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

Initial Configuration
NAS Manager
Advanced Disk and Volume Management
Systems Management
Backing Up the System
Recovering and Restoring the System
Shadow Copies
Advanced Features
Security Recommendations
Troubleshooting

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

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

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

Initial Release 15 Aug 2003

Back to Contents Page

Initial Configuration

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

- Configuring Your NAS System for the First Time
- Configuring Your NAS System Automatically on a Network (With DHCP)
- Configuring Your System Using a Keyboard, Monitor, and Mouse
- Other Documents You May Need

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

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

Configuring Your NAS System for the First Time

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

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

- If DHCP is implemented on your network, your system automatically configures the network settings. If you are unsure whether your network uses DHCP, contact your network administrator. See "Configuring Your NAS System Automatically on a Network (With DHCP)."
- You can use a keyboard, monitor, and mouse connected directly to the NAS system. See "Configuring Your System Using a Keyboard, Monitor, and Mouse."

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

1. Connect one end of the power cable to the NAS system and the other end to a power source.
2. Connect one end of an Ethernet cable into one of the 10/100/1000 RJ-45 NIC connectors (see Figure 1-1) on the back of your NAS system.

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

   NOTE: On PowerVault 775N systems, three RJ-45 NIC connectors are on the back panel. However, only the two connectors located in the center of the system's back panel can be used for NAS system network connections. The third RJ-45 connector, located in the lower right corner of the system's back panel, is an embedded remote access connector. Use it only for remote access functions.

   NOTE: On PowerVault 770N systems, two RJ-45 NIC connectors are on the back panel. However, only the connector located in the center of the system's back panel can be used for NAS system network connections. The

other connector is an embedded remote access connector. Use it only for remote access functions.

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

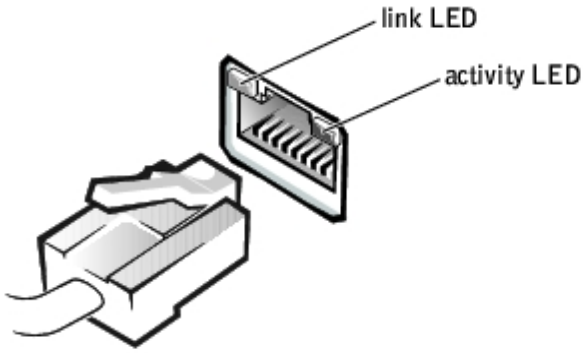
   The NAS system retrieves the required information to set up network parameters (the IP address, gateway subnet mask, and DNS server address) from a DHCP server on the network.

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

5. Verify that the link LED on the NIC connector is illuminated. See Figure 1-1.

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

Figure 1-1. NIC Connector



6. From a client system on the same network, open Microsoft® Internet Explorer 6.0 or later, type the default system name in the Web address field, and press <Enter>.

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

   You can also access the system directly through secure port 1279 by connecting to `https://DELLxxxxx:1279` where *xxxxxxx* is the system's service tag number.

   NOTE: If you cannot connect to the system through a Web browser, you must use another method to configure the IP address, gateway subnet mask, and DNS server. See "Configuring Your System Using a Keyboard, Monitor, and Mouse."

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

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

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

   See "NAS Manager."

Configuring Your System Using a Keyboard, Monitor, and Mouse

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

   For information about system connectors, see your *User's Guide*.
3. Push the power button to turn on the NAS system.
4. Log in to the NAS system.

   NOTE: The default administrative user name is `administrator` and the default password is `powervault`.
5. Log in to the NAS Manager.

   For more information, see "Logging Into the NAS Manager."
6. Configure the IP address.

   For more information, see "Configuring the Network Address for the NAS System" or your Windows online help.

Other Documents You May Need

Table 1-1 lists the additional documentation included with your system.

Table 1-1. Other Documents

Document	Type of Information
Setting Up Your System	General overview of system setup.
User's Guide	System features, technical specifications, and device drivers.
Installation and Troubleshooting Guide	Instructions for installing system hardware, as well as troubleshooting and diagnostic procedures for testing your system.
System Information Guide	Basic information about your system, including safety and regulatory information. Warranty information may be in this document or in a separate document.
Resource CD	Contains your system documentation.
Online help	Online help is available for the NAS Manager and the Windows Powered operating system. In addition, online help is provided with some of the system management and storage management software components. For more information on accessing online help, see "How to Find Online Help."
Readmes and Release Notes	Last-minute updates about technical changes to the system or advanced technical reference material intended for experienced users or technicians. These documents are located on the *Resource* CD.
Information updates	Documents that are sometimes included with the system to describe changes to the system or software documentation. Always read the updates before consulting any other documentation. The updates often contain information that supersedes information in the other documents.

Back to Contents Page

Back to Contents Page

NAS Manager

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

- Logging Into the NAS Manager
- Basic Navigation
- Changing the NAS Manager Language
- How to Find Online Help
- Configuring Network Properties
- Creating Users
- Using Shares
- Disk Quotas
- Using Logs
- Shutting Down the NAS System
- Managing Disks
- Managing Volumes
- Using the NAS Utilities

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

Logging Into the NAS Manager

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

Logging Into the NAS Manager on the Network

1. Open a Web browser from a client system.

   The NAS Manager supports client systems running Microsoft® Windows® operating systems and Internet Explorer 6.0 or later.

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

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

   You can also access the system directly through secure port 1279 by connecting to `https://DELL`*xxxxxxx*`:1279` where *xxxxxxx* is the system's service tag number.

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

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

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

You are now logged in to the NAS Manager.

Logging Into the NAS Manager Directly on the NAS System

1. Connect a keyboard, monitor, and mouse to the NAS system.
2. Turn on the NAS system and log into the system as an administrator.

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

3. Double-click the **NAS Manager** icon on the desktop of the NAS system.

   NOTE: If you are part of a domain, the NAS Manager icon may not be displayed. To access the NAS Manager, open Internet Explorer and enter `http://localhost`, and then click the **Administer this server** link to display the NAS Manager.

4. When prompted, enter the user name and password.

   The default user name and password for the NAS Manager are the same as for the NAS system.

Default Administrator User Name and Password

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

Basic Navigation

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

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

Primary Menu

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

- **Welcome** — Allows you to take a tour and set the administrator password, NAS system name, and default page.
- **Status** — Provides information about alerts and other status.
- **Network** — Provides access to basic network setup tasks such as setting the NAS system name, configuring properties of network interfaces, configuring global network settings, setting IP addresses and ports for the administration website, configuring Telnet, and changing passwords.
- **Disks** — Allows you to configure disks and volumes, set disk quotas, and create shadow copies.
- **Users** — Enables you to create, edit, and delete local users and groups.
- **Shares** — Enables you to manage local folders and create or modify file shares.

- **Maintenance** — Allows you to perform maintenance tasks such as backup and restore, apply software updates, check logs, change the language of the NAS Manager, and access the NAS server desktop.
- **Help** — Provides access to online Help for network attached storage.

Changing the NAS Manager Language

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

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

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

For information about changing the language settings for the NAS system itself, see "Advanced Features."

How to Find Online Help

The NAS Manager provides two kinds of help. The NAS Manager online help provides information about NAS Manager functionality and procedures. The Microsoft Windows Storage Server 2003 operating system online help, which you can access through the **Remote Desktop** link on the **Maintenance** page, documents the functionality of the Windows Powered operating system.

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

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

To start Windows Storage Server 2003 help, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Remote Desktop**.
4. Log in to the NAS system.

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

5. From the **Start** menu, click **Help and Support**.

Configuring Network Properties

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

Default System Name

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

You can also access the system directly through secure port 1279 by connecting to `https://DELL`*xxxxxxx*`:1279` where *xxxxxxx* is the system's service tag number.

Naming the NAS System

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

1. Log in to the NAS Manager.
2. Click **Network**.
3. Click **Identification**.
4. Type a new name for the NAS system in the **Server name** field.
5. If desired, in the **DNS suffix** field type in the domain information to append to the host name to create the fully qualified machine name.
6. Click **Workgroup** or **Domain**, depending on whether the system will be part of a workgroup or a domain.
7. If the system is part of a domain, type in the **User** and **Password** fields the information for the user who has permission to join the domain.

   Include the domain name when you enter the user name (*DOMAIN**USER*):
8. Click **OK**.
9. Click **OK** to reboot, or click **Cancel**.

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

Configuring the Network Address for the NAS System

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

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

online help.

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

To configure the IP address, perform the following steps:

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

   NOTE: If some of the text is missing due to column width, pass your cursor over the text in the column to see a pop-up window with a full description.
4. Click **IP**, and select **Use the following IP settings**.
5. Enter the desired IP address, subnet mask, and default gateway.

   If you do not have this information, contact your system administrator.
6. Click **OK**.

   The network address setup is complete.

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

Changing the Administrator Password

1. Log in to the NAS Manager.
2. Click **Network** and click **Administrator**.
3. Enter the current user name and password.
4. Enter the new password in the **New password** box.

   The password must be at least six characters and cannot be blank.
5. Enter the new password again in the **Confirm new password** box.
6. Click **OK**.

   NOTE: If you receive the error message stating that the password cannot be changed for this domain account or that the account name cannot be changed for this domain account when trying to change the administrator password or account name, you are logged on as a domain user. You must be logged on as the server administrator to change the administrator password.

Creating Users

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

Creating a Single Local User

NOTE: In a domain environment, you cannot create domain users through the NAS Manager.

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

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

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

Creating a Group of Local Users

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

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

   NOTE: If you are adding a domain group, you must also enter the user name and password that will allow you to add from that domain.
8. Click **OK**.

Using Shares

A share is a folder on the NAS system that can be accessed on the network by systems running Windows, Novell®

NetWare®, Macintosh, or UNIX® operating systems.

NOTE: You must use the NAS Manager's Remote Desktop to administer NetWare shares. See "Advanced Features" for more information.

A NAS system supports the following methods of sharing folders:

- DFS — Distributed File System (DFS) makes files that are distributed across multiple servers appear as if they reside in one place on the network.
- NFS — The Network File System protocol is used by client systems running UNIX.
- IPX — The Internet Packet Exchange protocol is used by client systems running NetWare. This protocol is not installed by default.
- FTP — The File Transfer Protocol is an alternative way of accessing a file share from any operating system. This protocol is disabled by default.
- HTTP — The Hyptertext Transfer Protocol is the protocol for accessing a file share from Web browsers.
- Microsoft SMB — The Microsoft SMB protocol is used by clients running a Microsoft Windows operating system.
- AppleTalk — The AppleTalk protocol is used by clients running a Macintosh operating system. This protocol is disabled by default.

Adding a Share

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

NOTICE: It is recommended that you create your data shares on the data drives. Shares that are created on the operating system drive will be deleted if you reinstall the operating system.

To add a share, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. On the **Shares** page, click **Shares**.
4. In the **Tasks** list on the **Shared Folders** page, click **New**.
5. Type the share name and share path.
6. If you entered a nonexistent folder in the **Share path**, click **Create folder**.
7. Check the appropriate box(es) to specify the types of protocols to enable.

   If you want to use a protocol that is grayed out, you must first enable it on the NAS system. See "Advanced Features" for information about enabling the AppleTalk and FTP protocols.
8. If you want to provide access to the share as part of a Distributed File System (DFS) namespace, select **Publish to DFS root: *servername**root***.

   A DFS namespace provides users with a logical grouping of shared resources that is independent of the resources' locations. Users can access resources without needing to know where the resources reside. If you move a shared folder, the move does not affect users. For more information about DFS and creating DFS roots, see "Using DFS."
9. Use the protocol tabs to configure the specific properties of each type of share.

See the context sensitive online help for more information on the properties for each protocol.

10. Click **OK**.

Modifying Share Properties

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

   The **Share Properties** page is displayed. Use this page to change the properties of the share, such as the protocols it supports.
6. Click **OK**.

Removing a Share

When you remove a share, the share becomes inaccessible; however, the actual files remain on the NAS system.

To remove a share, perform the following steps:

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

   A confirmation dialog appears.
6. Click **OK** to confirm the deletion, or click **Cancel** to keep the share.

Removing a Protocol From the Share

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

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

1. Log in to the NAS Manager.

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

Publishing a Share in DFS

A DFS namespace provides users with a logical grouping of shared resources that is independent of the resources' locations. Users can access resources without needing to know where the resources reside. Also, in DFS, you can move a shared folder without affecting users.

To publish a shared folder in DFS, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. On the **Shares** page, click **Shares**.
4. In the **Shared Folders** table, click the share that you want to publish in DFS.
5. Click **Publish in DFS**.
6. In the **Publish to DFS root** box, type the name of a DFS root.
7. Click **OK**.

For more information on DFS, see "Using DFS."

Disk Quotas

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

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

When you enable disk quotas, you can set both the disk quota limit and the disk quota warning level.

- The disk quota limit specifies the amount of disk space a user is allocated within a specific volume.
- The warning level specifies the point at which the event log displays that a user is nearing the quota limit within a specific volume.

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

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

Enabling, Disabling, or Setting Disk Quotas on a Volume

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volume Tools**.
4. On the **Volumes** page, click the volume to manage.
5. Click **Set Default Quota**.
6. On the **Default Quota for volume** page, click the **Use quota limits to manage use of the volume** check box.
7. Click the **Limit volume usage to** check box and enter the volume usage limit.
8. Click **OK**.

NOTE: Setting a default quota entry for a volume applies the setting to any users (without individual disk quotas) accessing the volume.

