the CD drive tray ejects the *Reinstallation* CD. See "Introduction" for information on initial system configuration.

System State Backup and Restore

Integrated Windows 2000 backup and recovery tools allows administrators to back up and restore the system state data.

System state data includes the following:

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

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 information and share information.

✎ NOTE: You must back up your system state to a hard-disk drive other than your operating system hard-disk drive to restore your system state after using the *Reinstallation* CD.

Backing Up System State Data

✎ NOTE: To use the NAS Manager you must be logged in as Administrator. The NAS Manager default administrator user name is `administrator` and the default password is `powervault`.

1 Click **Maintenance**.

2 Click **Terminal Services**.

3 Log in to the **Terminal Services** session.

4 Go to the **Advanced Administration Menu**.

5 Select **Administrative Tools** and click **Perform System State Backup**.

   The **Performing System State Backup** window displays.

6 Click **OK** to continue.

7 Select the location to store your system state backup and click **OK**.

✎ NOTE: **System State Backup** takes approximately five minutes to complete and requires approximately 250 megabytes (MB) of disk space.

You are recommended to regularly back up your system state to your RAID 5 protected data drives. This action enables you to go back to the most recent state if an operating system reinstallation is required.

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 from Windows 2000 Backup and Recovery Tools.

1 Click **Maintenance**.

2 Click **Backup**.

3 Log in to the system as administrator.

4   Click **Restore Wizard**.

The **Restore Wizard** window displays.

5   Click **Next**.

6   Click **Import File**.

The **Backup File Name** window displays.

You must import the file because your system will not be aware of previous backups after you complete a reinstallation from the *Reinstallation* CD.

7   Click **Browse.**

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

8   Browse for your file.

9   After locating your file, click **OK**.

The **What to Restore** window displays.

10   Click + symbol next to **File**.

11   Click + symbol next to **Media Created on**.

You are prompted for your backup file location.

12   If the location is correct, click **OK**; otherwise, browse to the correct backup file location.

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

13   Click + (symbol) next to **System State**.

You are asked to confirm your backup file location again.

14   If the location is correct, click **OK**; otherwise, browse to the correct backup file location.

15   Click the checkbox next to **System State**.

16   Click **Next**.

17   Click **Advanced**.

The **Where to Restore** window displays.

18   Click the original location as new the location to restore the files.

19   Click **Next**.

The **How to Restore** window displays.

20   Click **Always replace the files on disk**.

21   Click **Next**.

The **Advanced Restore Options** window displays.

22   Leave all checkboxes unchecked.

23   Click **Next**.

24   Click **Finish** to initiate the restore process

25   Restart your system after the restore process completes.

✎ NOTE: Windows must replace all locked files on the system; therefore, the restart system process might take approximately 15 minutes to complete.

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 installed and have a tape drive to back up your data volumes to tape.

You can get to 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 on the **Windows 2000 Backup and Recovery Tools**, see the Windows Powered Help. You can access Windows Powered Help by clicking **Windows Powered Help** in the **Advanced Administration Menu** under **Administrative Tools** or by clicking **Help** in the **Start Menu** when using the **Terminal Services Client**.

Supported Third-Party Backup Software

- VERITAS® Backup Exec®
  - Backup Exec 8.0, 8.5, and 8.6 for Windows NT® and Windows 2000

- Computer Associates® ARCserve*IT*™
  - ARCserve*IT* 2000 for Windows NT and Windows 2000
  - ARCserve*IT* 6.61 for Red Hat Linux

Third-Party Backup Software for Network Backups

You may back up your data volumes over the network to local area network (LAN)-attached backup servers. This backup requires that you already have a backup server on your network.

You are recommended to use backup software network accelerator agents to greatly improve network backup performance.

Installing Network Accelerator Agents

VERITAS Backup Exec and Computer Associates ARCserve network accelerator agents can both be installed remotely by installing the agent to the system from a remote system on the network.

See the documentation for your backup software for more information on how to install the network accelerator agents.

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.

Installing VERITAS Backup Exec

You must first install VERITAS Backup Exec on the Dell™ PowerVault™ NAS appliance, and then install VERITAS Remote Administrator on a remote system.

NOTE: Before installing the backup software, check **http://support.dell.com** for the latest driver and software updates. You might need to install these updates after completing the procedures below.

Installing VERITAS Backup Exec on the NAS Appliance

✐ NOTE: You do not need to attach a keyboard, mouse, or monitor to the NAS appliance before you install VERITAS Backup Exec. VERITAS Backup Exec supports installation using Terminal Services, and management using VERITAS Remote Administrator.

1 Insert the *VERITAS Backup Exec* CD in the CD drive of the NAS appliance.

2 From the NAS appliance web interface, click **Maintenance**, and then click **Terminal Services**.

3 Log into the NAS appliance.

4 Follow the instructions in the documentation that came with your backup software.

Installing VERITAS Backup Exec Remote Administrator on the Remote System

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

   The CD should autoplay.

2 If the CD does not autoplay, open Microsoft® Windows® Explorer and right-click the CD drive that contains the VERITAS software.

3 Select **Autoplay** from the menu.

4 Follow the instructions in the documentation that came with your backup software.

Using VERITAS Backup Exec Remote Administrator

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

   The **Connect to Server** window displays.

2 Enter the name of the NAS appliance in the **Server** field.

3 Enter 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 your backup operations just as you would from the local application. See the VERITAS Backup Exec documentation for more information on how to use the software.

Installing ARCserve 2000

To use ARCserve 2000 to back up your system, you must first install ARCserve 2000 on the NAS appliance, and then install ARCserve Manager on a remote system.

Installing ARCserve 2000 on the NAS Appliance

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

1 Insert the *ARCserve 2000* CD in the CD drive of the NAS appliance.

    The CD should autoplay.

2 If the CD does not autoplay, open Windows Explorer and right-click the CD drive that contains the ARCserve 2000 software.

3 Select **Autoplay** from the menu.

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

4 Follow the instructions in the documentation that came with your backup software.

Installing ARCserve Manager on the Remote System

1 Insert the *ARCserve 2000* CD in the CD-ROM drive of the remote system.

    The CD should autoplay.

2 If the CD does not autoplay, open Windows Explorer and right-click the CD-ROM drive that contains the ARCserve 2000 software.

3 Select **Autoplay** from the menu.

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

4 Follow the instructions in the documentation that came with your backup software.

Using ARCserve 2000 Remote Manager

1 On the remote system, click the **Start** button, 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 appliance in the **Server** field at the top of the screen to manage the backup software on the NAS appliance.

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 how to use the software.

Backing Up Persistent Images

Backing up persistent images eliminates the possibility of files changing during the backup job. Persistent images always contain the data that existed when the persistent image was taken. However, backing up persistent images requires that you perform several steps and should only be performed by advanced backup administrators. It is recommended that you use the available open file agents in VERITAS Backup Exec and Computer Associates ARCserve to backup your open files rather than backing up persistent images.

✍ NOTE: Do not use Computer Associates ARCserve to backup or restore persistent images.

To back up a persistent image correctly to ensure that you can restore it properly, perform the following steps:

1   Use the NAS Manager to create a persistent image.

✍ NOTE: For increased performance, only backup read-only persistent images.

2   On the NAS Manager primary menu, click **Maintenance** and then click **Terminal Services**.

3   Log on to the system.

4   Using the Windows Explorer, browse to the persistent image you created in step 1.

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

5   Right-click on the persistent image and click **Sharing...** .

6   Click the radio button adjacent to **Share this folder**.

7   Enter a name for the share in the **Share name** text box.

8   Click **Permissions**.

9   Set the desired permissions in the **Permissions** window and click **OK**.

10 Click **OK** in the **Properties** window to finish the share creation process.

11 On the system that is running VERITAS Backup Exec, set up VERITAS Backup Exec so that it is able to backup user shares.

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

12 In the Veritas Backup Exec **Backup Selections** window, browse to your NAS appliance under **Entire Network**.

13 Select the share name that you created for your persistent image.

14 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 these files is not recommended.

15 Click **Backup**.

16 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 will not create network traffic if you are backing up to a local backup device.

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 do a manual backup of persistent image files because each persistent image file name 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 will not be successful.

Restoring Persistent Images From Tape Backup

✍ NOTE: 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 system on your network that is running Veritas Backup Exec, click the **Restore Selections** tab to bring up the window that lists your previous backups.

2 Browse to your backup of the persistent image that you want to restore and 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 in the text boxes next to **Restore to drive** and **Restore to path**.

7   Click **Run Now** to run the restore immediately or click **Schedule** to schedule your restore job to run at a later time.

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 **http://support.dell.com** website for updated drivers and patches.

Installing Drivers for PowerVault Tape Drives

To install drivers for the PowerVault tape drives, perform the following steps.

1   Connect the Dell PowerVault tape device and restart the system.

2   Connect to the PowerVault NAS Manager.

3   Click **Maintenance** and then click **Terminal Services**.

4   Log in to a **Terminal Services Client** session.

5   On the **Advanced Administration Menu** under **System Management**, click **Computer Management**.

6   Click **Computer Management** in the left pane.

7   Click **System Tools** in the left pane.

8   Click **Device Manager** in the left pane.

9   Click **Unknown Devices** in the right pane.

10   Double-click **Unknown Tape Device**.

11   Click **Driver** in the pop-up 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 checkbox for **Specify a location**.

