Dell PowerVault

NX3500 System

Administrator’s Guide

Notes and Cautions

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

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

2012 - 01 Rev. A02

Contents

1

Introduction

The Dell PowerVault NX3500 clustered network attached storage (NAS) system is a high-availability storage solution. The solution aggregates multiple NAS controllers in a cluster and presents them to UNIX, Linux, and Microsoft Windows clients as one virtual file server.

About This Document

This document provides information on the features available to the storage administrator. It is organized as follows.

Chapter	Description
Introduction	Provides information on the PowerVault NX3500 cluster solution architecture and features.
Setting Up Your PowerVault NX3500 Solution	Provides instructions on setting up the PowerVault NX3500, the various topologies, and cabling options. It also includes the detailed setup procedure and available configuration options.
Accessing the Dell PowerVault NAS Manager	Provides an overview of the NAS Manager web console and instructions for accessing it.
Monitoring PowerVault NX3500	Provides descriptions and procedures for monitoring the PowerVault NX3500.
Monitoring PowerVault NX3500 Events	Provides procedures for searching events and defining queries.
Using Volumes, Shares, and Quotas	Provides instructions for managing NAS volumes, shares, and quotas.
Protecting Data on PowerVault NX3500	Provides procedures for configuring data protection options such as, snapshots, replication, and backup agent.

Chapter	Description
Managing the PowerVault NX3500	Provides procedures and descriptions about the initial configuration, system information, users management, license management, system time, networking, protocols, authentication, monitoring configuration, and maintenance.
Maintaining the PowerVault NX3500	Provides procedures for shutting down, powering up, upgrading, and running diagnostics.
Troubleshooting	Provides information on troubleshooting your NAS storage solution.
Command Line Interface	Provides basic information for using the PowerVault NX3500 CLI.
Internationalization	Provides information about unicode support in PowerVault NX3500.
BPS Alarms	Contains additional information on troubleshooting the Dell Backup Power Supply (BPS).
NAS Setup Worksheet	Provides a worksheet that will help you set up and configure your solution.

Other Information You May Need

Document	Description
Getting Started Guide	Provides an overview of system features, setting up your solution, and technical specifications. This document is shipped with your system and is also available at **support.dell.com/manuals**.
Hardware Owner's Manual	Provides information about solution features and describes how to troubleshoot the system and install or replace system components. This document is available at **support.dell.com/manuals**.
Rack Installation Instructions	Describes how to install your system into a rack. This document is shipped with your rack solution and is also available at **support.dell.com/manuals**.
Online Help	Provides information about configuring and managing the NAS Manager. The online help is integrated with the system and can be accessed from the NAS Manager.

Terms Used in the Document

Table 1-1. PowerVault NAS System Terms

Term	Description
Backup Power Supply	Provides back up battery power in the event of a power loss.
Client access VIP	Virtual IP addresses that clients use to access CIFS shares and NFS exports hosted by a PowerVault NAS system. The PowerVault NAS system supports multiple client access Virtual IPs (VIPs).
Controller (NAS controller or nodes)	NAS appliance installed with the Dell Fluid File System (FluidFS) software.
Controller pair	Two NAS controllers that are configured as pair in a PowerVault NAS clustered system. Cache data is mirrored between the paired NAS controllers.
Data Management Application (DMA)	Also known as the Backup Application Server.
Dell PowerVault Modular Disk Storage Manager (MDSM)	The management software that ships with the PowerVault MD32x0i or MD36x0i array.
Fluid File System	High-performance, scalable file system software installed on NAS controllers.
Host Port Identifier	Unique ID used to identify hosts in a network.
Internal network A (peer connection)	The PowerVault NX3500's internal network consists of two independent Gigabit Ethernet ports. The internal network is the infrastructure for PowerVault NX3500 clustering, including the heartbeat monitor, data transfer, and mirroring information between the controllers.
Internal network B (internal management or IPMI)	The PowerVault NX3500 internal management network (also known as internal network b) connects both controllers. All administrative related functions and controller reboots are performed on this network.

Table 1-1. PowerVault NAS System Terms *(continued)*

Term	Description
LAN or client network (primary network)	The network through which clients access NAS shares or exports. The PowerVault NAS system is connected to customer's IT environment and its NAS clients using this network.
NAS storage pool	Virtual disks created on the PowerVault MD32*x*0i or MD36*x*0i storage arrays dedicated to the PowerVault NX3500 system.
NAS volume (NAS container or virtual volume)	A virtualized volume that consumes storage space in the NAS storage pool. Administrators can create CIFS shares and NFS exports on a NAS volume and share them with authorized users. A PowerVault NAS system supports multiple NAS volumes.
NAS replication	Replication between two PowerVault NAS systems or between two NAS volumes.
NAS replication partners	PowerVault NAS systems participating in a replication activity.
Network Data Management Protocol	Network Data Management Protocol (NDMP) used for backup and restore.
Peer controller	The peer NAS controller with which a specific NAS controller is paired in a PowerVault NAS system.
Power module (battery unit)	One of the battery units in a BPS.
PowerVault MD3*xx*0i	Refers to the PowerVault MD3200i, MD3220i, MD3600i, MD3620i iSCSI storage solutions.
PowerVault NAS Configuration Utility (NASCU)	The setup wizard used to initially discover and configure a PowerVault NAS system. This utility is only used for the initial setup.
NAS Manager	The web-based user interface, which is part of the PowerVault NX3500 software, used to manage the PowerVault NAS system.
PowerVault NAS system	A fully configured, highly-available and scalable NAS appliance, providing NAS (CIFS and/or NFS) services, which is comprised of a pair of NAS controllers, a BPS, a PowerVault storage subsystem, and the NAS Manager.

Table 1-1. PowerVault NAS System Terms *(continued)*

Term	Description
Standby controller	A NAS appliance that is installed with the FluidFS software but not part of a cluster. For example, a new or replacement controller from the Dell factory is considered as a standby controller.
SAN network (iSCSI network)	The network that carries the block level (iSCSI) traffic and to which the storage subsystem is connected. **NOTE:** It is recommended that this network be isolated from the LAN or client network.

PowerVault NX3500 Architecture

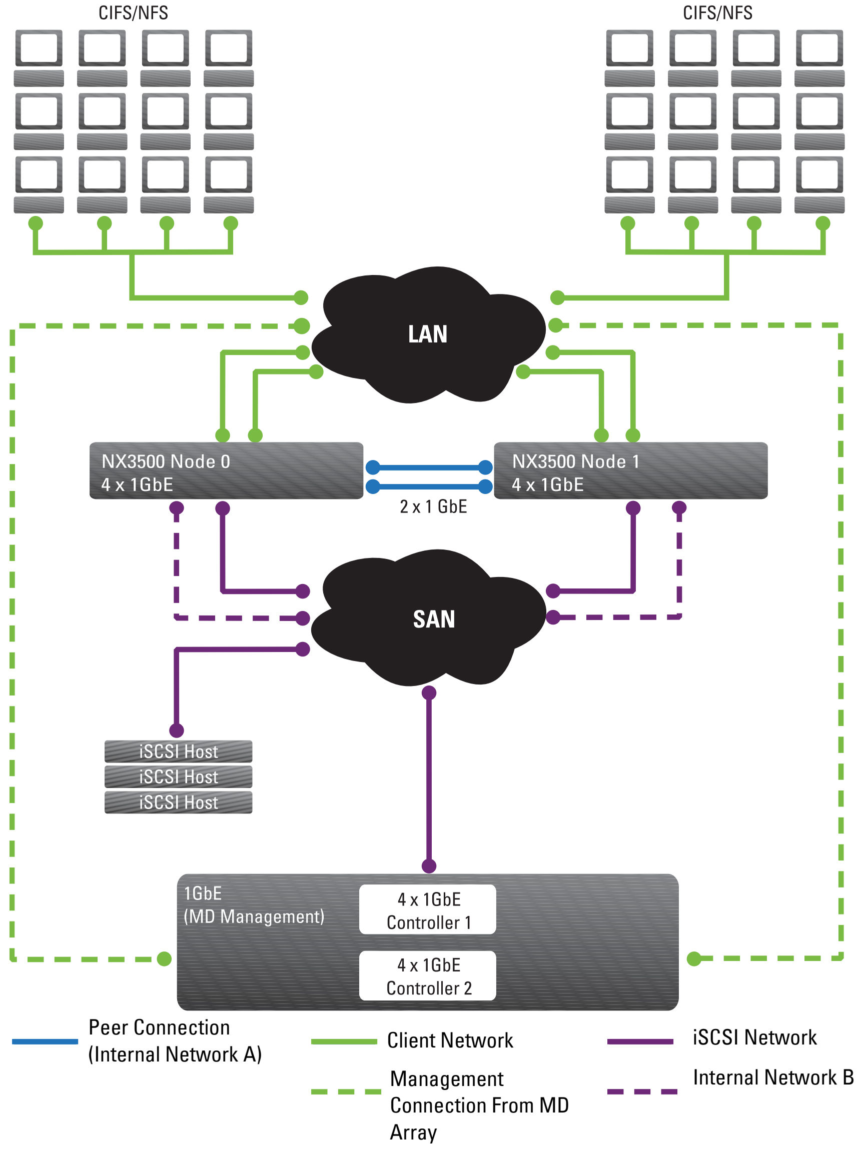
The PowerVault NX3500 combined with MD3*xxx*i provides you with a unified storage solution (see Figure 1-1). This solution provides you with access to both block and file storage (see Figure 1-2).

The PowerVault NX3500 clustered NAS solution consists of a pair of controllers and the PowerVault Modular Disk (MD) iSCSI storage array. In addition, both controllers are protected by BPS, which helps protect data during power failure.

Each controller has:

- Two connections (four for the solution) to the customer's LAN or client network.
- Two connections (four for the solution) to the customer's SAN network.
- Two controller peer to peer connections for the cluster's internal network.

Figure 1-1. PowerVault NX3500 Architecture



Key Features

The PowerVault NX3500:

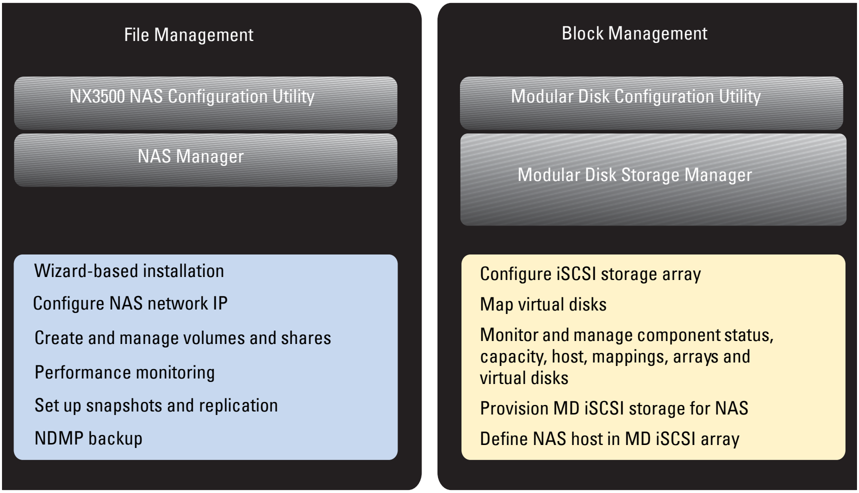
- Helps administrators expand existing capacity and improve performance when needed, without impacting the applications or users.
- Provides administrative functions for storage administrators who perform day-to-day system operations and storage management.
- Has a distributed file system, which creates a single interface to the data.
- Uses a quad core processor per controller.
- Is capable of storing terabytes in a single file system.
- Allows for dynamic increase in capacity.
- Has a centralized, easy to use, web-based NAS management console.
- Has on-demand virtual storage provisioning.
- Has granular disk space management.
- Is capable of providing user-accessible Point-In-Time snapshots.
- Is capable of sharing files with Microsoft Windows, Linux, and UNIX users.
- Offers flexible, automated online replication and disaster recovery.
- Features built-in performance monitoring and capacity planning.

PowerVault NX3500 Views

You can access the PowerVault NX3500 as a client or an administrator depending on the access privileges you have.

NOTE: It is recommended that you do not attempt to log on to both the CLI and NAS Manager at the same time.

Figure 1-2. File-Level Storage and Block-Level Storage


File Management
NX3500 NAS Configuration Utility
NAS Manager
Wizard-based installation
Configure NAS network IP
Create and manage volumes and shares
Performance monitoring
Set up snapshots and replication
NDMP backup
Block Management
Modular Disk Configuration Utility
Modular Disk Storage Manager
Configure iSCSI storage array
Map virtual disks
Monitor and manage component status, capacity, host, mappings, arrays and virtual disks
Provision MD iSCSI storage for NAS
Define NAS host in MD iSCSI array

Client View

To the client, the PowerVault NX3500 presents itself as a single file-server with a single file system, IP address, and name. The PowerVault NX3500's global file system serves all users concurrently without performance constraints. It offers end users the freedom to connect to the PowerVault NX3500 using their respective operating system's NAS protocols.

- NFS protocol for UNIX users.
- CIFS protocol for Windows users.

Administrator View

As an administrator, you can use either the CLI or the NAS Manager to configure or modify system settings, such as configuring protocols, adding users, and setting permissions.

The NAS Manager provides access to system functionality, using standard internet browsers.

System Components

The PowerVault NX3500 system consists of:

- Hardware
  - NAS controller pair
  - MD PowerVault storage
  - Backup power supply
- Network
  - SAN network
  - Internal network
  - LAN or client network

NAS Controller Pair

The PowerVault NX3500 clustered NAS solution consists of two NAS controllers configured as a pair. This redundant configuration ensures that there is no single point of failure. The controllers handle load balancing of client connections, manage read-write operations, perform caching, and interface with servers and workstations. The cluster and its internal networks are consolidated using a virtual IP.

The PowerVault NX3500 software is installed on both controllers. The software is a complete package, consisting of an operating system, volume management, distributed file system, and clustering technology.

Read-write operations are handled through mirrored non-volatile RAM (NVRAM). Mirroring the cache data between the paired NAS controllers, ensures a quick response to clients' requests, while maintaining complete data integrity. Data from the cache to permanent storage is transferred asynchronously through optimized data-placement schemes.

Each controller is equipped with a 12 GB RAM, most of which is used for caching. The file system uses the cache efficiently to provide fast and reliable writes and reads. Writing or modifying files occurs first in the cache. Data is then mirrored to the peer controller’s cache. This feature ensures that all transactions are duplicated and secured.

PowerVault MD Storage

The controllers connect to the PowerVault MD iSCSI storage array, which is a RAID subsystem. RAID storage subsystems are designed to eliminate single points of failure. Each active component in the storage subsystem is redundant and hot-swappable. The solution supports typical RAID configurations including RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10.

BPS

The BPS provides continuous power to the controllers. Each controller receives its power from a dedicated BPS and from the power grid. The controllers regularly monitor the BPS battery status, which requires the BPS to maintain a minimum level of power for normal operation. The BPS has sufficient battery power to allow the controllers to safely shut down.

The BPS enables the controllers to use the cache as NVRAM. The BPS provides the clustered solution enough time to write all the data from the cache to the disk if the controller experiences a loss of power.

NOTE: You can view the BPS events on the NAS Manager.

SAN Network

The SAN network is a critical part of the PowerVault NX3500 solution. The controller pair that resides on the SAN network communicates to the storage subsystem using the iSCSI protocol. The PowerVault NX3500 communicates on the SANa and SANb networks, rendering a high availability (HA) design.

Internal Network

The PowerVault NX3500 solution requires an internal network for peer-to-peer data transfer and management. To achieve complete data distribution and to maintain HA, each controller must have access to its peer controller. The internal network achieves this goal.

The internal network is classified into internal network A and internal network B.

NOTE: Ensure that the IP addresses you assign to internal network A and internal network B are from a private IP space and do not conflict with other subnets on your network.

Internal Network A

PowerVault NX3500's internal network A is comprised of two independent Gigabit Ethernet ports. The internal network is the infrastructure for the PowerVault NX3500 clustering, and includes heartbeat monitoring, data transfer, and mirroring of information between the controllers' caches. The internal network also distributes data evenly across all LUNs in the system.

NOTE: Internal network A is also referred to as peer-to-peer connections. The network uses point-to-point cable connections.

Internal Network B

Internal network B is the PowerVault NX3500 internal management network, which is plugged into the SAN switch and connects both controllers. All administrative related functions are performed on this network.

In the event where the controllers lose communication with each other but continue to function independently (known as the split-brain situation), the PowerVault management network automatically resets the suspected controller. This prevents the split-brain situation and ensures data integrity.

LAN or Client Network

After the initial configuration, a virtual IP (VIP) address connects the PowerVault NX3500 to the client or LAN network.

The VIP address allows clients to access the PowerVault NX3500 as a single entity, thereby providing access to the file system. It enables the PowerVault NX3500 to perform load balancing between controllers, and ensures that the service continues even if a controller fails.

The LAN or client network is comprised of two Gigabit Ethernet ports on each controller, which connect to the LAN or client network switches. The solution can have a maximum of four VIPs that serve the system. For more information, see “Setting Up Your PowerVault NX3500 Solution” on page 29. The PowerVault NX3500 solution is administered using the LAN or client network on the NAS Management VIP.

2

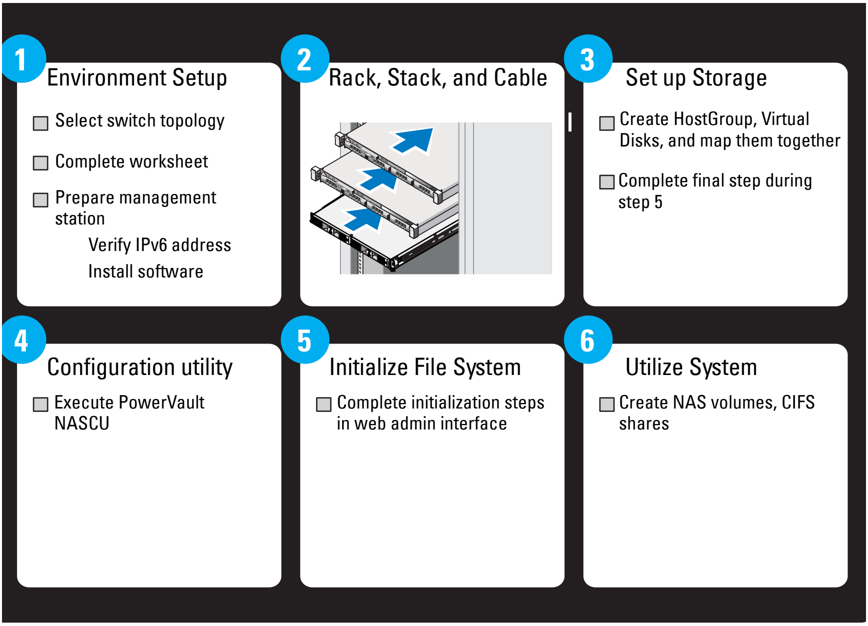
Setting Up Your PowerVault NX3500 Solution

This chapter describes the procedure to configure the Dell PowerVault NX3500 NAS cluster solution and integrate it into your environment.

A successful configuration of the PowerVault NX3500 involves:

- Setting up the environment (see "Setting Up the Environment" on page 30).
- Installing the solution in a rack.
- Setting up the MD storage solution (see "Setting Up Your MD Storage Solution" on page 45).
- Installing and running the PowerVault NAS configuration utility (see "Running the PowerVault NASCU" on page 53).
- Initializing the filesystem.
- Utilizing the system.

Figure 2-1. Setting Up Your PowerVault NX3500 Solution



1 Environment Setup

□ Select switch topology

□ Complete worksheet

□ Prepare management station

Verify IPv6 address

Install software

2 Rack, Stack, and Cable

3 Set up Storage

□ Create HostGroup, Virtual Disks, and map them together

□ Complete final step during step 5

4 Configuration utility

□ Execute PowerVault NASCU

5 Initialize File System

□ Complete initialization steps in web admin interface

6 Utilize System

□ Create NAS volumes, CIFS shares

Setting Up the Environment

To set up the environment:

1 Choose the topology and cable your solution.

2 Complete the NAS system setup worksheet.

3 Prepare your management station.

Choosing the Topology

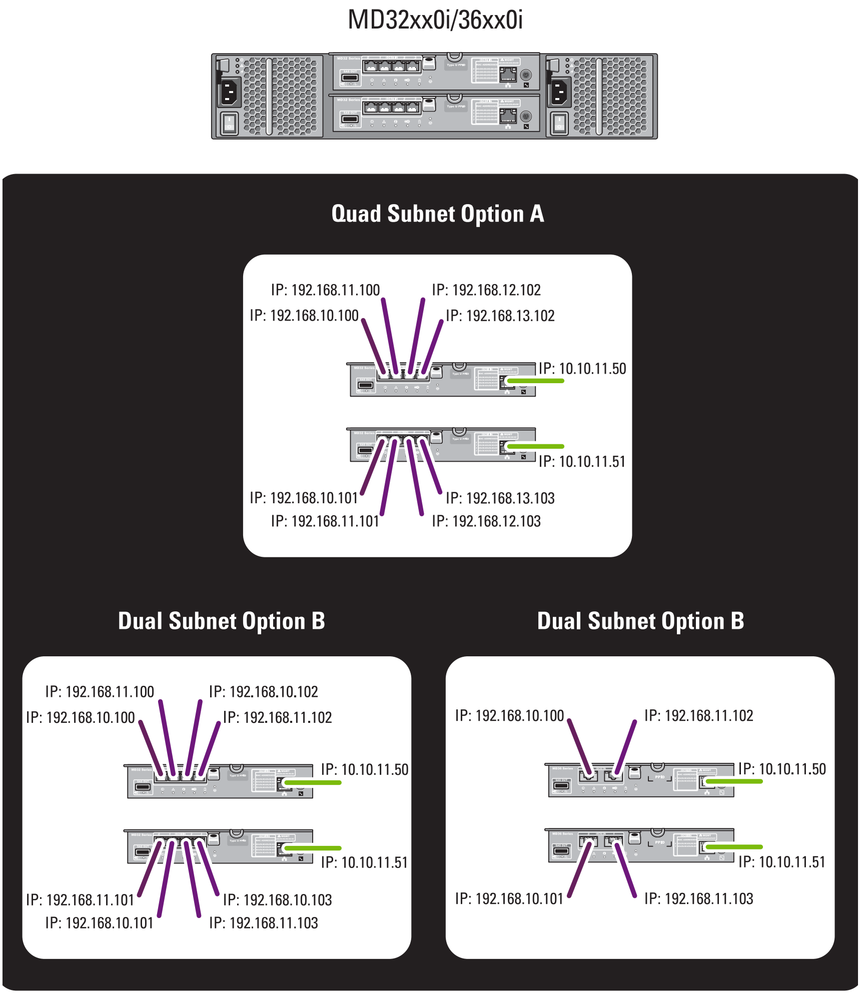
Choosing the topology involves choosing the MD topology and the switch topology.

MD Topology

Your MD array is equipped with eight ports across two controllers. You can configure the MD array for your solution using:

- Four subnets (See Figure 2-2)
  - Two for NAS
  - Two for Block
- Two subnets (See Figure 2-2)
  - Serves both NAS and Block

Figure 2-2. The MD Switch Topology



Choosing the Switch Topology

NOTE: The *two subnets* option would also be used for the MD36*xx*i.

The PowerVault NX3500 supports four switch topologies. The topologies are listed in Table 2-1 with their benefits and challenges. Choose the ideal topology for your environment and cable the solution accordingly.

Table 2-1. Switch Topologies for PowerVault NX3500 in the Non-Redundant and High Availability Options

Topology	Description	High-Availability	Non-Redundant
Dedicated SAN	This topology leverages the best practices of the industry relating to iSCSI and separates the SAN and LAN/Client traffic. The client cables are connected to a client switch and the SAN cables are connected to a SAN switch.	Figure 2-4 (recommended)	Figure 2-5
All-in-one solution	A basic topology where the SAN and the client cables are connected to the same switch.	Figure 2-6	Figure 2-7

The following settings are highly recommended on your switch:

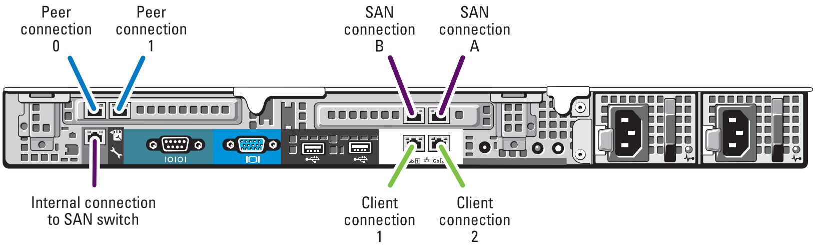
- Spanning Tree Portfast (required)
- Flow control (required)
- Jumbo frames (9000 MTU)

NOTE: Dell PowerConnect switches need to be configured to 9216 MTU or greater to accept frames of size 9000 MTU. Non-Dell switches may require a different MTU configuration for similar frame sizes. For more information on MTU configuration for non-Dell switches, see the switch-specific manual.

NOTE: Jumbo frames and flow control settings are mandatory for all ports used solely by the PowerVault NX3500 and file access, for block usage port setting, please refer to your array user guide for optimal performance setting.

Figure 2-3. NX3500 Node NIC Cabling

NOTE: See Figure 2-3 to connect the PowerVault NX3500 and MD ports to the appropriate switch in the for the best practice solution in the HA option.



PowerVault NX3500	Controller 0	Controller 1
Client connection 1	To client switch	To client switch
Client connection 2	To client switch	To client switch
Peer connection 0	Back to back (peer connection 0 to peer connection 0)	Back to back (peer connection 0 to peer connection 0)
Peer connection 1	Back to back (peer connection 1 to peer connection 1)	Back to back (peer connection 1 to peer connection 1)
SAN connection A	To SAN switch (A)	To SAN switch (B)
SAN connection B	To SAN switch (B)	To SAN switch (A)
Internal connection	To SAN switch (B)	To SAN switch (A)
PowerVault MD Storage Array	**Connection**	
Port 0	To SAN switch (A)	
Port 1	To SAN switch (B)	

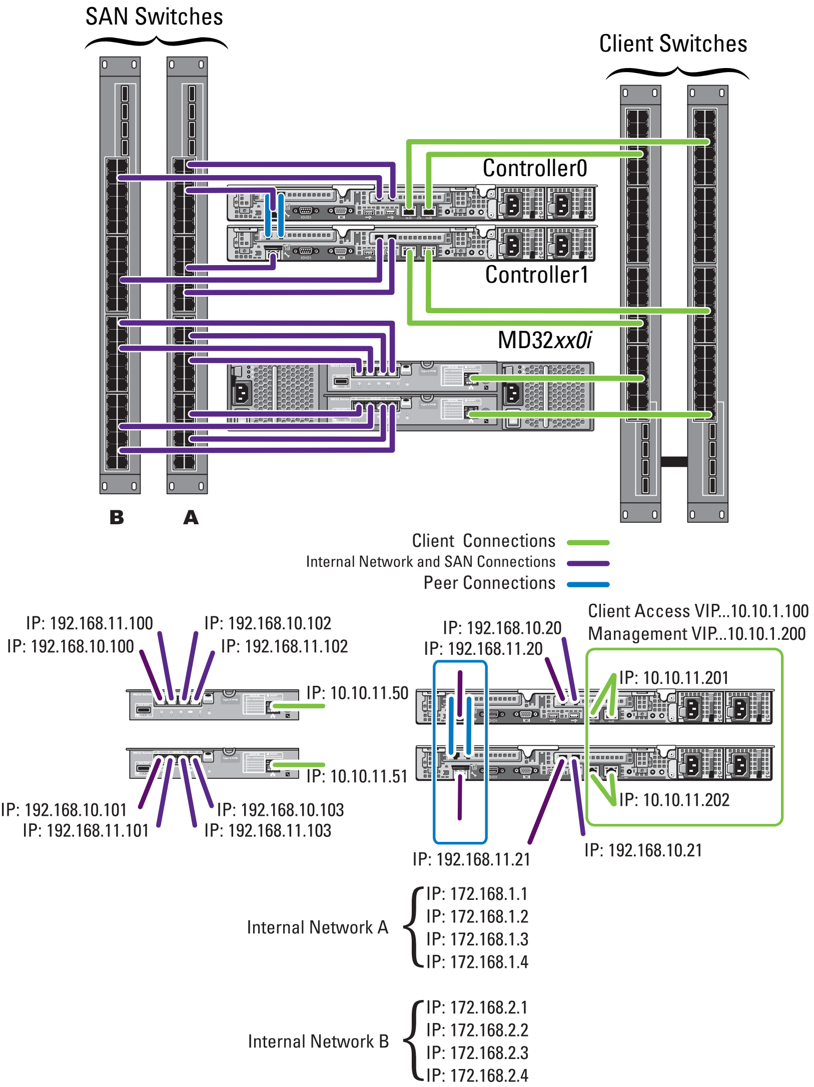
Best Practice Solution in the HA Option

The best practice solution is to isolate the SAN traffic from the LAN or client traffic with redundant switches for HA. All the client cables are split between the redundant client switches, and the SAN or internal network cables are split between the redundant SAN switches. Peer connections are always back to back.

NOTE: For cabling recommendation for existing MD-Series implementations that do not have stacked switches, see “Cabling Recommendation” on page 213.

NOTE: The PowerVault NX3500 solution expects only two subnets (iSCSI ports) per MD controller to be used by the solution. The other four ports are dedicated to block devices.