Adding Disk Quota Entries

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

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

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

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volume Tools**.
4. On the **Volumes** page, click the volume to manage.
5. Click **Set Quota Entries**.
6. On the **Set User Quotas for Volume** page click **New Quota Entry**.
7. Select a local user from the list box, or type the name of a domain account in the text box (in the format *domain_name**user_name*).
8. To allow unlimited disk space usage, click the **Do not limit volume usage** radio button, and then go to step 10. Otherwise, go to step 9.
9. To limit disk space, perform the following steps:
    a. Click the **Limit volume usage 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. Use the drop-down box to select kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or

exabytes (EB).

c. Enter the amount of disk space that, when filled, triggers a warning to the user or group member that the used disk space is near the disk-capacity limit. Use the drop-down box to select KB, MB, GB, TB, PB, or EB.

10. Click **OK**.

Modifying Quota Properties

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volume Tools**.
4. On the **Volumes** page, click the volume to manage.
5. **Click Set Quota Entries**.
6. On the **Set User Quotas for *volume*** page, click the user for whom you want to set a quota.
7. Click **Properties**.
8. On the **Quota Entry Properties for *volume**user*** page, click the **Do not limit volume usage** radio button to allow unlimited disk use, or perform the following procedure to limit disk space:

   a. Click the **Limit volume usage to** radio button.

   b. In the text box, enter a numerical value to specify the amount of disk space to assign to a particular user or group. Use the drop-down box to select **KB**, **MB**, **GB**, **TB**, **PB**, or **EB**.

   c. Enter the amount of disk space that, when filled, triggers a warning to the user or group member that the used disk space is near the disk-capacity limit. Use the drop-down box to select **KB**, **MB**, **GB**, **TB**, **PB**, or **EB**.

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

9. Click **OK**.

Disabling Disk Quotas on a Volume

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volume Tools**.
4. On the **Volumes** page, select the volume to manage.
5. Click **Set Default Quota**.
6. On the **Default Quota for *volume*** page, clear the **Use quota limits to manage use of the volume** check box.
7. Click **OK**.

Removing User Quota Entries

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volume Tools**.
4. On the **Volumes** page, select the volume to manage.
5. **C**lick **Set Quota Entries**.
6. On the **Set User Quotas for *volume*** page, click the user(s) for whom you want to remove a quota.
7. Click **Delete**.
8. Click **OK**.

Using Logs

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

The NAS system provides access to the following logs:

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

Viewing Log Entry Details

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

To view log entry details, perform the following steps:

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

Modifying Log Properties

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

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

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

Downloading Log Files

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

To download log files, perform the following steps:

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

Viewing Downloaded Log Files

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

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

Clearing Log Files

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

Shutting Down the NAS System

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

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

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

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

Managing Disks

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

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

Listing Available Disks and Viewing Properties

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

   NOTE: Controllers labeled as "Di" are integrated RAID controllers. Controllers labeled as "DC" and "QC" are PCI add-in cards.

5. Click **Select** in the **Tasks** column.

   A list of available disks is displayed along with the status of each disk.
6. Click the disk whose properties you want to view, and then click **Properties**.

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

Rescanning for Disks

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

   A list of available disks is displayed along with the status of each disk.
6. In the **Physical Disks** column on the **Disks** page, select the disk to rescan.
7. In the **Tasks** list, click **Rescan**.
8. On the **Rescan** page, click **OK** to start the rescan.

Creating a Hot Spare

NOTE: This procedure does not apply to the PERC 3/Di controller, which is the integrated RAID controller on PowerVault 775N NAS systems.

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.

1. Log in to the NAS Manager.

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

   A list of available disks is displayed along with the status of each disk.
6. In the **Physical Disks** column on the **Disks** page, select the disk to make a hot spare.
7. In the **Tasks** list, click **Make Hotspare**.

Freeing a Hot Spare

NOTE: This procedure does not apply to the PERC 3/Di controller, which is the integrated RAID controller on PowerVault 775N NAS systems.

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

   A list of available disks is displayed along with the status of each disk.
6. In the **Physical Disks** column on the **Disks** page, select the disk to free.
7. In the **Tasks** list, click **Free Hotspare**.

Managing Volumes

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

NOTE: You can also create volumes using Windows Logical Disk Manager. See "Creating a Dynamic Volume" in "Advanced Disk and Volume Management."

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

Creating a Volume

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Volumes**.

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

Preparing for Volume Expansion

NOTE: This procedure does not apply to the PERC 3/Di controller, which is the integrated RAID controller on PowerVault 775N NAS systems.

NOTE: You cannot expand system volumes in an internal RAID group.

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

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

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

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

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

NOTE: This process may take several hours to complete.

Expanding a Volume

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

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

To expand a volume, perform the following steps:

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

6. Click **OK**.

Deleting a Volume

NOTICE: If the volume is in use—for example, the volume is open in a browser window, the volume contains shares or snapshots, or another application is using the volume—a message displays stating that the operation has failed and that you need to use Array Manager. See "Advanced Disk and Volume Management" for more information. Ensure that you delete all shares and persistent images on that volume. The administrator can use Array Manager to force the deletion of the volume.

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

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

Viewing Volume Properties

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

Using the NAS Utilities

The NAS utilities provide advanced functionality on your NAS system. To access the NAS Utilities, perform the following steps:

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

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

4. On the NAS system desktop, double-click **NAS Utilities** to display the **NAS Utilities** window.

The following categories of tools are available through the through the **NAS Utilities** window:

- **Shared Folders** — Create, view, and set permissions for shared resources, view a list of all users connected over a network to the computer and disconnect one or all of them, and view files opened by remote users and close one or all of the open files.
- **Storage** — Perform volume management using the Windows Disk Management tool or disk management using Dell OpenManage™ Array Manager.
- **System Tools** — View event logs or monitor the utilization of operating system resources.
- **Administrative Tools** — Use tools such as Internet Information Services (IIS), Distributed File System (DFS), Remote Desktops, and Terminal Services Configuration Tool. See the online help for information about these tools.

Back to Contents Page

Back to Contents Page

Advanced Disk and Volume Management

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

- Using Array Manager to Manage Disk Arrays
- Disk Management
- Managing Volumes Using Disk Management

This section provides information about how to manage your physical hard drives, arrays, and volumes. You use Dell OpenManage™ Array Manager to create an array of disks, and the Microsoft® Windows® Disk Management tool to create and manage volumes.

To create a volume, perform the following tasks in the order listed:

- Initialize any disks that will be used (Array Manager). See "Initialize."
- Create a virtual disk (Array Manager). See "Creating Virtual Disks."
- Initialize the virtual disk (Disk Management). See "Initializing a Disk."
- Upgrade the disk from basic to dynamic (Disk Management). See "Upgrading a Basic Disk to a Dynamic Disk."
- Create the volume (Disk Management). See "Creating a Dynamic Volume."

Using Array Manager to Manage Disk Arrays

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

Array Manager allows you to configure your storage devices, arrays, and disks contained in your system.

Launching Array Manager From the NAS Manager

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

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

4. On the NAS system desktop, double-click **NAS Utilities** to display the **NAS Utilities** window.
5. Double-click **Storage**, and then double-click Disk Management (Dell OpenManage Array Manager).
6. If an Array Manager window with buttons such as **Create Volume** or **Create Virtual Disk** displays, click the task you want to perform, or close the window to view the Array Manager console.

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

Array Manager Console

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

Managing Disk Arrays

This section describes how to use Array Manager to configure and manage arrays with the Dell™ PowerEdge™ Expandable RAID Controller 3/Dual Channel (PERC 3/DC), PERC 3/QC, and PERC 4/DC controllers that are supported on your NAS system.

Creating Virtual Disks

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

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

To create a virtual disk, perform the following steps:

1. Right-click an array group.
2. Click **Create Virtual Disk** to display the **Create Virtual Disk Express Mode** window.

   NOTE: Using Express Mode to create a virtual disk selects the maximum number of disks for the selected RAID type. To manually select the number of disks, use Advanced Mode.
3. Select the RAID level that you want to use for the virtual disk.
4. Type the name of the disk in **Name** and click **Finish**.

   The virtual disk is displayed in the Array Manager console.

Deleting Virtual Disks

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

NOTICE: You must delete all shares and shadow copies 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 the shares correctly.

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

   A confirmation dialog box appears.
3. Click **OK** to continue.

The virtual disk disappears from the right pane.

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

Reconfiguring and Managing Virtual Disks

This section summarizes how you can change the virtual disk configuration through the NAS Manager.

NOTE: Because of hardware restrictions, the PERC 3/DC, 3/QC, and 4/DC controllers do 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 does not detect the change until a you perform a manual rescan or read/write to the drive.

Reconfiguring a Virtual Disk

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

NOTE: The NAS system supports RAID 1 to RAID 0 and RAID 5 to RAID 0 migrations.

1. Right-click a virtual disk.
2. Click **Reconfigure**.

   The **Virtual Disk Reconfiguration** 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. Select the RAID level in the **Type** drop-down menu.
4. Click **OK** to continue or **Cancel** to cancel the operation.
5. To view your progress, click the parent of the virtual disk.

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

Using 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.

   NOTE: The write-cache is enabled by default. Disabling write-cache may negatively impact your system's performance.

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.

Properties

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

Blink Virtual Disk

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

Unblink Virtual Disk

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

Disk Commands

Initialize

Initialize any array disk before you use it.

Perform the following procedure on any array disk on a supported RAID controller.

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

1. Right-click the array 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.

Format

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

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

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

Rebuild

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

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

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

   NOTE: This process may take several hours.

Assign Global Hot Spare

NOTE: This procedure does not apply to the PERC 3/Di controller, which is the integrated RAID controller on PowerVault 775N NAS systems.

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

NOTE: This procedure does not apply to the PERC 3/Di controller, which is the integrated RAID controller on PowerVault 775N NAS systems.

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

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

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

Prepare to Remove

Use this procedure to prepare for removing an array disk from a controller.

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

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

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

Properties

Use this command to display the array disk properties.

General Controller Commands

This section describes the general controller operations.

Rescan Controller

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

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

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

Flush

The **Flush** command forces the PERC 3/DC, 3/QC, 4/Di, and 4/DC controllers to write the contents of cache memory onto the virtual disks. You might want to use this option if you find your application or disks in an unstable condition.

Enable Alarm

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

To enable the alarm sound, perform the following steps:

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

Disable Alarm

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

To disable the alarm sound, perform the following steps:

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

Rebuild Rate

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

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

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

Properties

The **Properties** command displays controller attributes.

To view properties, perform the following steps:

1. Right-click the appropriate controller.

2. Click **Properties**.

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

Enclosure Management

The PERC 3/DC, 3/QC, and 4/DC controllers support storage enclosure management. Array Manager displays the properties of the enclosure's fans, power supply, and temperature probes. Array Manager also notifies you of enclosure status changes through events that are displayed on the **Events** tab and logged in the **Windows Powered Event Log**.

NOTE: PowerVault NAS systems support only PowerVault storage enclosures attached to supported RAID controllers.

Enclosure Components in the Tree View

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

Thermal Shutdown

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

Enclosure Fans

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

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

Enclosure Power Supplies

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

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

Enclosure Temperature Probes

The temperature probes that are installed in the enclosure are displayed under **Temperature Probes** in the tree view. You

can select **Temperature Probes** to display the individual temperature probes and their status information in the right pane. The status information includes the current temperature in Celsius and the warning and error thresholds for the temperature probe. The error threshold has a default value that cannot be changed. However, you can set the warning threshold. See the **Set Thresholds for Temperature** command in "Enclosure Commands" for information on setting the warning threshold.

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

Enclosure Commands

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

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

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

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

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

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

Disk Management

This section describes conceptual and procedural information about how to implement basic and dynamic disks using Array Manager.

Monitoring Disk Reliability

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

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

and puts an alert message in the Windows® Powered Event Log.

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

Managing Volumes Using Disk Management

This section describes how to use the Windows Disk Management tool to manage basic and dynamic volumes.

Accessing the Disk Management Tool

1. In the NAS Manager, click **Maintenance**.
2. Click **Remote Desktop** and log in to the NAS system.
3. Double-click the **NAS Utilities** icon on the desktop.
4. In the **NAS Utilities** window, double-click **Storage**, and then click **Disk Management (Local)**.

Initializing a Disk

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

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

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

NOTICE: Because of system recovery limitations, the operating system disk must remain a basic disk. Upgrade all data disks to dynamic during creation, except when using data disks in a cluster. To upgrade disks to dynamic, use the Windows Disk Management tool.

Upgrading a Basic Disk to a Dynamic Disk

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

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

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

1. Right-click the disk you want to upgrade, and then click **Convert to Dynamic Disk**.
2. When the **Convert to Dynamic Disk** window appears, select the disks to upgrade and click **OK**.
3. When the **Disks to Convert** window appears, select the disks that you want to covert to dynamic and click **Convert**.

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

Reactivating Dynamic Disks

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

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

   Mark the disk as **Online** after the disk is reactivated.

Merging Foreign Disks

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

Perform the following steps to merge foreign disks:

1. From the NAS Manager, click **Maintenance**, and then click **Remote Desktop**.

   NOTE: The default administrator user name is `administrator` and the default password is `powervault`.
2. On the NAS system desktop, double-click **NAS Utilities**.
3. In the **NAS Utilities** window, double-click **Storage**, and then double-click **Disk Management (Local)**.

   Foreign disks will appear in the disk list and graphical views as **Foreign**.
4. Right-click a foreign disk, and then click **Import Foreign Disks**.

   The **Import Foreign Disk Wizard** is displayed.
5. Select the foreign disks that you would like to merge to the system.

   By default all foreign disks are selected to be merged.
6. Click **Next**.
7. Click **Next** again to validate the volume status of each foreign disk.
8. Click **Finish**.

Volume Overview

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

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

It is recommended that you create all data 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. Select **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. When a message warns that all data on the partition will be lost and asks if you want to format the disk, click **Yes**.
3. Select **NTFS** as the file system type.