Deselect the other checkboxes.

16 Click **Next**.

The **Properties** dialog box displays.

17 Specify the folder name that contains the device drivers in the path for **Copy manufacturer's files from**.

18 Click **OK** and then click **Next**.

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

19 Make sure the wizard has selected the appropriate PowerVault tape device and 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 restart the machine.

2 Connect to the PowerVault NAS Manager.

3 Click **Maintenance** and then click **Terminal Services**.

4 Log in to a **Terminal Services Client** session.

5 In the **Advanced Administration Menu**, click **Computer Management** under **System Management**.

6 Click **Computer Management** in the left pane, and then click **System Tools.**

7 Click **Device Manager** in the left pane.

8 Click **Medium Changers** in the right pane.

9   Double-click **Unknown Medium Changer**.

10 Click **Driver** in the **Properties** window.

11 Click **Update Driver**.

    The **Upgrade Device Driver Wizard** displays.

12 Click **Next**.

13 Click the radio button next to **Search for a suitable driver for my device (recommended)** and then click **Next**.

14 In **Optional search locations**, click the checkbox for **Specify a location**.

    Deselect the other checkbox.

15 Click **Next**.

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

16 In the path for **Copy manufacturer's files from**, specify the folder name that contains the device drivers, and click **OK**.

17 Click **Next**.

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

18 Make sure the **Upgrade Device Driver Wizard** has selected the appropriate PowerVault tape device and click **Next**.

19 Click **Finish**.

20 Click **Close**.

6

SECTION 6

Dell ActiveArchive™

Dell ActiveArchive allows the creation and preservation of persistent images of Dell PowerVault™ 750N and 755N system data volumes. The Dell ActiveArchive software is installed on all PowerVault 75xN systems. It can be configured by using the NAS Manager.

This chapter provides information on the following topics:

- Introduction to persistent images
- Scheduling persistent images
- Adding persistent images to the schedule
- Deleting a persistent image schedule
- Editing the properties of a persistent image's schedule
- Taking a new persistent image
- Deleting a persistent image
- Configuring the persistent image environment
- Setting persistent image retention weights
- Accessing persistent images
- Restoring a volume

Introduction to Persistent Images

A persistent image is a point-in-time copy of a disk volume. Unlike conventional volumes, the information in the persistent image is static. 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. 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 file servers, thus eliminating the backup window required by other types of backup.

✍ NOTE: Persistent images are temporary backups of your data that reside on the same volume as your data. If the volume becomes damaged, you lose your data including the persistent image. 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 for the cache file.

NOTE: You cannot take a persistent image of the operating system drive (**C:**).

Cache Thresholds

The Dell ActiveArchive software has two thresholds that provide warnings when the cache file is approaching maximum capacity. The **Cache Full Warning Threshold** logs an event in the event log and displays an error in the NAS Manager status indicator when the cache file reaches the threshold (default is 80% full). The **Cache Full Threshold**, which is labeled **Begin deleting images** in the NAS Manager, specifies the threshold where the PowerVault NAS Manager deletes the oldest persistent images with the lowest retention weights until the cache file is below the **Cache Full Threshold** (default is 90% full).

Persistent Image Retention Weights

When the system reaches the cache full threshold, the system starts deleting files depending on the retention weight and age of the persistent image. The system first looks for the persistent image with the with the lowest retention weight in the cache file and deletes the oldest persistent image with that retention weight. After all persistent images with that lowest retention weight have been deleted, Dell ActiveArchive looks for and deletes the oldest files with the next higher retention weight.

Persistent Image Considerations

When using persistent images, system performance may 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, may 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 will not cause a performance degradation.

NOTICE: If you use the *Reinstallation* CD to reinstall your operating system, your persistent images will be deleted.

Storing Persistent Images

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

- Seven daily persistent images

- Two weekly persistent images

- Two monthly persistent images

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. To access the ActiveArchive directory from the NAS Manager home page, click **Disks** and then click **ActiveArchive**. Each persistent image is mounted as a volume on the file system to allow access by clients. Persistent images are created as read-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 will survive system power losses or reboots.

 NOTE: The ActiveArchive directory is a hidden folder. You must configure your system to view hidden files and folders to view your ActiveArchive directory.

Allowing User's Access to Persistent Images

To allow user's to access the persistent images, the system administrator must modify the permissions for the ActiveArchive directory. The files and folders within a persistent image are identical to the permissions on the original files and folders. Use the PowerVault NAS Manager to change the ActiveArchive directory permissions by performing the following steps.

1   On the NAS Manager primary menu, click the **Maintenance** tab.

2   Click **Terminal Services**.

3   Log on to a Terminal Services Advanced Client session.

4   Open the **Explorer**.

5   Select the drive on the left side.

6   Right-click the **ActiveArchive** directory and click **Properties**.

7   Click the **Security** tab and click **Add...**.

8   Add individual users or groups.

9   Give the selected members **Read** and **List Folder Contents** permissions.

Repeat these steps for the ActiveArchive directory on each volume the users will access. You do not need to change the permissions of the persistent images and their subdirectories. These files and folders will retain the original files' and folders' permissions.

Preparing Your Volumes for Persistent Images

Before you take or schedule persistent images, you must prepare each of your volumes for persistent images. This process creates the cache file and other files needed for taking persistent images.

![note icon] NOTE: This process might take several hours.

To prepare your volume for persistent images, perform the following steps:

1   On the NAS Manager primary menu, click **Disks** and then click **ActiveArchive**.

2   Click **Volume Settings**.

3   Click the radio button adjacent to the volume you want to prepare.

4   Click **Configure...** .

5   Use the drop-down menus to configure the required options. For information about the options, see Configuring Persistent Image Volume Settings.

6   Click **OK** to start the prepare process.

Scheduling Persistent Images

✎ NOTE: Before scheduling persistent images, prepare each of your volumes for persistent images. (See the Preparing Your Volumes for Persistent Images.)

When you click **Disks** and then **ActiveArchive**, 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 are identified by time and date, and 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 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.

Displaying the List of Persistent Images

The **Persistent Images** page displays all current active persistent images. Each entry identifies the date and time 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   On the NAS Manager primary menu, click **Disks**, then click **ActiveArchive**.

2   Click **Persistent Images**.

Adding Persistent Images to the Schedule

To add a persistent image to the schedule, perform the following steps:

1   On the NAS Manager primary menu, click **Disks**, then click **ActiveArchive**.

2   Click **Schedules**.

3   In the **Tasks** list on the **Schedules** page, click **New...**

4   Use the dropdown menus to select the **Starting time**, the frequency at which to repeat the persistent image (**Repeat every frequency**), the **Beginning day**, the **Volume(s)**, the **Retention Weight**, number of images (how long) to **Save** count, and the persistent image **Name**.

   ✎ NOTE: To select multiple volumes, press and hold the <Ctrl> key and select all volumes that are to be included in the persistent image.

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 would 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
- %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

5 Click **OK** to save the new scheduled persistent image.

Deleting a Persistent Image Schedule

1 On the NAS Manager primary menu, click **Disks**, then click **ActiveArchive**.

2 Click **Schedules**.

3 On the **Schedules** page, click the check box next to the scheduled persistent image to be deleted.

4 In the **Tasks** list on the **Schedule** page, click **Delete**.

5 Click **OK** to delete the item or **Cancel** to leave the item intact.

Editing the Properties of a Persistent Image's Schedule

1 On the NAS Manager primary menu, click **Disks**, then click **ActiveArchive**.

2 Click **Schedules**.

3 In the **Tasks** list on the **Schedules** page, click **Properties...**

4   Use the drop-down menus to select the **Starting time**, the frequency at which to repeat the persistent image (**Repeat every frequency**), the **Beginning day**, the **Volume(s)**, and the number of images to **Save**.

    ✍ NOTE: To select multiple volumes, press and hold the <Ctrl> key and select all volumes that are to be included in the persistent image.

5   Click **OK** to modify the schedule or **Cancel** to leave the schedule intact.

Using Persistent Images

✍ NOTE: Before taking a persistent image, prepare each of your volumes for persistent images. (See "Preparing Your Volumes for 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   On the NAS Manager primary menu, click **Disks**, then click **ActiveArchive**.

2   Click **Persistent Images**.

3   In the **Tasks** list on the **Persistent Images** page, click **New...**

4   Use the drop-down menu to select the **Volume(s)** to preserve.

    ✍ NOTE: To select multiple volumes, press and hold the <Ctrl> key and select all volumes that are to be included in the persistent image.

5   Select the **Retention Weight** for the persistent image.

6   Enter 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 would 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

- %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 create the persistent image.

Deleting a Persistent Image

1   On the NAS Manager primary menu, click **Disks**, then click **ActiveArchive**.

2   Click **Persistent Images**.

3   On the **Persistent Images** page, click the check box next to the persistent image that is to be deleted.

4   In the **Tasks** list, click **Delete**.

5   Click **OK** to delete the persistent image.

Setting Persistent Image Retention Weights

To change the retention weight (deletion priority) of a persistent image, you must edit the persistent image properties by selecting an image from the **Persistent Image** page and then clicking **Properties...** in the task list.