Figure 2-4. Dedicated SAN Solution in the High Availability Option

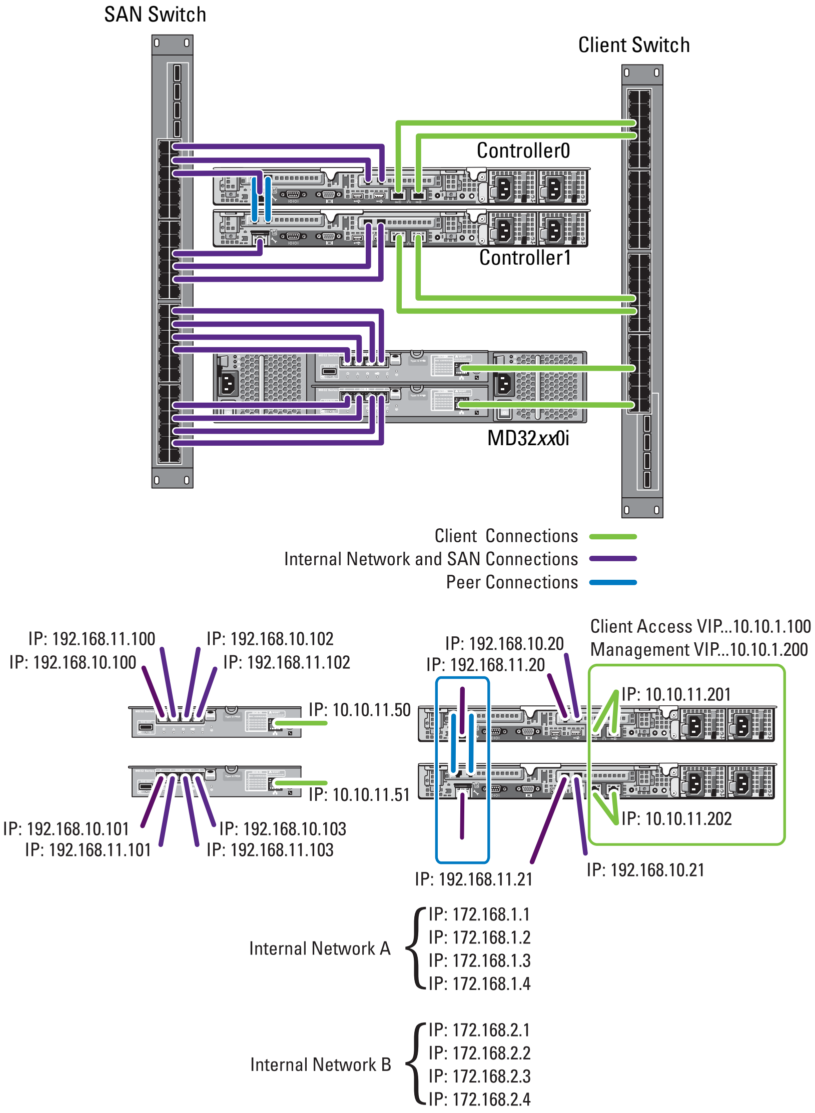


Dedicated SAN Solution in the Non-Redundant Option

The second configuration option is to isolate the SAN traffic from the client traffic, but without redundant switches. All the client cables are connected to the client switch and the SAN or internal network cables are connected to the SAN switch. Peer connections are always back to back.

In this configuration, the switches become a single point of failure. It is recommended that you separate the SAN subnets using virtual LANs.

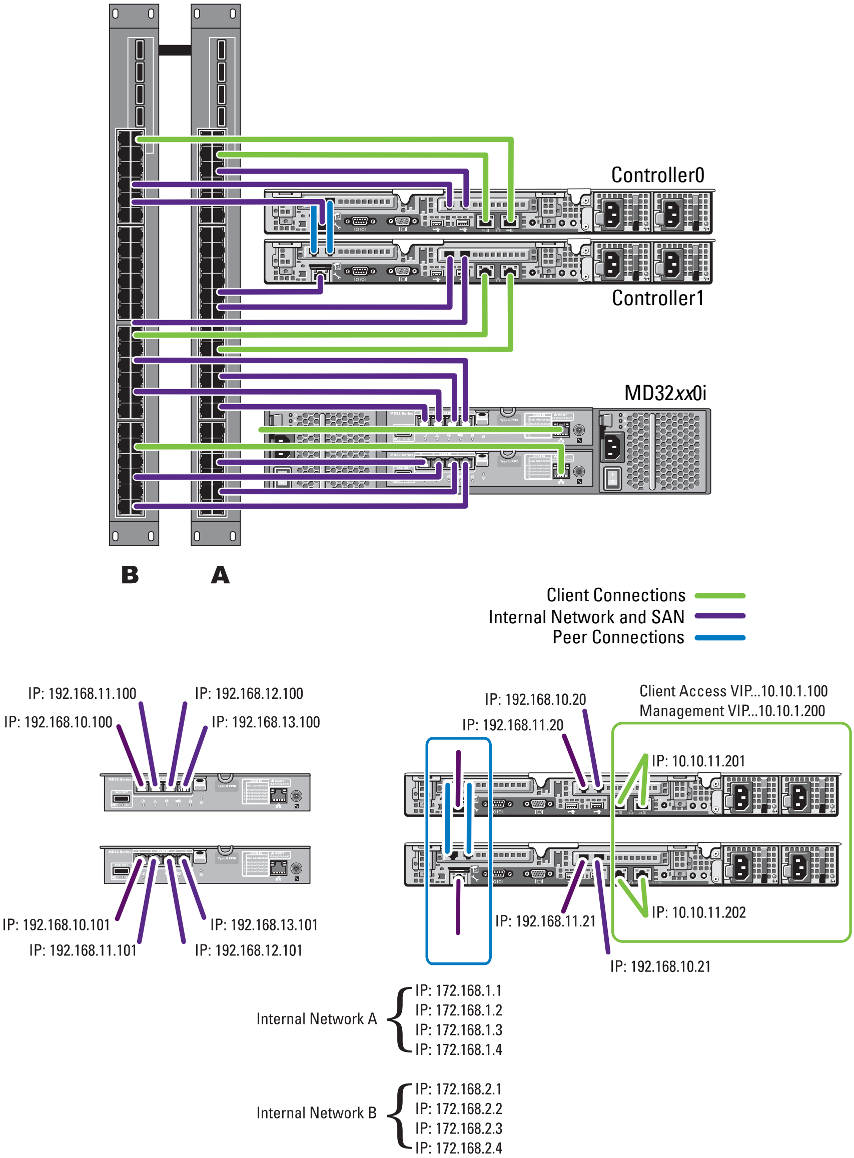
Figure 2-5. Dedicated SAN Solution in the Non-Redundant Option



All-in-One High-Availability Option

In an all-in-one high availability option, the redundant switches host both SAN or internal and client network traffic. The SAN or internal and client cables are split between the redundant switches. Peer connections are always back to back. It is recommended that you separate the SAN subnets using virtual LANs.

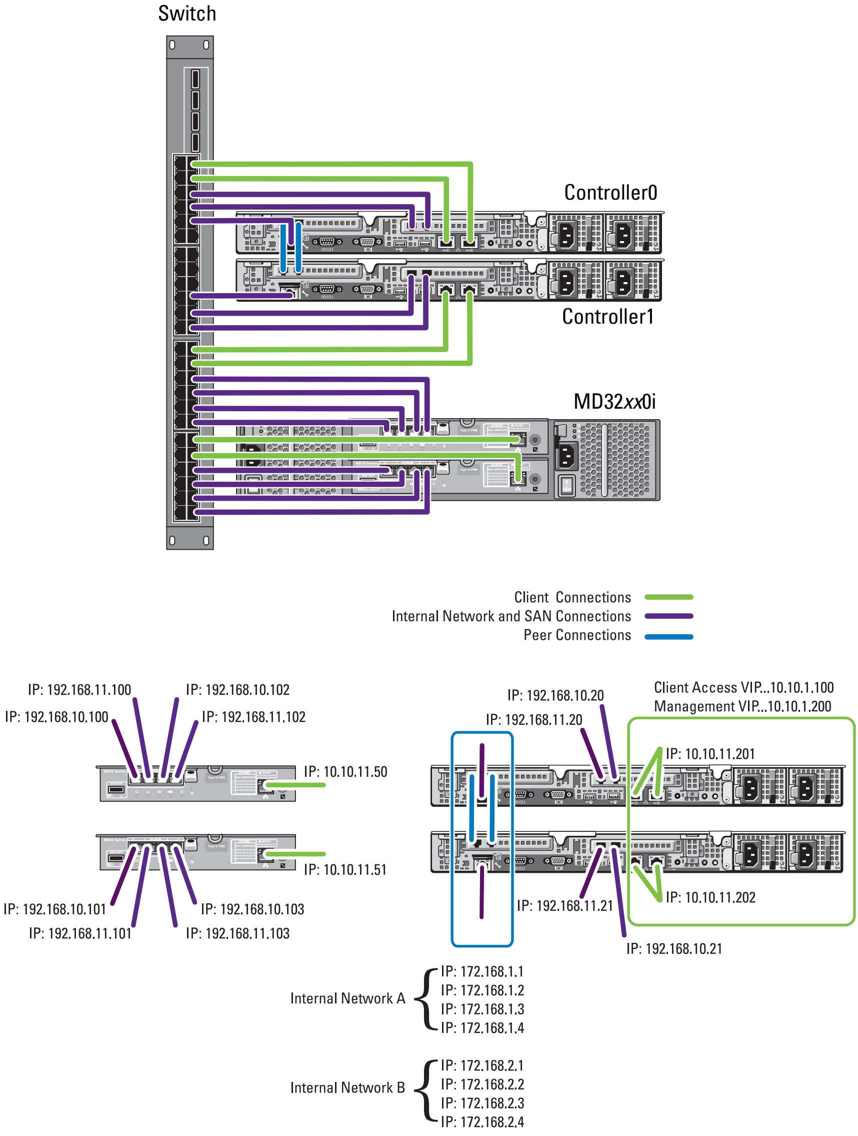
Figure 2-6. All-in-One High-Availability Option



All-in-One Non-Redundant Option

In an all-in-one non redundant option, both the SAN or internal and client cables are connected to the same switch. In this configuration, the switch is a single point of failure. It is recommended that you separate the SAN subnets using virtual LANs.

Figure 2-7. All-in-One Non-Redundant Option



Completing the NAS System Setup Worksheet

The NAS System Setup Worksheet will assist you in the overall setup and configuration of your solution.

NAS System Setup Worksheet

PowerVault NAS Configuration Utility		NAS Cluster IP Allocation			
Information Requested	**Value**	**IP Function**	**IPs Allocated**	**Sample IPs**	**Physical Connections**
Storage Array Identification		**Subnet 1—Primary Network**			
MD discovery IP		NAS management VIP	. . .	10.10.1.200	Client
MTU		Client access VIP	. . .	10.10.1.100	Client
NX3500 Controller Discovery		Controller 0 IP	. . .	10.10.1.201	Client
Controller 0 MAC address		Controller 1 IP	. . .	10.10.1.202	Client
Controller 1 MAC address		Subnet mask	. . .	255.255.255.0	Client
		Gateway	. . .	10.10.1.1	Client
NAS Appliance Identification		**Subnet 2—Internal or Private Network Group 1**			
NAS cluster name		Internal IP a0	. . .	172.168.1.1	Internal or Peer
PowerVault NAS Configuration Utility Results		Internal IP a1	. . .	172.168.1.2	Internal or Peer
NAS controller 0 IQN		Internal IP a2	. . .	172.168.1.3	Internal or Peer
NAS controller 1 IQN		Internal IP a3	. . .	172.168.1.4	Internal or Peer
NOTE: Use the IQNs recorded from the PowerVault NAS Configuration Utility (NASCU) to complete your mappings configuration on the MD3*xx*0i backend storage.		Subnet mask	. . .	255.255.255.0	Internal or Peer

PowerVault NAS Configuration Utility	NAS Cluster IP Allocation			
Environment Setup Checklist Management station: • Verify IPv6 enabled • Install PowerVault NASCU Switch topology Determine desired switch topology from one of the following configurations: • Dedicated SAN solution in the high-availability option • Dedicated SAN solution in the high-availability option • All-in-one high-availability option • All-in-one non-redundant option	**Subnet 3—Internal or Private Network Group 1**			
	Internal IP b0	. . .	172.168.2.1	Internal or Peer
	Internal IP b1	. . .	172.168.2.2	Internal or Peer
	Internal IP b2	. . .	172.168.2.3	Internal or Peer
	Internal IP b3	. . .	172.168.2.4	Internal or Peer
	Subnet mask	. . .	255.255.255.0	Internal or Peer
	Subnet 4—SAN Network Group 1			
	SANa IP 0	. . .	192.168.10.20	SAN (to Switch A)
	SANa IP 1	. . .	192.168.10.21	SAN (to Switch A)
	Subnet mask	. . .	255.255.255.0	
	Subnet 5—SAN Network Group 2			
	SANb IP 0	. . .	192.168.11.20	SAN (to Switch B)
	SANb IP 1	. . .	192.168.11.21	SAN (to Switch B)
	Subnet mask	. . .	255.255.255.0	

Power Vault MD Configuration				
	IP Function	**IPs Allocated**	**Sample IPs**	**Physical Connections**
	Controller 0 Port 0 IP	. . .	192.168.10.100	SAN (to Switch A)
	Controller 0 Port 1 IP	. . .	192.168.11.100	SAN (to Switch B)
	Controller 0 Port 2 IP	. . .	192.168.12.100	
	Controller 0 Port 3 IP	. . .	192.168.13.100	
	Controller 1 Port 0 IP	. . .	192.168.10.101	SAN (to Switch A)
	Controller 1 Port 1 IP	. . .	192.168.11.101	SAN (to Switch B)
	Controller 1 Port 2 IP	. . .	192.168.12.101	
	Controller 1 Port 3 IP	. . .	192.168.13.101	

Preparing Your Management Station

A management station is required to manage and configure the PowerVault NX3500. The solution can be accessed using either the CLI or the Dell PowerVault NAS Manager.

NOTE: You can log on to either the CLI or the NAS Manager at a time. It is highly recommended that you do not attempt to log on to both the CLI and NAS Manager at the same time.

The minimum requirements for the management station are:

- It has IPv6 enabled.
- The PowerVault NASCU is installed.

  NOTE: You can install Dell PowerVault NASCU from the *Dell Resource Media Fluid File System (FluidFS)* media that shipped with your solution.
- The PowerVault NX3500 is cabled appropriately, and the management station is on the same network as the LAN or client network.
- Has either Internet Explorer or Firefox installed with JavaScript enabled.

Installing the Solution in the Rack

Your solution requires a properly grounded electrical outlet, a compatible rack, and a rack installation kit. For information on installing the solution in the rack, see the *Setting Up Your PowerVault Network Attached Storage Solution* that shipped with your product.

Setting Up Your MD Storage Solution

This section assumes you have discovered and completed the initial configuration (naming, assigning iSCSI, and management port IPs) of your PowerVault MD3*xx*0i storage arrays in accordance with the topology you plan to use.

This section provides the steps necessary to configure the host group and virtual disks that are required for the PowerVault NX3500 system. For additional information regarding a task such as creating virtual disks, see the PowerVault Modular Disk Storage Manager (MDSM) *Help* or the Dell PowerVault MD3*xx*0i *Owner's Manual* at **support.dell.com/manuals**.

CAUTION: Correctly preparing the PowerVault Modular Disk (MD) storage array is critical for successfully configuring your NAS solution.

Complete the following tasks using PowerVault MDSM.

NOTE: PowerVault MDSM is available on the Resource media that shipped with your storage array.

1 Create a disk group for each virtual disk.

2 Create a virtual disk in each disk group.

3 Create a host group.

4 Map the virtual disks to the host group.

NOTE: See the MD storage array documentation at **support.dell.com/manuals**.

NOTE: Additional configuration is required after completing the steps in the PowerVault Configuration Utility. Challenge Handshake Authentication Protocol (CHAP) must be disabled on the PowerVault MD3*xx*0i storage array and the storage array must be configured for two logical SANs.

Creating Disk Groups

To create disk groups:

NOTE: It is recommended that you create a minimum of two disk groups. Each will house a virtual disk dedicated to the NAS storage pool.

1 Install and launch the PowerVault MDSM software on the management station.

2 Target the MD storage array you plan to use for your NAS storage.

See the Dell PowerVault MD3*xx*0i storage arrays *Deployment Guide* at **support.dell.com/manuals**.

3 Choose one of the following methods to start the **Create Disk Group Wizard** and proceed to step 4:

– To create a disk group from unconfigured capacity in the storage array:

a On the **Logical** tab, select **Unconfigured Capacity**.

b Select **Disk Group→ Create**.

Alternatively, you can right-click **Unconfigured Capacity**, and select **Create Disk Group** from the pop-up menu.

– To create a disk group from unassigned physical disks in the storage array:

a On the **Physical** tab, select one or more unassigned physical disks of the same physical disk type.

b Select **Disk Group→ Create**.

Alternatively, you can right-click the unassigned physical disks, and select **Create Disk Group** from the pop-up menu.

– To create a secure disk group:

a On the **Physical** tab, select one or more unassigned security capable physical disks of the same physical disk type.

b Select **Disk Group→ Create**.

Alternatively, you can right-click the unassigned security capable physical disks, and select **Create Disk Group** from the pop-up menu.

The **Introduction (Create Disk Group)** window is displayed.

4 Click **Next**.

The **Disk Group Name and Physical Disk Selection** window is displayed.

5 Type a name for the disk group in **Disk Group Name**.

NOTE: The disk group name should not exceed 30 characters.

6 Select the appropriate **Physical Disk Selection** choice; you can select:

For manual configuration, the Manual Physical Disk Selection window is displayed.

- **Automatic**, see step 7

For automatic configuration, the RAID Level and Capacity window is displayed.

- **Manual**, see step 10

7 Click **Next**.

8 Select the appropriate RAID level in **Select RAID Level**.

You can select RAID levels 1/10, 6, and 5. Depending on the RAID level selection, the physical disks available for the selected RAID level are displayed in the **Select Capacity** table.

9 In the **Select Capacity** table, select the relevant disk group capacity, and click **Finish**.

Repeat the procedure for a minimum of two disk groups and then proceed to "Creating Virtual Disks" on page 49.

If you have selected **Manual** configuration, proceed to step 10.

10 In the **Manual Physical Disk Selection** window, select the appropriate RAID level in **Select RAID Level**.

You can select RAID levels 0, 1/10, 6, and 5. Depending on the RAID level chosen, the physical disks available for the selected RAID level is displayed in **Unselected Physical Disks** table.

11 In the **Unselected Physical Disks** table, select the appropriate physical disks and click **Add**.

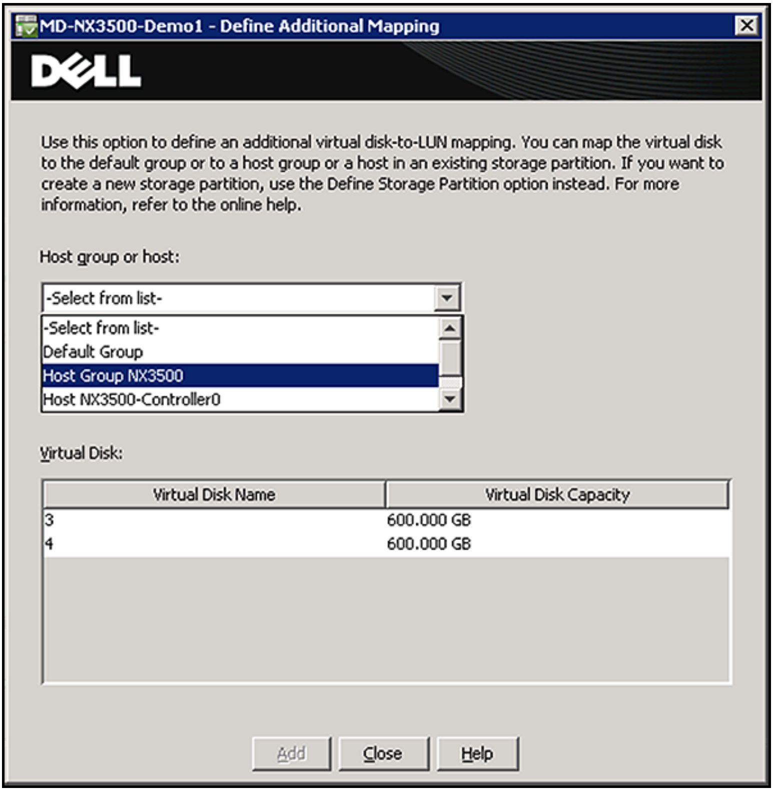
NOTE: You can select multiple physical disks at the same time by holding <Ctrl> or <Shift> and selecting additional physical disks.

To view the capacity of the new disk group, click **Calculate Capacity**.

12 Click **Finish**.

Repeat the procedure for a minimum of two disk groups.

Figure 2-8. Host Group and Virtual Disks



MD-NX3500-Demo1 - Define Additional Mapping

Use this option to define an additional virtual disk-to-LUN mapping. You can map the virtual disk to the default group or to a host group or a host in an existing storage partition. If you want to create a new storage partition, use the Define Storage Partition option instead. For more information, refer to the online help.

Host group or host:

-Select from list-

- -Select from list-
- Default Group
- Host Group NX3500
- Host NX3500-Controller0

Virtual Disk:

Virtual Disk Name	Virtual Disk Capacity
3	600.000 GB
4	600.000 GB

Creating Virtual Disks

NOTE: Before creating virtual disks, organize the physical disks into disk groups and then create a virtual disk within each disk group.

Create a minimum of two virtual disks dedicated for NAS storage. The NAS storage capacity can be expanded up to 16 virtual disks. The number of virtual disks must increment in pairs.

NOTE: Minimum virtual disk size required for the PowerVault NX3500 is 125 GB. Maximum virtual disk size required for the PowerVault NX3500 is 15 TB.

Table 2-2. Creating Virtual Disks

Item	Supported	Not supported
Number of VDs or LUNs	2, 4, 6, 8, 10, 12, 14, 16	1, 3, 5, 7, 9, 11, 13, 15
LUN sizes	125 GB, up to 15 TB	Up to 125 GB, greater than 15 TB
NOTE: LUN pairs should be of the same size.	VD1: 125 GB VD2: 125 GB Pair 1	VD1:125 GB VD2: 130 GB Pair 1
	VD3: 759 GB VD4: 759 GB Pair 2	VD3: 759 GB VD4: 650 GB Pair 2
	VD5: 1.33 TB VD6: 1.33 TB Pair 3	VD5: 1.33 TB VD6: 1.90 TB Pair 3
Host group	Single host group	Multiple host group

To create virtual disks from free capacity:

1 Start the **Create Virtual Disk Wizard**.

2 On the **Logical** tab, select **Free Capacity** from the disk group you created in the earlier steps.

3 Select **Virtual Disk** and then click **Create**.

The **Introduction (Create Virtual Disk)** window is displayed.

4 Click **Next**.

The **Specify Capacity/Name** window is displayed.

5 Select the appropriate unit for storage capacity in **Units** and enter the capacity of the virtual disk in **New Virtual Disk Capacity**.

6 Enter a name for the virtual disk in **Virtual Disk Name** (for example, *NX3500Lun0*).

NOTE: The virtual disk name should not exceed 30 characters.

7 In **Advanced Virtual Disk Parameters**, select one of the following options:

- **Use Recommended Settings**
- **Customize Settings**

8 Click **Next**.

9 In the **Customize Advanced Virtual Disk Parameters** window, select the appropriate Virtual Disk I/O characteristics type.

10 Select one of the following options:

- **File system (typical)**
- **Database**
- **Multimedia**
- **Custom**

NOTE: If you select **Custom**, you must select an appropriate segment size and preferred RAID controller module ownership. For more information, see the MD storage array documentation at **support.dell.com/manuals**.

11 Click **Finish**.

The virtual disks are created.

Creating a Host Group

To create a host group:

1 Launch the PowerVault MDSM and target the MD storage array you plan to use for your NAS storage.

2 Select the **Mappings** tab.

3 In the **Topology** pane, select the storage array or the **Default Group**.

4 Perform one of the following actions:

- Select **Mappings** and then **Define Host Group**.
- Right-click the storage array or the **Default Group,** and select **Define Host Group** from the pop-up menu.

5 Type the name of the new host group in **Enter New Host Group Name** (for example, *NX3500*).

NOTE: Host group name must have alphanumeric characters.

NOTE: Since the controllers are not configured yet, no hosts are available at this time. No host other than the NX3500 controllers should be added to this host group.

6 Click **OK**.

The host group is added to the storage array.

Creating Host-to-Virtual Disk Mappings

To create host-to-virtual disk mappings:

1 Launch PowerVault MDSM and target the MD storage array you plan to use for your NAS storage.

2 In the **Topology** pane, expand **Default Group** and select the host group you created in the previous steps.

3 In the tool bar, select **Mappings**→ **Define**→ **Additional Mapping**.

The **Default Additional Mapping** window is displayed.

4 In **Host group or host**, select the host group you created in the previous steps.

All defined hosts, host groups, and the default group appear in the list.

5 In the **Logical Unit Number** field, select a LUN. The supported LUNs are 0 through 255.

6 Select the virtual disk to be mapped in the virtual disk area.

The virtual disk area lists the names and capacity of the virtual disks that are available for mapping, based on the selected host group or selected host. Only select the virtual disks that were created specifically to be used by the PowerVault NX3500. You must select an even number of virtual disks, up to 16.

7 Click **Add**.

NOTE: The **Add** button is inactive until a host group or host, LUN, and virtual disk are selected.

8 To define additional mappings, repeat step 4 through step 7.

NOTE: After a virtual disk has been mapped, it is no longer available in the virtual disk area.

9 Click **Close**.

The mappings are saved. The **Topology** pane and the **Defined Mappings** pane in the **Mappings** tab are updated to reflect the mappings.

Running the PowerVault NASCU

The PowerVault NAS Configuration Utility (NASCU) walks you through the steps necessary to set up the network configuration and pair the PowerVault NX3500 controllers together. It also starts the process of pairing the system to the PowerVault MD3*xx*0i storage appliance. It is recommended that you determine your network configuration and IP address allocation for your NAS controllers before executing this utility. See "Completing the NAS System Setup Worksheet" on page 42.

Before running the PowerVault NASCU, ensure that:

- The PowerVault NASCU is installed and executed from a management station that has IPv6 enabled. The utility connects to and configures your controllers through the local link Ipv6 address. Ipv6 can be disabled, but only after the installation and configuration is complete.
- The management station is connected to the same switch as the client connections on your NAS controllers (see Table 2-1).

NOTE: Use the PowerVault NASCU only for initial configuration. After the PowerVault NX3500 is configured use the NAS Manager to make changes to the configuration.

Installing the PowerVault NASCU

NOTE: Do not attempt to use the PowerVault NASCU to reconfigure an already clustered PowerVault NX3500 solution.

For Windows-based management stations:

1 Insert the *PowerVault NX3500 Resource Media* into the optical drive.

If **autorun** is enabled on your system, the installer automatically launches after a few moments.

2 If **autorun** is enabled, proceed to step 5.

3 If **autorun** is disabled, or if **autorun** does not automatically launch the installer, open an explorer window and navigate to the optical drive where the *PowerVault NX3500 Resource Media* is located.

4 Open **StartHere.htm**.

5 Follow the prompts in the installer to complete the installation.

For Linux-based admin stations:

Graphical Installation

1 Insert the *PowerVault NX3500 Resource Media* into the optical drive.

2 Point the file-system explorer to the mounted optical drive.

3 Run **StartHere.htm**.

This launches an internet browser.

4 Follow the prompts in the installer to complete the installation.

Command-Line Installation

1 Insert the *PowerVault NX3500 Resource Media* into the optical drive.

2 Open a terminal window and change directories (cd) to the optical drive (For example, *cd /media/disk/media/cdrom*).

3 Change directories to the **InstData** folder.

4 Identify the build of operating system being used (32-bit or 64-bit) and change directory into either the **Linux_amd64/VM/ (64-bit)** or **Linux_i386/VM/ (32-bit)** folder.

5 Run the installer located in this folder by calling **sh ./pv-nas-config-utility-installer-linux-<build_type>.bin**.

6 Follow the steps in the installer to complete the installation.

Launching the PowerVault NASCU

For Windows-based operating systems:

1 Access the Windows desktop and double-click the **PowerVault NX3500 Configuration Utility** icon, or access the Windows start menu and navigate to **All Programs→ Dell→ PowerVault NAS**.

2 Click on **PowerVault NX3500 Configuration Utility**.

For Linux-based operating systems:

1 Execute the **PowerVault NASCU** from a terminal prompt.

2 Ensure that the currently logged-on terminal user is **root**.

To change the user to **root**:

a At the prompt, type `su` and enter the root password at the prompt.

b Navigate to the root home folder by typing **cd ~/**.

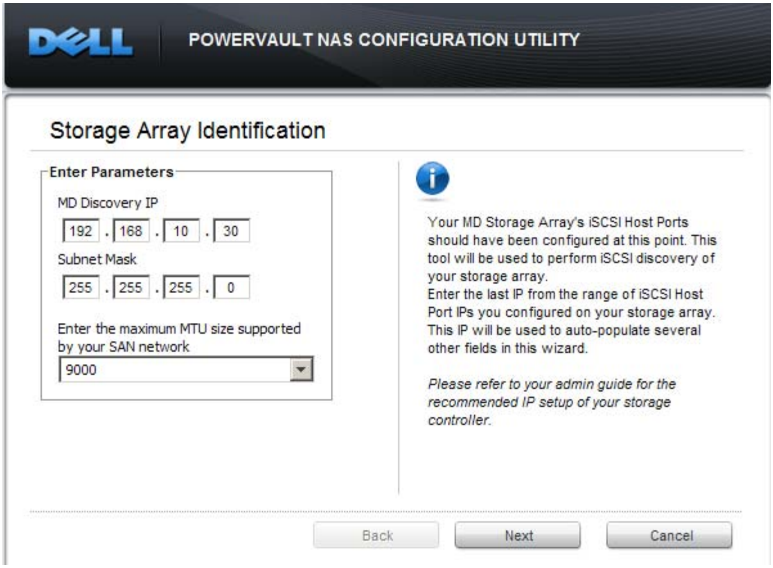
c Execute the **PowerVault NASCU** by typing **/bin/sh./Dell-PV-NAS-Config-Utility**.

The welcome screen is displayed.

The actual configuration is deferred until all settings are confirmed in the **Configuration Summary** screen.