   NOTE: Your NAS system supports only NTFS partitions. Formatting all partitions as NTFS allows for advanced features only available under that file system.
4. 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.
5. Enter an allocation size or use the default, which is automatically selected.

   NOTE: If you use NTFS file system file compression on the source volume, you cannot use an allocation unit size larger than 4 KB. Defragmenting a source volume with shadow copies causes the difference file, which contains all changed data, to grow. If the difference file grows beyond the allocated space, you might lose previous versions of some files. Having a large NTFS file cluster size decreases the growth of the difference file.
6. Select the file system type and formatting options:

   - **Perform a 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.

     NOTE: To decrease the time it takes to format your disk, use the **Quick Forma**t option.

   - **Enable file and folder compression** — This option can be used only if you selected NTFS format. Check this box to use this format method.
7. Click **OK** to begin formatting.

A progress bar displays in the list view.

Deleting a Partition or Volume

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

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

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

Working With Dynamic Volumes

Dynamic volumes are volumes created on dynamic disks using the Disk Management tool. This section discusses how to create and extend dynamic volumes.

Creating a Dynamic Volume

NOTICE: It is recommended to format the source volume where you want to enable Shadow Copies with an allocation unit size of 16 KB or larger if you plan to defragment the volume. If you do not create this allocation, previous versions of files may be deleted. If you require NTFS compression on the source volume, however, you cannot create an allocation larger than 4 KB. If you defragment a volume that is very fragmented, you may lose older versions of files.

NOTE: The maximum supported volume size is 2 TB.

1. Access the Disk Management tool.

   See "Accessing the Disk Management Tool."
2. In the bottom half of the window, right click on the basic disk that you want to make dynamic and click **Convert to Dynamic Disk**.
3. In the **Convert to Dynamic Disk** window, click to select the disk(s) that you want to convert and then click **OK**.
4. When the **Disks to Convert** window appears, click **Convert**.

Extending a Dynamic Simple or Spanned Volume

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

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

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

- The volume is formatted as FAT or FAT32.

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

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

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

   The selected volume appears in the dialog box along with its current size.
2. Enter the amount to extend the volume, and then click **OK**.
3. Click **OK**.

   The volume now shows the size of the extended volume.

   For more information about extending volumes, see the context-sensitive online help.

Back to Contents Page

Back to Contents Page

Systems Management

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

- Dell OpenManage Server Administrator
- Using Remote Access Controllers
- Alert Log Messages From Server Administrator
- Configuring SNMP Properties

This section provides information about systems management for your NAS system, including an overview of Dell OpenManage™ Server Administrator, using the embedded remote access (ERA) controller, and configuring SNMP properties.

Dell OpenManage Server Administrator

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

Server Administrator provides information about:

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

Integrated Features

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

Server Administrator Home Page

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

Instrumentation Service

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

and security.

Remote Access Service

The Remote Access Service provides a complete remote system management solution for systems equipped with remote access controllers. For more information on the Remote Access Service, see "Using Remote Access Controllers."

Storage Management Service

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

Diagnostic Service

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

Update Service

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

Logs

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

Accessing Server Administrator

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

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

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

To access Server Administrator directly from a client system on the same network, open Microsoft® Internet Explorer 6.0 or later. Connect to the secure port, 1311, of your NAS System. For example, type `https://DELL1234567:1311`; where `DELL1234567` is the name of your NAS system.

Additional Information About Server Administrator

See the Dell OpenManage documentation on the Dell Support website at **support.dell.com** for more information on the Dell OpenManage Server Administrator.

Using Remote Access Controllers

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

NOTE: RACs are optional on Dell™ PowerVault™ 770N NAS systems and require a daughter card.

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

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

See the *Dell OpenManage Remote RACADM User's Guide* for information about running the Remote Access Service from the command line.

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

Accessing a RAC From the NAS Manager

You can display or change the IP address or create or change the user name and password of the RAC administrator.

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

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

   NOTE: The default administrative user name is `administrator` and the default password is `powervault`.
4. In Server Administrator, click **System**, click **Main System Chassis**, and then click **Remote Access Controller**.
5. Click **Remote Connect**.
6. Click **Configuration** to configure the IP address.
7. Click **Log in to Remote Connect Interface**.

Additional Information About RACs

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

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

Alert Log Messages From Server Administrator

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

To see the trap logs, perform the following steps:

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

   NOTE: The default administrative user name is `administrator` and the default password is `powervault`.
4. Double-click **NAS Utilities** on the NAS system desktop.
5. In the **NAS Utilities** window, double-click **System Tools**, and then double-click **Event Viewer**.
6. Double-click the type of log you want to view.

Configuring SNMP Properties

Configuring SNMP Community Properties

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

   NOTE: The default administrative user name is `administrator` and the default password is `powervault`.
4. Right-click **My Appliance**, and click **Manage**.
5. In the **Computer Management** window, double-click **Services and Applications**, and then double-click **Services**.
6. In the right pane, double-click **SNMP Service** to display the **SNMP Service Properties** window.
7. Click the **Security** tab, and then click **Send authentication trap**.

   Select this option if you want a trap message sent when authentication fails.
8. Select **Accepted community names**, and then click **Add**.

9. Select **Community Rights**, and then select a permission level for this host to process SNMP requests from the selected community.
10. To view a description of a dialog box item, right-click the item, and then click **What's This?**
11. In **Community Name**, type a case-sensitive community name, and then click **Add**.
12. 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.
    - 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 **Remote Desktop**, and then log in to the NAS system as an administrator.

   NOTE: The default administrative user name is `administrator` and the default password is `powervault`.
3. Right-click **My Appliance**, and click **Manage**.
4. In the **Computer Management** window, double-click **Services and Applications**, and then double-click **Services**.
5. In the right pane, double-click **SNMP Service** to display the **SNMP Service Properties** window.
6. Click the **Agent** tab, select **Contact**, and then type the name of the user or system administrator.
7. Select **Location**, and then type the physical location of the system or the contact.
8. In the **Service** panel, select the appropriate check boxes for this system, and then click **OK**.
9. 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.

NOTE: The default password for the SNMP **set** command is `powervault`.

Back to Contents Page

Back to Contents Page

Backing Up the System

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

- System-State Backup
- Backing Up Data Volumes
- Windows Backup and Restore Tools
- Third-Party Backup Software
- Installing Tape Device Drivers for Windows Backup and Recovery Tools
- Using Tape Backups on a SAN

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

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

System-State Backup

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

System-state data includes the following:

- Registry
- COM+ class registration database
- System boot files
- Users and groups information
- Share configuration data

Backing Up System-State Data

Dell recommends that you regularly back up your system state data.

NOTE: System State Backup does not back up data about HTTP shares.

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

1. Log in to the NAS Manager as an administrator.

2. Click **Maintenance**.
3. Click **Remote Desktop** and log into the NAS system.

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

4. On the NAS system click the **System State Backup** icon on the desktop.
5. When the **Backup** window displays, click **Perform System State Backup**.
6. Click **OK** when a message appears stating that your system state data will be backed up.
7. In the **System State Backup Destination** window, select the folder where you want to store the backup file and click **OK**.

   The **Backup Progress** window displays the system state data being backed up.

Backing Up Data Volumes

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

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

- Microsoft® Windows® Server 2003 backup and restore tools
- VERITAS™ Backup Exec® Server Professional 9.0 for Windows NT®, Windows 2000, and Windows Server 2003
- Yosemite TapeWare 7.0

The following software is supported for remote network backups:

- VERITAS Backup Exec Server Professional 9.0 for Windows NT, Windows 2000, and Windows Server 2003
- Yosemite TapeWare 7.0

Windows Backup and Restore Tools

Windows backup and restore 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 connected to a tape drive that is installed to back up your data volumes to tape.

You can access the backup and restore tools by clicking the **Maintenance** tab on the NAS Manager primary menu and clicking **Backup**.

For more information, see the online help for backup and restore.

Third-Party Backup Software

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

Using Third-Party Backup Software for Network Backups

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

Installing Network Accelerator Agents

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

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

Installing and Using Third-Party Backup Software for Local Backups

VERITAS Backup Exec

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

Installing VERITAS Backup Exec on the NAS System

NOTE: VERITAS Backup Exec supports installation using Remote Desktop and management using VERITAS Remote Administrator.

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

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

Installing VERITAS Backup Exec Remote Administrator on a Client System

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

   The CD starts the software automatically.
2. If the CD does not start the software automatically, open Windows Explorer, right-click the CD drive that contains the

VERITAS software, and select **Autoplay** from the menu.

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

Using VERITAS Backup Exec Remote Administrator

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

   The **Connect to Server** window displays.

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

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

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

Yosemite TapeWare

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

Installing TapeWare on the NAS System

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

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

Installing Tape Device Drivers for Windows Backup and Recovery Tools

If you are using the Windows backup and restore tools, you might need to install drivers for both tape drives and tape media changers.

1. Connect the PowerVault tape drive, and then restart the system.
2. Log in to the NAS Manager.

3. Click **Maintenance**.
4. Click **Remote Desktop**, and then log in to the NAS system as an administrator.

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

5. On the NAS system desktop, right-click **My Appliance** and click **Properties**.
6. In the **System Properties** window, click the **Hardware** tab, and then click **Device Manager**.
7. Double-click the category in the right pane that contains the tape device.

   NOTE: Tape devices may appear under **Unknown Devices**, **Other Devices, or Medium Changers**.

8. Double-click the tape device.
9. Click the **Driver** tab.
10. Click **Update Driver**.

    The Hardware Update Wizard displays.

11. Click the radio button next to **Install from a list or specific location (Advanced)**, and then click **Next**.
12. Click **Search for the best driver in these locations**, and select the check box for the location of the driver.

    If you select **Include this location in the search**, click **Browse** and select the folder where the driver is located.

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

13. Click **Next**.

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

14. Ensure that the wizard has selected the appropriate PowerVault tape device, and then click **Next**.
15. Click **Finish**.
16. Click **Close** to exit the driver properties dialog box.

Using Tape Backups on a SAN

You can back up volumes on your NAS system to a tape device on a SAN. For more information, see your SAN documentation.

Back to Contents Page

Back to Contents Page

Recovering and Restoring the System

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

- Solutions to Try Before Reinstalling
- Recovery From System Failure
- Restoring System State Data
- Restoring Initial System Setup

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

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

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

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

Solutions to Try Before Reinstalling

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

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

Recovery From System Failure

If the operating system becomes inoperable, you can use the NAS system's Reinstallation CDs to reinstall the operating

system. After the operating system is reinstalled, the system state backup can be restored to recover system configuration information.

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

- Reinstall the operating system using the *Reinstallation* CDs.
- Restore the system-state backup (see "Restoring System State Data" in "Backing Up the System" for more information)

Reinstalling the Operating System

NOTICE: Using the *Reinstallation* CD deletes all data on the operating system drive. However, it does not delete any data on the data drives.

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

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

   NOTE: If a keyboard, monitor, and mouse are connected to the NAS system, you may receive messages during the reinstallation that state the CD does not contain the correct file. Disregard these messages and continue with the installation as documented in this procedure.
5. When the CD ejects, insert the second *Reinstallation* CD.
6. When the second CD ejects, insert the third *Reinstallation* CD.

   The system will reboot once while the CD is inserted.

   NOTE: When the third CD ejects, the reinstallation is still in progress. The system reboots several times during the reinstallation.

   It takes approximately 30 minutes for the reinstallation to complete.
7. Check **support.dell.com** for the latest software and driver updates and apply any necessary updates to the NAS system.
8. Use a client system's Web browser to connect to the NAS system.

Restoring System State Data

NOTE: To restore your system state, you must have previously backed up your system by clicking **Backup** on the **Maintenance** menu.

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

1. Log in to the NAS Manager.

2. Click **Maintenance**.
3. Click **Backup**.
4. Log on to the system as administrator.

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

   The **Welcome to the Backup or Restore Wizard** window displays.

   NOTE: If the window does not display, on the NAS system's desktop, click the **Start** button and select **Programs→ Accessories→ System Tools→ Backup,** and then click **Windows Backup/Recovery**.

5. In the **Backup or Restore Wizard** window, click **Next**.
6. In the **Backup or Restore** window, click **Restore files and settings**, and click **Next**.

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

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

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

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

   a. Click **Browse**.

      The **Open Backup File** window is displayed.

   b. Click **Browse**.

   The **Select file to catalog** window is displayed.

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

   The **What to Restore** window is displayed.

   d. Click the plus (**+**) sign next to **File**.
   e. Click the plus (**+)** sign next to the backup file (**.bkf**).

   You are prompted for your backup file location.

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

   The backup appears in the **What to Restore** window.

g. Click the plus (+) sign next to the backup file to display the **System State** icon.

h. Click the check box next to **System State**, and then click **Next**.

i. Click **Advanced**.

The **Where to Restore** window is displayed.

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

The **How to Restore** window is displayed.

k. Select **Replace existing files**, and then click **Next**.

The **Advanced Restore Options** window is displayed.

l. Clear all check boxes, and then click **Next**.

8. Click **Finish** to begin the restore process, and then click **OK**.
9. Restart your system after the restore process completes.

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

Restoring Initial System Setup

After the operating system is reinstalled on the NAS system, you may need to reconfigure the system's network settings. See "Initial Configuration" and "Configuring Network Properties" for information on reconfiguring the network settings.

Back to Contents Page

Back to Contents Page

Shadow Copies

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

- Introduction to Shadow Copies
- Configuring Volume Settings
- Using Shadow Copies
- Scheduling Shadow Copies
- Defragmenting a Volume Containing Shadow Copies

Shadow Copy service allows the creation of point-in-time copies of your NAS system's data volumes. Shadow Copy software can be configured using the NAS Manager.