1   On the NAS Manager primary menu, click **Disks**, and then click **ActiveArchive**.

2   Click **Persistent Images**.

3   In the **Tasks** list, click **Properties...**.

4   Select the **Retention weight**.

5   Click **OK** to update the persistent image.

Configuring the Persistent Image Global Settings

You can use drop-down menus to modify the various aspects of the persistent image environment.

1   On the NAS Manager primary menu, click **Disks**, and then click **ActiveArchive**.

2   Click **Global Settings** and configure the following options**.**

Ø 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 will overwrite 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 five 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 server should continue to retry to create a persistent image (default 15 minutes). A persistent image will not start until a period of relative inactivity, specified by the **Inactive Period**, occurs. If an interval longer than **Inactive Time-Out** passes before the persistent image can begin, the persistent image will not be taken and an error will be displayed in the NAS Manager status indicator and an error will be logged in the event log.

- **Image Directory Name** — Specifies the directory name which will be used for the persistent image mount point. Each persistent image appears as a subdirectory in the volume which is being imaged. The entire content of the volume, as it existed when the persistent image was created, appears under this directory.

Restore Defaults reestablishes the system defaults.

Configuring Persistent Image Volume Settings

You can use drop-down menus to modify volume settings.

1   On the NAS Manager primary menu, click **Disks** and then click **ActiveArchive**.

2   Click **Volume Settings**.

3   Click the radio button adjacent to the volume setting you want to change.

4   Click **Configure...** .

5   Use the dropdown menus to configure the following options.

> ✍ NOTE: Before changing the cache size, you must delete all persistent images on that volume.

- **Cache Full Warning Threshold** — Defines the percentage of cache space used that will trigger warning messages to the system event log.
- **Begin Deleting Images** — Defines the percentage of cache space used that will trigger 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 will allow more and larger persistent images to be maintained. Ensure that adequate space is available on the persistent image files location drive.

6   Click **OK**.

Accessing Stored Persistent Images in ActiveArchive

> ✍ 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 **ActiveArchives**.

> ✍ NOTE: The ActiveArchive directory is a hidden folder. You must configure your system to view hidden files and folders to view your ActiveArchive directory.

1   Right-click on **My Appliance**.

2   Click **Map Network Drive** from the menu.

3   Map to the root of the ActiveArchives volume.

Use "$" to specify the root of the volume. For example, in the **Folder** field, type \\<Dellxxxxxxx>\e$, where <Dellxxxxxxx> is the name of the PowerVault 750N or 755N system and where *e* is the drive letter of the volume.

4   Use Microsoft Windows Explorer to navigate to the **ActiveArchive** directory on the newly mapped drive.

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.

⊖ 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.

To restore volumes from a persistent image, perform the following steps:

1 On the NAS Manager primary menu, click **Disks**, then click **ActiveArchive**.

2 Click **Restore Persistent Images**.

3 On the **Persistent Images Restore** page, click the radio button next to the persistent image that is to be restored.

4 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 will restore all of the volumes in the persistent image.

✐ NOTE: If you want the ability to restore a single volume, you must take single volume persistent images.

7

SECTION 7

Advanced Features

This chapter includes descriptions of advanced features that cannot be performed from the PowerVault™ NAS Manager menus. The following topics are discussed:

- 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 (MSDSS)

- Uninterruptible power supply (UPS)

- Defragmenting a volume containing persistent images

To perform the procedures in this chapter, you must use the Terminal Services Advanced Client. To access the Terminal Services Advanced Client, perform the following steps.

Ø NOTE: To use the NAS Manager you must be logged in as Administrator. The NAS Manager default administrator user name is `administrator` and the default password is `powervault`.

1   From the NAS Manager, click **Maintenance**.

2   Click **Terminal Services**.

3   Log in as administrator.

Installing Multilanguage User Interface (MUI) Support

Ø NOTE: Installing the MUI for your language automatically installs the appropriate language locale.

The PowerVault 75*x*N NAS appliance allows you to change languages for its Microsoft Windows® Powered operating system's user interface. The MUI allows the PowerVault 75*x*N to display Windows Powered operating systems menus, dialogs and help files in multiple languages. The supported languages are Simplified Chinese, Traditional Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Spanish, and Swedish. You must install a language MUI from the *Localization* CD before it is available for use on the system.

NOTE: Installing and configuring the operating system MUI does not affect the language used by the NAS Manager.

1 Insert the *Localization* CD that came with the PowerVault 75*x*N into your NAS appliance CD drive.

2 From a client, connect to the NAS Manager.

3 Click the **Maintenance** tab and then click **Terminal Services** to create a Terminal Services Advanced Client session with the appliance.

4 Log in to the system as an **Administrator**.

5 Close the **Advanced Administration Menu** by clicking **Exit**.

6 Double-click **My Appliance** on the NAS desktop.

7 Browse to the CD drive and double-click the *Dell PowerVault Localization* CD to launch the *Localization* CD's web interface.

8 Click on 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. Next, from the drop-down menu, set the default MUI language.

10 Click **OK** to perform the installation.

11 If an **Insert Disk** windows appears, you must perform the following steps:

   a Click **OK**.

   b In the **Files needed** window, click **Browse** and browse to the **i386** directory on the *Localization* CD (if not already selected). Click **Open**.

   c In the **Insert Disk** window, 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.

After a MUI language has been installed, you can apply it to any user by performing the following steps:

1 From a client, connect to the NAS Manager.

2 On the primary menu, click the **Maintenance** tab.

3 Click **Terminal Services** to create a Terminal Services Advanced Client session with the NAS appliance.

4 Log in to the system as an **Administrator**.

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 click **Apply**.

7   Log off and log in again to the system for the new language MUI to take effect.

Installing and Configuring Support for Other Languages

✍ NOTE: Only install additional language locales if your desired language is not available with MUI support or you need additional locale support.

The Windows Powered operating system that comes installed in the PowerVault 75*x*N can be configured to support the ability to read and write documents in a number of languages. To install the software required to support a specific language, perform the following steps:

1   Insert the *Localization* CD that came with the PowerVault 75*x*N into the CD drive on your NAS appliance.

2   From a client, connect to the NAS Manager.

3   Click the **Maintenance** tab and then click **Terminal Services** to create a Terminal Services Advanced Client session with the NAS appliance.

4   Login to the system as an **Administrator**.

5   Close the **Advanced Administration Menu** by clicking **Exit**.

6   Double-click **My Appliance** on the NAS desktop.

7   Browse to the CD drive and open the *Localization* CD to launch the *Localization* CD's web interface.

8   Click on the **Install Language Locales Not Supported by MUI** link to launch the **Regional Options** control panel.

9   From the **Language Settings for the System** panel, select the languages to be configured.

10 Set the default language for the system by clicking **Select default...**, and then selecting the appropriate language from the drop-down menu. Click **OK**.

11 Click **Apply** to complete the operation.

12　If an **Insert Disk** windows appears, you must perform the following procedure:

　a　Click **OK**.

　b　From the **Files needed** window, click **Browse** and browse to the **i386** directory on the *Localization* CD (if not already selected).

　c　Click **Open** and then click **OK** from the **Insert Disk** window to allow the operating system to find the required files for installation.

13　After the installation is complete, you need to reboot your system.

✍ NOTE: For more information, see the Microsoft Windows Powered operating system's online Help.

Network Adapter Teaming

Adapter teaming allows the system to use the combined throughput of network adapters in parallel to increase performance or provide fault tolerance. Technologies supported by teaming are:

- Link aggregation supports scalable bandwidth up to 800 megabits per second (Mbps) full duplex, or up to eight gigabits per second (Gbps) in a Gigabit Ethernet environment. Link aggregation requires support in the network interface controller (NIC) and the switch.

- Cisco's Fast Ether Channel (FEC) supports scalable bandwidth up to 800 Mbps at full duplex. FEC requires support in the NIC and the switch.

- Broadcom's Smart Load Balance and Fail Over, supported by Broadcom's Advanced Server Program Driver, offers a simple method to team two Alteon or Broadcom Gigabit Ethernet adapters together to provide load balancing and fail over. The program also allows an onboard Intel® NIC to a member of a team to provide fail over only capabilities.

  When you install multiple Alteon or Broadcom Gigabit Ethernet adapters in the same server, you can pair them into teams to provide redundant adapter operation in the event of network failure. You can configure up to two teams, each with two adapters, on each server. If traffic is not seen on the primary adapter connection in a team failure of the adapter, cable, switch port, or switch (where the teamed adapters are attached to separate switches), the secondary team member becomes active, taking the MAC and IP address originally assigned to the primary adapter. Sessions should be maintained, causing no impact to the user.

  ✍ NOTE: Alteon or Broadcom Gigabit Ethernet adapters can be grouped into failover teams with an Intel 82559 LAN on motherboard (LOM); however, assigning a LOM to be a primary adapter is not supported.

Virtual Local Area Networks (VLANs) are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments. Each adapter supports up to 64 VLANs. With multiple VLANs on an adapter, a server with a single adapter can have a logical presence on multiple IP subnets.

NOTE: Adapters that are members of a Failover Team can also be configured to support VLANs. Since VLANs are not supported for an Intel LOM, if an LOM is a member of a Failover Team, VLANs cannot be configured for that team.