⚠ **CAUTION: Use this utility only to configure two unconfigured controllers. Do not attempt to use this utility on fully configured or clustered PowerVault NX3500 or to reconfigure IP addresses. This utility does not check for duplicate IPs or null entries.**

The **Storage Array Identification and Configuration** window is displayed.



Storage Array Identification

Enter Parameters

MD Discovery IP: 192 . 168 . 10 . 30

Subnet Mask: 255 . 255 . 255 . 0

Enter the maximum MTU size supported by your SAN network: 9000

Your MD Storage Array's iSCSI Host Ports should have been configured at this point. This tool will be used to perform iSCSI discovery of your storage array.
Enter the last IP from the range of iSCSI Host Port IPs you configured on your storage array. This IP will be used to auto-populate several other fields in this wizard.

Please refer to your admin guide for the recommended IP setup of your storage controller.

3 Type in the **MD Discovery IP** address, the **Subnet Mask,** and the MTU size.

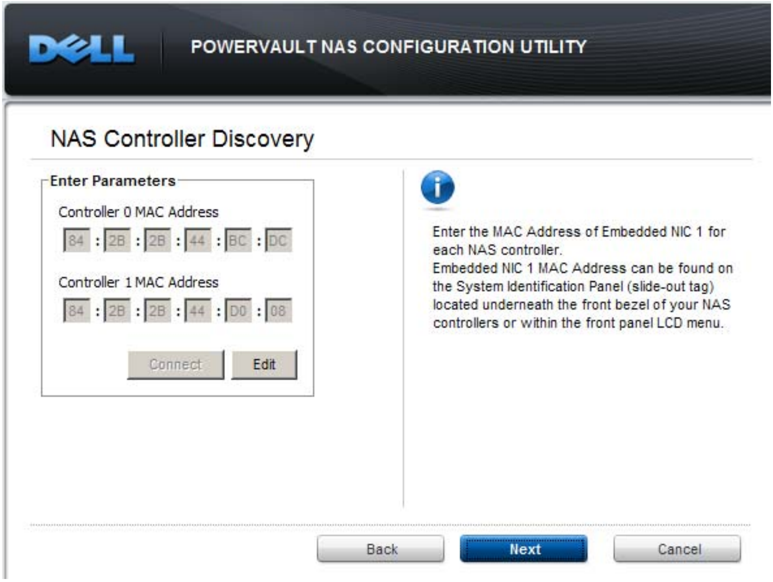
4 Click **Next.**

MD Discovery IP and subnet mask: This is one of the iSCSI Host port IPs configured on the MD array controller iSCSI ports. You can access this information from the MDSM. This IP address is used by the PowerVault NASCU to establish communication with the MD storage array.

SAN MTU size: This is the MTU setting for the SAN network. Using jumbo frames on the SAN network (MTU: 9000) is mandatory for new installations. For an existing MD setup, it is highly recommended that you use jumbo frames for optimal performance.

The **NAS Controller Discovery** window is displayed.

NOTE: Dell PowerConnect switches must be configured to 9216 MTU or greater to accept frames of size 9000 MTU. Non-Dell switches may require a different MTU configuration for similar frame sizes. For more information on MTU configuration for non-Dell switches, see the switch-specific documentation.



Controller 0 MAC Address: 84 : 2B : 2B : 44 : BC : DC

Controller 1 MAC Address: 84 : 2B : 2B : 44 : D0 : 08

Enter the MAC Address of Embedded NIC 1 for each NAS controller.
Embedded NIC 1 MAC Address can be found on the System Identification Panel (slide-out tag) located underneath the front bezel of your NAS controllers or within the front panel LCD menu.

5 Type in the Controller MAC addresses.

These are the string of numbers under the EMB NIC1 MAC Address on the Service Tag slide out tag.

Controller MAC addresses: These are used to establish communication with the PowerVault NX3500 controllers and perform initial configuration. This can be found on the System Identification slide out tab located underneath the front bezel of the controller. The back of the tab lists the "Embedded NIC 1 MAC address". The connect button starts the co-click.

6 Click **Connect** to check if NAS controllers are connected and click **Next**.

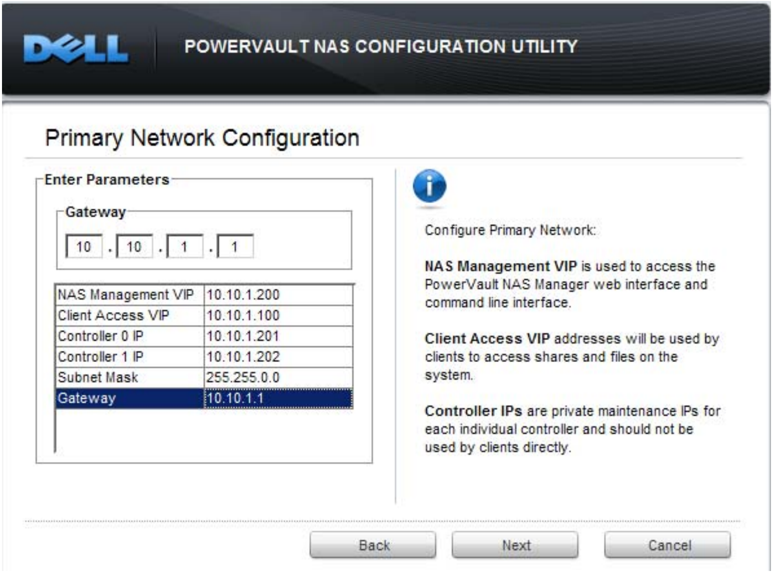
NOTE: The slide out tab has two MAC addresses. Ensure that you enter the embedded NIC Address and not the iDRAC address.

7 Enter the name used to identify the NAS cluster within the web administration interface.

8 Click **Next**.

The cluster name should be only alphanumeric characters with no spaces or special characters other than dashes.

The **Primary Network Configuration** window is displayed.



Primary Network Configuration

Enter Parameters

Gateway

10 . 10 . 1 . 1

NAS Management VIP	10.10.1.200
Client Access VIP	10.10.1.100
Controller 0 IP	10.10.1.201
Controller 1 IP	10.10.1.202
Subnet Mask	255.255.0.0
Gateway	10.10.1.1

Configure Primary Network:

NAS Management VIP is used to access the PowerVault NAS Manager web interface and command line interface.

Client Access VIP addresses will be used by clients to access shares and files on the system.

Controller IPs are private maintenance IPs for each individual controller and should not be used by clients directly.

9 Type in the required parameters and click **Next**.

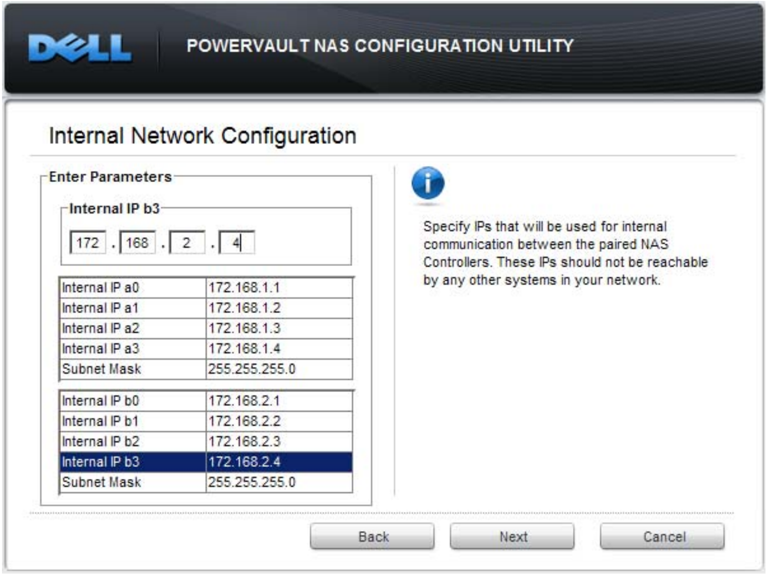
IP address descriptions are as follows:

- **Client Access VIP**: This is the IP address used to access CIFS and NFS shares.
- **NAS Management VIP**: This is the IP address used to access the NAS Manager and command line administration interfaces.

NOTE: Make a note of the NAS Management VIP address for use at a later stage.

- **Controller IPs**: Private maintenance IP addresses for each controller and should not be accessed by clients directly.
- **Gateway IP Address**: This is the IP address through which a system on the network can be reached at all times, such as a domain controller. The Gateway IP address should always be accessible to the PowerVault NX3500 controllers.

The **Internal Network Configuration** window is displayed.



Internal Network Configuration

Enter Parameters

Internal IP b3: 172 . 168 . 2 . 4

Internal IP a0	172.168.1.1
Internal IP a1	172.168.1.2
Internal IP a2	172.168.1.3
Internal IP a3	172.168.1.4
Subnet Mask	255.255.255.0

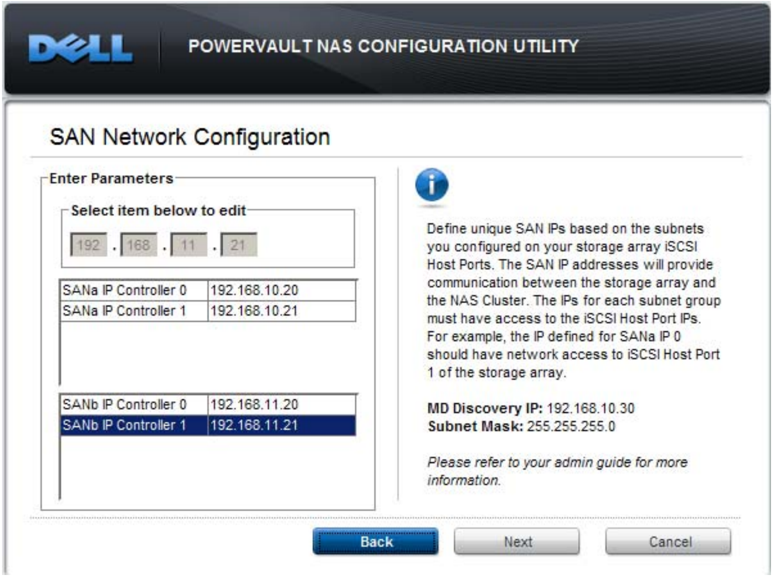
Internal IP b0	172.168.2.1
Internal IP b1	172.168.2.2
Internal IP b2	172.168.2.3
Internal IP b3	172.168.2.4
Subnet Mask	255.255.255.0

Specify IPs that will be used for internal communication between the paired NAS Controllers. These IPs should not be reachable by any other systems in your network.

10 Type in the required parameters in the **Internal Network Configuration** window and click **Next.**

Internal IPs: These are used for internal communication between the controller pair. IP addresses specified must be grouped in two different subnets and be completely isolated from any other system on the network. The PowerVault NASCU requests for these IP addresses to ensure that there are no IP address clashes with other systems on your network.

The **SAN Network Configuration** window is displayed.



POWERVAULT NAS CONFIGURATION UTILITY

SAN Network Configuration

Enter Parameters

Select item below to edit

192 . 168 . 11 . 21

SANa IP Controller 0	192.168.10.20
SANa IP Controller 1	192.168.10.21

SANb IP Controller 0	192.168.11.20
SANb IP Controller 1	192.168.11.21

Define unique SAN IPs based on the subnets you configured on your storage array iSCSI Host Ports. The SAN IP addresses will provide communication between the storage array and the NAS Cluster. The IPs for each subnet group must have access to the iSCSI Host Port IPs. For example, the IP defined for SANa IP 0 should have network access to iSCSI Host Port 1 of the storage array.

MD Discovery IP: 192.168.10.30
Subnet Mask: 255.255.255.0

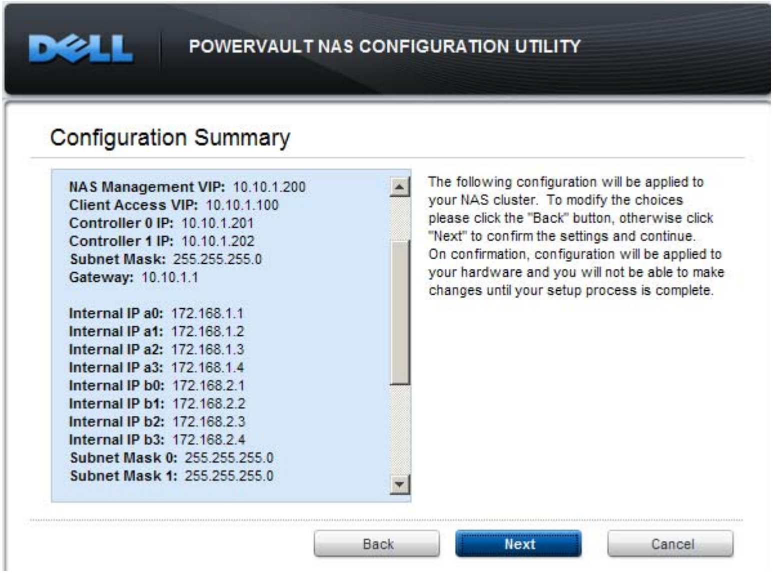
Please refer to your admin guide for more information.

11 Type in the required parameters and click **Next**.

SAN IPs: These are used for iSCSI communication with the backend storage device (PowerVault MD3*xx*0i). As a result, these IPs must be on the same subnets configured on the MD3*xx*0i storage array. iSCSI sessions are established with the MD3*xx*0i storage array over the two subnets specified.

NOTE: The MD storage array best practices recommend different subnets to be configured on each port of the MD controllers. For MD device such as the MD3200i with four ethernet ports per controller, the NAS cluster establishes iSCSI connections on two of the ports. The other two ports can be used to provision block storage to other iSCSI clients.

The **Configuration Summary** window is displayed.



Configuration Summary

NAS Management VIP: 10.10.1.200
Client Access VIP: 10.10.1.100
Controller 0 IP: 10.10.1.201
Controller 1 IP: 10.10.1.202
Subnet Mask: 255.255.255.0
Gateway: 10.10.1.1

Internal IP a0: 172.168.1.1
Internal IP a1: 172.168.1.2
Internal IP a2: 172.168.1.3
Internal IP a3: 172.168.1.4
Internal IP b0: 172.168.2.1
Internal IP b1: 172.168.2.2
Internal IP b2: 172.168.2.3
Internal IP b3: 172.168.2.4
Subnet Mask 0: 255.255.255.0
Subnet Mask 1: 255.255.255.0

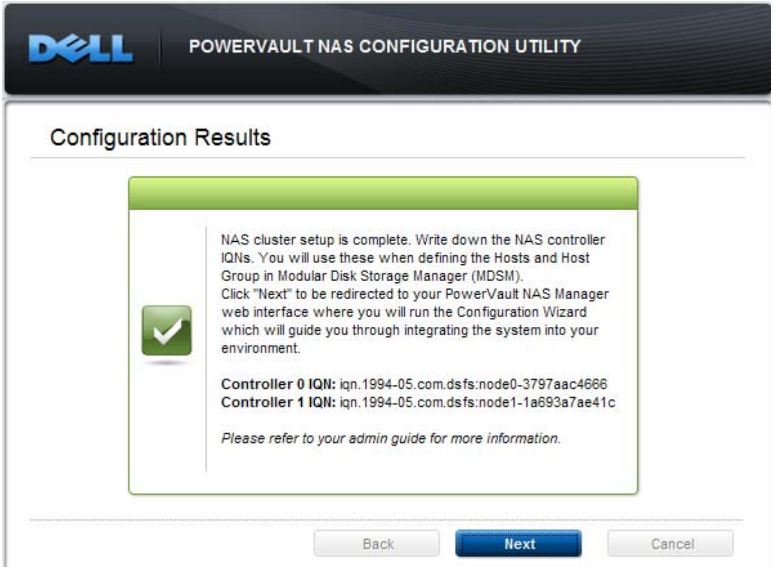
The following configuration will be applied to your NAS cluster. To modify the choices please click the "Back" button, otherwise click "Next" to confirm the settings and continue. On confirmation, configuration will be applied to your hardware and you will not be able to make changes until your setup process is complete.

All settings are applied to your controllers after this point. Listed below is a checklist of items to review:

- Ensure no duplicate IP addresses are present
- Check that IP groups are in the same subnet as required
- NAS cluster name follows expected naming convention
- SAN MTU setting matches MTU configuration of the switch connecting the NAS controllers to the backend MD3*xx*0i storage device

12 Click **Next** on the **Configuration Summary** window.

The **Configuration Results** window is displayed.



Configuration Results

NAS cluster setup is complete. Write down the NAS controller IQNs. You will use these when defining the Hosts and Host Group in Modular Disk Storage Manager (MDSM).
Click "Next" to be redirected to your PowerVault NAS Manager web interface where you will run the Configuration Wizard which will guide you through integrating the system into your environment.

Controller 0 IQN: iqn.1994-05.com.dsfs:node0-3797aac4666
Controller 1 IQN: iqn.1994-05.com.dsfs:node1-1a693a7ae41c

Please refer to your admin guide for more information.

Upon successful configuration, the PowerVault NASCU presents you with the NAS controller IQNs required to complete the pairing to the backend MD storage device. Copy the IQNs for both controllers to a notepad, which is entered into MDSM.

NOTE: Do not copy trailing white spaces along with the IQN, as this is interpreted as part of the IQN and causes an iSCSI login failure at a later part in the configuration.

NOTE: MDSM refers to IQNs as host port identifiers.

If there is an error, see "NAS Container Security Violation" on page 189.

When you click **Next**, the NAS Manager is launched in your default web browser. The **Configuration Wizard** is displayed and it guides you through the steps to configure and start the NAS service. If it does not open, follow the procedure in "Accessing the NAS Manager Web Interface" on page 64 to access the wizard.

NOTE: Before running the **NAS Manager Configuration Wizard**, create two hosts (one per controller) in the host group you created earlier. Enter the IQNs provided in the configuration results into the **Host Port Identifier** field for each controller. See "Define Two Hosts" on page 62. After defining hosts, proceed to the **NAS Manager Configuration Wizard**.

Define Two Hosts

Define the hosts as follows:

1. From the PowerVault MDSM for the array you plan to use for your NAS storage, perform one of the following actions:
   - Select **Mappings** and then **Define Host**.
   - Select the **Setup** tab, and click **Manually Define Hosts**.
   - Select the **Mappings** tab. Right-click the **Host Group** that you created (See “Creating a Host Group” on page 51.) in the **Topology** pane, and select **Define Host** from the pop-up menu.

     The **Specify Host Name** window is displayed.
2. In **Host name**, enter a host name (for example, *NX3500-Controller-0*).

   NOTE: The host name should be alphanumeric characters with the only special character "-".
3. Select **Add by creating a new host port identifier**. In the **New host port identifier** field, enter the IQN from the configuration results of the PowerVault NASCU and enter a user label for the host port identifier and click **Add**.

   NOTE: The user label cannot be the same as the host name, it should be based off the host name. For example: *NX3500-Controller-0-IQN*.
4. Click **Next**.

   The **Specify Host Type** window is displayed.
5. In **Host** type, select **Linux** as the operating system for the host.

   The **Host Group Question** window is displayed.
6. In this window, select **Yes**.

   This host shares access to the same virtual disks with other hosts.
7. Click **Next**.

The **Specify Host Group** window is displayed.

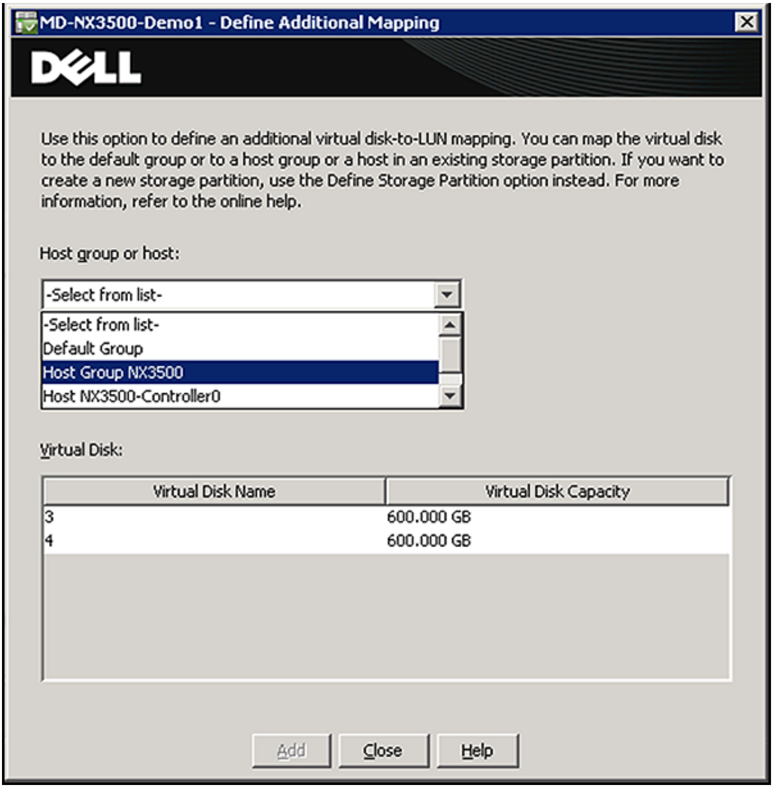
8 Select the host group you created (see "Creating a Host Group" on page 51), and click **Next**.

The **Preview** window is displayed.

9 Click **Finish and repeat** step 1 to step 9 for Controller1.

Proceed to the **NAS Manager Configuration Wizard** that was launched in your web browser.

Figure 2-9. Hosts in Host Group



MD-NX3500-Demo1 - Define Additional Mapping

Use this option to define an additional virtual disk-to-LUN mapping. You can map the virtual disk to the default group or to a host group or a host in an existing storage partition. If you want to create a new storage partition, use the Define Storage Partition option instead. For more information, refer to the online help.

Host group or host:

-Select from list-

-Select from list-
Default Group
Host Group NX3500
Host NX3500-Controller0

Virtual Disk:

Virtual Disk Name	Virtual Disk Capacity
3	600.000 GB
4	600.000 GB

NAS Manager Configuration Wizard

The **NAS Manager Configuration Wizard** helps complete the PowerVault NX3500 configuration and integrate the solution into the environment. It lets you set up the DNS, time management, user identification, and authentication parameters, and monitoring options as well as formatting and starting the file system.

You can leave the wizard at any time by selecting another page from the Navigation pane. Every page in the **Configuration Wizard** can also be accessed from the Navigation pane. This means that you can modify the system's configuration parameters directly, by accessing the appropriate page from the Navigation pane, without having to run the entire wizard.

Accessing the NAS Manager Web Interface

To access the NAS Manager:

1. Access the PowerVault NAS Manager web interface using the NAS Management VIP address you specified in the PowerVault NASCU.

   The **Security Alert** window is displayed.

   NOTE: The **Security Alert** window is displayed after you install the PowerVault NX3500 system, or after upgrading the system. Clicking **Yes** enables the current session. Clicking **View Certificate**, as explained in the following step, enables all future sessions.

2. Click **View Certificate**.

   The **Certificate** window is displayed.

3. Click the **Install Certificate** button.

   The **Welcome** window of the **Certificate Import Wizard** is displayed.

4. Click **Next**.

   The **Certificate Store** window is displayed.

5. Verify that **Automatically select the certificate store based on the type of certificate** is selected and click **Next**.

   The **Completing the Certificate Import Wizard** window is displayed.

6. Click **Finish**.

   A **Security Warning** window is displayed.

7 Click **Yes**.

A **Certificate Import Wizard** message is displayed: "`The import was successful`".

8 Click **OK**.

9 Click **OK** in the certificate window.

10 Access the NAS Manager.

The **PowerVault License file** window is displayed.

NOTE: This window is displayed only if the license has not been installed.

11 Browse to the **License file** and click **Install**.

The **PowerVault NAS Manager Login** window is displayed.

12 Type the **username** and **password** and click **Log in**.

NOTE: Use **admin** as the username. The default password is **Stor@ge!**. You have the option of changing the password later.

The PowerVault NAS Manager is displayed with the **Start Configuration Wizard** page open.

NOTE: If the Start Configuration page does not open automatically, click **System Management→ Maintenance→ Start Configuration Wizard**.

PowerVault NAS Manager Configuration Wizard

Table 2-3 describes the options available on the **PowerVault NAS Manager Configuration Wizard**.

Table 2-3. The PowerVault NAS Manager Configuration Wizard Options

Option	Description
Solution Integration	
DNS Configuration	Enables you to configure DNS parameters.
Time Configuration	Enables you to configure time zone parameters and synchronize the time zone with NTP servers.
Monitoring	
Email (SMTP) Configuration	Enables you to configure the system's alerting mechanism using email.
SNMP Configuration	Enables you to configure the system's SNMP access and trap parameters.
System Function	
Format File System	Enables you to format the file system.
System Stop/Start	Enables you to start the file system.
Change Passwords	Enables you to change the admin and CIFS Administrator's password.
System and Users Identity	
System Identity	Enables you to configure the system name and the Active Directory domain it belongs to.
CIFS Protocol Configuration	Enables you to allow file access using the CIFS protocol and specify how CIFS users are authenticated.
Identity Management Database	Enables you to configure additional identity databases, such as NIS or LDAP.
Cross Protocol: Windows to UNIX User Mapping	Enables you to configure user identity interoperability between Active Directory and UNIX identity databases.
Using Your System	

Table 2-3. The PowerVault NAS Manager Configuration Wizard Options *(continued)*

Option	Description
NAS Volumes Configuration	Enables you to configure NAS volumes.
CIFS Shares	Enables you to configure CIFS shares.
NFS Exports	Enables you to configure NFS exports.

3

Accessing the Dell PowerVault NAS Manager

The NAS Manager is a web-based user interface that enables you to configure and monitor your PowerVault NX3500 storage system.

Browser Requirements

- Firefox 3.6
- Internet Explorer 7, 8

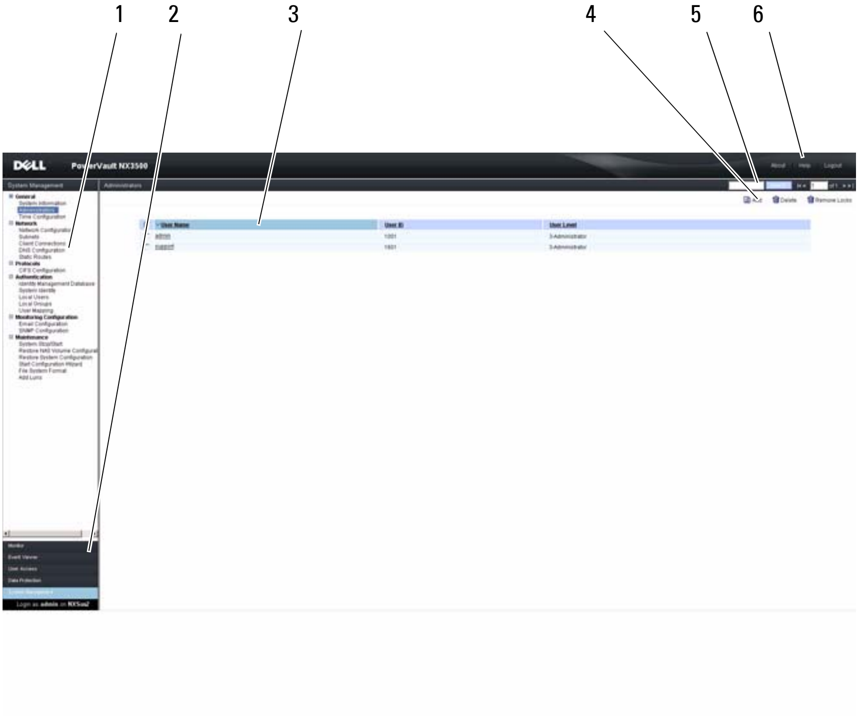
The NAS Manager can be displayed at resolutions of 1024 x 768 pixels or above. It is recommended to display the web interface at High Color, 16-bit resolution. Also, disable any type of pop-up blocker application while using the web interface as it may cause unpredictable behavior.

NOTE: It is highly recommended that JavaScript be enabled in your browser for NAS Manager to function properly.

NAS Manager Overview

The NAS Manager web interface comprises of the Admin tabs, Admin tree, Pages, Action bar, Search bar, and Toolbar.

Figure 3-1. NAS Manager Web Interface



User Name	User ID	User Level
admin	1001	3-Administrator
support	1601	3-Administrator

1	Admin tree	4	Action bar
2	Admin tabs	5	Search bar
3	Page	6	Toolbar

Action Bar

The **Action** bar, consists of additional functionality relevant to the current page displayed. For more information on the menus, see the *Online Help*.

Admin Tabs

The **Admin** tabs divide the administration tasks into functional groups. When you select a different tab, the options displayed in the Administration tree changes.

For more information on the **Admin** tabs and their functionality, see the *Online Help*.

Admin Tree

The **Admin** tree, located above the **Admin** tabs in the left pane, shows the available functionality and changes depending on the **Admin** tab selected. The **Admin** tree divides the functionality into groups and subgroups. This enables you to easily find the task you need to perform.

Toolbar

The NAS Manager toolbar, located on the upper right side of the page, displays the following options.

Table 3-1. The NAS Manager Toolbar Options

Option	Description
About	Selecting this opens the **About** screen with the current version information.
Help	Selecting this opens the online help in the section most relevant to the currently displayed page.
Logout	Selecting this enables you to exit the NAS Manager.

Page

The **Page** displays the function currently selected in the **Admin** tree or **Action** bar. You can enter information, make changes, or simply view the current status or configuration settings.

NOTE: The functionality and actions in NAS Manager are dynamic and are available as determined by the permissions allocated to each user.

NOTE: You can log on to either the CLI or the NAS Manager at a time. It is highly recommended that you do not attempt to log on to both the CLI and NAS Manager at the same time.

Search Bar

When a page contains a table of items, the **Search** bar is displayed and allows you to quickly find the relevant lines.

Each table displays up to 50 lines at a time. If more than 50 lines are available, they are split into multiple pages with 50 lines per page. You can move from one page to another by using the relevant buttons in the **Search** bar.

You can change the order a table is sorted by clicking on the column title. Click once to change the sorting order to ascending and click again to change the sorting order to descending.