NOTE: Shadow copies can be accessed through SMB and NFS shares. Shadow copies cannot be accessed through HTTP, FTP, AppleTalk, or NetWare shares.

Introduction to Shadow Copies

A shadow copy is a point-in-time copy of a shared file or folder. If you change a file on the active file system after making a shadow copy, the shadow copy 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 shadow copy or restoring a directory or file.

NOTICE: Shadow copies are temporary backups of your data that typically reside on the same volume as your data. If the volume becomes damaged and you lose your data, the shadow copy is also lost. Therefore, using shadow copies should not replace performing regular backups.

Difference File

The Shadow Copies service stores changed data in a difference file. A difference file resides on each volume of your system. You can use the NAS Manager to change the amount of space that is dedicated to the difference file.

Shadow Copies Considerations

When using shadow copies, note the following:

- When the shadow copy difference file reaches the maximum number of shadow copies (64 copies per volume), the system deletes the oldest shadow copy file.
- Shadow copies are read-only. You cannot edit them.
- Shadow copies are made of entire volumes. You cannot make shadow copies of individual files or folders.
- NFS clients can access shadow copy data as read-only files.
- If you add a volume and you plan to defragment that volume, format the source volume where you intend to enable shadow copies with an allocation unit size of 16 kilobytes (KB) or larger. If you do not format the shadow copies volume, defragmenting the volume can cause previous versions of files to be deleted.

NOTE: If you use NTFS file system file compression on the source volume, you cannot use an allocation unit size larger than 4 KB. Defragmenting the source volume causes the difference file to grow. If the difference file grows

beyond the allocated space, you might lose previous versions of some files. Having a large NTFS file cluster size decreases the growth of the difference file.

Storing Shadow Copies

The NAS system can store a maximum of 64 shadow copies per volume; however, if you exceed the maximum, the oldest copy is overwritten. This number of copies allows you to schedule multiple shadow copies. (Create your schedule depending on how the data is changing.)

Configuring Volume Settings

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Shadow Copies**.
4. Select the volume that you want to configure.
5. Click **Properties**.
6. Set the maximum size for shadow copies by either selecting **No limit** or selecting **Use limit** and entering the amount of disk space that can be used for shadow copies.
7. Click **OK**.

Using Shadow Copies

In addition to scheduling shadow copies, you can make new copies on demand, delete existing copies, configure the shadow copies environment, and set shadow copy retention weights.

Making a Shadow Copy on Demand

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Shadow Copies**.
4. Select the volume(s) of which you want to make a shadow copy.
5. In the **Tasks** list on the **Manage Shadow Copies** page, click **New Shadow Copy**.

The page refreshes and the number in the **Copies** column increases by 1.

Deleting a Shadow Copy

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Shadow Copies**.

4. On the **Manage Shadow Copies** page, select the volume for which you want to delete shadow copies, and then click **View Shadow Copies**.

   You can select only one volume at a time.

5. On the **Shadow Copies on Volume *x*** page, click the copies you want to delete, and then click **Delete**.
6. When asked if you want to delete the shadow copies, click **OK**.

Scheduling Shadow Copies

For any volume, you can schedule shadow copies to occur once, daily, weekly, or monthly.

Creating a Shadow Copies Schedule

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Shadow Copies**.
4. Select the volume for which you want to schedule shadow copies, and click **Set Schedule** in the **Tasks** list.
5. In the **Tasks** list, click **New**.
6. In the **New Shadow Copy for Volume *x*** page, click **Once**, **Daily**, **Weekly**, or **Monthly** and complete the information on the page.
7. Click **OK**.

   The scheduled shadow copy displays on the **Shadow Copy Schedules on Volume *x*** page.

8. Click **New** to schedule another shadow copy

   NOTE: It is recommended to schedule no more than two shadow copies per day.

Deleting a Shadow Copy Schedule

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Shadow Copies**.
4. Select the shadow copy schedule that you want to delete, and click **Set Schedule** in the **Tasks** list.
5. Select the scheduled shadow copy you want to delete.
6. In the **Tasks** list, click **Delete**.
7. Click **OK** to delete the scheduled shadow copy.

Editing a Shadow Copy Schedule

1. Log in to the NAS Manager.
2. Click **Disks**.
3. Click **Shadow Copies**.
4. Select the volume for which you want to edit shadow copy schedules, and click **Set Schedule** in the **Tasks** list.
5. Select the scheduled shadow copy you want to edit.
6. In the **Tasks** list, click **Properties**.
7. Change the settings as desired.
8. Click **OK** to save the shadow copy settings.

Accessing Shadow Copies

The files and folders within a shadow copy are identical to the permissions on the original files and folders.

Accessing Shadow Copies From Client Systems Running Windows

Clients running Windows operating systems must meet the following requirements, depending on the operating system, to access shadow copies:

- Client systems running Windows Server 2003 already have the software available to access shadow copies.
- Client systems running Windows XP need to install the previous versions pack. This pack is located in the **%systemroot%\system32\clients\twclient** directory of your NAS system.
- Client systems running Windows 2000 and Windows NT® need the shadow copy client system software, which is available at **microsoft.com**.

When the client software is installed, perform the following steps to access shadow copies:

1. Map to a share on the NAS system with the folder file that you want to access
2. Right click the folder or file you want to access and click **Properties**.
3. Click the **Previous Versions** or **Shadow Copies** tab to display previous versions that you can access.
4. Click the desired previous version.
5. Click **View** to browse the folder.
6. Click **Copy** to copy the contents to a new location.
7. Click **Restore** to restore the contents to the original location (If it is a folder, all subdirectories will also be restored).

Accessing Shadow Copies From Client Systems Running UNIX

Client systems running UNIX® do not require additional software to access a shadow copy. When a client system mounts a share with shadow copies, shadow copies are a pseudodirectory of the share in the format **.@GMT-YYYY.MM.DD-**

HH:MM:SS.

You can browse shadow copy pseudodirectories like any other directory. Permission rules are the same as for client systems running Windows, except that client systems running UNIX with permissions when the shadow copy was taken will have permissions to access the shadow copy.

Defragmenting a Volume Containing Shadow Copies

Defragmenting the source volume causes the difference file to increase. If the difference file increases beyond the allocated space, you might lose previous versions of some files. Even with 16 KB cluster size, the shadow copy difference file will increase. If the difference increases too much (greater than the maximum set), shadow copies will be deleted.

If you do not have to keep shadow copies, delete them before defragmenting to improve the performance of the defragmentation.

Back to Contents Page

Back to Contents Page

Advanced Features

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

- Using the Redundant Memory Feature
- Installing Multilanguage User Interface (MUI) Support
- Network Adapter Teaming
- Telnet Server
- FTP
- Server for Network File System (NFS)
- File Server for Macintosh
- Services for the Novell NetWare Operating System
- Microsoft Directory Synchronization Services
- Using Secure Sockets Layer
- Using DFS

This section includes descriptions of advanced features that cannot be performed from the Dell™ PowerVault™ NAS Manager.

To perform the procedures in this section, you must use the Remote Desktop. To access the Remote Desktop, perform the following steps:

1. Log in to the NAS Manager.
2. From the NAS Manager, click **Maintenance**.
3. Click **Remote Desktop**.
4. Log on as an administrator.

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

Using the Redundant Memory Feature

NOTE: Redundant memory is available only on Dell™ PowerVault™ 775N systems.

The NAS system's redundant memory feature (also known as "memory spare row") allows the system to identify a row of faulty RAM and to hot-swap the faulty memory with a reserved row of memory. The chip set reports a faulty row when the threshold of single-bit ECC errors in a single bank is exceeded. When a faulty row is reported, the system copies the faulty row to the spare row and then configures it for access.

System Requirements

To use the redundant memory feature, your NAS system must meet the following requirements:

- All three banks of system memory must use the same type of DIMM.
- The system must be operating in memory-interleaved mode.

Considerations for Using Redundant Memory

- When the redundant memory feature is enabled, only two-thirds of the installed memory is available to the system.

- The redundant memory feature is supported on a per-bank basis. The smallest unit of redundant memory is a bank.
- The spare bank can be used only once per boot. After a bank is swapped, the system has no more redundant memory until it is reset.

For information on enabling the your NAS system's redundant memory feature, see your system's *User's Guide*.

Enabling Redundant Memory

You can enable redundant memory in the System Setup program. See your *User's Guide* for information.

Installing Multilanguage User Interface (MUI) Support

The NAS system allows you to change languages for operating system's user interface. The MUI allows the NAS system to display operating systems menus, dialogs, and help files in multiple languages. If a language that is not available on the NAS system is desired, you must install it from the appropriate *Multilingual Support* CD.

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

1. Insert the *Multilingual Support* CD into the NAS system's CD drive.
2. From a client system, log in to the NAS Manager.
3. Click **Maintenance**, and then click **Remote Desktop**.
4. Log in to the system as an administrator.

   NOTE: The default administrator user name is `administrator` and the default password is `powervault`.
5. Double-click **My Appliance** on the NAS desktop.
6. Browse to the CD drive and double-click **Dell PowerVault Multilingual Support CD** to launch the CD's web interface.
7. Click the **Install Multilanguage User Interface (MUI) Support** link to launch the **Multilanguage File Installation** installer program.
8. In the installer window, select the languages to be installed, and select the default MUI language from the menu.
9. Click **OK** to perform the installation.
10. After the installation is complete, you must reboot your system.

Applying the MUI Language

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

1. From a client system, log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Remote Desktop**.
4. Log in to the system as an administrator.

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

5. Click the **Start** button and select **Settings**→ **Control Panel**.
6. In the **Control Panel**, double-click **Regional and Language Options**.
7. On the **Regional Options** tab, select the appropriate region under **Standards and Formats**.
8. Click the **Languages** tab and select the appropriate language used in menus and dialogs.
9. Log off and log in to the system again for the new language MUI to take effect.

Network Adapter Teaming

Network adapter teaming allows the system to use the combined throughput of multiple network ports in parallel to increase performance or to provide fault tolerance. Network adapter teaming on your NAS system supports the following technologies:

- Adaptive Load Balancing (ALB)
- Adapter Fault Tolerance (AFT)
- Link Aggregation
- Fast EtherChannel (FEC)
- IEEE 802.3ad

NOTE: When creating or removing network adapter teams, the IP address of the NAS system's LAN connections changes. To prevent disconnection from the NAS system during team configuration, connect a keyboard, monitor, and mouse to the NAS system when creating or removing teams. See "Configuring Your System Using a Keyboard, Monitor, and Mouse" in "Initial Configuration" before configuring your teams.

Adaptive Load Balancing

Adaptive Load Balancing (ALB) is a simple and efficient method for increasing the NAS system's network transmission throughput. The ALB software continuously analyzes transmission loading on each adapter and balances the load across the teamed ports as needed. Adapter teams configured for ALB also provide the benefits of adapter fault tolerance. To use ALB, the Ethernet ports on the NAS system must be linked to the same Ethernet switch.

Adapter Fault Tolerance

Adapter Fault Tolerance (AFT) provides the safety of an additional backup link between the NAS system and the hub or switch. If a hub, switch port, cable, or Ethernet port fails, you can maintain uninterrupted network performance. AFT is implemented with a primary adapter and a backup, or secondary, adapter. If the link to the primary adapter fails, the link to the secondary adapter automatically takes over.

Link Aggregation

Link aggregation is a performance technology developed by Intel® and others to increase a system's network throughput. Unlike ALB, link aggregation can be configured to increase both transmission and reception channels between your system and switch. Link aggregation works only with compatible Intel switches. To use link aggregation, the Ethernet ports of the NAS system must be linked to the same Intel Ethernet switch.

Fast EtherChannel

Fast EtherChannel (FEC) is a performance technology developed by Cisco Systems to increase a system's network throughput. Unlike ALB, FEC can be configured to increase both transmission and reception channels between your NAS system and switch. FEC works only with compatible Cisco switches. To use FEC, the Ethernet ports of the NAS system must be linked to the same Cisco FEC-compatible switch.

IEEE 802.3ad

IEEE 802.3ad is a performance technology standard that increases a system's network throughput. IEEE 802.3ad is similar to the FEC standard developed by Cisco. However, whereas FEC works only with FEC-compatible Cisco switches, IEEE 802.3ad works with all switches that support IEEE 802.3ad. To use IEEE 802.3ad, the Ethernet ports of the NAS system must be linked to the same IEEE 802.3ad switch.

Creating Intel PROSet II Network Teams

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Remote Desktop**.
4. Log in to the system as an administrator.

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

5. Double-click the network icon on the NAS system's system tray (near the time on the bottom right corner).

   The Network Teaming utility, Intel PROSet II, displays.

6. Click **Action**, click **Add to Team**, and then click **Create New Team**.

   The Teaming Wizard displays.

7. Select the type of team to create, and then click **Next**.

   The types of team include **Adapter Fault Tolerance**, **Adaptive Load Balancing**, **Fast EtherChannel* /Link Aggregation**, and **IEEE 802.3ad**.

8. Select the Intel adapters to include with this team, and then click **Next**.

   NOTE: Broadcom NICs cannot be selected.

9. Verify that the team contains the appropriate members, and then click **Finish**.
10. If the team needs to be modified, click **Back**.

Removing Intel PROSet II Network Teams

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.

3. Log in to the Remote Desktop session as administrator.

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

4. Double-click the network icon on the NAS system's taskbar.

The Network Teaming utility, Intel PROSet II, is displayed.

5. In the tree view, click the team that you want to remove.
6. Click **Action**, and then click **Remove**.

Removing an Intel PROSet II Adapter From a Network Team

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.
3. Log in to the Remote Desktop session as administrator.

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

4. Double-click the network icon on the NAS system's taskbar.

The Network Teaming utility, Intel PROSet II, is displayed.