- Intel's adaptive load balancing (ALB), supported by Intel's PROSet utility, offers a simple way to increase server throughput up to 400 Mbps using Intel PRO/100 NICs. Outgoing server traffic is balanced automatically among as many as four network adapters. Each additional adapter adds another 100 Mbps link. Since the adapters share the existing Internet protocol (IP) address, the network does not need to be segmented or reconfigured. ALB can also be used over gigabit Ethernet links, providing throughputs up to four Gbps.

  Intel's Intel's PROSet utility also provides support for Adapter Fault Tolerance (AFT), in which a secondary Intel PRO/100 adapter backs up the link between the primary server and the switch for continued operation if the primary link fails.

  When using the Intel PROSet utility with the PowerVault 75xN system, team members are limited to the network connectivity of the system. Valid team members include the 10/100 megabit (Mbit) embedded NIC, optional single-port 10/100 Mbit NIC, and the optional dual-port 10/100 Mbit NIC.

Creating Network Teams Using the Broadcom Advanced Server Control Suite

NOTE: This procedure is for Alteon and Broadcom NICs only.

To create Alteon or Broadcom network teams using the Network Teaming utility, Broadcom Advanced Server Control Suite, perform the following steps:

1 Click **Maintenance**.

2 Click **Terminal Services**.

3 Log in to the **Terminal Services** session as administrator.

4 Under **Administrative Tools** on the **Advanced Administration Menu**, click **Broadcom Network Teaming**. The **Broadcom Advanced Server Control Suite** window will be displayed on the desktop.

5 Click the tab on the **Load Balance/Virtual LAN** folder.

6 Click **Create Team...** .

7   Enter the team name and select the appropriate team mode. The types of team include Smart 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 click > adjacent to **Team Members** to add the adapter. Repeat for the second adapter.

✍ NOTE: Alteon and Broadcom Ethernet adapters can be grouped into failover teams with an Intel 82559 LOM; however, assigning a LOM to be a primary adapter is not supported.

11 Click **OK**.

Removing an Adapter From a Network Team

To remove an adapter from a network team through the Network Teaming utility, Broadcom Advanced Server Control Suite, perform the following steps:

1   Click **Maintenance**.

2   Click **Terminal Services**.

3   Log into the **Terminal Services** session as administrator.

4   Under **Administrative Tools** on the **Advanced Administration Menu**, click **Broadcom Network Teaming**. The **Broadcom Advanced Server Control Suite** window is displayed on the desktop.

5   Click the tab on the **Load Balance/Virtual LAN** folder.

6   Select the team name in the **Configuration** box.

7   Select an adapter in **Team Members** and click < adjacent to **Team Members** to remove the adapter.

8   Click **OK** to apply the change.

Changing the Network Team Mode Using the Broadcom Advanced Server Control Suite

✍ NOTE: This procedure is for Alteon and Broadcom network adapters only.

To change the team mode of an existing Broadcom network team through the Network Teaming utility, Broadcom Advanced Server Program, perform the following steps:

1   On the NAS Manager primary menu, click **Maintenance**.

2   Click **Terminal Services**.

3   Log in to the **Terminal Services** session as administrator.

4   Under **Administrative Tools** on the **Advanced Administration Menu**, click **Broadcom Network Teaming**. The **Broadcom Advanced Server Control Suite** window is displayed on the desktop.

5   Click the tab on the **Load Balance/Virtual LAN** folder.

6   Select the team name in the **Configuration** box.

7   Select the new type of team and click **OK** to apply the change. The types of team include Smart Load Balance and Fail Over, FEC/GEC, and Link Aggregation (IEEE 802.3ad).

Creating Network Teams Using the Intel PROSet Utility

✍ NOTE: This procedure is for Intel network adapters only.

Create network teams through the Network Teaming utility, Intel PROSet II. To access the Network Teaming utility from the NAS Manager, perform the following steps:

1   On the NAS Manager primary menu, click **Maintenance**.

2   Click **Terminal Services**.

3   Log in to the **Terminal Services** session as administrator.

4   Under **Administrative Tools** on the **Advanced Administration Menu**, click **Intel Network Teaming**.

    The Network Teaming utility, **Intel PROSet II**, displays.

5   Click **Action**, click **Add to Team**, and click **Create New Team…**.

    The **Teaming Wizard** displays.

6   Select the type of team to create and click **Next**.

    The types of team include AFT, ALB, FEC, and IEEE 802.3ad.

7   Select the adapters to include with this team and click **Next**.

8   Verify the team contains the appropriate members and click **Finish**.

9   If the team needs to be modified, click **Back**.

Removing Network Teams Using the Intel PROSet Utility

   ✍ NOTE: This procedure is for Intel network adapters only.

Remove network teams through the Network Teaming utility, Intel PROSet II. To access the Network Teaming utility from the NAS Manager, perform the following steps:

1   On the NAS Manager primary menu, click **Maintenance**.

2   Click **Terminal Services**.

3   Log in to the **Terminal Services** session as administrator.

4   Under **Administrative Tools** on the **Advanced Administration Menu**, click **Intel Network Teaming**.

    The Network Teaming utility, **Intel PROSet II**, displays.

5   In the tree view, click the team to remove.

6   Click **Action** and click **Remove**.

Removing an Adapter From a Network Team Using the Intel PROSet Utility

   ✍ NOTE: This procedure is for Intel network adapters only.

Remove an adapter from a network team through the Network Teaming utility, Intel PROSet II. To access the Network Teaming utility from the NAS Manager, perform the following steps:

1   On the NAS Manager primary menu, click **Maintenance**.

2   Click **Terminal Services**.

3   Log in to the **Terminal Services** session as administrator.

4   Under **Administrative Tools** on the **Advanced Administration Menu**, click **Intel Network Teaming**.

    The Network Teaming utility, **Intel PROSet II**, displays.

5   In the tree view, click the adapter to remove.

6   Click **Action** and click **Remove**.

Changing the Network Team Mode Using the Intel PROSet Utility

✎ NOTE: This procedure is for Intel network adapters only.

Change the network team mode through the Network Teaming utility, Intel PROSet II. To access the Network Teaming utility from the NAS Manager, perform the following steps:

1   On the NAS Manager primary menu, click **Maintenance**.

2   Click **Terminal Services**.

3   Log in to the **Terminal Services** session as administrator.

4   Under **Administrative Tools** on the **Advanced Administration Menu**, click **Intel Network Teaming**.

   The Network Teaming utility, **Intel PROSet II**, displays.

5   In the tree view, click the team to modify.

6   Click **Action** and click **Change Team Mode**.

7   In the **Teaming Wizard**, select the type of team to create and click **Next**.

   The types of team include AFT, ALB, FEC, and IEEE 802.3ad.

8   Click **OK** to close.

Services for UNIX

Services for UNIX (SFU) provides the tools needed to integrate UNIX and Windows networks by leveraging existing UNIX network resource 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 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. These tools include:

•   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 on 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 your 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.

UNIX Utilities

UNIX utilities provided with SFU are listed in below.

Table 7-1.   Categories of UNIX Utilities

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 will accept 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. NTLM must be supported on the client side of the login as well, however.

When using NTLM login, users are restricted to local drives on the system they are logged in to. 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 options available are:

- **Authentication** gives you the choices of **NTLM** and **Username/Password**.
- **Auditing** enables you to set event logging to a separate log file, or the Event Log, and set what events to log.
- **Server Settings** enables you to set the following options:
  - Maximum number of simultaneous connections
  - Maximum number of failed login attempts
  - Map < Alt> key to < Ctrl> < A>
  - Telnet Port
  - **Mode of Operation** allows you to choose **Console** or **Stream**.
  - **Default Domain Name** is the domain name that is automatically added to the login username. The default is ".", which disables this feature.
  - **Idle Session Timeout** is the time until an idle session is forcibly disconnected.

- **Terminate all programs when disconnecting** toggles with **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, logon date/time) and either send a message to the session or terminate it.

Services For UNIX MMC Console

SFU UNIX includes a single MMC for managing all of SFU. The MMC provides a cohesive management interface that lets you administer all systems on the network from any console. Further, since SFU supports the Windows Management Interface (WMI), management can be scripted from the command line.

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 perform User Name Mapping either from SFU or by clicking on **NFS** on the **Services** page of the NAS Manager.

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. Given that UNIX user names are case-sensitive, while 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 NIS 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.

In SFU, the **Username Mapping Service** and **NT Authentication Service** can be installed from the NAS appliance's share, **DomainUtils**.

To create User and Group Name Maps, access the **SFU Administration** window. To access the **SFU Administration** window, perform the following steps:

1 From the NAS Manager, click **Maintenance**.

2 Click **Terminal Services**.

3 Log in to **Terminal Services** as administrator.

4 Close the **Advanced Administration Menu.**

5 Click the **Start** button on the desktop task bar.

6 Click **Programs**.

7 Click **Windows Services for UNIX**.

8 Click **Services for UNIX Administration**.

   The **SFU Administration Console** displays.

9 Click **User Name Mapping**.

   The **User Name Mapping on Local Computer** window displays. You can use this window to define your user maps.

Defining Maps

To define simple maps in SFU, select the **Simple Maps** check box and perform the following steps:

1 Specify the **Windows Domain**.

2 Specify the **NIS Domain**.

3 Optionally, specify the **NIS Server**.

4 Click **Apply** to create the maps.

If you are defining advanced maps, you create user and group maps individually. In the NAS Manager, choose **Explict User Maps** or **Explicit Group Maps**. To create advanced maps in SFU, deselect the **Simple Maps** check box and perform the following steps:

1 Specify the **Windows Domain**.

2 Specify the **NIS Domain**.

3 Optionally, specify the **NIS Server**.

4 Create **User Map** or **Group Map** entries.

5 Click **List Windows Users** or **List Windows Groups.**

6   Click **List UNIX Users** or **List UNIX Groups**.

    This action refreshes your NIS and Windows maps.