The NAS Manager **Search** bar, located beside the page title, displays the following items.

Table 3-2. The NAS Manager Search Bar Options

Option	Icon Description	Description
Search filter field	N/A	Enter the string you want to use in the search. All text columns in the table are then searched.
Search button	N/A	Press this button after entering a search string to filter the table.
Go to first page	|<	Press this button to go to the first page of data.
Go to previous page	<	Press this button to go to the previous page of data.
Current page number	N/A	This field shows the current page number. You can modify this field and press <Enter> to quickly switch to a specific page.
Go to next page	>	Press this button to go to the next page of data.
Go to last page	>|	Press this button to go to the last page of data.

4

Monitoring PowerVault NX3500

NOTE: The information in this chapter refers to file management using the Dell PowerVault NAS Manager. Block management and monitoring is done using Dell PowerVault Modular Disk Storage Management (MDSM).

You can monitor the status of the Dell PowerVault NX3500 NAS clustered system using the **Monitor** tab in the NAS Manager. Here, you can view the overall status of the system on the **Dashboard** page, see the quotas usage report, and receive remote replication job status reports.

To access the monitoring pages, click the **Monitor** tab in the **Admin** tabs. By default, the **Dashboard** page is displayed.

Table 4-1. Monitor Tab Options

Field	Description
Overview	
Dashboard	Provides a single glance monitoring of the system.
Network Performance	Allows you to see network throughput for read and writes in IOPS and MBps for last day, week, month, and year.
Load Balancing	
Over time	Allows you to see processor load, CIFS connections, read and write throughput for each controller for last day, week, month, and year.
Client Connections	Allows you to see load balancing of client connections by protocol and controller. Lets you set the migration policy for each protocol.
CIFS Connections	Allows you to see a list of CIFS connections.
Hardware	
System Validation	Allows you to see the diagnostic test result of each of the system components.

Table 4-1. Monitor Tab Options *(continued)*

Field	Description
Component Status	Allows you to see the connectivity, power, and hardware status of each controller.
Capacity	
Space Utilization	Allows you to see free space, non-snapshot used space, and snapshot used space for each NAS volume for last day, last week, last month, and last year.
Quota Usage	Allows you to see the quota usage for each NAS volume for users and groups.
Replication	
NAS Replication	Allows you to see a list of NAS replication events.
NDMP	
NDMP Active Jobs	Allows you to see a list of NDMP active jobs.

Dashboard

The **Dashboard** page is displayed by default when you click the **Monitor** tab. It shows the status of the entire system in a single view. The **Dashboard** page includes five real-time and short-term sections:

- Status
- Capacity
- Current Performance
- Recent Performance
- Load Balancing

NOTE: The information in the screen is refreshed automatically every few seconds.

Status

The **Status** section displays the system status and a list of hardware components. Each hardware component type displays the total number of components and the number of problematic components. The list includes controllers and the Backup Power Supply (BPS). The power section of the controllers refers to the BPS.

Table 4-2. Status Section Options

Item	Status	Description
Overall State	On	The file system is started.
	Off	The file system is stopped.
	Stopping	The file system is stopping.
Service Status	Full Service	The system is fully operational and can be accessed by all clients. The system is in mirroring mode, that is, the write-back cache is protected by peer controller.
	Partial Service	The system may provide partial services to all clients.
	Full Service (journal)	The system is fully operational and can be accessed by all clients. The system is in journaling mode, that is, the write-back cache is protected and all the data is written directly to the disk rather than stored in the cache in order to preserve data integrity.
	No Service	The system does not provide service to any clients.
	Fault	The system has a problem providing service. The system may recover automatically within several minutes depending on the fault.
Servers Status	All Optimal	All the indicators of controllers' health are optimal.
	Not Optimal	Some indication of a problem exists, but this does not prevent service to clients. For example, this may result from power-loss to a power supply, or a network interface disconnection.
	Some Down	One controller is not responding, but the system provides service in a degraded mode. The server might recover automatically, depending on the reason.

Table 4-2. Status Section Options *(continued)*

Item	Status	Description
	Some Detached	One controller is detached, but the system provides service in a degraded mode. The controller will require manual intervention to recover (re-attach).
	Fault	Peer controllers are unable to provide service, and therefore the system does not provide service. This can happen if controllers are down or have lost access to the storage sub system.

Capacity

Table 4-3. Capacity Section Options

Color	Title	Description
Green	Free Space	The space allocated to NAS volumes but not yet in use.
Light Blue	Used space non-snapshot	The space allocated to NAS volumes and used for live data.
Purple	Used space snapshot	The space allocated to NAS volumes and used for snapshots.
Gray	Unallocated	The space, available on the LUNs, which is not allocated to any NAS volume.

Current Performance

The **Current Performance** section displays the current network throughput. The current network throughput includes data read-write throughput (MBps) and the number of read-write operations per second, per protocol.

NOTE: To display the **Network Performance** page, click the **Current Performance** title.

Table 4-4. Recent Performance Indicators

Color *	Operation	Description
Dark Purple	Read	Data read from the system (MBps).
Light Blue	Write	Data written to the system (MBps).
* See Table 4-5.		

Load Balancing

The **Load Balancing** section displays a table with real-time information about the PowerVault NX3500 status, processor utilization, and the number of connections for each controller. Table 4-5 provides a broad view of the system's load balancing.

NOTE: To display the **Load Balancing** page from the Dashboard, click the **Load Balancing** title.

Table 4-5. Processor Utilization Indicators

Color	Description
Light Green	Indicates the percentage of the processor in a controller that is busy.
Blue	Indicates the percentage of the processor in a controller that is idle.

Network Performance

The **Network Performance** page displays PowerVault NX3500 performance over time. This page contains four tabs, each provides a different period. For example, last day, last week, last month, and last year.

Table 4-6. Network Performance Indicators

Color	Protocol	Description
Green	CIFS	Data read or written using the CIFS protocol (MBps)
Blue	NFS	Data read or written using the NFS protocol (MBps)
Purple	Replication	Data read or written by NAS replication (MBps)
Yellow	NDMP	Data read or written by backup and/or restore
Magenta	Network	Network and protocol overhead, for example, metadata operations (MBps)

Client Network Throughput—Read or Write

At the top of the screen there are two graphs, **Client Network Throughput—Read** and **Client Network Throughput—Write**. The graphs display throughput information (read and write) by protocol.

Operations Per Second

The lower left side of the screen shows the operations per second (OPS) graph. The graph displays OPS information per operation.

Table 4-7. OPS Information Per Operation

Color	Operation	Description
Green	Read	The number of read operations per second.
Blue	Write	The number of write operations per second.
Magenta	Other	The number of meta-data operations per second.

Network Aggregated Throughput

The lower right side of the screen shows the Network Aggregated Throughput graph. The graph displays total network throughput by network.

Load Balancing

Over Time

The **Load Balancing Over Time** page displays the balance in load between PowerVault NX3500 controllers over time. The screen includes four tabs, each tab presents a different period, for example, last day, last week, last month, and last year.

CPU Load

The top left side of the screen displays the processor load graph. This graph displays the average processor utilization in percentage for each of the selected controllers.

CIFS Connections

The top right side of the screen displays the CIFS Connections graph. The graph displays the number of active connections for each of the selected controllers. Only CIFS connections appear in the graph (NFS clients are not connection oriented).

Throughput—Read or Write

The bottom of the screen displays two graphs:

- Throughput—Read
- Throughput—Write

The graphs display the combined actual throughput, excluding overhead (read and write) for each of the selected controllers.

Client Connections

The **Client Connections** page enables the following:

- Display the distribution of clients between controllers.
- Manually migrate specific clients from one controller to another.
- Set the policy for automatic client migration.

Displaying Client Distribution

The client's distribution page displays only clients that belong to the same subnet as the system (local clients). Clients that access the system through a router (or layer 3 switches) are not displayed in this page; instead, the router is displayed.

By default, the **Clients** tab displays a list of all the client connections. You can narrow the list down and display connections for specific Protocol, Controller, and Network.

The client connections table provides the following information.

Table 4-8. Client Connections Page

Field	Description
Client/router IP	The IP address of the client or router accessing the system.
Access using IP	The IP address used to access the system.
Assigned interface	The controller and network interface which were allocated for this client or router (either automatically by the system or manually by an administrator).
Current interface	The controller and network interface currently assigned to this client or router. The current interface can be different from the assigned interface after automatic connection fail-over. Depending on the Migration Policy, a connection that was migrated from its assigned controller to another controller, can remain on that controller. In such an event, the current interface is different from the assigned interface.
Protocol	The protocol that the client connection uses: CIFS, NFS, or Other. PowerVault NX3500 identifies the clients accessing with a recognized protocol, CIFS, or NFS and displays the actual protocol. For other local clients, for example, routers, the system displays the value 'Other' as the protocol.

Usage Considerations

Migrating Clients to Another Controller

If there is an imbalance in the network load, the system can rebalance the load by migrating clients between controllers, either automatically or manually. Choose whether the clients or routers in the list may be migrated to other controllers.

Select the connections you want to migrate from the list and click **Assign Interface**. The **Assign Interface** page displays, and lists the selected connections for approval.

Choose the controller you want to migrate the selected clients to. You can either choose a specific controller as the target or choose Assigned Controller.

- To migrate all the selected clients to a specific controller, choose a specific controller from the list.
- To migrate all the selected clients back to their original controllers after a failed controller is revived, choose the Assigned Controller. Each client can have a different assigned controller.

You can either let the system select the target interface on the controller, or choose a specific one.

NOTE: This operation will disconnect CIFS connections if they are migrated to a different controller.

- To enable automatic rebalance, select **Allow these clients to migrate to other controllers when rebalancing the network load**.
- To keep the selected clients assigned controller permanent (except during fail-over) clear **Allow these clients to migrate to other controllers when rebalancing the network load**.

Setting the Migration Policy

In case of a controller failure, the system automatically migrates each connection from the failed controller to another controller to allow clients to continue their work. This causes disconnections to CIFS clients. When the failed controller revives, the system can rebalance the load by migrating clients back to the revived controller automatically. This operation is called fail-back.

Clients that use NFS are stateless and are not affected during fail-back. Clients that use connection-based protocols (CIFS), may be disconnected during fail-back. To optimize the fail-back operation, the system provides you with the following policies for migration on recovery, which affect the load-balance and disconnections:

- Migrate Immediately—Always keep the system well balanced, at the cost of possibly disconnecting CIFS clients during work time.
- Migrate Automatically— Always keep the system well balanced if the controller failure is very short, at the cost of disconnecting CIFS clients. This option causes the system to remain unbalanced for a period of several days, if the failure remains for long time.

  This mode overcomes short controller failures because clients have not created new material during the short time failure. Therefore, the best practice is to rebalance them as soon as possible.

  If the failure is longer than 10 minutes, the system remains unbalanced until you rebalance it manually.
- Migrate Manually— Never migrates clients automatically. This requires manual intervention to rebalance the system.

  If the system requires manual intervention to rebalance it after fail-over, the system sends an appropriate email message to the administrator.

  You can configure the fail-back policy, as described above, per protocol and LAN or client network.

CIFS Connections

The **CIFS Connections** page enables you to monitor current CIFS connections. To manage CIFS connections, choose **Monitor→ Load Balancing→ CIFS Connections**. The **CIFS Connection** page is displayed.

Table 4-9. CIFS Connections

Field	Description
Process ID	The Client Connection ID.
User Name	The domain and name of the user.
Client	The client computer name.
Controller Name	The controller that the client is connected to.
Login Time	The connection time.

To disconnect a client from the CIFS protocol:

1 Select the check box beside the specific client.

2 Click **Disconnect** in the **Action** bar.

To disconnect all the connections for a specific controller:

1 Select the check box adjacent to the controller name.

2 Click **Disconnect** in the **Action** bar.

3 Click **Refresh** to update the information displayed.

Hardware

The **System Validation** page shows the current status of all components in the PowerVault NX3500. It provides information about processors, monitoring availability, NICs, IPMI, Ethernet bandwidth, BPS monitoring, cabling connectivity, temperatures, memory, network statistics, and Ethernet connectivity.

The **Component Status** page displays the current status of the PowerVault NX3500. It provides information about status, internal hardware, connectivity, and power for the two controllers.

Component Status

Viewing Detailed Status

To view additional details on the status of a specific controller, click the controller whose information you want to view. The **Controller Status** page is displayed. The following information is displayed for each controller.

Table 4-10. Controller Status Page

Field	Description
Controller	Displays the name of the selected controller.
Local IPMI Status	Displays the status of the IPMI on the selected controller.
Connectivity Status to Peer IPMI	Indicates whether the IPMI on the peer controller is accessible and responsive.
Number of CPUs	Displays the total number of processors in the controller, and indicates if any of the processors are overheated. **NOTE:** The total number of processors indicate the single processor with four cores.
Number of Ethernet NICs	Displays the total number of network ports in the controller, and indicates if any ports do not have links.
UPS Battery [%]	Displays the percentage of power stored in the BPS.
UPS Remaining Battery Time [minutes]	Displays the time in minutes that the BPS can support the system.

Capacity

Space Utilization

The **Space Utilization** page displays the current space utilization and space utilization over time. The screen shows five tabs, including the current and four over time tabs: last day, last week, last month, and last year.

Current Tab

The **Current** tab displays a list of NAS volumes.

Table 4-11. Current Tab

Field	Description
NAS Volume	The name of the NAS volume.
Allocated Space	The space allocated for this NAS volume (GB).
Free Space	Space allocated to NAS volumes but not yet in use (GB).
Used Space	Space allocated to NAS volumes and is in use (GB).
%Used by snapshot	Percentage of used space assigned to snapshots.

The last field of the NAS volume row displays a graph of the space utilization for each one of the volumes.

The end of the table provides a summary (total) row with the total for Allocated Space, Used Space, and Free Space.

The last row displays the total unallocated space. This is the space available for creation of new NAS volumes.

Table 4-12. NAS Volume

Color	Legend	Description
Blue	Used space non-snapshot	Space allocated to the NAS volume and used for live data.
Purple	Used space snapshots	Space allocated to the NAS volume and used for snapshots.
Green	Free space	Space allocated to the NAS volume but not yet in use.

Quota Usage

The **Quota Usage** page displays the quotas and usage of all users including users for which no quota has been defined. It includes users that have been removed from the system but still have usage.

To display the quotas usage, choose **Monitor→ Capacity→ Quota Usage**.

The **Quota Usage** page is displayed.

Replication

Active Remote Replication Jobs

The Active Remote Replication Jobs page enables you to monitor all active tasks (jobs) in the cluster. In addition, you can view the list of job histories (all non-active jobs that were executed on the cluster since the last installation).

To monitor and view jobs, choose **Monitor→ NAS Replication**.

The Active Remote Replication Jobs page is displayed.

Remote Replication Report

The Remote Replication Report page enables you to display all non-active jobs that were executed on the cluster since the last installation.

To display the Remote Replication Report page, choose **Monitor→ NAS Replication**.

5

Monitoring PowerVault NX3500 Events

You can monitor your Dell PowerVault NX3500 system by detecting normal and abnormal events within your system using the **Event Viewer** utility. You can use predefined queries to search for specific types of events such as Current, Major-Critical, and Remote Replication.

To open the **Event Viewer** tab:

1. Click **Event Viewer** in the **Admin** tabs to access the **Event Viewer** page.
2. Choose an existing query, or create a query by clicking **Filter** in the **Action** bar.

The following are the default (predefined) queries:

- **Current:** Displays the most recent events.
- **Major-Critical:** Displays the events most crucial to the functioning of the system.
- **Remote Replication:** Displays events related to backup of data.

When you click on a specific entry (row) in the **Event Viewer** page, an **Event Details** window opens providing you with more information about this entry. Here are the possible fields which could appear in a query.

Table 5-1. Event Viewer

Field	Description
Event ID	The identification of event.
Severity	The level of importance of the event.
Date	The date when the event occurred.
Microseconds	The time in microseconds the event occurred after service start.
Subsystem	The name of the subsystem on which the event occurred.
Module	The module which is involved in the event.
PID	The process ID.
Cleared	The event clear flag.
Context	The context of the event.
Description	A brief description about the event.

Event Search

The **Event Viewer** search utility enables you to find specific information about your PowerVault NX3500 in the system log. For example, if you want to debug a certain component and would like to view all the messages regarding that component. Other examples include searching for a string, or finding out if a certain service is currently activated.

To search the **Event Viewer**, select a predefined query or create your own query:

1. Click **Search** in the **Action** bar.

   The **Find** window is displayed.

2. In the **Find** box, type the word you would like to find (this is mandatory).
3. From the **in** drop-down list, select **All** to search all Event Viewer columns. Alternatively, select a specific column to search only that column.
4. From the **Direction** option, select **Up** or **Down**, to search either up or down the column(s).
5. Select the **Match case** check box if you would like your search to be case-sensitive.

The search utility highlights the first event that matches the case within the current page. If the query has more than one page, the search utility will search only the active page. When you click on a specific entry (row) in the Event list, an **Event Details** window opens providing you with more information about this entry.

6 Click the **Find Next** button to find the next item in the **Event Viewer** list, or click **Cancel** to exit the search utility.

Defining Queries

You can define several queries and search the PowerVault NX3500 log database according to these queries to monitor your PowerVault NX3500 system.

To define queries, in the **Action** bar of the **Event Viewer** page click **Filter**. You can modify, rename, or delete existing queries by selecting the specific query and clicking the right mouse button.

The **Create Query** page includes the following tabs:

- **Display**: Provides filtering capabilities. For more information, see the *Online Help*.
- **Sort**: Enables you to sort the fields you previously selected in the **Display** tab. For more information, see the *Online Help*.
- **Filter**: Enables you to choose the fields for your query.

Follow the steps below to define a query:

1 Click **Run Query** to run the query.

A pop-up window prompts you to define the query name.

2 Click **Close** to close the **Create Query** window.

6

Using Volumes, Shares, and Quotas

The **User Access** tab enables you to define and manage the PowerVault NX3500 from the client perspective.

To access the User Access parameters, in the **Admin** tree, click the **User Access** tab.

Table 6-1. User Access Parameters

Field	Description
NAS Volumes	
Configuration	Allows you to add and delete NAS volumes.
Shares	
NFS Exports	Displays the NFS exports for each NAS volume.
CIFS Shares	Displays the CIFS shares for each NAS volume.
Quota	
Default	Allows you to set the default quota per user and group for each NAS volume.
User Group	Displays the quota settings for user and group quota.

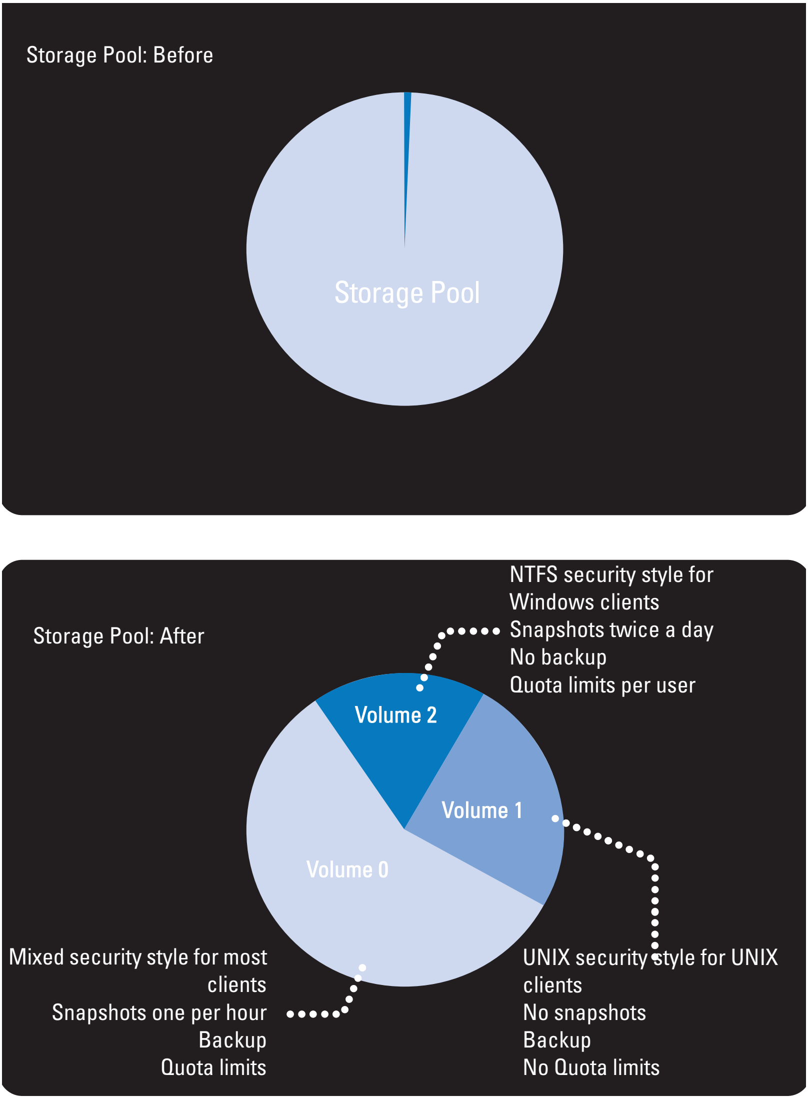
NAS Volumes

A NAS volume is a subset of the storage pool, with specific policies controlling its space allocation, data protection, and security style.

NAS volumes can be created and configured. Administrators can either create one large NAS volume consuming the entire NAS Pool or multiple NAS volumes. In either case you can create, resize, or delete these NAS volumes.

This section describes how an administrator allocates and deploys NX3500 storage using NAS volumes. In order to make NAS volumes available to users, they must be shared (exported) separately. Users need to specifically mount each share.

Figure 6-1. NAS Volumes



Usage Considerations

Choosing to define multiple NAS volumes enables administrators to apply different management policies such as, Backup, Snapshots, Quotas, and Security Style to their data. Without regard to the strategy used, the storage is managed as one storage pool and free space can easily be migrated between NAS volumes, by changing the NAS volume's allocated space.

Consider the following factors before choosing a strategy:

- General requirements
  - NAS volumes are logical; they can be easily created, deleted or modified (increased or decreased) based on the system capacity.
  - The NAS volume name should not contain more than 230 characters. It should contain only letters, digits and underscores (_) and should begin with either a letter or an underscore.
  - You can create as many virtual volumes as you want, but the total capacity cannot exceed the total storage capacity.
  - A single volume can occupy data of various types, by defining multiple shares on the volumes.
  - You can resize a virtual volume after creating it.
  - The minimum size of a NAS volume is 20MB (or if the volume has already been used, the minimum size is the stored data).
  - The maximum size of a NAS volume is the remaining unallocated space.
- Business requirements—A company or application requirement for separation or for using a single volume should be considered. NAS volumes can be used to allocate storage for departments on demand, using the threshold mechanism to notify departments when they approach the end of their allocated free space.
- Snapshots—Each NAS volume can have a dedicated snapshot scheduling policy to best protect the type of data it stores.
- Security style—In multiple protocol environments, it may be beneficial to separate the data and define NAS volumes with UNIX security style for UNIX-based clients, and NTFS for Windows-based clients. This enables the administrator to match the security style with business requirements and various data access patterns.

- Quotas—Quotas are also defined per NAS volume. Different quota policies can be applied to different NAS volumes, allowing the administrator to focus on managing quotas when it is appropriate.

Some of the usage examples are copy operations, list operations, and move operations. Table 6-2 provides an example of an organization that has various departments and how NAS volumes can be created. The right solution depends on the customer's requirements because NAS volumes are flexible and they can be expanded and reduced on demand.

Table 6-2. NAS Volume Example

Department	Preferred Access Management Control	Snapshots	Replication	Backup	CIFS or NFS Clients and R/W Mix (Common is 80/20)	Hourly Change % of Existing Data (1% And Above is High)
Post Production	NFS	Hourly	No	Weekly	20–20/80	1%
Administration and Finance	CIFS	No	No	Weekly	10–50/50	None
Broadcast	Mixed	No	No	Weekly	10–90/10	None
Press	CIFS	Daily	No	No	5–10/90	5% (approximately)
Marketing	CIFS	Daily	Yes	No	5–50/50	None

Solution 1

Create five NAS volumes based on the departments. The administrator logically breaks up the storage and the management into functional groups. In this scenario, the departmental requirements are quite different and supports the design to logically create NAS volumes along department lines.

This solution provides the following advantages:

- It is logically easy to manage the NAS volumes.
- The NAS volumes are created to match the exact needs of the department.

The disadvantage of this option is that the NAS volumes become difficult to manage if the number of departments in the organization increases.

Solution 2

Group departments that have similar security requirements into NAS volumes. The administrator creates three NAS volumes, one for NFS, one for CIFS, and another for mixed. The advantage is that the NAS volumes work separately between Windows and Linux. This solution has the following disadvantages:

- All files in a NAS volume are backed up.
- Unwanted services may be provided to certain departments. If a CIFS volume is created to backup data for the administration and finance departments, the press and legal departments will also get backups even though they do not require it.

Solution 3

NAS volumes can also be created based on the feature. The disadvantage of this solution is that user mapping is required. A user needs to choose one security style, either NTFS or UNIX, and based on the security style chosen the correct mapping for other users is set.

Managing NAS Volumes

You can view the current status of all NAS volumes, add new NAS volumes, and remove or modify existing NAS volumes.

To view the currently defined NAS volumes, select **User Access→ NAS Volumes→ Configuration**. The NAS volumes list is displayed.

Adding a NAS Volume

To add a NAS volume:

1. Click **Add** in the **Action** bar above the NAS volumes list.

   The **Add NAS Volume** page is displayed.

2. Enter the new NAS volume parameters and click **Save Changes** to create the NAS volume.

NOTE: Click **Revert** to restore default properties.

Modifying a NAS Volume

To modify the parameters of a specific NAS volume:

1. Click a specific NAS volume in the NAS volume list.

   The properties of the selected NAS volume are displayed.

2. Change the parameters as required and click **Save Changes**.

NOTE: If you change the allocated space for the NAS volume, the new allocation is bound by its used space (minimum) and the available space in Dell PowerVault NX3500 (maximum).

NOTE: NFS Exports, CIFS Shares, NAS Replication, or any reference to the NAS volume to be deleted must be removed before successful deletion of a NAS volume.

Removing a NAS Volume

To remove a NAS volume:

1. Ensure that the NAS volume is not mounted and warn relevant users they will be disconnected.
2. Select the specific NAS volume in the NAS volumes list and click **Delete** in the **Action** bar. The selected NAS volume is deleted.

NOTE: Deleting a NAS volume will delete all the NAS volume's files and directories as well as its properties, that is, shares, snapshots definitions, and so on. Once deleted, the NAS volume cannot be restored unless it is redefined and restored from backup.

The space used by this deleted NAS volume is reclaimed in the background.

NOTE: It is recommended that you define a new NAS volume after brief period of time.

Shares and Exports

User access to volume space is done by sharing directories using NFS exports and CIFS shares.

Managing NFS Exports

NFS exports provide an effective way of sharing files and data across UNIX/Linux networks. NFS clients can only mount directories that have been exported.

To manage the NFS exports list, from the **User Access** tab, under **Shares**, select **NFS Exports**. The **NFS Exports** page is displayed, and displays the list of currently defined NFS exports.

Adding an NFS Export to PowerVault NX3500

To add an NFS export:

1 Click **Add** on the **Action** bar.

The **Add NFS Export** page is displayed. It consists of two tabs, **General** and **Advanced**.

2 Enter the new export properties and click **Save Changes** to save the export parameters.

NOTE: Click **Revert** to restore the default parameters.

Modifying an NFS Export

To modify the parameters of a specific NFS Export in the NFS Exports list:

1 Select the NFS Export you want to edit by clicking its name in the list.

The **Edit NFS Export** page is displayed.

2 Modify the parameters as required.

This page contains the same fields and tabs as the **Add NFS Export** page.

3 Click **Save Changes** to modify the export according to your changes.

NOTE: Click **Revert** to restore the previously saved parameters.

Removing an NFS Export

To remove an NFS Export do the following:

1. Select the check box next to the NFS Export you want to remove.
2. Click **Delete** in the **Action** bar.

Access Using NFS

From a shell on a client system, use the **su** command to log in as **root** and type the following command:

```
mount -o rw,bg,hard,nointr,tcp,vers=3,timeo=
2,retrans=10,rsize=32768,wsize=32768
<client_access_vip>:/<exported_folder>
local_folder
```

NOTE: The above parameters are the recommended parameters. It is possible to change the protocol from tcp to udp, and the NFS version from 3 to 2.

To allow a UDP connection, you can configure the firewall settings in two primary ways:

- Adjust the firewall settings so that the source IP address comes from either of the two controllers and not the client VIP.
- Open the port range for UDP to allow ports as follows:

Service Name	FluidFS Port
portmap	111
Statd	4000 through 4008
Nfs	2049 through 2057
nlm (lock manager)	4050 through 4058
mount	5001 through 5009
quota	5051 through 5059

For TCP connections, no special settings are needed. Adjust the firewall settings to let any communication pass along the TCP connection.

Managing CIFS Shares

CIFS shares provide an effective way of sharing files and data across a Windows network.

Viewing the Properties and Status of CIFS Shares

To view information on the existing CIFS shares:

1. Click **User Access→ Shares→ CIFS Shares**.
2. Select a specific NAS volume or all NAS volumes from the **Show CIFS Shares for NAS Volumes** list.

Adding a CIFS Share

To add a CIFS share:

1. Click **User Access→ Shares→ CIFS Shares**.
2. On the **CIFS Share** page, click **Add**.
3. Click **General** to define general CIFS share parameters.
4. Click **Advanced** to define advanced CIFS share parameters.
5. In the **General** tab, if you have selected the option **Files should be checked for viruses**, click **Antivirus**, and define the antivirus policy.
6. Click **Save Changes** to save the share parameters.

   NOTE: Click **Revert** to restore default parameters.

   NOTE: Do not attempt to create a CIFS share using the Microsoft Management Console (MMC). Use MMC only to set share level permissions (SLPs). See "Setting Access Control Lists and Share Level Permissions on FluidFS" on page 100.