5. In the tree view, click the adapter that you want to remove.
6. Click **Action**, and then click **Remove from Team**.

Changing the Intel PROSet II Network Team Mode

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.
3. Log in to the Remote Desktop session as an administrator.

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

4. Double-click the network icon on the NAS system's taskbar.

The Network Teaming utility, Intel PROSet II, is displayed.

5. In the tree view, click the team to modify.
6. Click **Action**, and then click **Change Team Mode**.
7. In the Teaming Wizard, select the type of team that you want to create, and then click **Next**.

The types of team include **Fault Tolerance**, **Load Balancing**, **Fast EtherChannel* /Link Aggregation**, and **IEEE**

802.3ad.

8. Click **OK** to close.

For more information, see your Intel PROSet II help.

Creating Network Teams Using the Broadcom Advanced Server Control Suite

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.
3. Log in to the Remote Desktop session as `administrator`.

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

4. Double-click the network icon on the NAS system's taskbar.

   The **Broadcom Advanced Server Control Suite** window is displayed.
5. Click **Load Balance/Virtual LAN**.
6. Click **Create Team**.
7. Enter the team name and select the appropriate team mode.

   The types of team include **Start Load Balance and Fail Over**, **FEC/GEC**, and **Link Aggregation (IEEE 802.3ad)**.
8. Click **OK**.
9. Select the team name in the **Configuration** box.
10. Select an unassigned adapter to add to the team, and then click the arrow adjacent to the **Team Members** list to add the adapter.
11. Repeat step 10 for the second adapter.
12. Click **OK**.

Removing Broadcom Adapter From a Network Team

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.
3. Log in to the Remote Desktop session as `administrator`.

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

4. Double-click the network icon on the NAS system's taskbar.

   The **Broadcom Advanced Server Control Suite** window is displayed.

5. Click **Load Balance / Virtual LAN**.
6. Select the team name in the **Configuration** box.
7. Select an adapter in the **Team Members** list, and then click the arrow adjacent to **Load Balance Members** to remove the adapter.
8. Click **OK**.

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

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.
3. Log in to the Remote Desktop session as administrator.

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

4. Double-click the network icon on the NAS system's taskbar.

   The **Broadcom Advanced Server Control Suite** window is displayed.
5. Click **Load Balance / Virtual LAN**.
6. Right-click the team name in the **Configuration** box, and then click **Properties**.
7. Select the new type of team and click **OK** to apply the change.

   The types of team include **Start Load Balance and Fail Over**, **FEC / GEC**, and **Link Aggregation (IEEE 802.3ad)**.
8. Click **OK** to complete the change.

For more information, see your Broadcom Advanced Server Control Suite help.

Telnet Server

The Telnet server works optimally for most installations. It accepts logins from a variety of clients, including the Telnet clients shipped with Windows® 2000, Windows NT®, Windows 95, and Windows 98, Windows XP, and Windows Server 2003 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 Telnet server supports Windows NT LAN Manager (NTLM) for authentication of client logins. NTLM allows users to be automatically authenticated to the Telnet server based on their Windows NT login. This makes using Telnet completely transparent to users, while ensuring that clear text passwords do not pass over the network. However, NTLM must be supported on the client side of the login as well.

When users are logged in to a system that is using NTLM login, they are restricted to local drives on that system. If they need to map network resources, they can do so by explicitly mapping with full credentials.

Administration

The Telnet server is administered using the NAS Manager.

FTP

Enabling FTP Protocol

The File Transfer Protocol (FTP) is disabled on the NAS system by default. You must enable the FTP protocol for FTP client systems to access the NAS system.

To enable the FTP protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing Protocols**.
4. Click **FTP** and then click **Enable**.

Using Remote Desktop to Enable FTP Write Privileges

FTP write privileges to the NAS system's default FTP site are disabled by default. To enable write privileges to the default FTP site using Remote Desktop, perform the following steps:

1. Log in to the NAS Manager.
2. From the NAS Manager, click **Maintenance**.
3. Click **Remote Desktop**.
4. Log on as an administrator.

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

5. Double-click the **NAS Utilities** icon on the desktop of the NAS system.
6. Click **Administrative Tools**.
7. Click Internet **Information Services (IIS) Manager**.
8. Click **Local Computer**.
9. Click **FTP Sites**.
10. Right-click **Default FTP Site** and click **Properties**.
11. When the **Default FTP Site Properties** window is displayed, click **Home Directory**.
12. Click **Write** in the **FTP Site Directory** area.
13. Click **Apply** and then click **OK**.

Using Remote Desktop to Delete FTP Shares

To delete FTP shares using MMC, perform the following steps:

1. Log in to the NAS Manager.
2. From the NAS Manager, click **Maintenance**.
3. Click **Remote Desktop**.
4. Log on as an administrator.

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

5. Double-click the **NAS Utilities** icon on the desktop of the NAS system.
6. Click **Administrative Tools**.
7. Click Internet **Information Services (IIS) Manager**.
8. Click **Local Computer**.
9. Click **FTP Sites**.
10. Double-click **Default FTP Site** to expand its list.
11. Right-click on the share you want to delete and click **Delete**.

Server for Network File System (NFS)

Server for NFS can be used to provide disk resources from systems running Windows NT, Windows 2000, and Windows Server 2003 to any system on your network that supports NFS. To administer Server for NFS, perform the following steps:

1. Log into the NAS Manager.
2. Click **Maintenance**, and then click **Services**.
3. Click **Server for NFS**, and then click **Startup**.
4. In the **Set Service Properties** window, select whether you want Server for NFS to start automatically, manually, or whether you want to disable it.
5. Click **OK**.

NFS Write Cache

NFS write cache is enabled on Windows Storage Server 2003 Standard Edition. It is not enabled on Windows Storage Server 2003 Enterprise Edition because cached data will not fail over in a cluster configuration.

User Name Mapping

User Name Mapping provides mapping of names between the UNIX® and Windows environments. You can configure User Name

Mapping from the MMC Console or by using the NAS Manager to configure properties for the NFS Sharing Protocol. With User Name Mapping, you can create simple maps between Windows Powered user accounts and corresponding UNIX accounts. You can also use the Advanced Map feature to map accounts with dissimilar names. Because UNIX user names are case-sensitive, and Windows Powered operating system names are not, the use of User Name Mapping can greatly simplify maintaining and managing accounts in the two environments. User Name Mapping uses Network Information Service (NIS) or local Personal Computer Network File System (PCNFS) user and group files to authenticate users. Also, User Name Mapping supports bidirectional one-to-many mapping, allowing you to map a single UNIX or Windows Powered operating system account to multiple accounts in the other environment. For example, you can map more than one administrative account in a Windows Powered operating system to the UNIX root account.

Special Mappings

By default, the root user for the UNIX client is mapped to an unmapped user. This setting is commonly known as "root squashing." When an NFS authentication request is made for a user name mapped to an unmapped user, the result is an anonymous UID and GID (typically -2 and -1, respectively). Any files created by such a user will show file ownership as an anonymous Windows user.

NOTE: To prevent root squashing for specific NFS shares, the UNIX root user and group must be mapped to the Windows administrator user and group. The "access type" for the NFS share's permissions must also be set to root for each applicable client or client group.

To create user and group name maps, perform the following steps:

1. Log in to the NAS Manager.
2. From the NAS Manager, click **Shares**.
3. Click **Sharing Protocols**.
4. Click **NFS Protocol**, and then click **Properties**.
5. Click **User and Group Mappings**.
6. Use the **User and Group Mappings** window to define your user and group maps.

To configure the type of server to be used to access UNIX user and group names, perform the following steps:

1. On the **User and Group Mappings** window, click **General**.
2. Click **Use NIS server**, or click **Use password and group files** to select the server type.
3. Depending on whether you use an NIS server or password and group files, perform one of the following steps:
   - For password and group files, specify the location and filename of the UNIX password file and UNIX group file.

   NOTE: The UNIX password file and group file formats must conform to the UNIX standard for these files.

   - For NIS server, type the NIS domain and, optionally, the name of the NIS server.
4. Click **OK** to apply the configuration.

To define simple maps, perform the following steps:

1. In the **User and Group Mappings** window menu, click **Simple Mapping**.
2. Click **Enable Simple Mapping**.
3. Specify the **Windows Domain**.
4. Click **OK** to create the maps.

If you are defining explicit maps, you create user and group maps individually. To create explicit maps, perform the following steps:

1. On the **User and Group Mappings** window menu, click **Explicit User Mapping** to create user maps, or click **Explicit Group Mapping** to create group maps.
2. Specify the **Windows Domain**. If the server is configured as **PCNFS**, go to step 4.
3. Click **List UNIX Users** to populate the **UNIX users** box.
4. Create map entries by selecting a Windows user or group and a UNIX user (UID) or group (GID) from the list and clicking **Add**.
5. Click **OK** to create the maps.

Basic Scenarios

For UNIX and Windows NT User Name Mapping, an NIS Server must already exist in the UNIX environment, or UNIX user and group files must exist on the PowerVault NAS system. User Name Mapping associates UNIX users and groups to Windows NT users and groups. You can use two types of maps, simple and explicit. Simple maps define a one-to-one relationship between the same user names and groups. Explicit maps define a relationship between dissimilar user names and groups.

Workgroup

In the workgroup scenario, you configure User Name Mapping locally on the NAS system. All maps are contained on this system.

Filename Character Translation

Although Windows and UNIX file systems do not allow certain characters in filenames, the characters that are prohibited by each operating system are not the same. For example, a valid Windows filename can not contain a colon (:), but a UNIX filename can. If a UNIX user attempts to create a file in an NFS share and that file contains an illegal character for Windows in its name, the attempt will fail.

You can use filename character translation to replace characters that are not allowed in a file system by mapping them to characters that are valid. To enable filename character translation, create a text file that maps Windows to UNIX characters, and then modify the registry entry that specifies the path and name of the translation file.

The filename character translation text file is a list of mapped characters in a format such as the following:

```
0xnn : 0xnn [ ; comment ]
```

where *nn* is the hexadecimal value of the character

The entry for a map from the UNIX character ":" to the Windows character "-" in the filename character translation text is as follows:

```
0x3a : 0x2d ; Map ':' (0x3a) to '-' (0x2d)
```

To map the character combination "()" to the character "^", add the following entry:

```
0x28 0x29 : 0x5e ; Map '()' to '^'
```

To set up the character translation, perform the following steps:

1. Log in to the NAS Manager.
2. From the NAS Manager, click **Maintenance**.
3. Click **Remote Desktop**.
4. Log on as an administrator.

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

5. Double-click the **NAS Utilities** icon on the desktop of the NAS system.
6. Double-click **Administrative Tools**.
7. Double-click **Microsoft Services for Network File Systems**.
8. Click **Server for NFS**.
9. On the right pane, click **Server Settings**.
10. Set the desired filename character translation.

File Server for Macintosh

File Server for Macintosh (FSM) provides the tools needed to integrate Macintosh and Windows networks by leveraging existing Macintosh network resource and expertise. FSM is disabled by default on the NAS system. See "Enabling the AppleTalk Protocol" for information about enabling FSM.

Enabling the AppleTalk Protocol

The AppleTalk protocol is disabled on the NAS system by default. You must enable the AppleTalk protocol for Macintosh clients to access the NAS system.

To enable the AppleTalk protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **AppleTalk Protocol**, and then click **Enable**.

Disabling the AppleTalk Protocol

To disable the AppleTalk protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **AppleTalk Protocol**, and then click **Disable**.

Configuring the AppleTalk Protocol

To configure the AppleTalk protocol, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Shares**.
3. Click **Sharing** Protocols.
4. Click **AppleTalk Protocol**, and then click **Properties**.
5. In the **AppleTalk Service Properties** window, type the log on message that will be displayed when the user logs on, click the **Security** check box if you allow workstations to save passwords and select the type of authentication to be used, and specify the number of concurrent sessions that are allowed.
6. Click **OK** to complete the configuration.

Adapter Bindings

FSM can bind to only one network adapter. By default, it is bound to the embedded 10/100TX network adapter. To change the binding in systems with multiple network adapters, the AppleTalk protocol properties for the network adapter to be used by AppleTalk must be modified to accept inbound connections.

AppleTalk Protocol Adapter Binding

To modify the AppleTalk protocol adapter binding for systems with multiple network adapters, perform the following steps from the NAS Manager:

1. Log in to the NAS Manager.
2. Click **Network**.
3. Click **Interfaces**.
4. Click the radio button next to an enabled adapter to bind the AppleTalk protocol.

   NOTE: The AppleTalk protocol must bind to an adapter that is enabled, regardless of whether the File Server for Macintosh is disabled.

5. On the **Tasks** menu, click **AppleTalk**.
6. Click the check box next to **Enable inbound AppleTalk connections on this adapter**.
7. Optionally, if you use AppleTalk zones, select the appropriate zone in the drop-down box.
8. Click **OK**.

Microsoft UAM Volume

A user authentication module (UAM) is a software program that prompts users for an account name and password before they log in to a server. The Macintosh Chooser has a standard UAM built in that uses the clear-text password or Apple's RandNum Exchange method of security.

Microsoft Authentication offers an additional level of security because the password is used as a key to encrypt a random number. If the system administrator has determined that encryption is an important security measure, you may be asked to use Microsoft Authentication in addition to Microsoft UAM authentication.

Requirements

To use Microsoft UAM 5.01, you must have a Macintosh client running AppleShare Client 3.8 or later or Macintosh 8.5 or later operating system. If you do not meet the minimum requirements, the Microsoft UAM Installer installs the old Microsoft UAM 1.0 module. If you upgrade your system software, you need to run the Microsoft UAM Installer again.