7   Create map entries by selecting a Windows user/group from the list and a UNIX user
    (UID)/group (GID) from the list and clicking **Add**.

Map Maintenance

You can maintain your maps from the **User Name Mapping** tree of the SFU window. Map
maintenance allows you to save currently defined maps and to restore saved maps.

To back up the currently defined maps, perform the following steps:

1   From the SFU window, click **User Name Mapping**.

2   Click **Map Maintenance**.

3   Specify a name and location of a file in which to back up the maps.

4   Click **Backup**.

To restore the a previously backed up set of maps, perform the following steps:

1   From the SFU window, click **User Name Mapping**.

2   Click **Map Maintenance**.

3   Specify the name and location of the file that contains the saved maps.

4   Click **Restore**.

Basic Scenarios

For UNIX and Windows NT Username Mapping, an NIS Server must already exist in the
UNIX environment. Username Mapping associates NIS users and groups to
Windows NT users and groups. There are two types of maps that can be used; simple and
advanced. Simple maps define a one-to-one relationship between same name users and
groups. Advanced maps define a relationship between dissimilar names and groups.

Workgroup

In the Workgroup scenario, you configure Username Mapping locally on the PowerVault
75*x*N system. All maps are contained on this system.

Domain

In the Domain scenario, you configure Username Mapping on the domain controller. The Username Mapping Service and the NT Authentication Service must be installed on the Domain Controller. If multiple Domain Controllers are present, NT Authentication must be installed on each Domain Controller.

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.

Microsoft UAM Volume

A user authentication map (UAM) is a software program that prompts users for an account name and password before they log on to a server. The Macintosh **Chooser** has a standard UAM built in, which 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 5.0, you must have a Macintosh client running AppleShare Client 3.8 or newer or Mac OS 8.5 or newer. If you do not meet these minimum requirements, the Microsoft UAM Installer will install the old Microsoft UAM 1.0 module. If you upgrade your system software, you will need to re-run the Microsoft UAM Installer.

Installing User Authentication

Log on to the Microsoft UAM Volume on the system to access the MS UAM file. Then drag this file to the AppleShare Folder in your System Folder.

To gain access to the Microsoft Authentication files on the system, perform the following steps:

1 Click **Chooser** on the **Macintosh Apple** menu.

2 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.

3 Select the system from the list of file servers, and click **OK**.

4 Click **Registered User** or **Guest**, and then click **OK**.

5 Select the **Microsoft UAM Volume**, and then click **OK**.

6 Close the **Chooser** dialog box.

To install the authentication files on the Macintosh workstation, perform the following steps:

1 Double-click the **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 will report whether the installation succeeded.

If the installation has succeeded, Macintosh users of this workstation will be offered Microsoft Authentication when they connect to the system.

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 Filers with multiple network adapters, perform the following steps from the NAS Manager:

1 On the NAS Manager primary menu, click **Maintenance**.

2 Click **Interfaces**.

3 Click the radio button next to the adapter you want to use for the AppleTalk protocol.

4   On the **Tasks** menu, click **AppleTalk**.

5   Click the check box next to **Enable inbound AppleTalk connections on this adapter**.

6   (Optional) If you use AppleTalk zones, select the appropriate zone in the dropdown box.

7   Click **OK**.

Services for 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.

Configuring the NWLink IPX/SPX Compatible Protocol

To configure this protocol, you need the internal network number, the frame type, and the network number.

Internal Network Number

Internal network numbers are used for internal routing and are generally only needed 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 autodetect the frame type for the client. In most cases, this is successful. However, occasionally the autodetect feature chooses 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 that if more than one frame type exists, choose the one that would be detected first. For example, if frame type Ethernet 802.2 and Ethernet 802.3 are bound to the same segment, then configure frame type Ethernet 802.2. The order of detection is Ethernet 802.2, Ethernet 802.3, Ethernet II, and then Ethernet SNAP.

Microsoft Directory Synchronization Services

Microsoft Directory Synchronization Services (MSDSS) lets you 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:

- 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, to install MSDSS, and then to import information from the existing NetWare environment.

The larger the environment, the more new servers you will need. If you are planning to have more than one domain, then you will 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 gain access to 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 in order to use 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 today. MSDSS works in all these 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 free up the hardware for the Windows 2000 Server operating system.

Outline of the 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 need to adapt the guidelines to suit your environment and goals.

Small Environment

A small company with a LAN-based and uncomplicated network is often a likely candidate for a quick migration. After doing all the preparations described in the above section, perform these 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 comes with your operating system software).

3 Install the Novell Client for Windows 2000 from the Novell Web site (**http://www.novell.com/download/**).

4 Replace services or applications that require NDS with software compatible with Active Directory. (NDS applications should be moved 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 \\<Dell*xxxxxxx*>\DomainUtils where <Dell*xxxxxxx*> is the name of the PowerVault 75xN system.

6 Log on to the NDS tree or bindery server as Administrator.

7 Log on 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 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 will 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 will 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 will also run the File Migration utility.

   e Specify the path to the **Active Directory container** into 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 **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 select **custom object mapping**, you will be 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 as described in the **Help** printout "To migrate files." The prompts will 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 right converts, by default, to **Read** because it does not have an equivalent NFTS 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 indicates **Unavailable**, then you are not currently logged on to that tree or Bindery server. Log on, and then press < F5> after reselecting the volume to view the directories within the displayed volume.

- On the **Step 4** - **Log File** tab, choose 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 respectively under **NetWare scan logs** and **Windows scan logs**. You can select a number of acceptable errors; if this number is exceeded, the process aborts, letting you 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 will 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 the users know how to handle their password for the first time they log on (for possible password options, see "MSDSS Password Management" in "MSDSS Deployment: Understanding Synchronization and Migration)" available at **http://www.microsoft.com**.

Medium-Sized or Large Environment

An organization large enough to have WAN links will probably choose either to synchronize its networks temporarily while performing a gradual migration over time (up to three months for a large network), or it will prefer 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 comes with your operating system software).

3   Install the Novell Client for Windows 2000 from the Novell Web site **http://www.novell.com/download/**.

4   Install MSDSS from the PowerVault 75*x*N system **DomainUtils** share.

✍ NOTE: To access MSDSS software, map a network drive to \\<Dell*xxxxxxx*>\DomainUtils where <Dell*xxxxxxx*> is the name of the PowerVault 75*x*N system.

5   Log on to the NDS tree or Bindery server with administrative credentials.

6   Log on 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 and point to **Programs—> Administrative Tools—> Directory Synchronization** to start MSDSS, and let the prompts 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 **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 (for NDS only) click **Custom** and then **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 chose one-way synchronization, you should now perform all user, group, and 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, computers, and/or files. If you plan to continue by migrating in stages from NetWare to Active Directory, do the following in the time-frame that is convenient for you:

   •   Install and configure File and Print Services for NetWare (to let NetWare clients access files and printers on Windows 2000 servers) and Gateway Services for NetWare (to let 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 further information see the Novell Web site, **http://support.novell.com/servlet/Knowledgebase** and the Windows 2000 Web site, **http://www.microsoft.com/windows2000**.

Uninterruptible Power Supply (UPS)

When you are in **Terminal Services Advanced Client**, you can control the settings for your UPS. In **Power Options** on the **Control Panel**, the operating system includes default settings for an American Power Conversion Uninterruptible Power Supply.

The default settings are:

   •   Enable all notifications.

      –   Seconds between power failure and first notification: 5
      –   Seconds between subsequent power failure notifications: 120

   •   Shut down when the UPS battery is almost exhausted.

   •   Turn off the UPS.

If you are using a UPS and want to change these settings, you need to connect a keyboard, mouse, and monitor to the system. See Microsoft Windows 2000 Help for more information.

The system is configured to accept a serial connection from the UPS in serial port 2, called the UPS port in the *Dell PowerVault 750N Systems Installation and Troubleshooting Guide* and the *Dell PowerVault 755N Systems Installation and Troubleshooting Guide*. By default, this serial port is configured to interact with APC Smart-UPS systems.

See the documentation for your UPS for more information on how to use it.

Upgrading to a Multiprocessor System

When upgrading your PowerVault 75*x*N NAS appliance from microprocessor to two microprocessors, the hardware abstraction layer (HAL) must be updated to enable your system to use the extra processor.

✎ NOTE: If your system contained two processors when you received it, you do not need to perform this procedure.

✎ NOTE: If you have a two-processor system and reinstall the operating system from the *Reinstallation* CD, you do not need to perform this procedure. The operating system reinstall includes this upgrade.

To update the HAL file on your NAS appliance follow the following procedure:

1   Open the NAS Manager, and click the **Maintenance** tab.

2   Click **Terminal Services**.

3   When prompted, log on to a **Terminal Services Advanced Client** session.

4   In the **PowerVault Advanced Administration Menu**, click **Administrative Tools** and then click **Computer Management** to launch the Computer Management Console.