Modifying a CIFS Share

Once you determine whether a CIFS share is a general access directory or user-based directory, you cannot change this setting. However, you can change the parameters of the general access or user-based directory settings.

To modify the parameters of a specific CIFS share:

1. Click on the CIFS share that you want to edit.
2. In the **Edit CIFS Share** page, click **General** to modify general CIFS share parameters.

3 Click **Advanced** to modify advanced CIFS share parameters.

4 In the **General** tab, if you have selected the option **Files should be checked for viruses**, click **Antivirus** and modify antivirus policy.

5 Click **Save Changes** to save the share parameters or click **Revert** to restore the previous parameters.

Setting Access Control Lists and Share Level Permissions on FluidFS

This section provides information about setting up access control lists (ACLs) and share level permissions (SLP) on Fluid File System (FluidFS). It is recommended that a Windows administrator follow the best practices as defined by Microsoft.

Both ACLs and SLPs are supported by FluidFS. However, SLPs are limited as they only address full control, modify and read rights for any given user or group.

CIFS Storage Administrator Account

A built-in local CIFS storage administrator account serves the primary purpose of setting ownership of the CIFS share. The account can also be used to set ACLs when the NAS service is not joined to an Active Directory domain. This built-in account has a randomly generated password for security purposes. You must change this password before attempting to set any ACLs or SLPs.

Active Directory Configuration

FluidFS has the ability to join an Active Directory domain. This can be done using the NAS Manager or the CLI. For more information, see "Configuring the Active Directory Service" on page 133.

Setting ACLs or SLPs on a CIFS Share

The first time a CIFS share is created, the owner of the share must be changed prior to setting any ACLs or attempting to access this share. If the PowerVault NX3500 is joined to an Active Directory domain, the following methods can be used for setting ACLs:

- Using an Active Directory domain account that has its primary group set as the Domain Admins group.

- Mapping a network drive to the CIFS share where ACLs are intended to be set.

To use an Active Directory domain account that has its primary group set as the Domain Admins group:

1 Open Windows Explorer. In the address bar type, `\\<Management Vip>\C$`.

  This gives you complete access to all NAS volumes and their CIFS shares. The NAS volume is represented as a folder.

2 Navigate to this folder and a list of all CIFS shares for this NAS volume is displayed as folders. Right-click a CIFS share (folder) and select **Properties** from the popup menu.

3 Click the **Security** tab and click **Advanced**.

4 Click the **Owner** tab and then click the **Edit** tab.

5 Click **Other users or groups…** ,and choose a user account that is a part of the domain administrators user group or any other global group that has the rights to set ACLs.

6 Ensure that **Replace owner on subcontainers and objects** is selected and click **Apply**.

7 Click **Ok** and return to the **Advanced Security Settings** window.

  You can now select the **Permissions** tab and follow Microsoft best practices to assign ACL permissions to users and groups accordingly.

  NOTE: If you have both CIFS shares and NFS shares defined on the same NAS volume, you will see both the NFS and CIFS shares contained within as folders. Attention should be given when setting ownership and setting ACLs that this is done on a CIFS share and not an NFS export.

To map a network drive to the CIFS share where ACLs are intended to be set:

1 Select **Connect using a different user name**. When prompted, use the following credentials:

  `<NetBios Name of NX3500>\Administrator`

  By default, the NetBios name is *CIFSStorage*. If it has not been changed, enter, `CIFSStorage\Administrator`.

  NOTE: You can change the NetBios name in the NAS Manager by navigating to **System Management→ Authentication→ System Identity**.

2. Follow the previous set of instructions to set the owner of the CIFS share to either a domain admin user account or the Domain Admins group.
3. After the owner is set, unmap the network drive.
4. Remap the network drive using an account that is a part of the domain administrators user group that ownership was set to previously. Follow Microsoft best practices and assign ACL permissions to users and groups accordingly.

If the NAS service is not joined to an Active Directory domain, the built-in CIFS administrator account A*dministrator* must be used to set any ACLs. To define SLPs, use MMC.

NOTE: Do not attempt to create a CIFS share using Microsoft Management Console (MMC).

Access Using CIFS

Mapping From Microsoft Windows

Microsoft Windows offers several methods to connect to CIFS shares.

To map from Windows, select one of the following options:

Option 1

Open a Command prompt and execute the net use command:

```
net use <drive letter>: \\<netbios name>\<share name>
```

Option 2

1. From the Start menu, select **Run**.

   The **Run** window is displayed.

2. Type the path to the PowerVault NX3500 share to which you want to connect:

   ```
   \\Client Access VIP >\<share name>.
   ```

3. Click **OK**.

   The **Explorer** window is displayed.

Option 3

1 Open **Windows Explorer,** choose **Tools→ Map Network Drive**.

The **Map Network Drive** dialog box is displayed.

2 From the **Drive** drop-down list, select any available drive.

3 Type the path in the **Folder** field or browse to the shared folder.

4 Click **Finish**.

Option 4

NOTE: This option lets you connect to the share but not map to it.

1 On Windows **Desktop**, click on **Network neighborhood**, and locate the PowerVault NX3500 server.

2 Select the PowerVault NX3500 server, double click on it.

3 From the **CIFS shares** list, select the share that you want to connect to.

Configuring CIFS Shares Level Permissions

Configuring CIFS Share Level Permissions (SLP) can only be done using the Microsoft Management Console (MMC).

Administrators can use a predefined MMC file (.msc) from Windows Server 2000/2003/2008 start menu and add a shared folder snap-in to connect to PowerVault NX3500 cluster.

The MMC does not let you chose which user to connect with to a remote computer.

By default it will use the user logged on to the machine to form the connection.

To use the correct user in the MMC connection:

- If the PowerVault NX3500 you are trying to manage is joined to an Active Directory, log in to the management station with <*domain*>**Administrator**.
- Before using MMC, connect to PowerVault NX3500 by using the client access Virtual IP address in the address bar of windows explorer. Log in with the administrator account and then connect to MMC.

If you are doing the latter, you may need to reset the local administrator password first. See "Resetting Local Administrator Password" on page 104.

If there are no predefined MMC files:

1 Click **Start**→ **Run**.

2 Type `mmc` and click **OK**.

3 Click **File**→ **Add/Remove Snap-in**.

4 Select **Shared Folders** and click **Add**.

5 In the **Shared Folders** window, choose **Another computer** and type your PowerVault NX3500 system name (as configured in the DNS). Alternatively, you can use the Client Access VIP address.

6 Click **Finish**.

The new shares tree is displayed in the **Console Root** window.

7 Right-click on the required share, and choose **properties** to set share level permissions.

8 In the **Share Properties** window, choose the **Share Permission** tab.

Removing a CIFS Share

To remove a CIFS share:

1 Select the check box next to the CIFS share that you want to remove.

2 Click **Delete** in the **Action Bar**.

NOTE: Removing a CIFS share does not remove the files and folders. To understand how to manage this optimally, see "Setting Access Control Lists and Share Level Permissions on FluidFS" on page 100.

Resetting Local Administrator Password

NOTE: During installation a random password is generated. Reset the password.

To reset the local administrator password:

1 Log in to the NAS Manager.

2 **System Management**→ **Authentication**→ **Local Users**.

3 Choose **Administrator** user.

4 Choose **Change password**.

You can now use the Administrator user to browse in MMC as described above. This is also referred to as the local CIFS administrator.

Quotas

This section details managing PowerVault NX3500 Quotas for a user, or a group on a specific volume. Quota values always relate to a specific volume and are specified in units of MB.

Default Quotas

To manage the default quotas of a volume, choose **User Access→ Quota→ Default**.

The **Default Quota** page is displayed with a drop down dialog for each volume.

The following information is provided for each entry:

Table 6-3. Default Quotas

Field	Description
NAS volume	The NAS volume to set a default quota rule.
Default quota per user	The amount in MB a user is limited to or unlimited.
Alert administrator when quota reaches	The amount in MB when an alert is sent to the administrator or disabled.
Default quota per group	The amount in MB a group is limited to or unlimited.
Alert administrator when quota reaches	The amount in MB when an alert is sent to the administrator or disabled.

The default quota can be overridden by user specific or group specific quotas.

User or Group Specific Quotas

To add, edit, or delete a specific user or group quota, choose **User Access→ Quota→ User/Group**.

The **User/Group Quota** page is displayed with a drop down dialog for each volume. User/Group specific quotas override default quotas. All quota rules are applied only to the specific NAS volume selected.

Quota Types

- **User**—Per user quota.
- **All of group**—Total quota of the entire group.
- **Any user in group**—Per user quota for any user that belongs to the group.

Adding a Quota

To add a quota:

1. Click **Add** in the **Action** bar to add a user or group quota.

   The **Create Quota** page is displayed.

2. Select the volume and quota type and fill in the relevant entries where required.
3. Click **Save Changes** to save the new quota definition.
4. Click **Revert** to restore the default parameters.

Modifying a Quota

To modify an existing quota:

1. Click the specific **Group/User** in the **User/Group Quota** page.

   The **Edit Quota** page is displayed.

2. Modify the quota rules as desired and click **Save Changes**.

Deleting a Quota

To delete a quota rule:

1. Select the check box next to the specific quota rule.
2. Click **Delete** in the **Action** bar.

The selected quota rule is deleted from the list.

7

Protecting Data on PowerVault NX3500

Data protection is an important and integral part of any storage infrastructure. The data on your PowerVault NX3500 can be protected in a number of ways such as replication, backing up of data using a Data Management Application (DMA) and so on.

This chapter explains how to set up and manage replication on a Dell PowerVault NX3500 system or multiple PowerVault NX3500 systems. It also describes how to back up and restore data, and protect your data against virus attacks.

Table 7-1. Data Protection Options

Field	Description
SnapShots	
Policies	Allows you to view or modify the snapshot policy and schedule of a NAS volume.
List	Displays the snapshots for the NAS volumes.
Restore	Allows you to restore a NAS volume to its exact contents when a snapshot was taken.
Replication	
Replication Partners	Displays the trusted systems defined as replication partners.
NAS Replication	Allows you to add the replication policy and schedule of NAS volumes.
NDMP	
NDMP Configuration	Allows you to enable backups, add and delete backup server; change backup password, username, and NDMP client port.
NDMP Active Jobs	Displays all the active backup and/or restore jobs.

Field	Description
Antivirus	
Antivirus Hosts	Allows you to add and delete anti-virus hosts and corresponding ICAP port.

Replication

Replication is used in various scenarios to achieve different levels of data protection. Some of these include:

- Fast backup and restore: Maintain full copies of data for protection against data loss, corruption, or user mistakes.
- Disaster recovery: Mirror data to remote locations for failover.
- Remote data access: Applications can access mirrored data in read-only or read-write mode.
- Online data migration: Minimize downtime associated with data migration.

NAS Replication

Replication leverages the snapshot technology in the PowerVault NX3500 file system. After the first replication, only deltas are replicated. This allows for faster replication and efficient use of the CPU cycles. It also saves on storage space while keeping data consistent.

Replication is volume based and can be used to replicate volumes on the same PowerVault NX3500 system (see Figure 7-1) or a volume on another PowerVault NX3500 system (see Figure 7-2). When replicating a volume to another PowerVault NX3500 system, the other system must be setup as a replication partner.

Once a partner relationship is established, replication is bi-directional. One system could hold target volumes for the other system as well as source volumes to replicate to that other system. Replication data flows through a secure ssh tunnel from system to system over the client network.

A replication policy can be setup to run on various schedules as well as on demand. All system configurations (user quotas, snapshot policy, and so on) are stored on each volume. When a volume is replicated, the target volume holds identical information. When removing a replication policy, an option is provided for transferring the volume configuration.

Figure 7-1. Local Replication

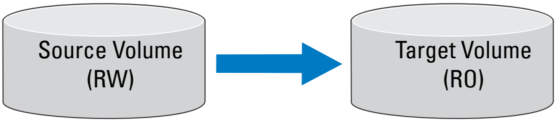
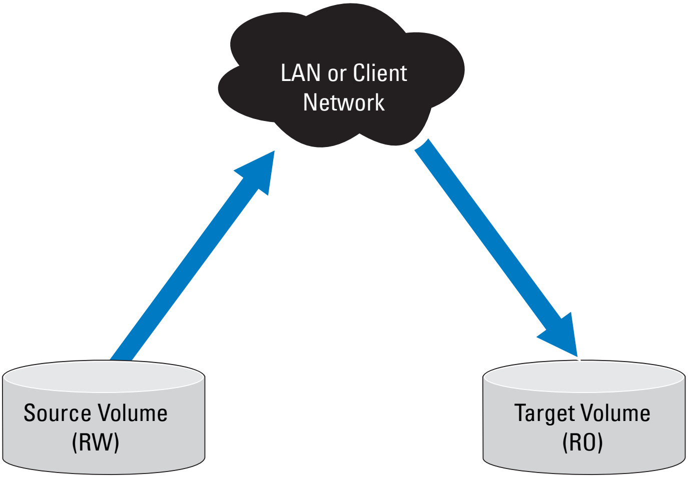


Figure 7-2. Partner Replication



Activating Replication

After purchasing a key, customers can activate replication using the following syntax:

```
system general licensing set replication XXXXXXX
```

Setting Up a Replication Partner

From the NAS Manager, navigate to **Data Protection→ Replication→ Replication Partners**.

From the **Action** bar, click **Add** and enter the NAS management VIP for the remote partner you would like to replicate to. Add the credentials of an admin on the remote system to add the partner. On the remote system, the source system now becomes a partner as well. This is a bi-directional replication trust. Source volumes and target volumes can be located on either system.

Adding a Replication Policy

From the NAS Manager, navigate to **Data Protection→ Replication→ NAS Replication**.

Add a policy by clicking the **Add** button. A policy can be a local volume replication or a remote volume replication. For local replication, choose localhost as the destination system.

Managing Replication Policies

To manage a replication policy (either local or remote), access the NAS Manager or the CLI. A schedule can be set to hourly, daily, or weekly intervals. You can also choose to replicate a volume on demand. Since replication may slow down client traffic, it is recommended to stagger the replication schedules or set the replication time during a time when the system is not under heavy load. When a policy is active, the target volume is read-only to all clients. No writes can occur to this target volume as it is a mirror of the source volume.

From the NAS Manager, navigate to **Data Protection→ Replication→ NAS Replication**.

Click on the hyperlink in the source system to modify a replication policy or click **Add** to create one.

Deleting a Replication Policy

When deleting a replication policy, both volumes contain the system configuration of the source system. It is optional to transfer the source system configuration to the target system volume. This configuration includes users, quotas, snapshot policies, security style and other properties. Check the appropriate check box when deleting to transfer all properties. This option is useful in disaster recovery.

NOTE: If the replication policy is deleted from the target volume's system, a warning is issued and the policy must be deleted from the source system as well.

From the NAS Manager, navigate to **Data Protection→ Replication→ NAS Replication**.

Click on the hyperlink on the source system to modify a replication policy.

Removing a Replication Partner

When deleting a replication partner, make sure both systems are up and running. If one of the systems is down or unreachable, a warning message is displayed. This warning is for information only. Once the system that is unreachable or down comes back up, the replication partner must be deleted from that system. If both systems are up, the replication partner is deleted on both systems.

From the NAS Manager, navigate to **Data Protection→ Replication→ Replication Partners**.

Select the check box next to the relevant Replication Partner Name and click **Delete**.

Managing Snapshots

Snapshots

Snapshot technology creates a point in time backup of the data that resides on a volume. There are various policies that can be set for creating a snapshot. These policies include when a snapshot is to be taken, how many snapshots to keep, and how much NAS volume space can be used before snapshots are deleted. Snapshots are based upon a change set. When the first snapshot of a NAS volume is created, all snapshots created after the baseline snapshot is a delta from the previous snapshot.

Activating Snapshots

Snapshots are a licensed feature. Customers are provided a key to activate snapshots using the CLI. The syntax is as follows:

```
system general licensing set snapshots XXXXXXX
```

Creating a Snapshot (Without a Policy)

To create a snapshot:

1. In the NAS Manager, navigate to **Data Protection→ Snapshots→ List**.
2. Create a snapshot by clicking the **Create** button.
3. Choose the NAS volume from the drop-down menu and give the snapshot a unique name.

Adding or Modifying a Snapshot Policy

From the NAS Manager, navigate to **Data Protection→ Snapshots→ Policies**.

Add or modify a snapshot policy by selecting the appropriate NAS volume from the dropdown menu. There are several options on this page.

- **Alert Administrator:** Sends an alert to the administrator when the snapshot space reaches a certain percentage of the total volume size.
- **Periodic, Hourly, Daily, or Weekly:** These options can be combined to set particular schedules. Also, each option has a number of snapshots to keep. Therefore, it is advised to keep this number as low as possible since creating snapshots impact system performance.

Accessing Snapshots

Once the snapshot is created, you can access a special folder from Export or Share.

Access the special folder from UNIX under the directory called **.snapshots** under each NFS Export.

Access the special folder from Microsoft Windows under the directory **.snapshots** under each Share. (This integrates into Shadow Copies and enables previous versions.)

Snapshots retain the same security style as the Active file system. Therefore, even using Snapshots, users can access only their own files based on existing permissions. The data available when accessing a specific Snapshot is at the level of the specific share and its subdirectories, ensuring that users cannot access other parts of the file system.

Restoring Data

You can restore data in two ways:

- Copying and pasting: Individual file restores

  If you have accidentally deleted or modified a file and would like to restore it, access the snapshot directory located in the current NFS Export or Share, find the requested snapshot (according to its time of creation) and copy the file to its original location. This method is useful for the day-to-day restore activities of individual files.

- Restoring a NAS Volume from a Snapshot

  If you need to restore an entire volume (in case of application error or virus attacks), where copy and paste of huge amounts of data takes a lot of time, the entire NAS Volume can be restored.

Restoring a NAS Volume From a Snapshot

1. From the NAS Manager, navigate to **Data Protection→ Snapshots→** Restore.
2. Choose the NAS volume to be reverted and a snapshot revision name to revert to.

   All data written to the volume after the reverted snapshot was taken is deleted. A snapshot taken of the volume after the reverted snapshot is deleted as well.

Deleting a Snapshot

From the NAS Manager, navigate to **Data Protection→ Snapshots→ List**.

Click on the check box next to the snapshot name you wish to delete and then click the **Delete** button.

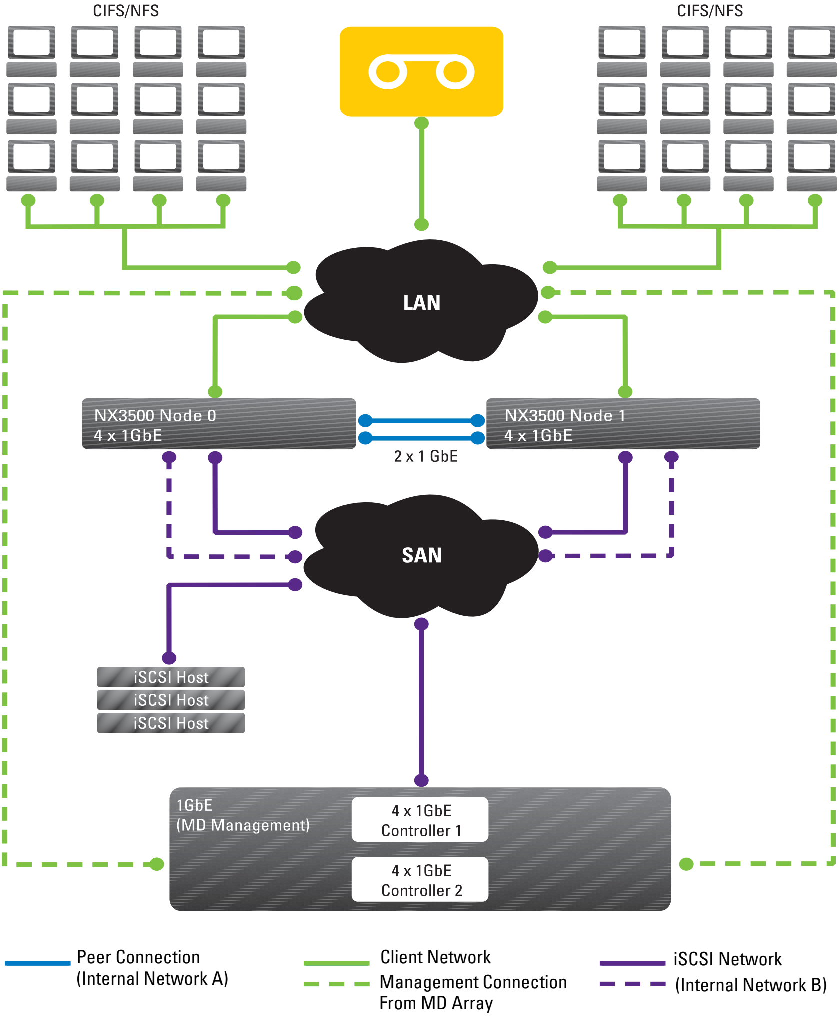
Backing Up and Restoring Data

It is recommended that you back up your data in regular intervals.

The PowerVault NX3500 system supports backup and restore using Network Data Management Protocol (NDMP). An NDMP agent installed on the PowerVault NX3500 ensures that stored data can be backed up and restored using an industry-standard Data Management Application (DMA) that supports NDMP protocol, without needing to install vendor-specific agents on the NAS appliance.

In order to perform backup and restore operations, a DMA needs to be configured to be able to access the NAS appliance using the LAN or client network. PowerVault NX3500 does not use a dedicated address for backup operations, any configured LAN or client network address can be used for backup and restore operations.

Figure 7-3. Backing Up and Restoring Data



NDMP backups on PowerVault NX3500 are performed using the LAN or client network. The DMA should be configured to access one of the client VIPs (or a DNS name) of the PowerVault NX3500 cluster.

The PowerVault NX3500 does not support a dedicated backup IP address configured on LAN or client network. All Virtual IPs configured on the LAN or client network can be used by backup software to take backups and perform restores.

The PowerVault NX3500 NAS system provides a generic user interface to enable the NDMP agent and is programmed to work independent of the installed NDMP agent.

Supported Applications

The PowerVault NX3500 is certified to work with the following DMAs:

- Symantec BackupExec 2010R3
- Symantec NetBackup 7.0 or later
- CommVault Simpana 9.0 or later

Enabling NDMP Support

To enable NDMP support:

1 From the NAS Manager, click **Data Protection**→ **NDMP**→ **NDMP Configuration**.

   The **NDMP Agent Configuration** page is displayed.

2 Select **Enable NDMP**.

3 Enter the IP address of the DMA server.

   NOTE: DNS names are not supported.

4 Click **Save Changes**.

Changing NDMP Password

User name and password are required when configuring an NDMP server in the DMA. The username is *backup_user* and cannot be changed.

To change the NDMP password:

1. Click **Data Protection→ NDMP→ NDMP Configuration**.
2. Click **Change Backup User Password.**
3. Enter **admin** password and the new password for backup_user.
4. Click **Save Changes**.

Modifying DMA Servers List

In order to take an NDMP backup of the PowerVault NX3500 NAS system, the Backup Application server must be included in the whitelist of the DMA servers.

To add a DMA server to the list:

1. Click **Data Protection→ NDMP→ NDMP Configuration**.
2. Type the IP address of the DMA server in the empty DMA Server field.

   DNS names are not supported.
3. Click **Save Changes**.
4. If no empty fields are available, click **Add DMA Server** button on the **Action** tab and go to step 2.

To remove a DMA server from the list:

1. Click **Data Protection→ NDMP→ NDMP Configuration**.
2. Select the check box next to the DMA server you would like to remove.
3. Click **Remove DMA Server** on the **Action** bar.

NOTE: Removing the DMA server from the whitelist does not interrupt backup-restore operation already in progress to/from that DMA server.

Specifying NAS Volume for Backup

Most Backup Applications automatically list the available volumes to backup. In Symantec NetBackup 7.0 you can manually type in the volume path.

The PowerVault NX3500 system exposes backup volumes at the following path: **/mnt/backup/**<*NASVolumeName*> where <*NASVolumeName*> is the exact name as it appears in the user interface.

Displaying Active NDMP Jobs

All backup or restore operations being processed by the PowerVault NX3500 can be seen on the NDMP Active Jobs page, under **Data Protection→ NDMP** or **Monitor→ NDMP.**

For each session, the following information is displayed.

- **Session ID**: The unique identifier for this session.
- **Initiator DMA**: DMA IP address that initiated this session.
- **Controller**: Which controller is processing the session.
- **Started On**: Timestamp of session creation.
- **Path**: What path is being backed up or restored by the session.
- **Job Type**: Type of a session. Valid types are DATA_RESTORE and DATA_BACKUP.

Terminating an Active NDMP Job

You can terminate an active NDMP job. To terminate an active NDMP job:

1. Go to the NAS Manager and select **Data Protection→ NDMP→ NDMP Active Jobs**.
2. Select the check box next to the session to be terminated.
3. Click **Kill Active NDMP Job**.

   Multiple sessions may be selected at a time.

NDMP Design Considerations

- Use DNS name for the NDMP server when setting up backup in DMAs, so that load-balancing is used.
- Limit the number of concurrent backup jobs to one per controller to make data transfer quick.
- Your solution supports only a three-way backup, wherein the DMA server mediates the data transfer between NAS appliance and storage device. Make sure the DMA server has enough bandwidth.

Using Antivirus Applications

Overview

Dell PowerVault NX3500 contains integration with industry standard ICAP-enabled antivirus software to ensure files written from CIFS clients are virus-free.

Supported Applications

The antivirus host must run Symantec ScanEngine 5.2, which is ICAP-enabled.

Adding Antivirus Hosts

To enable the Antivirus option:

1. Click **Data Protection→ Antivirus→ Antivirus Hosts.**

   The **Antivirus host configuration** page is displayed.

2. Enter the Antivirus host IP addresses and the port numbers for all antivirus hosts.
3. Click **Save Changes**.

Enabling Antivirus Support Per CIFS Share

Antivirus support is available on per-CIFS share basis.

1. Click **User Access→ Shares→ CIFS Shares**.
2. Click on the CIFS share you would like to enable AV support for.
3. Select **Files should be checked for viruses** at the bottom of the page.
4. Click the **Antivirus** link that is displayed on top of the page next to **General** and **Advanced**.
5. Configure the behavior for handling virus-infected files (Optional).
6. Configure which files should be checked for viruses (Optional).
7. Configure the exclusion list (Optional).
8. Click **Save Changes**.

8

Managing the PowerVault NX3500

You can view and set general system information, configure the file system and network parameters and set the required protocols through the **System Management** tab. In addition, you can also configure the authentication settings.

To access the **System Management** options, launch the Dell PowerVault NAS Manager. Click the **System Management** tab. The **General Information** page is displayed.

Table 8-1. System Management Options

Field	Description
General	
Systems Information	Shows system version, system ID, and system name.
Administrators	Allows you to add, delete, and remove locks on administrators.
Time Configuration	Allows you to define the time zone, the NTP server, and the current date and time.
Network	
Network Configuration	Allows you to define the IP address of your default gateway, LAN or Client MTU, and load balancing method.
Subnets	Allows you to add, edit, and delete subnets.
Client Connections	Displays connections for each protocol and controller. Allows migration of user connections to a controller.
DNS Configuration	Allows you to define the DNS server IP address and suffix.
Static Routes	Allows you to add static routes.
Protocols	
CIFS Configuration	Allows you to configure your CIFS protocol; the way users' identities are authenticated, DOS code page and UNIX character set.

Table 8-1. System Management Options *(continued)*

Field	Description
Authentication	
Identity Management Database	Allows you to define the UNIX identity database, the NIS domain, the NIS servers, or LDAP configuration.
System Identity	Allows you to define the system name, the netbios name, the fully qualified domain name, domain controller or workgroup name.
Local Users	Allows you to add, edit, and delete local users.
Local Groups	Allows you to add, edit, and delete local groups.
User Mapping	Allows you to select whether to automatically map users in Active Directory to users in the UNIX user repository and vice versa. Lets you map a guest account.
Monitoring Configuration	
Email Configuration	Allows you to setup event e-mails, define the e-mail address, define the maximum e-mail size and maximum time to wait.
SNMP Configuration	Allows you to define system contact, system location, read community, trap recipient, and minimum trap severity.
Maintenance	
System Stop/Start	Allows you to start, stop or perform an orderly shutdown of system.
Restore NAS Volume Configuration	Allows you to restore the NAS volume configuration after selecting which parameters should be restored.
Restore System Configuration	Allows you to restore the NAS system configuration after selecting which system-wide parameters should be restored.
Start Configuration Wizard	Allows you to run the configuration wizard which guides you through the steps of integrating the NAS system into your environment.
File System Format	Runs discovery of controllers, assigned LUNs, and allows you to format the LUNs.
Add LUNs	Runs discovery of controllers, assigned LUNs, and allows you to add LUNs to the system.

Managing the System

You can perform management operations on the cluster using the NAS Manager.

A NAS Management virtual IP address is required in order to access the NAS Manager. This IP address allows you to manage the cluster as a single entity.

Additional IP addresses are required for both the individual controllers in the system and for the system. These IP addresses must not be accessed by clients directly.

Managing Client Access

The **Subnets** page enables you to set one or more virtual IP addresses through which clients access the system's shares and exports. If your network is routed, it is recommended to define more than one virtual IP address.

You can define multiple subnets to allow clients to access the PowerVault NX3500 directly and not through a router. Configure a single name on your DNS servers for each subnet, to enable load-balancing between these IP addresses.

NOTE: All the virtual IP addresses must be valid IP addresses on the networks allocated by the site system administrator.

The **Subnets** page also lets you update the IP address ranges used internally by the system, for management and interconnect purposes.

You can view the current configuration of the system subnets, add new subnet information, and remove or modify existing subnets. Configure a single name on your DNS servers for each subnet, to enable load balancing between these IP addresses.