Installing User Authentication

Log in to the Microsoft UAM Volume on the system to access the **MS UAM** file, and then drag this file to the **AppleShare Folder** in your **System** folder.

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

1. Create a user with a password of less than eight characters.
    a. Log in to the NAS Manager.
    b. Click **Users**.
    c. Click **Local Users**.
    d. Click **New**.
    e. Complete the information in the **Create New User** window and click **OK**.

    NOTE: The password can be no longer than eight characters. Passwords longer than eight characters cannot be used when mapping an Apple share without a UAM.

2. Click **Chooser** on the **Macintosh Apple** menu.
3. Double-click the **AppleShare** icon, and then click the **AppleTalk** zone in which the system with Services for Macintosh resides.

    Ask your system administrator if you are not sure of the zone.

4. Select the system from the list of file servers, and click **OK**.
5. Click **Registered User**.
6. Enter the user name and password you created in step 1, and then click **OK**.
7. Select the **Microsoft UAM Volume**, and then click **OK**.
8. Close the **Chooser** dialog box.

To install the authentication files on the Macintosh workstation, perform the following steps:

1. Double-click **Microsoft UAM Volume** on the Macintosh desktop.
2. Double-click the **Microsoft UAM Installer** file on the Microsoft UAM volume.
3. Click **Continue** in the **Installer Welcome** screen.

The installer reports whether the installation succeeds.

If the installation succeeds, Macintosh users of this workstation are offered Microsoft Authentication when they connect to the system.

Restarting Workstation Services

If File Services for Macintosh cannot establish communications to the local RPC service, you may need to restart the Workstation Service.

To restart the Workstation Service, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Services**.
3. Click **Workstation**, and then click **Startup**.
4. In the **Set Service Properties** window, select whether you want Server for NFS to start automatically, manually, or whether you want to disable it.
5. Click **OK**.

Services for the Novell NetWare Operating System

Services for NetWare (SFN) are compatible with Novell® NetWare® Bindery service for authentication and file access using the internetwork packet exchange/sequenced packet exchange (IPX/SPX) network protocol. Services for NetWare are disabled by default.

For information about enabling SFN, see the file **install.rtf**, which is located in the **c:\sfn\fpnw** directory of your NAS system.

NOTE: SFN is not installed by default.

Configuring the NWLink IPX/SPX Compatible Protocol

To configure this protocol, you need the internal network number, frame type, and network number.

Internal Network Number

Internal network numbers are used for internal routing and are generally needed only for servers. You should not need to change this option on your system.

Frame Type and Network Number

Frame types define the packet formats that are used by different networks. It is important that all systems in a network have the same frame type so that they can communicate with the rest of the network.

When you are configuring your system, it attempts to automatically detect the frame type for the client. In most cases, this is successful. However, the automatic detection feature occasionally selects an inappropriate frame type, usually because more than one frame type exists on the network. If this happens, you should manually set the frame type to match the one specified

on your NetWare server.

NOTE: If more than one frame type exists, you should select the one that is detected first. For example, if the frame types Ethernet 802.2 and Ethernet 802.3 are bound to the same segment, configure frame type Ethernet 802.2. The order of detection is Ethernet 802.2, Ethernet 802.3, Ethernet II, and then Ethernet SNAP.

Configuring the IPX Protocol

By default, the IPX protocol is configured on the NAS system to automatically detect frame types. To use the IPX protocol, you must change your NAS system's IPX properties to manually detect frame types.

To configure the IPX protocol to manually detect frame types, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.
3. Log in to the NAS system as an administrator.

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

4. Right-click **Network Places** on the NAS system's desktop, and then click **Properties**.
5. In the **Network Connections** window, right-click the network adapter used by the NAS system and select **Properties**.
6. In the **Local Area Connection Properties** window, click **NWLink/IPX/NetBIOS Compatible Transport Protocol**, and click **Properties**.
7. In the **NWLink/IPX/NetBIOS Compatible Transport Protocol** window, select **Manual Frame type detection**.
8. Click **Add**.
9. In the **Manual Frame Detection** window, select a frame type, enter a network number for the IPX network, and then click **OK**.
10. Click **OK**.
11. Click **OK** to close the **Local Area Connection** window.
12. Close the **Network and Dial-Up Connections** window.

The IPX protocol is now configured on the NAS system to manually detect frame types.

Microsoft Directory Synchronization Services

Microsoft Directory Synchronization Services (MSDSS) allows you to synchronize a wide variety of data stored in the Active Directory service with Novell Directory Service (NDS) and NetWare 3.*x* binderies.

MSDSS is a highly flexible service that helps Novell users to perform the following tasks:

- Adopt Windows 2000 Server and the Active Directory service
- Reduce directory management through two-way synchronization
- Migrate NDS and bindery information to Windows 2000 Server

MSDSS supports two-way synchronization with NDS and one-way synchronization with NetWare 3.*x* binderies to provide a

complete directory interoperability solution. MSDSS also supports password synchronization and provides a directory migration service.

MSDSS allows NetWare users to deploy Active Directory without having to replace existing directories or bear the cost of managing two separate directories. As a result, users have the flexibility to:

- Consolidate directory management when multiple directories are required
- Manage accounts from either directory
- Use directory-enabled applications, devices, and services based on the Windows 2000 Active Directory service

MSDSS is easy to use and makes synchronization and Active Directory setup easy through its management interface. It is fully featured to allow users a choice of management, synchronization, and migration options.

MSDSS supports all major NetWare platforms and most Novell directories and binderies, and it includes support for IPX/SPX and TCP/IP network protocols.

Windows Server 2003 MSDSS Domain Controller

To implement MSDSS, you must install the Windows Server 2003 operating system and the MSDSS software (available on the *Microsoft Services for NetWare Version 5* or later CD) on at least one system. In Windows Server 2003, when you promote a system running Windows Server 2003 to an Active Directory server, it becomes a domain controller. You use this domain controller to configure Active Directory, install MSDSS, and then import information from the existing NetWare environment.

The larger the environment, the more new servers you need. If you are planning to have more than one domain, then you need new hardware for the first domain controller in each domain.

You must also install Novell Client Access software on the MSDSS server or servers. MSDSS uses Novell Client Access to authenticate and to access NDS. While accessing NDS, it authenticates, but does not use a license. MSDSS also uses Novell Client Access to map one directory's contents to another, taking into account the fact that the object classes in Novell's NDS or bindery directories are different from Active Directory object classes. Novell Client Access is also required to use the File Migration utility to migrate files.

You can install Novell Client Access in four modes: **IP only**, **IPX only**, **IP and IPX combined**, and **IP with IPX Compatibility Mode**. Most NetWare environments still use IPX. MSDSS works in all the modes because it uses Novell Client Access to access the lower layers.

If you are migrating NDS, you can import the user and group information from one NDS server to the MSDSS server because you have one user database per tree. You can then migrate the file system. Remember that each Novell server has its own file system, which is not replicated to other servers (whereas NDS is replicated to other servers). After the files are migrated, you can uninstall NDS from the server to provide more space for the Windows Server 2003 operating system.

Outline of the MSDSS Deployment Procedure

The next two sections describe the procedures for implementing MSDSS in a smaller (local area network [LAN] only) or larger (wide area network [WAN]) network. You should adapt the guidelines to suit your environment and goals.

Small Environment

A small company with a LAN-based, simple network is often a likely candidate for a quick migration. After doing all the preparations described in the previous section, perform the following steps (adjusted, if necessary, to your situation):

1. Back up your NetWare system and user data.

2. Install and configure a Windows domain controller (see the documentation that came with your operating system software).
3. Install the Novell Client for Windows from the Novell website at **www.novell.com/download**.
4. Replace services or applications that require NDS with software that is compatible with Active Directory. (Remove NDS applications before you begin using MSDSS, except for ZENworks, which can be replaced by IntelliMirror at any time.)
5. Install MSDSS from the system **DomainUtils** share.

   NOTE: To access MSDSS software, map a network drive to **\\Dell*xxxxxxx*\DomainUtils**, where *xxxxxxx* is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`.

6. Log in to the NDS tree or bindery server as `administrator`.
7. Log in to the appropriate Windows domain as a member of the Domain Admins group.
8. On the MSDSS server, open the Help files, and then print out the procedures "To perform a one-time migration" and "To migrate files."
9. Click the **Start** button, and then point to **Programs→ Administrative Tools→ Directory Synchronization** to start MSDSS.
10. Follow the instructions as described in the Help printout, "To perform a one-time migration." The prompts guide you through the following steps:
    a. Right-click **MSDSS** in the console tree, and then click **New Session** to start the New Session Wizard.
    b. Specify whether objects are to be copied from NDS or Bindery.
    c. Click **Migration**.
    d. If you plan to migrate files as well as directory objects, click the **Migrate Files** check box.

       You must also run the File Migration utility.
    e. Specify the path to the Active Directory container in which you want to copy items.
    f. Accept the default domain controller in which to store the migration log.
    g. Specify the NDS Container or Bindery Container from which to copy items.
    h. Provide the name and password of the Novell administrative account.
    i. On the **Initial Reverse Synchronization** page, specify the password options (such as **Set passwords to the user name**.)

       When you are performing a migration, this page does not include the option to actually perform an initial reverse synchronization, but it is the page where you specify which password option you want to use.
    j. Set **synchronization mode** to **default object mapping** or to **custom object mapping**.
    k. If you selected **custom object mapping**, you are prompted to manually establish one-to- one relationships between pairs of objects.
    l. Click **Finish**.

After the user accounts are migrated, you can migrate the file system (migrating the users before the files allows you to migrate file-system permissions). Follow the instructions in the Help printout, "To migrate files." The prompts guide you through the following steps:

- To start the File Migration Utility, click the **Start** button and point to **Programs→ Administrative Tools→ File Migration Utility**.

- To view mapping relationships, click **View Maps**.
- To view mapped access rights for the users, groups, organization units, and organizations to be migrated, click **Access Rights**.

  The **NDS Modify** option converts, by default, to **Read** because it does not have an equivalent 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 displays **Unavailable**, then you are not currently logged in to that tree or Bindery server. Log in, and then press <F5> after reselecting the volume to view the directories within the displayed volume.
- On the **Step 4 — Log File** tab, select your logging options, and then click **Next**.
- On the **Step 5 — Scan** tab, click **Scan**, and then click **Next**.

  The utility scans all source volumes and counts and displays the number of directories and files in each. It ensures that proper access has been given to each source volume, directory, and file. If any errors occur, the utility displays them under **NetWare scan logs** and **Windows scan logs**, respectively. You can select a number of acceptable errors; if this number is exceeded, the process aborts, allowing you to return to previous steps to correct the errors.
- On the **Step 6 — Migrate** tab, click **Migrate**.

Manually migrate (or use third-party utilities to migrate) object security permissions and system accounts, printer objects, application objects, and other objects that MSDSS does not migrate from Bindery or NDS to Active Directory. (MSDSS migrates NetWare user accounts, groups, and distribution lists for Bindery and NDS, and, for NDS only, MSDSS also migrates NDS organizational units and organizations.)

1. Upgrade your NetWare server(s) to the Windows 2000 Server or Professional, or Windows Storage Server 2003, operating system.
2. On each Windows desktop in your NetWare network, uninstall Novell Client Access.

   You must configure the desktops to join the Windows 2000 domain.
3. Optionally, upgrade NetWare clients (workstations) to the Windows 2000 Professional operating system.
4. Configure all client systems (both Windows and non-Windows), to join the Windows domain.

   Be sure that the users know how to handle their password the first time they log in (for possible password options, see "MSDSS Password Management" in "MSDSS Deployment: Understanding Synchronization and Migration)" at **www.microsoft.com**.

Medium-Sized or Large Environment

An organization large enough to have WAN links probably selects to synchronize its networks temporarily while performing a gradual migration over time (up to 3 months for a large network), or it prefers to use synchronization to establish a mixed Novell/Windows 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 domain controller (see the documentation that came with your operating system software).
3. Install the Novell Client for Windows from the Novell website at **www.novell.com/download**.
4. Install MSDSS from the NAS system **DomainUtils** share.

   NOTE: To access MSDSS software, map a network drive to **\\Dell*xxxxxxx*\DomainUtils**, where *xxxxxxx* is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`.

5. Log in to the NDS tree or Bindery server with administrative credentials.
6. Log in to the appropriate Windows domain as a member of the **Domain Admins** group.
7. On the MSDSS server, open the Help files, and then print out the steps (briefly summarized below) for "To perform a one-way synchronization" or "To perform a two-way synchronization."
8. Click the **Start** button, point to **Programs**→ **Administrative Tools**→ **Directory Synchronization** to start MSDSS, and then allow the prompts to guide you through the following tasks:
   a. Start the New Session Wizard (right-click **MSDSS** in the console tree).
   b. Select **Novell Bindery** or **Novell Directory Services (NDS)** for one-way synchronization, or select **Novell Directory Services (NDS)** for two-way synchronization.
   c. Select **One-way synchronization (from Active Directory to NDS or Bindery)** or select **Two-way synchronization (from Active Directory to NDS and back)**.
   d. Specify the path to the **Active Directory** container into which you want to copy items.
   e. Accept the default domain controller in which to store the session database.
   f. Specify the NDS Container or Bindery Container from which to copy items.
   g. Provide the name and password of the Novell administrative account.
   h. On the **Initial Reverse Synchronization** page, select **Perform an initial reverse synchronization**.
   i. Still on the **Initial Reverse Synchronization** page, specify the password options (such as **Set passwords to the user name**).
   j. On the **Object Mapping Scheme** page, click **Default** (to accept the default mapping for each source and target directory pair) or **Custom** (for NDS only), and then click **Object Mapping Table** (to specify objects for which you want to establish a one-to-one relationship, regardless of the object location in either directory tree).