5   In the left panel, browse to **Computer Management (local)—> System Tools—> Device Manager**.

6   In the right panel, double-click **Computer** to expand the branch. Ensure that you have **ACPI Uniprocessor PC** support.

7   Double-click the computer type (**ACPI Uniprocessor PC**) that is listed under the **Computer** branch, click the **Drivers** tab, click **Update Driver**, and then click **Next**.

8   Click **Display a list of known drivers for this device**.

9   Click the appropriate computer type (**ACPI Multiprocessor PC**), click **Next**, and then click **Finish**.

10   When prompted, click **yes** to **reboot** your system.

Using Secured Socket Layers

This section explains how secured socket layers (SSL) are used in the NAS appliance. 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 that is used to establishing 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 a Secure Sockets Layer (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 that allows you to positively identify them before allowing them access to the site. *Server certificates* contain information about the server that 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 Web site might be hesitant to provide credit card information, despite having viewed the contents of your company's server certificate. This may 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 (CA). 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 Web site 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 may 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 750N/755N Certificate

By default, the PowerVault 750N/755N 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 (CA) is present in the network, the Administrator can choose to change the default PowerVault 750N/755N certificate. The Administrator must then use the wizards to first request a certificate and then apply it to the appliance.

Obtaining a Server Certificate From a Certification Authority

✍ NOTE: If you are replacing your current server certificate, the Internet Information Services (IIS) will continue 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, visit the Microsoft Security Web site. In the **By Category** list, select **Certification Authority Services**.

To obtain a server certificate, perform the following steps:

1 On the PowerVault NAS Manager primary menu, click **Maintenance.**

2 On the **Maintenance** page, click **Terminal Services**.

3 Log on to an Terminal Services Advanced Client session.

4 In the **Advanced Administration Menu**, click **System Management,** and then from the list, click **Internet Information Services**

5 Navigate to and right-click on the **Administration site** section, and 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.

They will process the request and send you the certificate.

📝 NOTE: Some certification authorities require you to prove your identify 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 Services online help.

Console Redirection

Console redirection allows you to maintain a NAS appliance from a remote location by redirecting keyboard input and text output through the serial port. Graphic output is not redirected. Console redirection can be used under the disk operating system (DOS) for tasks such as setting up a common basic input/output system (BIOS) configuration or setting up a redundant array of independent disks (RAID) configuration. In a typical installation, the system is connected to a port concentrator that allows you to connect several systems via a shared modem. After you use a modem or other remote connection to log into the port concentrator, you can select which system you want to manage with console redirection. This document describes the simplest connection possible: connecting to a system with a null modem cable.

Minimum Hardware and Connection Requirements

To use console redirection, you must have the following:

- An available serial port (COM port) on a client system (This port must not conflict with any other ports on the system.)

- Available serial port 1 (COM 1) on the NAS appliance

  ✍ NOTE: Console Redirection is enabled by default in the NAS appliance BIOS.

- A null modem cable to connect the server to the client system

Software Requirements

Your remote terminal emulation software should meet the following specifications:

- American National Standards Institute (ANSI) or VT100/220 terminal emulation with a window size of 80 x 25 characters

- 9600, 19.2K, 57.6K, or 115.2K bits per second (bps) via serial (COM) ports

- Recommended: the ability to create keyboard command macros

All versions of the Microsoft® Windows® operating systems come with HyperTerminal terminal emulation software. However, the version of HyperTerminal included with most Windows operating systems does not provide the correct screen size, the arrow and function keys do not work, and there is no method of creating macros. It is recommended that you either upgrade your version of HyperTerminal to HyperTerminal Private Edition 6.1 or later or select new terminal emulation software. You may be eligible for a free upgrade from your current version of HyperTerminal from Hilgraeve at **http://www.hilgraeve.com**.

Configuring Console Redirection on the System

Console redirection is enabled by default for VT100/220 using serial port 1 (COM 1). If you decide to reconfigure console redirection or disable it, go through the system setup program. The **Console Redirection** field allows you to select only the terminal type. The options available are listed in Table 7-2.

Table 7-2. Terminal Emulation Types

Terminal Type	Terminal Emulation
ANSI	ANSI. Used for utility partition applications or MS-DOS.
VT100/220	VT100/220. Used for utility partition applications or MS-DOS.

If you select **VT100/220** but not all the characters are visible on the screen, you should go back to the system setup program and select **ANSI** as your terminal type. ANSI can display the full set of ASCII characters.

Configuring Console Redirection on the Client System

✏️ NOTE: The examples in this document assume that you have upgraded to Hilgraeve's HyperTerminal Private Edition 6.1 or later. If you are using other terminal emulation software, see the help file for that software.

Configuring the Ports

1 Click the **Start** button, point to **Programs—> Accessories—> Communications**, and click **HyperTerminal**.

2 Enter any name for the new connection and select any icon.

3 Click **OK**.

4 From the **Connect to** pulldown menu, select a COM port available on your client system and click **OK**.

   After you have selected an available COM port, the COM port properties window is displayed.

5 Select **Bits per second**.

   Console redirection supports 9600, 19.2K, 57.6K, or 115.2K bps.

6 Set **Data bits** to **8**.

7 Set **Parity** to **None**.

8 Set **Stop bits** to **1**.

9 Set **Flow control** to **Hardware**.

10 Click **OK**.

Configuring the Terminal Settings

After you configure the ports, configure the terminal settings by performing the following steps:

1 In HyperTerminal, click **File**, click **Properties**, and select the **Settings** tab.

2 Make sure that the **Function, arrow, and ctrl keys act as** field is set to **Terminal Keys**.

3 Make sure that the **Backspace key sends** field is set to **Ctrl+H**.

4 Change the **Emulation** setting from **Auto detect** to **ANSI** or **VT100/220.**

This setting should be the same as the setting you selected for the **Console Redirection** field on the server.

When you click **Terminal Setup**, you should see a setting for the number of rows and columns.

5 Change the number of rows from 24 to 25 and leave the number of columns at 80. If you do not have these settings, then this is an indication that you must upgrade your terminal emulation software.

Rebooting the System

Console redirection is designed to yield control of the serial ports to the operating system, which allows serial debugging and redirection of the operating system to function correctly without interference from the system BIOS.

To use console redirection to shut down a system and troubleshoot it or to change small computer system interface (SCSI) BIOS configurations, perform the following steps:

1 Restart the system. See "Configuring Special Keys," found later in this document, for a recommendation on how to do this.

2 When the system begins to reboot, use console redirection to watch and interact with the system during the power-on self-test (POST). While the system is booting, you can do the following:

- Enter the system setup program.
- Enter the SCSI setup menus.

Configuring Special Keys

Console redirection uses ANSI or VT100/220 terminal emulation, which are limited to basic ASCII characters. There are no function keys, arrow keys, or control keys in this character set. However, most BIOS software requires the use of function keys and control keys for ordinary functions. You can emulate a function key or control key by using a special key sequence, called an escape sequence, to represent a specific key.

For console redirection, an escape sequence starts with an escape character. This character can be entered in a number of different ways, depending on the requirements of your terminal emulation software. For example, 0x1b, ^ [, and <Esc> all refer to the same escape character. Some terminal software uses predefined macros to send the proper escape sequences. In HyperTerminal, you can define macros by selecting **Key Macros** from the **View** menu. Macros can be assigned to almost any possible key for almost any key combination. Create a macro for each of your function keys. Table 7-3 and Table 7-4 list the escape sequence that must be sent to represent a special key or command.

📝 NOTE: When defining macros in HyperTerminal, you must press <Ins> before <Esc> to signify that you are sending an escape sequence rather than escaping out of the dialog box.

Table 7-3.   VT100/220 Supported Escape Sequences

Key	Supported Sequences	Terminal Emulation
Up arrow	<Esc> [<Shift> a	VT100/220
Down arrow	<Esc> [<Shift> b	VT100/220
Right arrow	<Esc> [<Shift> c	VT100/220
Left arrow	<Esc> [<Shift> d	VT100/220
F1	<Esc> <Shift> op	VT100/220
F2	<Esc> <Shift> oq	VT100/220
F3	<Esc> <Shift> or	VT100/220
F4	<Esc> <Shift> os	VT100/220
F5	<Esc> <Shift> ot	VT100
F6	<Esc> <Shift> ou <Esc> [1 7 ~	VT100 VT100/220
F7	<Esc> <Shift> ov <Esc> [1 8 ~	VT100 VT100/220
F8	<Esc> <Shift> ow <Esc> [1 9 ~	VT100 VT100/220
F9	<Esc> <Shift> ox <Esc> [2 0 ~	VT100 VT100/220
F10	<Esc> <Shift> oy <Esc> [2 1 ~	VT100 VT100/220

Table 7-3.   VT100/220 Supported Escape Sequences

Key	Supported Sequences	Terminal Emulation
F11	<Esc> <Shift>oz <Esc> [2 3 ~	VT100 VT100/220
F12	<Esc> <Shift>oa <Esc> [2 4 ~	VT100 VT100/220
Home	<Esc> [1 ~	VT220
End	<Esc> [4 ~	VT220
Insert	<Esc> [2 ~	VT220
Delete	<Esc> [3 ~	VT220
Page Up	<Esc> [5 ~	VT220
Page Down	<Esc> [6 ~	VT220
Shift-Tab	<Esc> [<Shift>z <Esc> [0 <Shift>z	VT100 VT220

Table 7-4.   ANSI Supported Escape Sequences

Key	Supported Sequences
Up arrow	<Esc> [<Shift>a
Down arrow	<Esc> [<Shift>b
Right arrow	<Esc> [<Shift>c
Left arrow	<Esc> [<Shift>d
F1	<Esc> <Shift>op
F2	<Esc> <Shift>oq
F3	<Esc> <Shift>or
F4	<Esc> <Shift>os
F5	<Esc> <Shift>ot
F6	<Esc> <Shift>ou
F7	<Esc> <Shift>ov

Table 7-4.   ANSI Supported Escape Sequences

Key	Supported Sequences
F8	<Esc> <Shift>ow
F9	<Esc> <Shift>ox
F10	<Esc> <Shift>oy
F11	<Esc> <Shift>oz
F12	<Esc> <Shift>oa

After you create these macros, pressing <F1> on the keyboard while running the terminal emulation software sends <Esc><Shift>op to the system. When these three characters are transmitted, the system interprets them as <F1>. You need this functionality to change the settings in the System Setup program or to continue if there is an error on your system and you are prompted to press <F1>.