The total number of NAS service IP addresses depends on the bonding mode for the NAS service:

- For Adaptive Load Balancing (ALB), specify two IP addresses multiplied by the number of NAS nodes. For PowerVault NX3500 NAS service, specify four NAS service IP addresses.
- For LACP (IEEE 802.3), specify one IP address multiplied by the number of NAS nodes. You need only one IP address for each node because the two client network interfaces in each node are bonded together. For PowerVault NX3500 NAS service, specify two NAS service IP addresses.

NOTE: If you choose LACP, ensure you configure the LACP bond in client switches. Create an LACP bond for the switch ports to which the two client interfaces of a node are connected and repeat this procedure for each node.

Viewing the Defined Subnets

To view the defined subnets, click **System Management→ Network→ Subnets**.

Modifying a Subnet

To modify a subnet:

1 Select a specific subnet in the subnets list.

  The properties of the selected subnet are displayed.

2 Change the parameters as required.

3 Click **Save Changes** to save the NAS volume parameters, or click **Revert** to restore the previously saved properties.

NOTE: You cannot rename the Primary subnet, or any internal subnet (Interconnect and Management). If you need to update the IP addresses of an internal subnet, you must stop the file system before editing the desired IP addresses.

Removing a Subnet

To remove a subnet, select the specific subnet from the subnets list and click **Delete** in the **Action** bar. The selected subnet is deleted.

NOTE: You cannot delete the Primary subnet, or any internal subnet (Interconnect and Management).

Managing Administrator Users

To manage administrator users:

1. In the NAS Manager, select **System Management**→ **General**→ **Administrators**.

   The **Administrators** page is displayed, displaying the list of currently defined administrators.

2. Click on an administrator listed in the **User Name** column to view the properties of that specific administrator.

Adding an Administrator

When defining an administrator, you specify the administrator permission level. Permission levels are predefined in the system.

The defined permission levels are as follows:

- Administrator
- View only

The permission level defines the set of actions that are allowed by the user at this level.

To add an administrator:

1. Click **Add** in the **Actions** bar to add an administrator to the list.
2. Click **Filters** to define filter rules for SNMP traps.
3. Define the minimum trap severity that is sent for various categories of traps.

   The default option is to send major traps for all categories.

4. Click **Save Changes** to save the information you have entered.

   The new administrator parameters are saved by the system.

5. Click **Revert** to restore the previous parameters.

Changing the Administrator's Password

To change the administrator's password:

1. Click on an administrator listed in the **User Name** column in the Administrator list.

   The properties of the selected administrator are displayed.

2. Click **Change Password** in the **Action** bar.

   The **Change Password** window is displayed.

3. Follow the instructions to change the password.

Modifying an Administrator

To modify an administrator:

1. Click on an administrator listed in the **User Name** column in the Administrator list.

   The properties of the selected administrator are displayed.

2. Modify the properties as required, except for the user name.

Modifying an Administrator's E-Mail Filter Rules

The e-mail alerts are grouped by topics such as Administration changes, Hardware and Replication. Each alert specifies its severity, either major or informative.

To define the types of e-mail alerts an administrator can receive:

1. From the **User Name** column in the Administrator list, select the administrator whose properties you want to modify.

   The properties of the selected administrator are displayed.

2. Select the **Filters** tab.
3. For each topic, set the minimum severity level of alerts, after which the system sends an e-mail. To completely avoid sending alerts of that topic, select **None**.

Removing an Administrator

To remove an administrator:

1. Select the check box next to the specific administrator in the Administrator list.
2. Click **Delete** in the **Action** bar.

   The selected administrator is removed from the list.

Managing Local Users

This section is intended for sites that use the PowerVault NX3500 system to manage local users. If your site is configured with an external NIS/LDAP database, you can skip this section.

After local users are configured, they can access the cluster even when an external NIS is introduced.

For local users, access to the file system is determined by volumes, shares, and exports.

To allow PowerVault NX3500 to use local user definitions:

1 Select **System Management→ Authentication→ Identity Management Database**.

2 Select **Users are not defined in an external user database**.

3 For CIFS users, select **System Management→ Protocols→ CIFS Configuration**.

4 In the **CIFS Protocol Configuration** page define the Authentication mode to be **Authenticate users via local users database**.

5 To manage the **Local Users** list, select **System Management→ Authentication→ Local Users**.

Adding Local Users

To add local users:

1 With the **Local Users** page displayed, click **Add** in the **Action** bar.

The **General** tab of the Add User page is displayed. Enter the required information.

2 Select the **Advanced** tab for additional and optional fields.

3 Click **Save Changes** to save the new local user information which is displayed in the Local Users list.

NOTE: Click **Revert** to restore the previously saved properties.

Modifying Local Users

To modify local users:

1. Click the specific User Name in the **Local Users** list.

   The **Edit User** page is displayed.

2. Modify the properties as required, except for the user name.

Deleting Local Users

To define local users:

1. Select the check box next to the specific local user.
2. Click **Delete** in the **Action** bar.

   The selected Local User is deleted from the list.

Changing the Password

The **Change Password** option is accessed from the **Edit User** page.

To change the password of a local storage user:

1. Click **Change Password** in the **Action** bar.

   The **Change Password** dialog box is displayed.

2. Enter your NAS Manager password.
3. Enter the new password twice (New password or Retype password).
4. Click **Save Changes** to save the new password.

Managing Local Groups

If your site is configured with external NIS database, you can skip this section.

You should only define local groups in case you have very few Linux/UNIX end users who require access to PowerVault NX3500 using NFS, and only if there is no external NIS database.

PowerVault NX3500 groups assist in the organization and management of users. When defining users, you can assign local storage users to one or more groups. The PowerVault NX3500 system may also include groups or users defined externally, such as groups defined in a UNIX system.

To manage the Local Groups list, select **System Management→ Authentication→ Local Groups**.

The Local Groups page is displayed with the list of currently defined groups.

Adding a Local Group

To add a local group:

1. Click **Add** in the **Action** bar to add a group to the Local Groups list.

   The **Add Group** page is displayed.

2. Fill in the relevant entries where required.
3. Click **Save Changes** to save the new group which is then displayed in the Local Groups list.

NOTE: Click **Revert** to restore the previously saved parameters.

Modifying a Local Group

To modify a local group:

1. Click the specific Group Name in the Local Groups list.

   The **Edit Group** page is displayed.

2. Modify the Group ID as required.

Deleting a Local Group

To delete a local group:

1. Select the specific group.
2. Click **Delete** in the **Action** bar.

   The selected group is deleted from the list.

Authentication

The Authentication entry allows you to configure the authentication authorities, such as Network Information Services (NIS), Active Directory (AD), and Light-weight Directory Access Protocol (LDAP). In addition, you can manage local users and groups and map user names from Windows SIDs to UNIX UIDs.

PowerVault NX3500 supports the following configuration modes:

- Active Directory Authentication Mixed Mode and Native Mode
- NIS authentication only
- LDAP authentication only
- Local internal users only
- NIS or LDAP and Active Directory

Configuring an Identity Management Database

An Identity Management Database allows the system to authenticate and manage user-level access control. This database is responsible for managing the users and their passwords, the groups, and the relationship between users and groups.

If the system belongs to an Active Directory domain, then it also serves as an identity management database. You can define additional UNIX databases if needed.

UNIX identity management databases include NIS and LDAP, and they are relevant only when clients access the system using the NFS protocol (UNIX/Linux clients).

You can choose one of the following options, based on your network environment:

- Enable user authentication through an NIS database
- Enable user authentication through an LDAP database
- Disable the use of an external UNIX identity management database

Enabling User Authentication Through an NIS Database

To enable user authentication:

1. Click **System Management→ Authentication→ Identity Management Database**.
2. Click **Users and groups are defined in a NIS database and** set the NIS database properties.
3. Type the domain name of the NIS database in the **Domain name** field.
4. Type the name or IP address of the NIS server in the **NIS server** field.
5. To add an NIS server for redundancy purposes, click **Add NIS server** and type the name of the new NIS server or its IP address in the **NIS Server** field.
6. To remove an NIS server from the list, select the NIS server that you want to delete and click **Delete NIS server(s)**.
7. Click **OK** when prompted to accept the changes.
8. Click **Save Changes** to save the configuration.

NOTE: Click **Revert** to restore the previous configuration settings.

Enabling User Authentication Through an LDAP Database

To enable user authentication:

1. Click **System Management→ Authentication→ Identity Management Database**.
2. Click **Users and groups are defined in an LDAP database**. Set the LDAP server properties as follows:
   a. Type the name or IP address of the LDAP server in the **LDAP server** field.
   b. Type the base DN (distinguishable name) that you want to use for authentication purposes in the **Base DN** field.

      The Base DN (Distinguishable Name) is a unique LDAP string representing the domain to use for authentication. It is usually in the format: dc=domain,dc=com.
3. Click **Save Changes** to save the configuration.

NOTE: Click **Revert** to restore the previous configuration settings.

Disabling the Use of an External UNIX Identity Management Database

To disable the use of an external UNIX identity management database:

1. Click **System Management→ Authentication→ Identity Management Database**.

   The **Identity Management Database** page is displayed.

2. Click **Users are not defined in an external user database**.
3. Click **Save Changes** to save the configuration.

NOTE: Click **Revert** to restore the previous configuration settings.

Active Directory

The Active Directory service stores information about all objects on the computer network and makes this information available for administrators and users to find and apply. Using the active directory, users can access resources anywhere on the network with a single logon.

Similarly, administrators have a single point of administration for all objects on the network which can be viewed in a hierarchical structure. The Active Directory entry allows you to configure the active directory settings and set user authentication options. In addition, you can join the active directory to the domain.

Synchronizing PowerVault NX3500 With the Active Directory Server

If your site uses Active Directory and the PowerVault NX3500 system is part of the Windows network, synchronize the time clock to the Active Directory server. See "Synchronizing PowerVault NX3500 With a Local NTP Server" on page 141.

Configuring the Active Directory Service

To configure the active directory service:

1 Select **System Management→ Authentication→ System Identity**.

The **PowerVault NX3500 Identity** page is displayed. This page shows the current configuration and whether PowerVault NX3500 is already joined to an Active Directory domain.

2 Click **Save Changes** to save the active directory parameters.

NOTE: Click the **Revert** button to restore previously saved parameters.

Through the **Advanced Configuration** option, you can specify a domain controller to override the default controller selected by the system.

Network Configuration Overview

This section describes how to configure the PowerVault NX3500 to best fit your network.

Accessing the System

To access the system you need to define an IP address your clients can access. It is recommended to also add this IP address to your DNS server so that clients can access the system via a name in addition to an IP address.

NOTE: The Client Access VIP is configured during initial configuration using the PowerVault NX3500 Configuration Utility. You can see the address you configured by going to the NAS Manager **System Management→ Network→ Subnets**. Click **Primary** at the bottom of the page to see the client access VIP labeled VIP address.

Since the system's architecture is a cluster of two controllers, this IP address is a virtual IP address (VIP) which serves every controller in the cluster. This allows clients to access the system as a single unit, enables the system to perform load balancing between controllers, and additionally allows services to continue even if a controller fails. Clients benefit from the system's high availability and high performance irrespective of the system's architecture.

Client users access the system through a variety of network topologies. Depending on the physical capabilities of the network infrastructure, the PowerVault NX3500:

- Belongs to all LAN or client subnets. From a performance perspective, this is the most optimal configuration. In such network configurations, it is sufficient to define one client access virtual IP address (VIP) for each subnet. For more information, see "Accessing the System" on page 133.
- Does not belong to any of the LAN or Client subnets, in which case all clients are considered routed. In such situations, the clients access the data via a router or layer 3 switches. In such network configurations it is recommended to define multiple client access virtual IP addresses in a single subnet, and provide some mechanism for clients to select an IP address from that list (see the following comments regarding DNS configuration).
- Belongs to some of the LAN or Client subnets, in which case some clients are flat and some are routed. In such network configurations it is recommended to use both methods described above, and inform the users about the VIPs they need to use, depending on whether they are flat or routed.

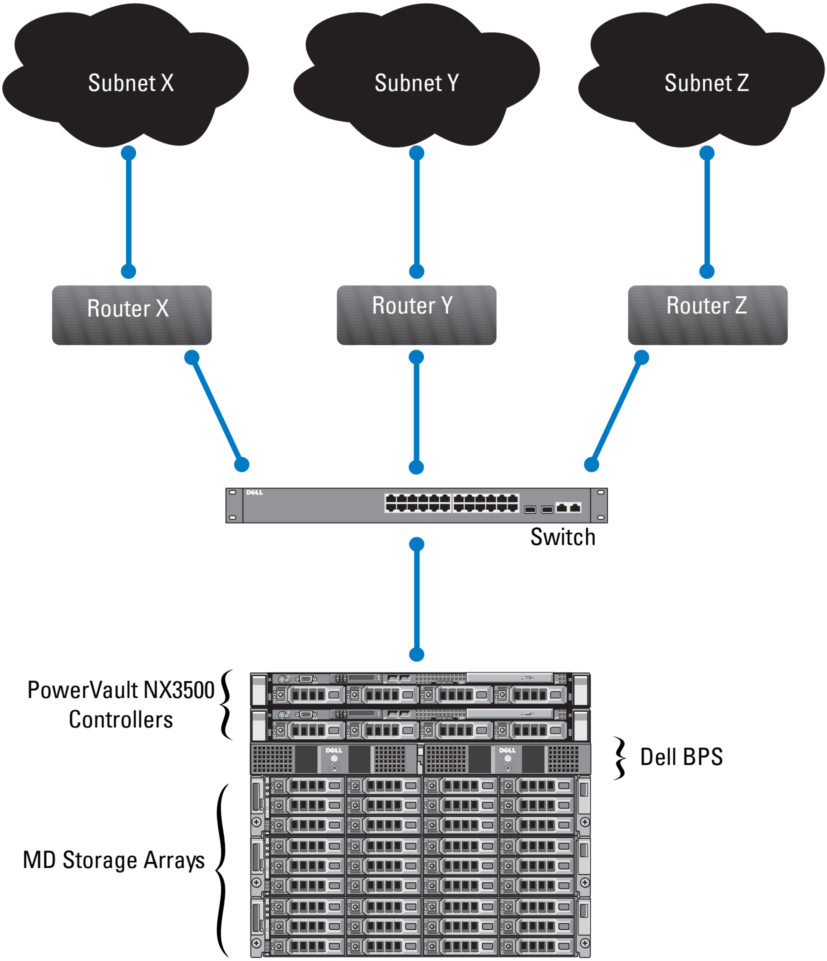
It is recommended to define an entry in the DNS for every subnet that the system belongs to, so that clients can access the data without remembering the VIPs. If there are multiple VIPs in the subnet, define a single name in your DNS server that will issue IP addresses from that list in a round-robin fashion and that all the clients can access the system.

NOTE: Do not intermix VIPs from different subnets in a single DNS name. For more information on bonding mode and VIP setting, see "Managing Client Access" on page 123

Performance and Static Routes

Routed networks provide another opportunity to enhance performance through a feature called static routes. This feature allows you to configure the exact paths in which the system communicates with various clients on a routed network.

Figure 8-1. Network Configuration



Consider the above network, there can be only one default gateway for the system. Let us assume you select *router* X.

Packets that are sent to clients in subnet Y would be routed to router X, which would then be sent back (through the switch) to router Y. This means these packets travel through router X needlessly, reducing the throughput to all subnets in your network.

The solution is to define, in addition to a default gateway, a specific gateway for certain subnets–configuring static routes. To do this you would have to describe each subnet in your network and identify the most suitable gateway to access that subnet.

You do not have to do so for the entire network - a default gateway is most suitable when performance is not an issue. You can select when and where to use static routes to best meet your performance needs. See "Managing Static Routes" on page 137.

Configuring DNS

Domain Name System (DNS) is the name resolution service that enables users to locate computers on a network or on the Internet (TCP/IP network) by using the domain name. The DNS server maintains a database of domain names (host names) and their corresponding IP addresses providing name-to-address and address-to-name resolution services on the IP network. You can configure one or more external DNS server (external to PowerVault NX3500 but within the site) to be used for name resolutions.

To configure DNS parameters, select **System Management→ Network→ DNS Configuration**.

Adding DNS Servers

To add a DNS server:

1 Click **Add DNS Server** in the **Action** bar.

A new empty row is added to the list of DNS servers.

2 Set the IP address of the client environment primary DNS.

Removing DNS Servers

To remove DNS servers:

1 Select the required DNS server.

2 Click **Delete** in the **Action** bar.

Adding DNS Domains

To add DNS domains, click **Add DNS Suffix** in the **Action** bar. A new empty row is added to the list of suffixes.

Deleting DNS Domains

To delete DNS domains:

1. Select the required domain.
2. Click **Delete** in the **Action** bar.
3. Click **Save Changes** to save changes to the DNS parameters.

NOTE: Click **Revert** to restore the previously saved parameters.

Managing Static Routes

To minimize hops between routers, static routes are suggested in routed networks when there are multiple direct paths from PowerVault NX3500 to various routers.

Select **System Management→ Network Management→ Static Routes**. The Static Routes List page is displayed, displaying the list of currently defined static routes.

Adding Static Routes

When defining a static route, you must specify the subnet properties and the gateway through which to access this subnet. When the Static Routes List page is displayed, click **Add** in the **Action** bar. The **Properties** tab of the Add Static Routes page is displayed.

Modifying a Static Route

To modify a static route:

1. Select the required static route and click **Edit** in the **Action** bar.

   The properties of the selected static route are displayed.

2. Modify the properties as required.

Deleting a Static Route

Select the required static route and click **Delete** in the **Action** bar. The selected static route is deleted from the list.

Defining File System Protocols

File system protocols are networking protocols that provide file system sharing services. The PowerVault NX3500 acts as a file system server by complying with the following protocols:

- CIFS: The Common Internet File System is for Microsoft Windows users or other CIFS clients. Directories are shared using CIFS shares.
- NFS: The Network File System protocol is for UNIX clients or services. It works at the NFS layer. Directories are shared using NFS exports.

The **Protocol** entries enable you to manage the CIFS and NFS protocols at the system level.

Configuring CIFS Parameters

The **CIFS Protocol Configuration** enables Windows users to connect to the PowerVault NX3500 system. You can also enable Linux users to access the system using the CIFS protocol, and authenticate them through NIS, LDAP or the PowerVault NX3500 local users.

Configuring General CIFS Parameters

In the **General** tab you can choose whether you want the users to be authenticated using the Active Directory domain, or an internal user database. You can also enable or disable the use of the CIFS protocol.

To authenticate users using the Active Directory domain to which the system is joined:

1. Select **System Management→ Protocols→ CIFS Configuration**.
2. Click **General**.
3. Select **Allow clients to access files via the CIFS protocol** to enable the CIFS file sharing protocol.
4. Type a short description of the server in the **System description** field.

   This description is displayed in the Windows Explorer title.

5 Select **Authenticate users' identity via Active Directory and local user database**.

6 Click **Save Changes** to save the CIFS configuration parameters.

This restarts all user connections.

To authenticate users using an internal user database:

1 Select **System Management→ Protocols→ CIFS Configuration**.

2 Click **General**.

3 Select **Allow clients to access files via the CIFS protocol** to enable the CIFS file sharing protocol.

4 Type a short description of the server in the **System description** field.

This description is displayed in the Network Neighborhood.

5 Select **Authenticate users' identity via local users database**.

6 Click **Save Changes** to save the CIFS configuration parameters.

This restarts all user connections.

To deny users from accessing files using the CIFS protocol:

1 Select **System Management→ Protocols→ CIFS Configuration**.

2 Click **General**.

3 Clear the **Allow clients to access files via the CIFS protocol** check box.

4 Click **Save Changes** to save the CIFS configuration parameters.

This restarts all user connections.

Configuring Advanced CIFS Parameters

In the **Advanced** tab you can set the following:

- Which character sets is used by DOS code pages.
- Which UTF-8 character set is used by PowerVault NX3500.

To configure advanced CIFS parameters:

1 Select **System Management→ Protocols→ CIFS Configuration**.

2 Click **Advanced** and configure the parameters.

3 Click **Save Changes** to save the CIFS configuration parameters.

This restarts all user connections.

Configuring System Time Parameters

You can configure the system's time clock, determine how to automatically update time using an NTP server, and configure the time zone for your system on this page. Synchronizing the time clock is critical for the proper functioning of the system.

This enables:

- Windows clients to mount the system.
- Scheduled activities, such as snapshot and replication tasks, to occur at the appropriate time.
- The correct time to be recorded in the system log.

Changing the Time Zone

To change the time zone:

1. Click **System Management→ General→ Time Configuration**.
2. Select the correct time zone for the region that the cluster is located in, from the **Time zone** list.
3. Click **Save Changes**.

Manually Configuring the Current Date and Time

If your environment does not include any time synchronization servers, configure the current date and time manually.

Follow the steps below to configure the current date and time manually:

1. Click **System Management→ General→ Time Configuration**.
2. Select **There is no NTP server to synchronize time with**.
3. Type the current date and time in the appropriate fields, using the format: HH:MM:SS, where HH indicates a 24-hour format. For example, *17:38:23*.
4. Click **Save Changes**.

Removing an NTP Server

If an NTP server is no longer in the LAN or client network, remove the NTP server.

To remove an NTP server:

1. Select the NTP server you want to remove.
2. Click **Delete NTP server(s)**.
3. Click **Save Changes**.

Synchronizing PowerVault NX3500 With a Local NTP Server

Network Time Protocol (NTP) helps in synchronizing and coordinating time distribution. The NTP server helps in synchronizing the clocks over the network.

If the system is not part of a Windows network, configure it to synchronize with a local NTP server (if such a server exists), or with an NTP server on the Internet. However if the system is part of a windows network, the AD can serve as the NTP server.

To configure the PowerVault NX3500 system to be synchronized with a local NTP server or an NTP server on the Internet:

1. Click **System Management→ General→ Time Configuration**.
2. Select **Time should be synchronized with an NTP server.**
3. Select **NTP Server.**
4. Type the name of the local NTP server or Internet NTP server in the **NTP server** field.
5. If you want to add a redundant NTP server, click **Add NTP Server** and type the name of the redundant NTP server in the **NTP server** field.
6. Click **Save Changes**.

9

Maintaining the PowerVault NX3500

This chapter provides information on shutting down and turning on the system in the event of a planned outage or for moving the system to another location. This chapter also discusses the procedure for upgrading the software and running diagnostics.

NOTE: See the *Dell PowerVault NX3500 Hardware Owner's Manual* on **support.dell.com**, for information on hardware service and maintenance.

Shutting Down the PowerVault NX3500 System

NOTE: Follow the procedure strictly to prevent data inconsistency.

NOTE: This procedure shuts down both the controllers.

To shutdown the system:

1. Open a web browser and connect to the NAS Management Virtual IP (VIP) address that was configured during the installation procedure.
2. From the NAS Manager, select **System Management→ Maintenance→ System Stop/Start**.
3. In the **System action to perform** list, click **Shutdown**.
4. Click **Next**.
5. When prompted as to whether you want to continue with the shutdown procedure, click **OK**.

   The following message is displayed: `The system is shutting down`.
6. This operation copies the file-system cache to the disks, stops the file system and shuts down the controllers.
7. Turn off the backup power supply (BPS) by pressing the button (located at the front of the BPS) for a few seconds.
8. In order to shut down a single node, press the power button on the desired node.
9. The NAS services automatically transfer over to the other node before shutting down.

Turning On the PowerVault NX3500 Solution

Before turning on the system, ensure that all the cables are connected between the controllers in the rack, and the components are connected to the facility's electrical power.

Turn on the components in the following order:

1. MD expansion enclosures
   - Turn on all the expansion enclosures by pressing the ON/OFF switches on the two power supplies located at the back of the storage arrays.
   - Wait until the power, controllers and disk LEDs have finished blinking and are steadily lit.
2. MD storage arrays
   - Turn on all the MD storage arrays by pressing the ON/OFF switches on the two power supplies located at the rear of the units.
   - Wait until the power, controllers and disk LEDs have finished blinking and are steadily lit.
3. BPS units

   Turn on the BPS units by pressing the Test/ON button located at the front of the BPS device, for a few seconds.
4. PowerVault NX3500 system

   Press the power buttons on the front of each controller.

Installing the Service Pack

The PowerVault NX3500 system uses a service pack methodology to update to a later version of the software.

NOTE: To update your system with the latest service pack, see **support.dell.com**.

NOTE: It is recommended that you use “binary mode FTP transfer”. If the service pack is transferred using an FTP program that is set to auto, the service pack file is recognized as text and is transferred in ascii mode. This adds control characters to the service pack file, which may cause the embedded checksum to fail.

To upgrade the service pack:

1 Download the service pack from **support.dell.com/downloads**.

2 Upload the service pack by opening the URL:
ftp://admin@ ManagementVIP:44421/servicepack
using Windows Explorer (not Internet Explorer) or any other FTP client utility).

   NOTE: The controller IP address you should use to FTP the service pack is displayed on the screen if you type `service-pack instructions`. Do not modify the name of the service pack in any way.

3 After the upload is complete, launch the CLI (see "Accessing the CLI" on page 196) and run the following command:

```
service-pack start
```

   Parameter(s):

   servicePackName—service pack name

   [**-blocking/-noblocking**]— indicates if the CLI should stay blocking during service pack installation (blocking by default)

   Example:

   DellFS-a.b.ccc-SP.sh

   Where, *DellFS-a.b.ccc-SP.sh* is the service pack name.

   NOTE: Perform the service pack update in a maintenance window. It can take approximately between 30–45 min for the update process. It is recommended that all I/O to the NX3500 be stopped before updating your solution.

   The controllers are restarted during the upgrade process, which will have the following impact on clients:

- CIFS being stateful protocol, all CIFS clients will disconnect and reconnect during the controller restart.
- NFS clients will pause intermittently but I/O will resume without any manual intervention.

4 Run mass rebalance to rebalance the CIFS clients between NX3500 controllers. From the GUI, select **Loadbalancing → Client connections → Mass rebalance**.

The service pack is successfully updated and you can resume all NAS management and I/O operations.

To upgrade your PowerVault MD storage array, see your MD Owner's Manual.

Expanding the PowerVault NX3500 Storage Capacity

You can expand the storage capacity of your system without affecting the services to the clients. However, the process occurs over a period depending on the total number of the existing and added LUNs, the total storage capacity, and system workload.

You can add additional LUNs from the storage capacity that is already available on your storage array to the PowerVault NX3500 system.

Prerequisites

This procedure requires a management workstation with the following functionalities:

- Modular Disk Storage Manager Software (MDSM) is installed and has available storage capacity that can be allocated to the PowerVault NX3500.
- The PowerVault NX3500 NAS Manager web interface is deployed.
- Is located on the LAN/client network.

To expand the PowerVault NX3500 storage capacity:

1 Create a Disk Group from the unconfirmed capacity on the MD storage array that is providing storage to the PowerVault NX3500. See "Creating Disk Groups" on page 46.

2 Create an even number of Virtual Disks ensuring that the total number of virtual disks that are assigned (including those already assigned) to the PowerVault NX3500 does not exceed 16. See "Creating Virtual Disks" on page 49.

NOTE: The virtual disk pairs must be of the same size.

3 Map the virtual disks to the Host Group created for the PowerVault NX3500 controllers. See "Creating Host-to-Virtual Disk Mappings" on page 52.

4 Add LUNs to PowerVault NX3500.

Adding LUNs to PowerVault NX3500

The new Virtual Disks/LUNs that have been allocated to PowerVault NX3500 host group in MDSM, are now ready to be discovered using the NAS Manager.

1 Launch the NAS Manager on your Management Station and log in as **admin.**

2 Click **System Management→ Maintenance→ Add LUNs.**

The page may take a few minutes to display. It will run iSCSI discovery for all Virtual Disks/LUNs allocated to the PowerVault NX3500 system.

Each LUN can be identified using its world-wide name. In the NAS Manager, the world-wide name of a LUN is prefixed by Dell FluidFS. The unique set of numbers and characters following the prefix is the world-wide name.

On the Modular Disk Storage Manager (MDSM), check that the proper virtual disks are assigned to the PowerVault NX3500 by clicking **Logical→ Virtual Disk**. In the properties pane, view the Virtual Disk world-wide identifier.

CAUTION: Before proceeding to add the LUNs, ensure that an even number of unformatted LUNs is displayed and that the number combined with the formatted LUNs does not exceed 16.

3 Click **Add LUNs** to add the new LUNs to the PowerVault NX3500 system.

The system performs an incremental file system format on the new LUNs. This process will take some time depending on the size and the number of the LUNs.

When complete, the new space is available for use.

Running Diagnostics on PowerVault

Running diagnostics helps you troubleshoot issues before seeking help from Dell.

The diagnostics options available on your solution are:

- Online Diagnostics
- Offline Diagnostics

Online Diagnostics

Online diagnostics can be run while the system is still online and serving data. There are five diagnostic options available:

- PerformanceDiagnostic
- NetworkDiagnostic
- ProtocolsDiagnostic
- FileSystemDiagnostic
- GeneralSystemDiagnostic

To run any of these options:

1 Using an SSH client, log on to the PowerVault NX3500 CLI (using the NAS Management VIP) as **admin**.

2 From the CLI run the diagnostic command

   `diag start` <*one of the five options*>

   For example, *`diag start PerformanceDiagnostic`*

To retrieve the diagnostic file:

1 Use an ftp client after the diagnostics is complete:

   ftp://admin@ ControllerIP:44421/diagnostics

2 Enter your **admin** password.

   NOTE: The controller IP address you should use to retrieve the diagnostic file is displayed on the screen.

Offline Diagnostics

NOTE: Connect a keyboard, mouse and monitor before you perform the following procedure.

Offline diagnostics requires your solution to be offline, which means out of production and not serving data. This is generally helpful to troubleshoot low-level hardware issues.

It uses the following Dell native tools:

- MP Memory
- Dell Diagnostics

MP Memory

MP Memory is a Dell-developed, MS DOS-based memory test tool. This tool is efficient for large (greater than 4 GB) memory configurations. The tool supports single-processor or multiprocessor configurations, as well as processors using the Intel Hyper-Threading Technology.

MP Memory operates only on Dell PowerVault servers that are Intel processor-based. This tool complements Dell 32-Bit Diagnostics tests and helps provide complete, comprehensive diagnostics on the controller in a pre-operating system environment.