      MSDSS does not support custom object mapping for Bindery.

   k. Still on the **Object Mapping Scheme** page, click **Filters** if you want to configure a filter for this synchronization session.
   l. On the **Session Name** page, accept the default session name or specify a new name.
   m. Click **Finish**.
9. If you selected one-way synchronization, you should now perform all user, group, and NDS organizational unit container (OU) object management from Active Directory. If you established two-way synchronization, you can now manage user, group, and OU objects from either Active Directory or NDS.
10. If you plan long-term coexistence between Active Directory and NetWare, you are now finished, unless you want to migrate a subset of users, systems, and/or files. If you plan to continue by migrating in stages from NetWare to Active Directory, perform the following tasks in the time-frame that is convenient for you:
    - Install and configure File and Print Services for NetWare (to allow NetWare clients access to files and printers on

Windows servers) and Gateway Services for NetWare (to allow Windows clients access files and printers on NetWare servers).

- Replace services or applications that require NDS with commensurate software compatible with Active Directory. Perform large conversions (such as GroupWise to Exchange) as separate projects.
- Migrate the pilot group of users and their files (adapt instructions from the migration steps provided in the "Small Environment" section). Get the pilot group's feedback, and then set a schedule to migrate additional groups of users, according to the priorities you have established.
- Migrate the rest of the users as appropriate (for example, if you migrate the set of applications they use, it is time to migrate them as well).

For more information, see the Novell website at **support.novell.com/servlet/Knowledgebase** and the Windows 2000 website at **www.microsoft.com/windows2000**.

Using Secure Sockets Layer

This section explains how secure sockets layer (SSL) are used in the NAS system. It also explains how to use your own certificate, if you have one, and how to regenerate your certificate.

Introduction to SSL Certificates

Certificates contain information used to establish system identities over a network. This identification process is called authentication. Although authentication is similar to conventional forms of identification, certificates enable Web servers and users to authenticate each other before establishing a connection to create more secure communications. Certificates also contain encryption values, or keys, that are used in establishing an SSL connection between the client and server. Information, such as a credit card number, sent over this connection is encrypted so that it cannot be intercepted and used by unauthorized parties.

Two types of certificates are used in SSL. Each type has its own format and purpose. *Client certificates* contain personal information about the clients requesting access to your site, which allows you to positively identify them before allowing them access to the site. *Server certificates* contain information about the server, which allows the client to positively identify the server before sharing sensitive information.

Server Certificates

To activate your Web server's SSL 3.0 security features, you must obtain and install a valid server certificate. Server certificates are digital identifications containing information about your Web server and the organization sponsoring the server's Web content. A server certificate enables users to authenticate your server, check the validity of Web content, and establish a secure connection. The server certificate also contains a *public key*, which is used in creating a secure connection between the client and server.

The success of a server certificate as a means of identification depends on whether the user trusts the validity of information contained in the certificate. For example, a user logging on to your company's website might be hesitant to provide credit card information, despite having viewed the contents of your company's server certificate. This might be especially true if your company is new and not well known.

For this reason, certificates are sometimes issued and endorsed by a mutually trusted, third-party organization, called a certification authority. The certification authority's primary responsibility is confirming the identity of those seeking a certificate, thus ensuring the validity of the identification information contained in the certificate.

Alternatively, depending on your organization's relationship with its website users, you can issue your own server certificates. For example, in the case of a large corporate intranet handling employee payroll and benefits information, corporate management might decide to maintain a certificate server and assume responsibility for validating identification information and

issuing server certificates. For more information, see "Obtaining a Server Certificate From a Certification Authority."

PowerVault 77*x*N Certificate

By default, your NAS system has a self-generated and self-signed certificate. The configured SSL port is 1279.

Using a Custom Certificate

If a certification authority is present in the network, the administrator can choose to change the default certificate for your NAS system. The administrator must use the wizards to first request a certificate and then apply it to the NAS system.

Obtaining a Server Certificate From a Certification Authority

NOTE: If you are replacing your current server certificate, the Internet Information Server (IIS) continues to use the old certificate until the new request has been completed.

Find a certification authority that provides services that meet your business needs, and then request a server certificate.

NOTE: For the latest list of certification authorities supporting IIS, see the Microsoft Security website. In the **By Category** list, select **Certification Authority Services**.

To obtain a server certificate, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**, and then click **Remote Desktop**.
3. Log in to the NAS system as an administrator.

   NOTE: The default administrative user name is `administrator` and the default password is `powervault`.
4. Double-click the **NAS Utilities** icon on the NAS system's desktop.
5. In the **NAS Utilities** window, double-click **Administrative Tools**, and then double-click **Internet Information Services**.
6. Double-click the local system to expand it, and then double-click **Web Sites**.
7. Right-click the **Administration** icon, and then select **Properties**.
8. In the **Administration Properties** window, click **Directory Security**.
9. Click **Server Certificate** to access the Web Server Certificate Wizard.
10. Use the Web Server Certificate Wizard to create a certificate request.
11. Send the certificate request to the certification authority.

    The certification authority processes the request and sends you the certificate.

    NOTE: Some certification authorities require you to prove your identity before processing your request or issuing you a certificate.
12. Use the Web Server Certificate Wizard to install your certificate.

For more information about SSL, see the Internet Information Server online help.

Using DFS

DFS creates a logical, hierarchical view of file shares that exist on servers distributed in one or more Windows 2000/Windows Server 2003 domains. DFS can help you manage file resources on distributed enterprise networks, and it enables users to locate files across the network without needing to know the physical server on which the data is stored.

Two methods are available to deploy DFS—stand-alone or integrated into the domain.

Stand-alone DFS does not require Active Directory (AD), and does not have the full functionality of DFS. It is mostly intended for backwards compatibility and support for networks without AD. Domain integrated DFS takes full advantage of all the intended functionality by utilizing AD. Some of the functionality domain-integrated DFS offers is load-balancing, fault-tolerance, and Kerberos-based security.

NOTE: Only one DFS root is allowed on the Standard Edition of the Microsoft Windows Storage Server 2003 operating systems. Multiple DFS Roots are allowed in the Enterprise Edition of the Microsoft Windows Storage Server 2003 operating system.

Creating a Standalone DFS Root

1. Use the Windows operating system to create a directory on the NAS system.

   This directory will become the DFS root
2. Right click the directory you created and select **Sharing and Security**.
3. Click **Share this folder**. and then click **OK**.
4. Access the DFS utility.
   a. In the NAS Manager, click **Maintenance**.
   b. Click **Remote Desktop**, and then log in to the NAS system as an administrator.

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

   c. On the NAS system desktop, double-click **NAS Utilities** to display the **NAS Utilities** window.
   d. Double-click **Administrative Tools** to expand the list to show **Distributed File System**.
5. Right-click **Distributed File System** and click **New Root**.
6. Click **Next** in the **New Root Wizard** window.
7. Click **Stand-alone root** and then click **Next**.
8. Select the server that will host the DFS root, or click **Browse** to find the server if you do not know the name, and click **Next**.
9. For **Root name**, enter the name of the directory that you created in step 1.
10. Enter additional comments, if necessary, and click **Next**.
11. Click Finish to create the DFS root.

NOTE: For information about creating DFS links see "Publishing a Share in DFS" or "Creating Shares in DFS."

Creating a Domain-Integrated DFS Root

1. Use the Windows operating system to create a directory on the NAS system.

   This directory will become the DFS root.
2. Right click the directory you created and select **Sharing and Security**.
3. Click **Share this folder**. and then click **OK**.
4. Access the DFS utility.
   a. In the NAS Manager, click **Maintenance**.
   b. Click **Remote Desktop**, and then log in to the NAS system as an administrator.

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

   c. On the NAS system desktop, double-click **NAS Utilities** to display the **NAS Utilities** window.
   d. Double-click **Administrative Tools** to expand the list to show **Distributed File System**.
5. Right-click **Distributed File System** and click **New Root**.
6. Click **Next** in the **New Root Wizard** window.
7. Click **Domain root** and then click **Next**.
8. Enter the domain that the new root will be a part of in **Domain name**.
9. Select the server that will host the DFS root, or click **Browse** to find the server if you do not know the name, and click **Next**.
10. For **Root name**, enter the name of the directory you created in step 1.
11. Enter additional comments, if necessary, and click **Next**.
12. Click Finish to create the DFS root.

NOTE: For information about creating DFS links see "Publishing a Share in DFS" or "Creating Shares in DFS."

Creating Shares in DFS

After creating a DFS Root (see "Creating a Standalone DFS Root") perform the following steps to create DFS links.

NOTE: The directory that is to be added to the DFS structure must be shared.

1. Access the DFS root.
   a. In the NAS Manager, click **Maintenance**.
   b. Click **Remote Desktop**, and then log in to the NAS system as an administrator.

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

   c. On the NAS system desktop, double-click **NAS Utilities** to display the **NAS Utilities** window.

d. Double-click **Administrative Tools** to expand the list, and then double-click **Distributed File System** to display the DFS root(s).

2. Right click the DFS root to which you want to link and click **New Link**.
3. For **Link name** enter a name for the new link.
4. Enter the path to the shared resource on the target server.
5. Add comments if desired.
6. Click **OK**.

Back to Contents Page

Back to Contents Page

Security Recommendations

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

- Standard Security Recommendations
- Additional Security Recommendations
- Maximum Security Recommendations

Standard Security Recommendations

This section provides information about standard security practices that Dell recommends to secure your NAS system:

Non-Secure HTTP Ports

The NAS Manager can be connected to through port 1279, which uses Secure Sockets Layer (SSL) to encrypt data going to and coming from the NAS system to provide data security. See "Using Secure Sockets Layer" for more information.

The system can also be connected through port 80, which is not SSL-encrypted. It is recommended to disable nonsecure http ports in the NAS Manager.

Passwords

The default administrator user name for your NAS system is `administrator` and the default password is `powervault`. Change the default administrator password as soon as possible. See "Changing the Administrator Password." Additionally, Dell recommends the following password practices for your NAS system:

- Use passwords that are longer than six characters.
- Do not use blank or simple passwords.
- Do not use dictionary words.
- Do not use personal information such as name, children's names, birth dates, and so forth.
- Use a mix of numerals and upper and lowercase letters. For example, *Rs4326tH*.

FTP and Telnet

For security reasons, FTP and Telnet are disabled by default on the NAS system. If either of these protocols are enabled on a share on the NAS system and you need to disable them, see "Removing a Protocol From the Share."

Antivirus Software

Dell recommends using antivirus software on your NAS system to protect against viruses.

Microsoft Security Updates

Microsoft regularly posts security update patches to its website at **microsoft.com**. Dell recommends that you regularly check to ensure that your NAS system has the most recent security update.

Apple Environments

If you are using your NAS system in an Apple environment, install the Microsoft® User Authentication Module (UAM) on the NAS system. If AppleTalk is not installed on the NAS system, client access is not encrypted. See "File Server for Macintosh" for more information.

Secure Socket Layer (SSL) Certificates

SSL certificates enable Web servers and users to authenticate each other before establishing a connection to create more secure communications. See "Using Secure Sockets Layer" for information.

Microsoft Baseline Security Analyzer

Use the Microsoft Baseline Security Analyzer (MBSA) to search for any security vulnerabilities. MSSA scans Windows-based servers for common security misconfigurations. The tool scans the operating system and other installed components such as Internet Information Services (IIS). MBSA also checks systems for missing security patches, and recommends critical security patches and fixes.

Additional Security Recommendations

In addition to the practices mentioned in "Standard Security Recommendations," Dell recommends the following practices to ensure security:

- Format all volumes as NTFS.
- Disable automatic log on.
- Disable the guest account.
- Do not install IIS sample applications.
- Disable parent paths.
- Move the MSADC and Scripts virtual directories from the default website to another location.

Ensure that you place appropriate restrictions on any Anonymous Logon groups. To allow UNIX® users who do not have Windows user accounts to access resources on a system running Windows, you must explicitly add the Anonymous Logon group to the Everyone group and assign the Anonymous Group appropriate permissions. For more information, see."Server for Network File System (NFS)."

Maximum Security Recommendations

This section provides information about practices recommended for maximum security on your NAS system.

- Allow no more than two administrators on the NAS system.
- Do not allow passwords that have no expiration date.
- Enable Logon Success and Logon Failure auditing.
- Disable unnecessary services.
- Disabling unnecessary services also increases performance.
- Remove the IISADMPWD virtual directory.
- Enable application logging options for all Web and FTP sites.
- Ensure that Internet Explorer zones have secure settings for all users.
- Use the NAS system only for shares and services that are actively used.
- Disable http sharing if http shares are not used.

Disabling HTTP Shares

1. Log in to the NAS Manager.
2. Click **Shares**.
3. On the **Shares** page, click **Sharing Protocols**.
4. Click **HTTP** and then click **Properties**.
5. Click **Security**.
6. Click **Disable Web Sharing**.

Back to Contents Page

Back to Contents Page

Troubleshooting

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

- Tools and Techniques
- Troubleshooting

Tools and Techniques

Because your Dell™ PowerVault™ NAS system is a "headless" system that does not have a keyboard, mouse, or monitor, you must use other methods for troubleshooting issues and conditions. This section provides suggestions for and information about alternative troubleshooting tools and techniques.

Ping Your NAS System

If you are unable to connect to the NAS system using the NAS Manager, try to ping the NAS system. From a client system, click the **Start** button, click **Run**, and then type `cmd`. At the command prompt in the **cmd.exe** window, type `ping` *`system_name`*, and then press <Enter>.

NOTE: The default system name is DELL*xxxxxxx*, where *xxxxxxx* is the system's service tag number. For example, if your service tag number is 1234567, type `http://DELL1234567`. You can also access the system directly through secure port 1279 by connecting to https://DELL*xxxxxxx*:1279, where *xxxxxxx* is the system's service tag number.