In addition to macros for the function keys, it is recommended that you set up macros for the additional escape sequences listed in Table 7-5.

.

Table 7-5.   Additional Escape Sequences

Key Combination	Supported Sequence
<Alt> *key*	<Esc> *key*
<Ctrl><Alt><Del>	<Esc> <Shift>r <Esc> r <Esc> <Shift>r (This combination reboots the server.)
<Ctrl><Shift>i	<Esc> <Ctrl><Shift>i
<Ctrl <Shift>j	<Esc> <Ctrl><Shift>j
<Ctrl><Shift>h	<Esc> <Ctrl><Shift>h
<Ctrl><Shift>m	<Esc> <Ctrl><Shift>m
<Ctrl>2	<Esc> <Ctrl>2

Defragmenting a Volume Containing Persistent Images

⊃ NOTICE: Defragmenting a volume containing persistent images without using the following procedure can delete your persistent images and will degrade your system performance.

🖉 NOTE: If you do not have persistent images on your volume, this procedure does not apply.

🖉 NOTE: To defragment a volume, you must delete all persistent images on that volume.

To defragment a volume containing persistent images, perform the following steps:

1 On the NAS Manager primary menu, click **Disks**.

2 Click **ActiveArchive**.

3 Click **Schedules**.

4 Select a scheduled persistent image and click **Delete**.

5 Repeat until all scheduled persistent images are deleted.

6 Click **Back**.

7 Click **Persistent Images**.

8 Select a persistent image and click **Delete**.

9 Repeat until all persistent images are deleted.

10 Click **Maintenance**.

11 Click **Terminal Services**.

12 Log in to the system.

13 Click **Exit** to close the **Advanced Administration Menu**.

14 Double-click **My Appliance**.

15 Right-click the drive you are going to defragment.

16 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.

SECTION 8

Online Server Diagnostics

Dell OpenManage™ Server Diagnostics is a suite of diagnostic programs that run locally on your Dell™ PowerVault™ NAS appliance or remotely on a NAS appliance connected to the network. You select diagnostic tests to run from a hierarchical menu that represents a NAS appliance's hardware. You can select tests for various parts of an appliance and run them simultaneously or sequentially in a single session. You can view results for each individually selected test module.

Server Diagnostics diagnoses problems on individual appliances. It does not address problems that arise on the network level, unless the problem resides with a specific network interface controller (NIC) on a single appliance.

Features

Server Diagnostics offers test modules for the following appliance components. Some tests can be run only on the local system.

- Microprocessor
- Hard-disk drive
- Diskette drive
- DVD/CD drive
- Tape drive
- Memory
- Peripheral component interconnect (PCI) bus
- Modem
- Small computer system interface (SCSI)
- Serial port
- Parallel port
- Self-monitoring, analysis, and reporting technology (SMART) drive
- Extended SMART drive
- NIC
- Complimentary metal-oxide semiconductor (CMOS)
- Keyboard (local system only)
- Mouse (local system only)

- Monitor (local system only)
- Printer (local system only)
- Video (local system only)

Installing the Online Server Diagnostics

📝 NOTE: To perform these steps you must be using a NAS Manager Terminal Services Advanced Client session.

To log on to a Terminal Services Advanced Client session, perform the following steps:

1 Log on to the NAS Manager.

2 On the NAS Manager primary menu, click the **Maintenance** tab.

3 On the **Maintenance** page, click **Terminal Services**.

4 Log in to a **Terminal Services Advanced Client** session.

5 In the **Advanced Administration Menu** window, click **Exit** and then **OK** to close the window and return you to the NAS desktop.

To install the Server Diagnostics, perform the following steps:

1 Insert the *Dell PowerVault 75xN Resource* CD into the CD drive of your NAS appliance.

2 If the installation program does not start automatically, click the **Start** button and click **Run**.

3 In the **Run** dialog box, click **Browse**, double-click the CD, and double-click **setup.exe**.

4 Click **Next** to display the *Resource* CD menu.

5 Click **Resources**.

6 Click **Install Dell Online Server Diagnostics** to launch the **InstallShield Wizard**.

7 In the **InstallShield Wizard** window, click **Next**.

8 Read the software license agreement and click **Yes** if you accept the terms of the agreement.

9 Enter you name and the company name and then click **Next**.

10 Click **Next**.

11 Click **Next** to add program icons.

12   Click **Next**.

13   When the **InstallShield Wizard** completes installing the files, click **Finish**.

Installing the JAVA Runtime Environment

If your system does not have the Java 2 Runtime Environment installed on it, you will be asked whether you want to install it the first time you run the Online Server Diagnostics.

1   Because the Java 2 Runtime Environment is needed to run the Online Server Diagnostics, click **Yes**.

2   Click **Yes** to accept the agreement.

3   Click **Next**.

   After the installation is completed, you can run the Online Server Diagnostics.

Using the Online Server Diagnostics

This section explains how to start, configure, and run your server diagnostics:

Starting the Online Server Diagnostics

To start the diagnostics, perform one of the following procedures:

1   On the NAS Manager primary menu, click **Maintenance**.

2   Click **Online Server Diagnostics**.

Specifying a Target Appliance

   NOTE: Online Server Diagnostics must be installed on both the remote appliance and the local appliance.

To specify the NAS appliance on which you want to run diagnostic tests (the target), perform the following steps:

If you have not already done so, start the diagnostics.

In the **Welcome** window, perform one of the following tasks:

• To run diagnostics on the local server, click **Run diagnostics on NNN.NNN.NNN.NNN**.

- To run diagnostics on a remote appliance on the network, specify the IP address of the remote appliance in the **Remote IP Address** box, and then click **Run diagnostics on specified IP**.

  In the remote login window, type the user ID of a local administrator group member for the specified appliance in the **User Name** box, and click **Login**.

  This action opens the main window, from which you may select and run diagnostic tests.

Configuring Online Server Diagnostics

Server Diagnostics enables you to set the preferred options for running diagnostic tests.

To set the options in Server Diagnostics, perform the following steps:

1 If you have not already done so, start the Server Diagnostics.

2 Specify a target NAS appliance.

3 In the main window, click **Advanced Settings**.

4 In the **Advanced Settings** window, set the options you need. See "Advanced Settings" for a description of each option.

Running Online Server Diagnostics

To run a diagnostic, perform the following steps:

1 If you have not already done so, start the Server Diagnostics.

2 Specify a target NAS appliance.

3 In the main diagnostics window, use the component selector to specify the components you want to test.

   - Use the diagnostic tree to select the individual tests you want to run.

   - Click **Select All** to select all tests in the tree. To erase your selections, click **Clear All**.

4 Click **Next**.

   The **Progress** window opens and the diagnostic tests begin. Use the progress viewer to monitor the success or failure of each test.

5 When the tests finish, click **View Log** to see detailed results for each test.

6   If a test fails, click **View Details** to see a brief description of why the test failed.

🡆 NOTICE: Do not use your browser's refresh function while running Server Diagnostics. This function closes the **Server Diagnostics** window without stopping the test and causes the following error message to be displayed: `The diagnostic engine is busy. This may be due to either an improper logoff or someone else running the diagnostics on this machine. In the case of an improper logoff, please wait xx minutes for the diagnostic engine to time out. (XX is the Default_timeout setting, which is initially set to 10 minutes.) Click here to close this window.`

Exiting Diagnostics

To exit the Server Diagnostics program, click **Logoff**.

📝 NOTE: If you close the server diagnostics window without clicking **Logoff**, you must either wait 10 minutes or log off your system completely before you can restart Server Diagnostics.

For further information, refer to the Online Help available within the Server Diagnostics.