Dell Diagnostics

Unlike many diagnostic programs, the Dell Diagnostics helps you check your computer's hardware without any additional equipment and without destroying any data. If you find a problem you cannot solve by yourself, the diagnostic tests can provide you with important information you will need when talking to Dell service and support personnel.

CAUTION: Use the Dell Diagnostics only to test Dell systems. Using this program with other systems may cause incorrect system responses or error messages.

To run Dell diagnostics:

1. Insert the Dell PowerVault NX3500 Resource media into the controller's DVD drive and reboot the controller.

   The controller boots to the DVD.

2. Select **Option 2→ Hardware Diagnostics**.

   The following choices are displayed:

a **Mpmemory diagnostic** (supports console-redirection in output log only).

- Press <ESC> key to stop testing.
- Displaying (the end) of test result log: memory.txt (Press any key when ready).

b **Delldiag** text-based diagnostic (full console-redirection support).

c Loop **Mpmemory** and diagnostic in batch mode.

d Select **Quit**.

3 Choose the appropriate option.

CAUTION: Do not choose File System Reinstall. This reinstalls the image on your controller and may cause loss of data. Do not choose FirmwareReset on a functional system as it resets IPs on the controller and may cause loss of data.

Reinstalling the PowerVault NX3500

NOTE: Connect a keyboard, mouse, and monitor before you perform the following procedure.

To reinstall the PowerVault NX3500 software:

1 Insert the Dell PowerVault Resource media into a powered down node.

The administrator is presented with the following warning message.

```
This operation will erase your current operating
system configuration. This operation cannot be
reversed once initiated. Please consult your
documentation before proceeding. Enter the
following string at the prompt to proceed:
resetmysystem.
```

2 Boot to the Media and select option one (File System Reinstall).

3 Type `resetmysystem` at the prompt.

The software starts installation automatically.

4 When the software installation is complete, the controller automatically ejects the media.

5 Once the media is ejected, the controller is ready to be set up.

6 To complete the set up, see "Setting Up Your PowerVault NX3500 Solution" on page 29 if you are installing both the controllers.

NOTE: The PowerVault NX3500 software will not install on unsupported hardware. If the PowerVault NX3500 media is inserted into a system other than a PowerVault NX3500, the user is prompted with a message and the system will fail to install the software.

Replacing a PowerVault NX3500 Controller

You may have to replace the PowerVault NX3500:

- In the event of a catastrophic failure where the existing controller cannot be brought back online.
- When an administrator wishes to replace the hardware.

Prerequisites

Before replacing the PowerVault NX3500 ensure that:

- You have physical access to the controllers.
- A keyboard, monitor, and mouse are connected to the controllers.
- The controller is verified as failed (if it is replaced with a new one).

The procedure for replacing a PowerVault NX3500 involves the following steps:

- Detaching the controller.
- Removing and replacing the controller.
- Attaching the new controller.

Detaching the PowerVault NX3500 Controller

In order to bring the cluster into the single-controller mode you need to detach a controller while any hardware is being replaced. This ensures that the system can be brought back to service with minimal downtime.

You may have to detach the controller under the following circumstances:

- A controller needs to be replaced with a new standby controller.
- A controller needs to be repaired, possibly after replacing some components.
- The administrator wants to attach a working controller to another (more critical) cluster.
- The administrator wants to discard the cluster (for example, in order to use the standby controllers to create a new cluster elsewhere).

To detach a controller:

1 Log in to the CLI using the management access VIP address.

  To obtain this address, in the NAS Manager, go to the **System Management** tab and click **Network**→ **Subnets**→ **Primary**→ **Management Console VIP**.

2 Execute the following command:

  ```
  system maintenance controllers detach start
  <controllerID> -nosaveConf
  ```

  NOTE: Depending on the configuration and the controller being detached, you may have to disconnect and reboot the system. This will only occur if the controller being detached is the primary controller being accessed by the CLI.

  If a controller was alive and working prior to initiating the detach procedure, it shuts down and upon reboot it will appear as a standby controller. In the case of a failed controller, the system adjusts in a manner that allows the connection of a new controller.

Removing and Replacing the PowerVault NX3500 Controller

To remove and replace the PowerVault NX3500 controller:

1 Disconnect all cables from the back of the controller.

2 Remove the failed system from the rack.

3 Install the new system in the rack.

4 Connect all cables to the new system.

  Ensure that the network cables are placed in the proper ports. If necessary, refer to the color coding table for client, SAN, internal, and peer port connections included with this document.Place the file system reinstall DVD in the drive and power on the newly replaced PowerVault NX3500 controller.

5 Select the **Firmware reset** option when the re-install DVD boots to the menu.

  This process may take some time to complete, and the system may restart numerous times until all the firmwares are updated. Completing this step ensures that the new controller firmwares are up to date.

6 After completing the Firmware reset stage, select the **File System Reinstall** option from the boot menu.

The reinstall process takes around 20–40 minutes to complete depending on the configuration.

Attaching the PowerVault NX3500 Controller

Before completing this procedure, verify that the controller being attached is in standby mode and powered up.

To attach the new controller to the cluster:

1 Plug-in a USB disk-on-key to the peer controller, and create a configuration for the new controller by logging in to the CLI on the management IP address and running the following command:

```
system maintenance controllers save-conf
<controllerID>
```

This command saves the system configuration on the USB disk-on-key.

2 Transfer the disk-on-key to the new controller, and let it run until the message "ready to be attached/clusterized" (after it configures the network) is displayed.

The process begins automatically.

NOTE: Do not remove the USB key until the reconfiguration has occurred.

3 Log in to the CLI on the management IP address and run the following command:

```
system maintenance controllers attach start
<controllerID>
```

4 If you get disconnected, to view the progress, log in to the CLI again and execute the following command:

```
system maintenance controllers attach status
```

This process takes some time to complete.

10

Troubleshooting

Troubleshooting CIFS Issues

Clients Cannot Access CIFS Files

Description	The Dell PowerVault NX3500 system supports antivirus scans on a per CIFS share basis. When a file on a share is opened by a client application the PowerVault NX3500 system sends the file to an antivirus host to be scanned. **NOTE:** Microsoft Windows Explorer is also an application, similar to the DOS command, moreover, it implicitly opens some file types, such as Microsoft Office files. If no antivirus host is available, access to the file and to the whole share, is inhibited.
Cause	Since the antivirus hosts are not available on the PowerVault NX3500 system, files cannot be opened on an antivirus enabled CIFS share.
Workaround	Ensure that the problem appears only on antivirus enabled shares, while clients accessing other shares do not experience such problems. Check the status of the antivirus hosts and the network path between the PowerVault NX3500 system and the antivirus hosts.

CIFS Access Denied

Description	CIFS access to a file or folder is denied.
Cause	A client without sufficient permissions performs an operation on a file/folder.
Workaround	Check the permissions on the file/folder and set the required permissions.

CIFS ACL Corruption

Description	CIFS ACL corruption.
Cause	• ACLs were accidently changed by a user or script. • ACL is corrupted after an antivirus application accidently quarantined corresponding files. • ACL got corrupted after data recovery by backup application due to compatibility issues. • ACL got corrupted after migrating data from different location by using 3rd party application, for example, *RoboCopy*.
Workaround	Check the current ACL setting in the Windows client. Redefine the ACLs for the files by using a Windows client the same way you initially defined it. In case you cannot redefine your ACLs since you currently do not have permissions, perform the following steps: **a** Restore the files from snapshots or backup. **b** In the case you have migrated the data from different location using Robocopy application, there is a good chance you can restore ACLs by copying only ACLs metadata, instead of re-copying the whole data. **c** In case all file system ACLs' are corrupted you can restore all data from the NAS replication partner.

CIFS Client Clock Skew

Description	CIFS client clock skew.
Cause	The client clock must be within 5 minutes range from the Kerberos server (that is Active Directory) clock.
Workaround	Configure the client to clock-synch with the Active Directory (as an NTP server) to avoid clock skews errors.

CIFS Client Disconnection on File Read

Description	CIFS client disconnection on file read.
Cause	Extreme CIFS workload during controller failover.
Workaround	Client needs to reconnect and open the file again.

CIFS Client General Disconnection

Description	CIFS client disconnection.
Cause	In case the system identified a general issue with the CIFS service, it automatically recovers but the failure causes all users to be disconnected and the above event to be triggered.
Workaround	If this issue repeats frequently, contact Dell.

CIFS Client Login Failure

Description	CIFS client login failure.
Cause	User supplied wrong password upon connection.
Workaround	Interactive users can retry with correct password. Applications and servers might need special attention as the user/password, which is usually set in a script or configuration file, has probably expired.

CIFS Connection Failure

Description	CIFS client share access denied.
Cause	The user is unknown in the Active Directory server, and the NAS system mapped this user to a guest user. If the share does not allow guest access, the user receives an access denied alert.
Workaround	Ensure that the user is listed in the Active Directory server the NAS is using. Alternatively, you can remove the guest limitation for the share. If the user can now access the share as guest, the newly created files are owned by the nobody/guest user.

CIFS Delete-On-Close Denial

Description	Files are deleted while they are in use.
Cause	If a file is deleted when it is open, it is marked for deletion, and is deleted after it is closed. Until then, the file appears in its original location but the system denies any attempt to open it.
Workaround	Notify the user who tried to open the file that the file has been deleted.

CIFS File Access Denied

Description	CIFS file access denied.
Cause	Client has insufficient privileges to perform the requested operation on the file.
Workaround	This is an informative event. The user may request to modify the file ACL to allow access.

CIFS File Sharing Conflict

Description	CIFS file sharing conflict.
Cause	When a file is opened using the CIFS protocol, the opening application communicates the sharing mode that must be used while this file is open. This sharing mode describes what other users' activities are allowed on this file, while it is open. This definition is sent by the application and the user cannot control/configure it. Once there is a violation of the sharing definition, the user receives an access denied error and this event is issued.
Workaround	This is an informative event, the admin may contact the locking user and request to close the application referencing this file. It could be that the application which opened the file did not shut down gracefully. It is recommended to reboot the client if possible.

CIFS Guest Account Invalid

Description	CIFS service cannot start.
Cause	A valid CIFS guest account is required for CIFS functionality.
Workaround	Configure the system guest account with a valid account.

CIFS Locking Inconsistency

Description	CIFS service is interrupted due to CIFS interlocking issues.
Cause	CIFS client interlocking scenarios.
Workaround	System recovers itself automatically, issuing the above event when recovered.

CIFS Maximum Connections Reached

Description	Maximum number of CIFS connections per NAS controller has been reached.
Cause	Each NAS controller is limited to 200 concurrent CIFS connections. • The system is in an optimal state and the number of CIFS clients accessing one of the controllers reaches the maximum. In such a scenario, consider adding NAS controllers. The system is limited to two controllers. • The system is in optimal state but the clients are significantly unbalanced between NAS controllers. In this case rebalance the clients using the NAS Manager. • The system is in degraded state (one or more NAS controllers are down) and the CIFS clients are left over on the remaining controller. In this case wait until the system returns to optimal or decrease the number of CIFS clients using the system.
Workaround	If all NAS controllers are in optimal mode, the connections are divided between both of them.

CIFS Share Does Not Exist

Description Client attempts to connect to an inexistent share.

Cause

- Spelling mistake on client side.
- Accessing the wrong server.

Workaround List the available NAS shares and verify that all shares are displayed and nothing has changed unintentionally.

Verify that you can access the problematic share using a Windows client:

1. Click **Run**.
2. Enter the NAS service IP and share name: \\<NAS-IP>\<share-name>.

CIFS Path Share Not Found

Description Client accessed a share which refers to an inexistent directory in the NAS container.

Cause

- The NAS system is restored from a backup or remote replication. During restore time, the directory structure is not complete and a few directories may not exist.

  Communicate the status and wait for the restore process to complete.
- A client with an authorization to access a higher directory in the same path deleted or altered a directory, which is mounted by another client.

  If multiple users are accessing the same dataset, it is recommended to apply a strict permission scheme to avoid such conflicts.

Workaround List all available shares on the NAS and identify the problematic share. It should have an indication that it is not accessible.

1. Restore the problematic path from a backup.
2. Manually create the missing directories. Set permissions to control access as required.
3. Remove the share and communicate to the client.

CIFS Write to Read Only Volume

Description	Client tries to modify a file on read-only volume.
Cause	A NAS volume is set to read-only when it is the target of a replication. The most frequent reason for this event is either: • The user meant to access the target system for read purposes, but also tries to modify a file by mistake. • The user accesses the wrong system due to similarity in name/IP. • The user is accessing a NAS container, which was made a replication target without his knowledge.
Workaround	In order to write to this volume, replication must be detached first. Refer the user to the correct location.

Troubleshooting NFS Issues

Cannot Mount NFS Export

Description	When attempting to mount an NFS export, the mount command fails due to various reasons such as: • Permission denied. • Server not responding due to port mapper failure - RPC timed out or input/output error. • Server not responding due to program not registered. • Access denied. • Not a directory.

Cause	• The client connects using NFS/UDP and there is a firewall in the way. • The client is not in the export list, the server could not recognize the client system through NIS, or the server does not accept the identity you provided. • The PowerVault NX3500 system is down or has internal file system problems. • The mount command got through to the port mapper, but the rpc.mountd NFS mount daemon was not registered. • Client system's IP address, IP range, domain name or netgroup is not in the export list for the volume it is trying to mount from the PowerVault NX3500 server. • Either the remote path or the local path is not a directory. • The client does not have root authority or is not a member of the system group. NFS mounts and unmounts are only allowed for root users and members of the system group.

Workaround	If the issue is due to NFS/UDP and firewall, check if the client mounts using UDP (this is usually the default) and there is a firewall in the path. If a firewall exists, add an appropriate exception to the firewall. If the issue is due to permissions: • Verify the path you provided is correct. • Check that you are trying to mount as root. • Check that the system's IP address, IP range, domain name or netgroup is in the exports list. If the server not responding due to a port mapper failure: • Check the PowerVault NX3500 status. • Check the network connection by trying to NFS mount from some other system. • Verify if other users experience the same problem. If the server is not responding due to the program not registered, check if the port mapper on your client is up. If the issue is due to access denied: • Get a list of the server exported file systems using the command: `showmount -e <NX3500 hostname>` • Check the system name or netgroup name is not in the user list for the file system. • Check the file systems related to the NFS through the PowerVault NX3500 user interface. If the issue is due to the directory, check the spelling in your command and try to run the mount command on both directories.

NFS Export Does Not Exist

Description Attempted to mount an export that does not exist.

Cause This failure is commonly caused by spelling mistakes on the client system or when accessing the wrong server.

Workaround

1. Check the available exports on the NAS; verify that all the required exports exist.
2. On the problematic client, verify that the relevant export is available to this client:

```
% showmount -e <Server name/IP>

Export list for <Server name/IP>:

/abc
10.10.10.0

/xyz
10.10.10.0
```

3. If the export is available, review the export name spelling in the relevant mount command on the client. It is recommended to copy paste the export name from the showmount output to the mount command.

NFS File Access Denied

Description This event is issued when an NFS user does not have enough permissions for the file on a NAS container.

Cause File ownership is UID/UNIX and the user is not privileged to access the file, or, file ownership is SID/ACL and after translation to UID/UNIX the permissions do not allow access to the file.

Workaround For native access (when CIFS user accesses SID/ACL file or NFS user accesses UID/UNIX file) understanding the missing permission is standard.

If the access is non-native, translation rules come to effect and it is recommended to contact Dell Technical Support.

NFS Insecure Access to Secure Export

Description	User tries to access a secure export from an insecure port.
Cause	Secure export requirement means that the accessing clients must use a well-known port (below 1024), which usually means that they must be root (uid=0) on the client.
Workaround	• Identify the relevant export and verify that it is set as secure (requires secure client port). • If the export must remain secure, see the NFS client documentation in order to issue the mount request from a well-known port (below 1024). • If a secure export is not required (e.g., the network is not public), ensure that the export is insecure and retry accessing it.

NFS Mount Fails Due to Export Options

Description	This event is issued when NFS mount fails due to export options.
Cause	The export list filters client access by IP, network or netgroup, and screens the accessing client.
Workaround	1 Verify the relevant export details. Write down all existing options so that you are able to revert to them. 2 Remove IP/client restrictions on the export and retry the mount. 3 If the mount succeeds, verify that the IP or domain is explicitly specified, or that it is part of the defined network or netgroups. Pay attention to pitfall scenarios, where the network netmask is not intuitive, for example, 192.175.255.254 is part of 192.168.0.0/12 but not of 192.168.0.0/16. 4 Once the mount succeeds, adjust the original options accordingly.

NFS Mount Fails Due to Netgroup Failure

Description

This event is issued when client fails to mount an NFS export because the required netgroup information cannot be attained.

Cause

This error is usually the outcome of a communication error between the NAS system and the NIS/LDAP server. It can be a result of network issue, directory server overload, or a software malfunction.

Workaround

Repeat the below process for each configured NIS server, each time leaving just a single NIS used, starting with the problematic NIS server.

1. Inspect the NIS/LDAP server logs and see if the reason for the error is reported in the logs.
2. Network test:
   - a Try pinging the NAS from a client located in the same subnet as the NIS/LDAP server.
   - b Try pinging the NIS/LDAP server from a client located in the same subnet as the NAS.

   If a packet loss is evident on one of the above, resolve the network issues in the environment.
3. Using a Linux client located in the same subnet as the NAS and configured to use the same directory server, query the netgroup details from the NIS/LDAP server using the relevant commands. Ensure that the reply is received in a timely manner (up to 3 seconds).

You can temporarily workaround the problem by removing the netgroup restriction on the export and/or by defining an alternative directory server.

Identify the relevant export and the options defined for it, while focusing on the netgroup definition. Document the used netgroup in order to restore it once the issue is solved and remove the netgroup limitation.

NFS Mount Path Does Not Exist

Description	Client tries to mount an unexisting mount path on a NAS container.
Cause	This error usually occurs in one of the following scenarios: • When accessing a system which is being restored from backup or remote replication. The full directory structure is available only when the restore is complete. • When a client with an authorization to access a higher directory in the same path deletes or alters a directory which is being mounted by another client. • When multiple users are accessing the same data set, it is recommended to apply a strict permission scheme to avoid this scenario.
Workaround	1 If the NAS system is being restored, communicate the current status to the client and instruct the client to wait for the restore process to complete. 2 In the other case, there are three options: a Restore the problematic path from a backup. b Manually create the missing directories to enable the mount. Clients receive errors when trying to access existing data in a deleted path. c Remove the export and communicate this to the client. 3 List all available exports on the NAS and identify the problematic export. It should have an indication that it is not accessible. 4 Delete the export or create the directory where the export points to.

NFS Owner Restricted Operation

Description	NFS client is not permitted to perform the requested action to the specific file.
Cause	NFS user attempted a `chmod` or `chgrp` operation while not being the owner of the file.
Workaround	This is a minor, user-level issue. Frequent events of this type may indicate a malicious attempt to access restricted data.

NFS Write to Read-Only Export

Description	NFS client tries to perform modifications on a read-only export.
Cause	An NFS export can be defined as a read-only export. A client accessing a read-only export cannot perform write operations or modify included files.
Workaround	This event, by itself, does not require any administrative intervention.

NFS Write to Read-Only Volume

Description	An NFS user tries to modify a file on a read-only volume.
Cause	A NAS volume becomes read-only when it is set as the target in a replication relation. Modifying a read-only volume is inhibited, until the replication relation is removed and the volume returns to a simple, normal state.
Workaround	Inform the user(s) of the state of the NAS volume.

NFS Write to Snapshot

Description	An NFS user tries to modify a file located in a snapshot.
Cause	NAS volume snapshots cannot be modified by design.
Workaround	Snapshot data cannot be modified. A snapshot is an exact representation of the NAS volume data at the time of its creation.

NFS Access Denied to a File or Directory

Description	User cannot access the NFS file or directory despite the fact that the user belongs to the group owning the NFS object and the group members are permitted to perform the operation.
Cause	NFS servers (versions 2 and 3) use the Remote Procedure Call (RPC) protocol for authentication of NFS clients. Most RPC clients have a limitation, by design, of up to 16 groups passed to the NFS server. If a user belongs to more than 16 UNIX groups, as supported by some UNIX flavors, some of the groups are not passed and are not checked by the NFS server and thus the user's access may be denied.

Workaround	A possible way to verify this problem is to use newgrp to temporarily change the primary group of the user and thus ensure it is passed to the server. The simple workaround, although not always feasible, is to remove the user from unnecessary groups, leaving only 16 groups or less.

Troubleshooting Replication Issues

Replication Configuration Error

Description	Replication between the source and destination NAS volumes fails because the source and destination systems' topologies are incompatible.
Cause	The source and destination systems are incompatible for replication purposes.
Workaround	Upgrade the PowerVault NX3500 which is down.

Replication Destination Cluster is Busy

Description	Replication between the source NAS volume and the destination NAS volume fails because the destination cluster is not available to serve the required replication.
Cause	Replication task fails because the destination cluster is not available to serve the required replication.
Workaround	Administrators must verify the replication status on destination system.

Replication Destination FS is Busy

Description	Replication between the source NAS volume and the destination NAS volume fails because the destination cluster file system is temporarily unavailable to serve the required replication.
Cause	Replication task fails because the destination cluster is temporarily unavailable to serve the required replication.
Workaround	The replication continues automatically when the file system releases part of the resources. Administrators should verify that the replication continues automatically after a period of time (an hour).

Replication Destination is Down

Description	Replication between the NAS source volume and the NAS destination volume fails because the destination NAS volume is down.
Cause	Replication task fails since the file system of the destination NAS volume is down.
Workaround	Administrators should check if the file system is down in the destination system using the monitoring section of the NAS Manager. If the PowerVault NX3500 file system is not responding, administrators should start the system on the destination cluster. The replication continues automatically after the file system starts.

Replication Destination is Not Optimal

Description	Replication between the NAS source volume and the NAS destination volume fails because the destination NAS volume is not optimal.
Cause	Replication fails because file system of the destination NAS volume is not optimal.
Workaround	The administrators should check the system status of destination system using the monitoring section of the NAS Manager to understand why the file system is not optimal. The replication continues automatically after the file system recovers.

Replication Destination Volume is Busy Reclaiming Space

Description	Replication between the NAS source volume and the NAS destination volume fails because the destination NAS volume is busy freeing up space.
Cause	Replication task fails because the destination NAS volume is busy freeing up space.
Workaround	The replication continues automatically when the space is available. The administrators should verify that the replication automatically continues after a period of time (an hour).

Replication Destination Volume is Detached

Description	Replication between the NAS source volume and the NAS destination volume fails because the NAS destination volume is detached from the NAS source volume.
Cause	Replication task fails because the destination NAS volume was previously detached from the source NAS volume.
Workaround	The administrators should perform the detach action on the NAS source volume. If required, reattach both NAS volumes in a replication relation.

Replication Disconnection

Description	Replication between the NAS source volume and the NAS destination volume fails because the connection between source and destination systems is lost.
Cause	Network infrastructure disconnection between the source and the destination.
Workaround	The administrator should check if the replication is automatically restored. If the replication is not automatically restored, check the network communication between the source cluster and the destination cluster. Network communication can be checked by using a third party system in the same subnet that can ping both the source and destination clusters.

Replication Incompatible Versions

Description	Replication between the NAS source volume and the NAS destination volume fails because the system version of the source NAS cluster is higher than the system version of the destination cluster.
Cause	Replication task fails since the system version of the NAS source volume is higher than the system version of the destination cluster.
Workaround	Administrators should upgrade the system version of the destination cluster to match the system version of the source cluster.

Replication Internal Error

Description	Replication between the source and the destination NAS volumes fails due to an internal error.
Workaround	Contact Dell to resolve this issue.

Replication Jumbo Frames Blocked

Description	Replication between the NAS source volume and NAS destination volume fails because the jumbo frames are blocked over the network.
Cause	Replication task fails because jumbo frames are blocked over the network.
Workaround	The administrator should verify that the network configuration between the source cluster and the destination cluster has enabled transferring jumbo frames across the switches or routers.

Replication Destination Does Not Have Enough Space

Description	Replication between NAS source volume and NAS destination volume fails because there is not enough space in the destination NAS volume.
Cause	Replication task fails because there is not enough space in the destination NAS volume.
Workaround	Increase the space of the destination NAS volume.

Replication Source is Busy

Description	Replication between the NAS source volume and the NAS destination volume fails because the file system of the source NAS volume is busy replicating other NAS volumes.
Cause	Replication task fails because the file system of the source NAS volume is busy replicating other NAS volumes.
Workaround	The replication continues automatically when the file system releases part of the resources. The administrators should verify that the replication is automatically continues after a period of time (an hour).

Replication Source is Down

Description	Replication between the NAS source volume and the NAS destination volume fails because the file system of source NAS volume is down.
Cause	The file system of the source NAS volume is down.
Workaround	Administrators should check if the PowerVault NX3500 is down in the source system, by checking the monitoring section of the NAS Manager. If the PowerVault NX3500 is down, the administrators should start the system on the source cluster. The replication continues automatically when the file system starts.

Replication Source is Not Optimal

Description	Replication between the source and the destination NAS volumes fails because the file system of the source NAS volume is not optimal.
Cause	Replication fails since the file system of the source is not optimal.
Workaround	The administrator should check the system status of source system, using the monitoring section in the NAS Manager, to understand why the file system is not optimal.

Replication Source Volume is Busy Reclaiming Space

Description	Replication between the NAS source volume and the NAS destination volume fails because the source NAS volume is busy reclaiming space.
Cause	Replication task failed since the source NAS volume is busy reclaiming space.
Workaround	The replication continues automatically when space is available. Administrators should verify that the replication is automatically continues after a period of time (an hour).

Troubleshooting Active Directory Issues

Group Quota For an Active Directory User Does Not Work

Description	Group quota is defined for an Active Directory group; however, when a group member consumes space, the actual usage of the group does not grow and the group limitation is not enforced.
Cause	The PowerVault NX3500 quota enforcement is performed based on the UID and GID of the file (UNIX) or the SID and the GSID of the primary group of the user (NTFS), if defined. For Active Directory users, the Primary Group setting is not mandatory, and if not defined, the used space is not accounted to any group. For group quota to be effective with Active Directory users, their primary group must be assigned.
Workaround	To setup the primary group for an Active Directory user: 1 Open the Active Directory management. 2 Right-click on the desired user. 3 Select the **Member Of** tab. 4 The group you need should be listed. Click the group and then click the **Set Primary Group** button. Now quotas will take effect for the user's group.

Active Directory Authentication

Description	A valid Active Directory user fails to authenticate.
Cause	Probable causes may be: • The user is trying to authenticate using a wrong password. • The user is locked or disabled in Active Directory. • Active Directory domain controllers are offline or unreachable. • System clock and Active Directory clock are out of sync.
Workaround	1 Check the PowerVault NX3500 system event log in the NAS Manager for errors. 2 Verify that the user is not disabled or locked in Active Directory. 3 Verify that domain controllers are online and reachable using the network. 4 Kerberos requires client/server clocks to be in sync. Verify the system time is in sync with the domain controller time and if required, configure the NTP setting of the system.

Troubleshooting Active Directory Configuration

Description	Unable to add Active Directory users and groups to CIFS shares.
Cause	Probable causes may be: • Unable to ping the domain using FQDN. • DNS may not be configured. • NTP may not be configured.

Workaround	When configuring the system to connect to an Active Directory domain: 1 Ensure that you use FQDN and not the NETBIOS name of the domain or IP address of the domain controller. 2 Ensure that the user has permissions to add systems to the domain. 3 Use the correct password. 4 See **DNS Configuration** tab and enter the correct information. 5 Configure the NTP information and ensure that the system time matches the domain time. 6 If multiple NAS systems are used, ensure that you set different NETBIOS names. The system defaults to CIFS Storage as the name. 7 Ensure that you select **Authenticate users' identity via Active Directory and local users database**.

Troubleshooting BPS Issues

Backup Power Supply LED Displays a Solid Amber Light

Description	BPS LED is solid amber, with or without an audible alarm.
Cause	Probable causes may be: • The BPS is running on battery power with the battery charge below 30% (low battery condition). • Active alarm on the BPS.
Workaround	If the BPS LED is solid amber and no audible alarm: 1 Verify that BPS AC in cable is plugged in, and that utility power is present. 2 Check the NAS appliance event log for messages if the BPS is on battery power. 3 Restore utility power. For more information about the workaround, see "BPS Alarms" on page 209.

Backup Power Supply LED Flashes Green and Amber

Description	BPS LED displays green and amber, with or without an audible alarm.
Cause	Probable causes may be: • Flash upgrade is in progress • BPS is in bootloader mode
Workaround	If a flash upgrade is in progress, (slow alternating pattern between green and amber) wait for about 10 minutes—After a service pack upgrade procedure or a BPS module replacement procedure, a BPS firmware upgrade may be required and is performed automatically by the NAS appliance after the service pack upgrade reboot. **NOTE:** During a firmware upgrade, do not disconnect the ACin cable or USB cable on the BPS module. If the BPS LED is in bootloader mode (fast alternating pattern between green and amber): 1 Verify that ACin cable is connected to the BPS. 2 Verify that USB cable between the BPS module and NAS appliance controller is connected. 3 Reboot the NAS appliance controller connected to the BPS.

Backup Power Supply Displays a Blinking Amber LED

Description	BPS LED is blinking amber.
Cause	A blinking amber LED indicates that the BPS is on battery power due to loss of utility power, but not yet in low battery mode (when charge is below 30%).
Workaround	• Locate the BPS that has a blinking amber LED in the rack. Check the back of the BPS and verify that corresponding BPS module has the ACin cable plugged in and other end of the cable is plugged into the utility power. • Verify the utility power is present.

BPS LED Is Off

Description	BPS LED is off and does not turn on when the power button is pressed.
Cause	This issue occurs either because the battery is not installed correctly, there is no power to the BPS, or there is a hardware failure.
Workaround	1 Remove the BPS module bezel. Ensure that the battery is installed properly and turn on the BPS by pressing the BPS power button. 2 Verify if the BPS cables are connected properly and that the utility power matches the BPS specifications. LV models require a 120 V input and HV models require a 208 V input. Turn on BPS by pressing the BPS power button. 3 If none of the above actions resolves the issue, contact Dell technical support.