If you can ping the NAS system but cannot access it through the NAS Manager, your NAS system might still be booting into the Microsoft® Windows® operating system and might not have started the Microsoft Internet Information Services (IIS).

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

My Network Places

If you have a client system running Windows 2000 or Windows XP on the same subnet as the NAS system, double-click **My Network Places**. Browse through the network and locate your NAS system.

System LEDs and Beep Codes

If your NAS system is not booting or responding properly, you can diagnose some problems using the system's LEDs and beep codes. For more information about the LEDs and beep codes, see your system's *Installation and Troubleshooting Guide*.

Remote Desktop

You can use the Remote Desktop to connect to your NAS system from a client system. You can access Remote Desktop through the NAS Manager.

To access Remote Desktop from the NAS Manager, perform the following steps:

1. Log in to the NAS Manager.
2. Click **Maintenance**.
3. Click **Remote Desktop**.
4. Enter the administrator user name and password and click **OK**.

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

Troubleshooting

Use the following tables to help you troubleshoot various conditions that might occur on your NAS system:

- Table 10-1, "General Troubleshooting"
- Table 10-2, "NAS Manager"
- Table 10-3, "UNIX and Red Hat Linux"
- Table 10-4, "Macintosh and AppleTalk"

Table 10-1. General Troubleshooting

Issue	Possible Cause	Resolution
I just created a new volume on my system but cannot see the volume on Windows Explorer through Remote Desktop.	Remote Desktop cannot update to show a new volume during the session in which it was created.	Log off Remote Desktop. When you reconnect to Remote Desktop, the volume should be visible.
I see the following error message in the event log: `WMI ADAP was unable to load the winspool.drv performance library due to an unknown problem within the library: 0x0`	This is an issue with the WDAP Performance library and is documented on Microsoft's website.	Connect to the system via Remote Desktop, and then open a local command prompt. Type the following command: `WINMGMT/CLEARADAP`. When the prompt returns, type `WINMGMT/RESYNCPERF winmgmt service PID`.
I have just enabled FTP services on my NAS system, but I am unable to upload files using FTP even though I am the administrator.	By default, no user has write privileges on the default FTP site.	The FTP permissions must be configured using the Microsoft Management Console (MMC). To access the MMC, log into **Remote Desktop**. Right click **My Appliance**, and select **Manage**.Double-click internet Information Services, and then right-click **FTP Sites**. Set the permissions in the **FTP Sites Properties** window.
I have deleted an FTP share and folder from my NAS system. However, when I use Remote Desktop to confirm the removal, I can still see the shared folder in the FTP section of the MMC.	By default, this folder is not deleted by the NAS Manager.	Manually remove this listing from the listed shared folders in the FTP section of the MMC.
The BIOS does not see hard drive 0.	The hard drive has failed or the operating system files or boot record is missing or corrupt.	The NAS system can automatically boot from hard drive 1. See "Recovery From System Failure."
I cannot connect to or ping the NAS system after turning it on.	The NAS system has not finished booting.	Wait at least 5 minutes for the NAS system to finish booting. If you still cannot connect, attempt the procedures in "Solutions to Try Before Reinstalling" in "Recovering and Restoring the System."
My network connection seems	You are using a Broadcom	Your system's network connection will operate at a speed

slow.	NetXtreme Gigabit Ethernet Server Adapter without the correct drivers, and you have enabled the wake-on-LAN (WOL) feature through the System Setup program.	of 10/100 until the operating system loads the correct drivers. When the correct drivers are installed, the connection speed will increase to 10/100/1000.
I cannot get console redirection to work correctly. Only a few keys work on the keyboard, and none of the keys work when trying to configure the BIOS.	<Scroll Lock>, <Caps Lock>, or <Num Lock> might be set on your keyboard. Also, your operating system may not support all of the keys on your keyboard.	Ensure that the <Scroll Lock>, <Caps Lock>, and <Num Lock> lights are turned off on the keyboard. If these lights are not on and the problem persists, see "Ping Your NAS System" in "Advanced Features."
During a Remote Desktop session to the NAS system, I mapped a network share from the NAS system. Now the system does not reboot correctly and hangs during shutdown.	Having a share mapped from the NAS system causes the system to hang during shutdown.	Make sure that when you map a share, you do not select **Reconnect at logon**. To disconnect the drive, right-click **My Appliance** on the NAS system desktop, and select **Disconnect Network Drive**. Click the CD share in the **Disconnect Network Drive** window, and then click **OK**. If you cannot log in to the NAS system, reboot the system. Then connect using Remote Desktop and disconnecting the drive. If Remote Desktop does not work, try connecting directly to the NAS system with a keyboard, monitor, and mouse. See "Configuring Your System Using a Keyboard, Monitor, and Mouse" in "Initial Configuration."
I cannot connect to the NAS system using the IPX protocol.	IPX networks require that you assign an IPX network number to all clients. By default, the NAS system does not assign an IPX number to the network.	Change the IPX protocol on the NAS system to manually detect frame types. See "Configuring the IPX Protocol" in "Advanced Features."
After restoring files from a backup, the modified dates of folders are inconsistent.	The modified dates of folders reflect either the date you performed the restore or the date the folder was modified.	Do not take action. This design issue occurs only with folders; the files' modified dates are consistent.
When connecting to my NAS system using Remote Desktop, I receive a message that the Terminal Server has exceeded the maximum number of allowed connections.	The NAS system supports only two current Remote Desktop sessions at a time.	Log off of the other Remote Desktop sessions.
The system summary and the task manager show twice as many processors as are actually installed in the system.	The NAS system provides a hyperthreading option, which allows one physical processor to appear to the operating system and other applications as two logical processors.	Do not take action. Your NAS system is operating correctly.

Table 10-2. NAS Manager

Issue	Possible Cause	Resolution
I am trying to select the **Administer My Appliance** link on the opening page of the NAS Manager, but the link does not function properly.	The user account that you used to log in to the domain does not have administrator privileges. The link does not work for users without administrator privileges.	Type the address of the NAS Manager in your browser. For SSL connections, type: `https://`*`servername`*`:1279` or `https://`*`IPaddress`*`:1279`
I have just deleted a volume, and now I am unable to view my shares in the NAS Manager.	If a volume with shares is deleted, then the NAS Manager cannot display any shares until the shares that were directed to the deleted volume are removed.	Use Remote Desktop to remove the shares for the deleted volume. Exit the NAS Manager, and restart the system. The shares should now be visible.

I have just added an HTTP share but cannot see it from the NAS Manager.	For security purposes, directory browsing is not enabled by default on an HTTP share directed to the same folder or volume as another share.	To enable directory sharing for an HTTP share, from the NAS Manager **Maintenance** page, click **Remote Desktop**, and then modify the Web sharing properties of the folder.
I have just changed the IP address of my system, and now I cannot administer it through the NAS Manager.	Although the IP address changed, your local host is still trying to communicate with the system using the old IP address. It takes approximately 15 minutes for the IP address to automatically update on most networks.	Close Microsoft Internet Explorer. Reconnect using the newly created IP address. Type: `https://IPaddress:1279`. It takes approximately 15 minutes for the DNS server to recognize the new IP address.
I can only see the first 100 items in the NAS Manager Web user interface.	The NAS Manager will only display 100 items per page.	To display the next 100 items, click the down-arrow icon at the top of the list.
In the NAS Manager, if I click **OK** and then click **Cancel**, it doesn't seem to cancel the operation.	Clicking **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.
When I select the **Check All** box and then deselect one or more choices on some screens in the NAS Manager, the **Check All** box remains selected.	The **Check All** box is not automatically deselected. However, this does not mean that all items in the list are selected.	This behavior does not affect functionality. The **Check All** box does not indicate what has specifically been selected or deselected.
I have changed the password for the administrator account; however, several minutes have passed and I have not been primoted for the new password.	The NAS Manager does not automatically refresh the account information for the administrator while in the NAS Manager. Instead, it performs the refresh as a timed function.	The password was successfully changed. If you want to confirm that the new password is in effect, close the browser, and then reconnect. The new password should work, but the old one should not.
I am looking for a topic on the context-sensitive online help in the NAS Manager, but it says `No Topic Available`.	Some sections of the NAS Manager do not have context-sensitive help.	For information on a specific function, see the Windows Powered Help, which is available by logging into a Remote Desktop Session and clicking the **Start** button and selecting **Help and Support**. You can also see the appropriate section in this *Administrator's Guide*.
I tried to clear the FTP log or the Web (HTTP) Shares log in the **Maintenance** section of the NAS Manager, but I received an error message and the log was not cleared.	The logs are currently locked by the NAS system for the FTP service and to support the NAS Manager. The logs cannot be cleared in the NAS Manager.	Connect to the NAS system using Remote Desktop and clear these logs by using MMC. You can access MMC by logging into a Remote Desktop session and then right-clicking **My Appliance** and selecting **Manage**.
While viewing the properties of a user, I selected the **General** tab. The fields for this user are now all blank.	You were already on the **General** tab and the page did not refresh properly.	Select **Cancel** or click **Back** on your browser. Reselect the user for whom you wanted to view properties.
I added members to a local group using the NAS Manager, but when I click **OK**, the screen only refreshes.	You might have removed and then added the same member to the local group. This may cause the screen to refresh instead of update correctly.	Reselect the **Local Groups** tab in the NAS Manager primary menu. Add or remove the appropriate members to or from the local group.
I cannot change the WINS addresses when I click **Network** on the NAS Manager primary menu, click **Network Interfaces**, and then click **WINS** in the **Tasks** list.	The NAS Manager grays out the **WINS Servers Configuration** page unless you set the **IP Address Configuration** page to **Use the following IP settings**.	To set the WINS addresses from the NAS Manager, click **Network** on the primary menu, click **Interfaces**, and click **IP** in the **Tasks** list. On the **IP Address Configuration** page, click the radio button for **Use the following IP settings**, and then type the IP address, Subnet mask, and the default gateway in the appropriate text boxes.

Table 10-3. UNIX and Red Hat Linux

Issue	Possible cause	Resolution
I cannot access the NAS Manager from my Red Hat® Linux client system.	The NAS Manager is not supported by the Red Hat Linux operating system and does not work with the NAS Manager.	Use a client system running Windows to connect to the NAS Manager.
While updating client access to an NFS share, the **No Access** option is displayed, but the **Root** option is not.	Only the **All Machines** category options are displayed during this update.	Add the appropriate client systems, and then select **OK**. After you have added the client system, navigate back to the **NFS** tab for this share and select the correct options for the individual **Client Machines**.
Every time I try to obtain a directory listing from an NFS client on the root of a system volume, I get an error message, such as `Permission Denied`.	The problem you are experiencing involves a **System Volume Information** directory created by Microsoft Index Server. The NFS service does not have access to this directory and returns an error message to the client when trying to list its properties. This issue only occurs when sharing the root of a drive letter.	Ignore this error. The **System Volume Information** directory is not used by NFS clients or your system by default.
Sometimes I am unable to delete folders that have been used and that are shared to a client system that is running NFS.	This situation occurs with NFS discretionary access lists (DACLs) and inheritance. When the folder to be shared is created, the only access control entry (ACE) created by default is **Everyone** with **Full Control**. When an NFS client creates a directory or a file in this directory (mounted share), Services for UNIX® (SFU) creates a new DACL that replaces the inherited **Everyone** with **Full Control** ACE. This DACL contains an **Everyone** ACE with the appropriate UNIX file creation access and may contain two other ACEs for the mapped user and group. If this happens, the administrator of the client system that is running Windows cannot delete the file or directory unless that administrator takes ownership through the client system that is running Windows and changes the access.	As the administrator, use a client system running Windows to take ownership and change the access to allow yourself to delete the share folders. When you delete the NFS share folders, ensure that there are no open file handles for the share. If you are unsure, delete the share, and then restart NFS.
When updating the client system's access to an NFS share, the **All Machines** client group is reset from the **No Access** access type to **Read-Write** access.	The NAS Manager might reset the **All Machines** client system's group to **Read-Write** when the client systems do not have read-only or read-write access.	Add a client system that has read-write or read-only access, and then set the **All Machines** client system group to **No Access**.
My NAS system is	NFS write-back cache is disabled.	If your system is not part of a cluster, you

experiencing low NFS performance.		can enable NFS write-back cache to improve performance. See "Advanced Features" for more information.
The BIG5, EUC-KR, EUC-TW, GB2312-80, KSC5601, and Shift-JIS character encoding schemes for NFS shares cannot be specified in the NAS Manager.	The NAS Manager user interface supports only EUC-JP and ANSI character encoding for NFS shares.	Access the NAS system's desktop and modify the NFS share properties of the folder directly.
The NFS client system group **All Machines** is reset to **No Access** when another client system group is set with the same access permissions and root.	Setting a client group to use the same permissions as **All Machines** causes **All Machines** to be reset to **No Access**.	Access the NAS system's desktop and modify the NFS share properties of the folder directly.
I am getting inconsistent map definitions when I use the NAS Manager and the MMC to create user name maps.	Modifications to user name maps are cached and may not take effect immediately.	Use only one tool to administer user name maps.

Table 10-4. Macintosh and AppleTalk

Issue	Possible cause	Resolution
I am getting event errors for Services for Macintosh.	Services for Macintosh are bound to the onboard NIC by default. If this NIC has been disabled, binding errors occur.	Bind the AppleTalk protocol to an enabled NIC. See "AppleTalk Protocol Adapter Binding" in "Advanced Features."
From a Macintosh client, users cannot modify or delete a file that a Windows client has accessed.	The time between clients and the system is not properly synchronized.	Ensure that client systems have their time synchronized to within 10 minutes of the time zone.

Back to Contents Page