Learning About Diagnostic Tests

To get detailed information about specific diagnostic tests, perform the following steps:

1   If you have not already done so, start the Server Diagnostics.

2   Specify a target NAS appliance.

3   In the main window, use the component selector to specify the component that you want to test.

4   Click **Learn More** to open a secondary window that describes the tests available for the selected component.

9

SECTION 9

Troubleshooting

Table 9-1. Troubleshooting Issues

Issue	Possible cause	Resolution
I cannot access my Dell ActiveArchive™ from an NFS or Macintosh Client.	Only Microsoft® Windows® (CIFS) clients can access the persistent images stored in the ActiveArchive folders for each volume.	Access ActiveArchive folders through the Windows client to perform data recovery.
I am trying to select the **Administer My Appliance** link on the opening page of the PowerVault 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 people without administrator privileges.	Type the address of the PowerVault NAS Manager manually in your browser. Type http://<*server-name or IP address*>:1278 for non-SSL connections and https://<*server-name or IP address*>:1279 for SSL connections.
XCOPY will not copy my persistent images.	Dell ActiveArchive is enabled. XCOPY will not read the persistent images on a volume.	Do not use XCOPY to copy persistent images.
I have just deleted a volume in Dell OpenManage™ Array Manager and now I am unable to view my shares in the PowerVault NAS Manager.	In the event that a volume with shares is deleted, PowerVault NAS Manager will not 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 PowerVault NAS Manager and restart. Shares should be visible.
I have just added an HTTP share but cannot see it from PowerVault 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 for security purposes.	To enable directory sharing for an HTTP share, from the PowerVault NAS Manager **Maintenance** page, click **Terminal Services Advanced Client** and modify the Web sharing properties of the folder.

Table 9-1.   Troubleshooting Issues

Issue	Possible cause	Resolution
I am getting event errors for Services for Macintosh.	Services for Macintosh are bound to the onboard network interface card (NIC) by default. If this NIC has been disabled, binding errors will occur.	Bind the AppleTalk protocol to an enabled NIC. See "AppleTalk Protocol Adapter Binding."
I configured the system using Kick-Start and I cannot get to the PowerVault NAS Manager using a browser.	The system may not be connected to the network, or the network settings may not be correct.	Check to make sure that the system is connected to the network. If it is, then check to make sure that you entered a correct IP address in the Kick-Start Application Menu. If the problem persists, use the serial port as described in the "Configuring Your System Using a Serial Connection" to access the PowerVault NAS Manager and check that the configuration settings were correct.
From a Macintosh client, users cannot modify or delete a file that a Windows client has accessed.	The time is not properly synchronized between clients and the system.	Make sure that clients have their time synchronized within ten minutes relative to the time zone.
I rebooted through the PowerVault NAS Manager from a Macintosh client. Several minutes have passed and the page has not refreshed.	PowerVault NAS Manager does not automatically refresh the screen when the NAS appliance has finished rebooting.	Close Internet Explorer and then reconnect to the PowerVault NAS Manager.
I just created a new volume on my system but cannot see the volume on **Windows Explorer** through **Terminal Services**.	**Terminal Services** will not update to show a new volume during the session in which it was created.	Exit from **Terminal Services** and reconnect. The volume should now be visible.

Table 9-1.   Troubleshooting Issues

Issue	Possible cause	Resolution
Every time I try to do a directory listing from an NFS client on the root of a system volume, I get an error message, usually `Permission Denied.`	The problem you will experience has to do with a System Volume Information directory, created by Microsoft Index Server. The NFS service does not have access to this directory, and returns an error 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.
I have just changed the IP address of my system and now I cannot administrate it through PowerVault NAS Manager.	Although the IP address changed, your local host is still trying to communicate with the system using the old IP address.	Close Microsoft Internet Explorer (or for Linux only, Netscape 6.0 or later). Re-start the PowerVault NAS Manager.
In PowerVault NAS Manager if I click **OK** and then click **Cancel**, it doesn't seem to cancel the operation.	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.
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 Web site.	Connect to the system via **Terminal Services Advanced Client** and open a local command prompt. Enter the following: `WINMGMT/CLEARADAP.` When the prompt returns, enter `WINMGMT/RESYNCPERF winmgmt service PID.`
I have noticed that my Dell OpenManage Array Manager Log file has exceeded it's maximum log size.	The maximum log file size has been exceeded because the notification message can not be seen and cleared through **Terminal Services** or PowerVault NAS Manager.	Use Dell OpenManage Array Manager to clear the logs periodically.

Table 9-1. Troubleshooting Issues

Issue	Possible cause	Resolution
I have tried logging on to my Dell OpenManage Remote Assistant Card (DRAC) through the Web console software and I cannot log on. I configured my DRAC using the PowerVault **Advanced Administration Menu** and I can ping the IP address I assigned the card. What should I do?	There are spaces before or after the user name or password entries.	Reedit the configuration file to ensure there are no spaces before or after any of the user and password entries.
I get a password prompt when navigating through Local Groups in the PowerVault 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 be displayed in the future.
When I select the **Check All** box and then deselect one or more choices on some screens in the PowerVault NAS Manager, the **Check All** box remains selected	The **Check All** box does not automatically deselect. This does not indicate 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 rebooted my NAS appliance from a Macintosh client, but several minutes have passed and my NAS appliance has not rebooted.	The most likely cause is that the NAS appliance has come back online but the client screen has not refreshed.	Close Internet Explorer and reconnect to the NAS appliance. The NAS appliance should behave normally.
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 PowerVault NAS Manager does not automatically refresh the account information for the administrator while in the PowerVault NAS Manager. Instead, it does the refresh as a timed function.	The password was successfully changed. If you want to confirm that the new password is in affect, close the browser and then reconnect. The new password should work, but the old one should not.

Table 9-1. Troubleshooting Issues

Issue	Possible cause	Resolution
I have just brought my new NAS appliance up 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 get to 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 appliance. 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 PowerVault NAS Manager.	Manually remove this listing from the listed shared folders in the FTP section of the MMC.
I cannot use the **Back** button in Netscape Navigator for the Online Help in the PowerVault NAS Manager.	This feature is not supported.	Use the **Previous Topic** link to navigate back to earlier topics.
I am using Netscape Navigator to administer my NAS appliance through the PowerVault 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: • Wait for the page to finish loading • Refresh the page several times.

Table 9-1. Troubleshooting Issues

Issue	Possible cause	Resolution
I am looking for a topic on t he context sensitive online help in the PowerVault NAS Manager, but it says `No Topic Available.`	Some sections of the PowerVault NAS Manager do not have context sensitive help.	For information relating to a specific function, see the Windows Powered Help, which is available by clicking Windows Powered Help on the Advanced Administration Menu that is available through Terminal Services, or see the appropriate section in this *Administrator's Guide*.
I cannot see my persistent images.	Persistent images reside in the ActiveArchive directory, which is a hidden folder.	Configure your system to view hidden files and folders.
I cannot take persistent images of my file system.	The cache file is still being created.	Wait until the cache file is created and then attempt to take the persistent image again. To confirm that the persistent image cache file has been created, check the **Status Area** of the **ActiveArchive** section of the PowerVault NAS Manager.
I cannot take persistent images of my file system.	The cache file is full.	Delete one or more persistent images until sufficient space is free in the cache file to create the additional persistent images.
I cannot take a persistent image of my **C:** drive.	A persistent image cannot be taken of the **C:** drive.	Taking a persistent image of the **C:** drive is not supported.
I notice that the date and time for the ActiveArchive directory changes every time I reboot my NAS appliance.	The ActiveArchive directory date and time are reset at each reboot. The new dates and times do not mean that the dates and times of your persistent images have been altered.	Take no action. This is the normal functionality of Dell ActiveArchive.

Table 9-1. Troubleshooting Issues

Issue	Possible cause	Resolution
I have deleted a persistent image, but when the Persistent Images page redisplays 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 PowerVault 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.
I tried to clear the FTP log or the Web (HTTP) Shares log in the Maintenance section of the PowerVault NAS Manager, but I received an error message and the log was not cleared.	These logs are currently locked by the NAS appliance for the FTP service and to support the PowerVault NAS Manager. These logs cannot be cleared in the PowerVault NAS Manager.	Connect to the NAS appliance using Terminal Services and clear these logs 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 in the **General** area and the page did not refresh properly.	Select **Cancel** or click **Back** of your browser. Next, reselect the user for whom you wanted to view properties.
While updating client access to an NFS share, the option to select **No Access** is displayed, but the option to select **Root** is not.	Only the **All Machines** category options are displayed during this update.	Add the appropriate clients and 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**.
From a Macintosh client, I cannot connect to the administration part of the PowerVault NAS Manager using the **Administer This Appliance** link on the **HTTP Shares** page of the PowerVault NAS Manager.	The internally generated certificate is not supported by Internet Explorer for Macintosh.	You can administer the NAS appliance using the address HTTP://<*servername*>:1278; however, this is a nonsecure link.

Table 9-1. Troubleshooting Issues

Issue	Possible cause	Resolution
I added members to a local group using the PowerVault NAS Manager, but when I click the **OK** button, the screen only refreshes.	You might have removed and then added the same member to the local group. This might cause the screen to refresh instead of updating correctly.	Reselect the Local Groups tab in the PowerVault NAS Manager menu bar. Next, add or remove the appropriate members to or from the local group.
After using Terminal Services to connect to my NAS appliance, I am unable to type in my native language.	The NAS appliance is set to English, the default language	You can install your native language character set from the Localization CD that was shipped with your system. For installation instructions, see "Advanced Features" in this *Administrator's Guide*.

Index

volume *(continued)*
    creating, 3-2
    deleting, 3-2, 3-18
    expanding, 3-3
    formatting, 3-17

W

warnings, 13

warranty information, 11

Windows 2000
    backup and recovery tools, 5-6
    help, 2-3
    installing tape drives, 5-12