Troubleshooting NAS File Access and Permissions Issues

Cannot Change the Ownership of a File or a Folder

Description	Every file on the NAS system is owned by either a UNIX or NTFS user. Inability to change ownership is treated differently, depending on whether the access is native or non-native.
Cause	The user is not authorized to perform the ownership change.
Workaround	An authorized user should perform this action.

Cannot Modify NAS Files

Description	A user or an application cannot modify a file.
Cause	• The client cannot modify a file due to lack of permissions on the file. • The NAS volume has reached full capacity and the file system denies any write requests, including overwrites. • The NAS volume is a target in a replication relationship and is read only.
Workaround	1 If the problem appears only on some files, this is a permission issue. Verify that the user account has modify permissions on the file or use a different user account. 2 If the problem is related to a specific NAS volume: a Verify there is enough free space on the NAS volume or expand it. b Verify that the accessed NAS volume is not a target of a replication.

Mixed File Ownership Denied

Description	Both file owner and group owner must be from the same identity type (UNIX vs NTFS). An attempt to set different identity types was detected.
Cause	It is impossible to change only the file owner id to UID if the original file ownership is SID/GSID.
Workaround	To change the file ownership to UNIX style ownership, set UID and GID at same time.

Problematic SMB Access From a Linux Client

Description	A Linux/UNIX client is trying to mount a PowerVault NX3500 share using SMB (using /etc/fstab or directly using smbmount).
	A Linux/UNIX client is trying to access the file system using the smbclient command, such as:
	`smbclient //<nas>/<share> -U`
	`user%password -c ls`

Workaround	It is recommended that you use the NFS protocol interfaces to access the PowerVault NX3500 FluidFS systems from Linux/UNIX clients. To workaround this issue: 1 Ensure that your admin creates NFS exports to same locations that you use to access using CIFS and connect to them using mount command from Linux/UNIX clients. 2 Use NFS based interfaces to access the PowerVault NX3500. For example, from the NAGIOS Linux management system, use the `/check_disk` command instead of the `/check_disk_smb` command.

Strange UID and GID Numbers on Dell NAS System Files

Description	New files created from ubuntu 7.*x* clients get the UID and GID of 4294967294 (nfsnone).
Cause	By default, ubuntu 7.*x* nfs clients do not specify rpc credentials on their nfs calls. As a result, files created from these clients, by any user, are owned by 4294967294 (nfsnone) UID and GID.
Workaround	To force UNIX credentials on nfs calls, add the **sec=sys** option to the PowerVault NX3500 mounts in the ubuntu fstab file.

Troubleshooting Networking Issues

Name Server Unresponsive

Description	All NIS, LDAP, or DNS servers are unreachable or not responding.
Workaround	For each server: 1 Ping the server from a client on PowerVault NX3500 subnet and verify it responds. 2 Issue a request to the server from a client on the PowerVault NX3500 subnet and verify it responds. 3 Check server logs to see what causes the server not to respond to requests.

Specific Subnet Clients Cannot Access the PowerVault NX3500 System

Description	Users (new or old), accessing from specific network(s), cannot access the PowerVault NX3500 system.
Cause	This issue is due to a conflict between the users' subnet addresses and the NAS system internal network's address. The NAS system routes the response packets to the wrong network.
Workaround	1 Check the internal network addresses of the NAS system and verify if there is a conflict with the problematic client network addresses. 2 If a conflict exists, manually change the conflicting NAS internal network address using either the NAS Manager or CLI.

Troubleshooting DNS Configurations

Description	Unable to connect to the PowerVault NX3500 using the system name and/or unable to resolve host names.
Cause	Probable causes may be: • Unable to ping system using Fully Qualified Domain Name (FQDN). • Unable to connect to the NAS Manager using system name.
Workaround	1 Verify that the client IP information is set correctly. 2 Verify that the PowerVault NX3500 controller is configured to the correct DNS server. 3 Contact DNS server administrator to verify the DNS record creation.

Determining the IQN of the PowerVault NX3500 Controllers Using CLI

Description	Determining the IQN of the PowerVault NX3500 controllers using CLI.
Workaround	Using an ssh client and the NAS Management VIP, log in to the PowerVault NX3500 solution CLI as an admin. From the command line type the following command: `system maintenance luns iscsi-configuration view`

Troubleshooting RX and TX Pause Warning Messages

Description	The following warning messages may be displayed when the NAS Manager reports connectivity in a Not Optimal state:
	`Rx_pause for eth(x) on node 1 is off.`
	`Tx_pause for eth(x) on node 1 is off.`

Cause	Flow control is not enabled on the switch(es) connected to a PowerVault NX3500 controller.
Workaround	See the switch vendor's documentation to enable flow control on the switch(es).

Troubleshooting NAS Manager Issues

NAS Dashboard is Delayed

Description	NAS dashboard metrics is delayed and does not show the updated values as soon as it updated.
Cause	The NAS Manager view is refreshed every 40 seconds but the information regarding specific metrics is collected in different intervals, due to which there is no correlation between screen refresh to actual metrics refresh.
Workaround	Use the process in FluidFS that collects information regarding various matrices in the system. • Status fields (overall state, service status, servers status)—Information is been collected every 40 seconds. • Capacity—Information is collected every 1800 seconds. • Current performance (NFS, CIFS, Replication, NDMP, Network)—Information is collected every 40 seconds. • Recent performance (the graph)—Information is collected every 60 seconds. • Load balancing (CPU, number of connections)—Information is collected every 40 seconds.

NAS System Time is Wrong

Description	Scheduled tasks are running in wrong times. The date/time of event log messages is wrong.
Cause	• The time on the NAS system is incorrect. • No NTP server is defined for the NAS system. • The NTP server servicing the PowerVault NX3500 is either down or has stopped providing NTP services. • There are network problems communicating with the NTP server.

Workaround	1 Identify the NAS NTP server from the **System Configuration/ Time Configuration** page. Record the host name(s) or IP address(es) for further reference. 2 If no NTP server is defined, define one. It is recommended synchronizing the NAS system clock with the NTP server used by the Active Directory Domain Controller (ADDC). This avoids time difference issues and possible authentication problems. In many cases the ADDC is also the NTP server. 3 Verify that the NTP server is up and provides the NTP service. 4 Check the network path between the NAS system and the NTP server, using ping, for example. Verify that the response time is in the millisecond range.

Cannot Connect to the NAS Manager

Description	Unable to connect to the NAS Manager.
Cause	Probable causes may be: • The user is attempting to connect using an incorrect IP address or is using the wrong system name. • The client computer's IP information is configured incorrectly. • The user is using an incorrect user name or password. • The user's browser properties are preventing the connection.
Workaround	1 Verify that the client's IP information is set correctly. 2 Verify that the DNS information is configured correctly. 3 Verify the user name and password. 4 Verify the proxy information in the browser's settings. 5 If you are using Microsoft Windows Server 2008, disable IE ESC.

Blank Login Screen

Description	Unable to connect to the NAS Manager and the login screen is blank.
Cause	Probable causes may be: • Java script is disabled. • IE SEC is enabled.
Workaround	• If Java script is disabled, enable Java script. For information about enabling Java script, see the browser's help. • If IE SEC is enabled, disable it.

Troubleshooting Backup Issues

Troubleshooting Snapshots

Description	Taking and deleting snapshots fail.
Cause	Probable causes may be: • There are many client I/O requests waiting to be serviced, including a request to remove a large directory. • There are many snapshot creation/deletion requests being currently processed. • Another snapshot request for the volume is currently being executed. • The total number of snapshots reached the system limit.

Workaround	• For a manual request failure, retry taking or deleting the snapshot after a minute or two. • If the request originated from the snapshot scheduler, wait another cycle or two. If the failure persists, try taking or deleting the snapshot manually on the same volume. • Check the dashboard if the system is under heavy workload. If the system is under a heavy workload, wait until the workload decreases and reissue the snapshot request. • Check the snapshot schedule. A very dense snapshot schedule has a negative impact on the overall performance of the system. The accumulated snapshot rate should not exceed 20 snapshots per hour per system. • Check the total number of snapshots in the system. If the number is in the thousands, delete a few snapshots and retry.

Troubleshooting an NDMP Internal Error

Description

Backup or restore fails with an internal error.

Cause

NDMP internal errors are indicators of a file system not being accessible or a NAS volume not being available.

Workaround

If the backup application cannot connect to a NAS appliance:

1. Log in to the NAS Manager or open a remote terminal to the appliance.
2. On the NAS Manager, go to **Data Protection→NDMP→NDMP Configuration** page. In NAS CLI, go to **Data Protection→NDMP→Configuration** menu.
3. Verify that NDMP is enabled. If NDMP is enabled, go to step 5.
   - On the NAS Manager, the **Enabled** check box should be checked.
   - In the NAS CLI, type `view` and ensure that **State** is set to **Enabled**.
4. If NDMP is not enabled, enable it. For more information, see "Backing Up and Restoring Data" on page 114.
5. Verify that backup application IP address is configured in NDMP.
   - On the NAS Manager, the DMA server list should include the IP address of the backup application.
   - In the NAS CLI, type `view` and ensure that the **DMA Servers** list includes the IP address of the DMA application trying to access the NAS appliance.

If the backup appliance can connect to a NAS appliance but cannot log in, use backup_user as the user name for the NDMP client, while setting up the NDMP backup/restore in your backup application. The default password for NDMP client is **Stor@ge!**

	To change the password: 1 Log in to the NAS Manager or open remote terminal to the appliance. 2 In the NAS Manager, go to **Data Protection→ NDMP→ NDMP Configuration** page. In NAS CLI, go to **Data Protection→ NDMP→ Configuration** menu. 3 In the NAS Manager, click **Change Password**. In the NAS CLI, run the `set -Password "pwd"` command. If the backup application can log into the NAS appliance, but if no volumes are available for backup, verify that the NAS appliance has NAS volumes created on it.

Troubleshooting System Issues

Troubleshooting System Shutdown

Description	During a system shutdown using the NAS Manager, the system does not stop and the controllers do not shutdown after 20 minutes.
Cause	The system shutdown procedure is comprised of two separate processes: • Stopping the file system • Powering down the PowerVault NX3500 controllers The file system may take a long time to clean the cache to the storage either due to lot of data, or due to an intermittent connection to the storage. During the powering down stage, the issue could be due to the OS kernel hanging on the controller or failing to sync its state to the local drive.
Workaround	If the file system has stopped and if one of the controllers are still up, you can physically power down the controller using the power button. If file system has not stopped, you must let it continue working. The file system reaches a 10 minute timeout, flushes its cache to the local controllers, and continues the shutdown process.

NAS Container Security Violation

Description	NAS container security violation.
Cause	Selecting security style for a NAS container dictates the dominant protocol to be used to set permissions on files in this volume. NFS for UNIX security style volumes and CIFS for NTFS security style volumes. Consequently, this makes some operations invalid: • Setting UNIX permissions for a file in an NTFS Security style container. • Setting UID/GID ownership for a file in an NTFS Security style container. • Setting ACL for a file in a UNIX Security style container. • Changing read-only flag for a file in a UNIX Security style container. • Setting SID/GSID ownership for a file on UNIX Security style container. The NAS container security style should reflect the main protocol used to access its files.
Workaround	If a user frequently needs to perform a cross-protocol security related activity, split the data into separate NAS containers based on the main access protocol.

Multiple Errors Received During File System Format

Description	You receive multiple errors during a file system format.
Cause	Probable causes may be: • Wrong SAN IPs are used in the PowerVault NAS Configuration Utility (NASCU). • Wrong IQNs used while defining hosts in the MDSM. • Uneven number of LUNs are mapped to the host group. • LUN size is below the minimum required size. • Less than minimum number of required LUNs.

Workaround

If wrong SAN IPs are used while running the PowerVault NASCU:

1. Verify that the MD discovery IP used while running the PowerVault NASCU is on the same subnet as one of the two SAN IPs configured on your controllers.
2. To verify MD discovery IP, log in to your NAS Manger IP using CLI and run the following command:

   ```
   Kjd
   ```

   This command shows the MD discovery IP.
3. If the IP is not in the same subnet as the IPs configured for your SAN, change the MD discovery IP to one of the subnets defined on your controller's SAN A and B.

If wrong IQNs are used while defining hosts in MDSM, verify that the IQNs displayed in MDSM match the controller IQNs. To verify the controller IQNs:

1. Compare if the iqns displayed in MDSM are the same as the ones under the **Mappings** tab in the hosts section in the NAS Manager.
2. If there is a mismatch, correct the IQNs used for the hosts in MDSM and try formatting the system. The LUNs must be discovered and formatted.

If the issue is due to uneven number of LUNs:

1. If an error is encountered, verify that even number of LUNs are mapped to the host group. An odd number of LUNs is not supported. LUNs have to grow in pairs starting from 2 to 16.
2. If uneven LUNs are used, correct the count by adding or removing a LUN.
3. Try to format the system.

If the LUN size is below minimum requirements:

1. Verify that the LUNs are larger than the minimum required size of 125 GB.
2. If the LUNs are less than 125 GB, change LUN size to meet or exceed the minimum required size.
3. Try to format the system.

	If the LUN count is below the minimum requirements: 1 Verify that more than one LUN is mapped to the host group. The minimum number of LUNs required is 2. 2 If the number of LUNs is less than 2, add LUNs to meet the required minimum LUN count of 2. 3 Try to format the system.

Associating LUN Names to Virtual Disks

Description	Determining which LUNs in the PowerVault NAS Manager are virtual disks in the Modular Disk Storage Manager.
Workaround	Open the NAS Manager web interface and go to **System Management→ Maintenance→ Add Luns**. This page displays all LUNs that the PowerVault NX3500 cluster has access to (assigned to the PowerVault NX3500 host group). Each LUN can be identified using its world-wide name. In the NAS Manager web interface, the LUN's world-wide name is preceded by a prefix. Open MDSM and go to the **Logical** tab and click **Virtual Disk**. The virtual disk world-wide identifier is displayed in the **Properties** pane. This workaround enables you determine which virtual disks are assigned to the NAS file system.

Identifying Controllers

Description	Identifying PowerVault NX3500 controllers.
Workaround	To identify a controller, use the LCD located on the front panel of the PowerVault NX3500 controller. The LCD displays systemname.controller#. For example, *NX3500.Controller0*

Troubleshooting NAS Configuration Utility Issues

Error Received While Running the PowerVault NASCU

Description	Error occurred while running the PowerVault NX3500 NAS Configuration Utility.
Cause	The error could be caused by either hardware setup, network switch configuration, or cluster system configurations.
Workaround	If the discovery page displays a connection failure: 1 Check the MAC addresses for cluster controllers. Embedded NIC 1 MAC addresses can be found on system identification panel (slide-out tag) located below the front bezel of NAS controllers. 2 Check if IPv6 is enabled on the management station where the NAS Configuration Utility is running. 3 Check if system is already in service mode. If the system is in service mode, the NAS Configuration Utility should block users from any further action and guide them through exiting the utility. If the failure is in the configuration NAS cluster page: 1 Capture the failure message screenshot from the NAS Configuration Utility window during clusterization. 2 Collect the cluster configuration file, the NAS Configuration Utility log file, and the result file from the installation directory and zip the config folder from the installation directory. 3 The NAS Configuration Utility should lead users to the restore window, where nodes are restored to standby mode. 4 Look for the failure messages in captured screen shot and find out the potential cause of the failure. Correct those failures and reconfigure the system using the NAS Configuration Utility. 5 If the failure still persists, collect all the files in a bundle package and contact Dell support.

Cannot Launch PowerVault NX3500 NAS Configuration Utility

Description	Cannot launch PowerVault NX3500 NAS Configuration Utility.
Cause	Probable causes maybe: • NAS Configuration Utility installer failed to install. • JAVA runtime environment is not properly installed.
Workaround	Perform the following: • Determine if the NAS Configuration Utility installer completed successfully. • Check to see if the minimum of JRE1.4x is installed successfully. – On Microsoft Windows, run java -version from command console to display a valid JRE version. – On Linux, run java --version from terminal console to display a valid JRE version.

11

Command Line Interface

Overview

The PowerVault NX3500 Command Line Interface (CLI) provides a convenient way to manage the PowerVault NX3500 system. It can be used to configure subsystems, manage administrative users, enable licensed features, and to monitor the system. The CLI contains a set of commands to view, edit, add, delete, enable, disable, and set PowerVault NX3500 entities, such as exports, shares, volumes, and accounts.

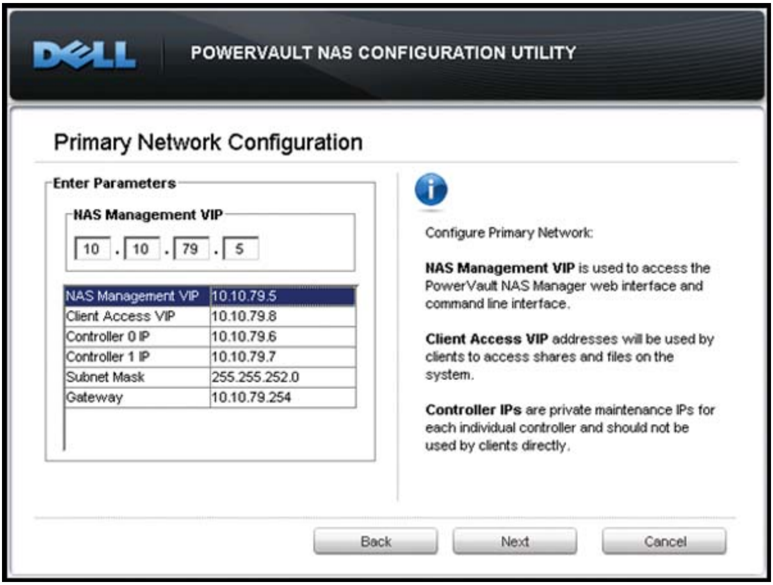
From the CLI, you can enter a specific menu and then execute its commands, as required. The following commands are available throughout the system:

- **help**: lists the currently available menus or commands. At any moment while using the CLI, you can either type "help" or type "?" to see the available options/menus.
- **back**: moves back one level in the menus hierarchy.
- **main**: returns to the main menu.
- **exit**: exits the PowerVault NX3500 CLI.

Accessing the CLI

To access the CLI from an administrator workstation, use an SSH client, and connect to the NAS Management VIP address you specified during cluster setup.

Figure 11-1. Accessing CLI via the NAS Management VIP



Primary Network Configuration

Enter Parameters

NAS Management VIP: 10 . 10 . 79 . 5

NAS Management VIP	10.10.79.5
Client Access VIP	10.10.79.8
Controller 0 IP	10.10.79.6
Controller 1 IP	10.10.79.7
Subnet Mask	255.255.252.0
Gateway	10.10.79.254

Configure Primary Network:

NAS Management VIP is used to access the PowerVault NAS Manager web interface and command line interface.

Client Access VIP addresses will be used by clients to access shares and files on the system.

Controller IPs are private maintenance IPs for each individual controller and should not be used by clients directly.

In a Linux prompt, type: *ssh admin@<ipaddress>*.

A **Welcome** window is displayed, listing the installed software version and the available commands in the top level menu.

NOTE: Tab completion is available: type the first few characters of the command or menu name and press the **Tab** key. The name is completed to the longest unambiguous sub-string. Press the **Tab** key again to see the available commands beginning with the given string.

For example, to access a system that was defined with a NAS Management VIP of 10.10.1.200:

```
# ssh admin@10.10.1.200
```

```
The authenticity of host '10.10.1.200
(10.10.1.200)’ can't be established.

RSA key fingerprint is:

1b:13:7c:9d:12:e2:74:69:4e:8c:93:75:1a:93:94:b5.

Are you sure you want to continue connecting
(yes/no)? yes

Failed to add the host to the list of known hosts
(/users/john/.ssh/known_hosts).

admin@172.41.2.202's password: Stor@ge!

Last login: Sun Dec 26 03:04:51 from 172.41.200.12

Welcome to "NX3500-sup3" (1.0.326)

Installed on Thu Dec 23 07:38:45 IST 2010

Hello admin, welcome to the NAS Manager command
line interface (version 1.0.366)!
```

CLI Menu Options

The following menus and menu options are available with the PowerVault NX3500.

Table 11-1. CLI Menu Options

Menu	Options
data-protection	The data-protection menu lets you set the backup and snapshot configuration to protect your data. It includes the following menu items: **replication**: *lets you utilize an additional storage repository.* **snapshots**: *lets you freeze and restore the files to a previous state.* **anti-virus**: *lets you manage anti-virus hosts.* **ndmp**: *lets you configure backup service and watch active-jobs.*

Table 11-1. CLI Menu Options *(continued)*

Menu	Options
system	The system menu lets you configure various system-wide properties. It includes the following menu items: **general**: *lets you view general system information, configure administrator users and manage system licensing.* **time-configuration**: *lets you configure the time zone and NTP server.* **monitoring-configuration**: *lets you configure e-mail support, syslog and SNMP.* **maintenance**: *lets you stop or start the system, save the system configuration, attach and detach controllers and do iSCSI luns discovery.* **protocols**: *lets you configure the file system protocols.* **authentication**: *lets you select the required NIS and LDAP settings, configure the Active Directory, manage users and groups, and configure user mappings.* **networking**: *lets you configure a variety of network settings.*
access	The access menu lets you define quotas, file system options, and configure NAS volumes. It includes the following menu items: **quota**: *lets you set default and individual quotas for users and groups in volumes.* **cifs-shares**: *lets you set the CIFS shares options.* **cifs-home-shares**: *lets you set the CIFS home shares options.* **nfs-exports**: *lets you set the NFS export options.* **nas-volumes**: *lets you configure NAS volumes.*
events	The **events** menu lets you monitor your PowerVault NX3500 system by detecting normal and abnormal events.

Table 11-1. CLI Menu Options *(continued)*

Menu	Options
monitor	The monitor menu lets you monitor your PowerVault NX3500 system. It includes the following menu items: **quota**: l*ets you view the system quota usage.* **traffic-statistics**: *lets you view system various statistics, for example, CIFS/NFS IO read/write per second.* **replication**: *lets you view the status of previous and current remote replication tasks.* **connections**: *lets you view the connections to the system via CIFS protocol.* **export-data**: *lets you create CSV (comma separated values) reports for over-time analysis of performance, load balancing and capacity.* **system-validation**: *lets you validate the system configuration functionality wise.* **hardware-components**: *lets you view the status of the controllers, BPS devices and storage subsystems.*
diags	The **diag** menu lets you run general, network, protocols and performance diagnostics on the system.
service-pack	The service pack menu keeps your PowerVault NX3500 system up to date.

12

Internationalization

Overview

The PowerVault NX3500 system provides full Unicode support allowing support of various languages concurrently. Directories and file names are maintained and managed internally in Unicode format (UTF-8).

Regardless of the encoding type used by the client who creates a file, the PowerVault NX3500 system stores its file name or directory name in Unicode format. When a non-Unicode client creates a file on a share, mount or volume, the file is immediately converted to the appropriate Unicode representation by the PowerVault NX3500 system.

Unicode Client Support Overview

Unicode clients may access Unicode directories and files natively, while other non-Unicode clients (such as Windows 98, Windows ME, Mac OS 9.x clients) may gain access to the file system due to the PowerVault NX3500 systems' ability to provide code page conversions of file names, directories, shares and volumes, according to the code page used by the client.

Native Unicode clients include the following:

- Microsoft Windows 7/Server 2008 R2
- Microsoft Windows Vista/Server 2008
- Microsoft Windows XP
- Microsoft Windows 2000/2003
- Microsoft Windows NT
- UNIX-based clients

NFS Clients

NFS clients may configure a different code page for different shares, while supporting concurrently non-Unicode clients that use different languages.

For further information on configuring code pages see "Managing NFS Exports" on page 97.

CIFS Clients

CIFS users may configure a code page to be used for all non-Unicode Windows and DOS clients.

NOTE: The web Interface provides full Unicode support. To display and use Unicode data using the CLI, a UTF-8 XTERM should be used.

Unicode Configuration Parameters

The following configuration parameters may contain Unicode characters.

Table 12-1. Unicode Configuration Parameters

Parameter	Unicode Character
CIFS	Server description
Home Shares	Directory name
SNMP	Contact Location
NFS Exports	Directory name
CIFS Shares	Name Directory Description Users Groups

Unicode Configuration Limitations

Following are the Unicode configuration limitations:

- File Size and Directory Name
- Clients Compatibility Problems
- Japanese Compatibility Issues

File Size and Directory Name

The size of the file and the directory names are limited to 255 bytes, which may be less than 255 characters when using Unicode, because each UTF-8 character occupies between one and six bytes.

Clients Compatibility Problems

In some cases different vendors use different UTF-8 encoding for the same code page entries. The result is either be that these characters are not displayed, or that these are substituted by other characters similar in shape.

Japanese Compatibility Issues

Administrators using the CLI are able to enter Japanese characters in configuration parameters only through the web interface, because XTERM applications such as KTERM does not enable you to use UTF-8 characters.

The following table details the Japanese incompatible characters.

Table 12-2. Japanese Incompatible Characters

Character	UNIX	Windows	Macintosh
WAVE DASH (~)	U+301C (WAVE DASH)	U+FF5E (FULLWIDTH TILDE)	U+301C (WAVE DASH)
DOUBLE VERTICAL LINE (||)	U+2016 (DOUBLE VERTICAL LINE)	U+2225 (PARALLEL TO)	U+2016 (DOUBLE VERTICAL LINE)
MINUS SIGN (-)	U+2212 (MINUS SIGN)	U+FF0D (FULLWIDTH HYPHEN MINUS)	U+2212 (MINUS SIGN)

Table 12-2. Japanese Incompatible Characters *(continued)*

OVERLINE (‾)	U+FFE3 (FULLWIDTH MICRON)	U+FFE3 (FULLWIDTH MICRON)	U+203E (OVERLINE)
CENT SIGN (¢)	U+00A2 (CENT SIGN)	U+FFE0 (FULLWIDTH CENT SIGN)	U+00A2 (CENT SIGN)
POUND SIGN (#)	U+00A3 (POUND SIGN)	U+FFE1 (FULLWIDTH POUND SIGN)	U+00A3(POUND SIGN)
NOT SIGN (¬)	U+00AC (NOT SIGN)	U+FFE2 (FULLWIDTH NOT SIGN)	U+00AC (NOT SIGN)

The PowerVault NX3500 provides a special code page for the CIFS service, to support portability between protocols. If you are working in a multi-protocol environment and wish to share files and directories between protocols, it is recommended to use this option.

When the CIFS service is configured to use UTF-8-JP for the internal encoding (UNIX code page), Windows incompatible encoding is mapped to the appropriate UNIX/ Mac O/S encoding on PowerVault NX3500. This ensures that in any case correct and incorrect characters are mapped correctly.

13

Frequently Asked Questions

NDMP

1 Is NDMP a High Availability (HA) protocol? What happens if a backup session is interrupted due to connection loss?

NDMP is not HA. A session that is interrupted is terminated.

2 How does NDMP work?

At the beginning of the NDMP session, a Fluid File System (FluidFS) snapshot is taken on the target NAS filesystem. This snapshot is then transferred over to the Data Management Application (DMA). At the end of the session the snapshot is deleted.

3 Are NDMP snapshots special?

No, they are regular one-time FluidFS snapshots.

4 Who provides load balancing?

NDMP has no load balancing built in. Single DMA backing up 10 volumes from single client VIP force all 10 sessions on the same node. Use DNS round-robin to provide load balancing, by specifying a DNS name of your NAS appliance in the DMA.

5 Why do I see ndmp_backup_xxxx_nodeX snapshot on my volume?

This is the snapshot taken by NDMP. After a successful backup session, this snapshot is deleted. If backup session is terminated with an error, the snapshot may be left in place, and can be safely deleted manually.

6 How many DMAs can run backup at any given time?

Up to 16 DMAs can be set up on PowerVault NX3500. There is no limit on the number of DMAs taking backup at any point in time.

7 Can I restore a single file?

Yes.

8 Can I restore old backup to another NAS appliance?

Yes.

9 Can I restore backup to another NDMP appliance?

Yes. The data from NDMP is sent in raw format, so the target appliance supports it.

10 Can I see which active backups are currently in progress?

Yes, using NAS CLI you can see the active backups currently in progress, run `data-protection ndmp active-jobs` list.

11 Can I use NDMP to backup a network drive I have mapped to my client?

No, you cannot use NDMP to backup a network drive.

Replication

1 How does replication work?

Replication utilizes FluidFS snapshot technology and other calculations to ensure the replicated virtual volume's data matches the source virtual volume data at the date and time a replication task was started. Only the blocks that have been modified since the last replication task are transferred over the client network.

2 How long does replication take?

This depends on the amount of data on the virtual volume and the amount of data that has changed since the last replication cycle. However, replication is a lower level task which receives priority over serving data. Typically, replication with little changes finishes in less than a minute.

3 Can I replicate a virtual volume to multiple virtual target volumes?

No, once a source volume has a replication policy with a target virtual volume, neither virtual volume can be used for replication (source or destination).

4 Why can I not write to the target virtual volume with NFS or CIFS?

Once a replication policy is set, the target virtual volume is read only. When the replication policy is detached, the target virtual volume will no longer be read only.

5 I am on the target system and I cannot trigger a replication for my destination virtual volume.

Replication operations must be performed on the source virtual volume.

6 Can I replicate to the same system?

Yes, you can replicate from one source virtual volume to a destination virtual volume on the same system.

7 Is bi-directional replication supported between two systems?

Yes, you can have a mix of target volumes and source volumes on replication partners.

8 Can I have multiple replication partner systems?

Yes, multiple replication partners are allowed; however, you cannot replicate one virtual source volume to multiple target volumes.

9 When I delete the replication policy, I am asked if I want to apply the source volume configuration to the target volume configuration. What does this mean?

This means that you have the option to transfer all virtual volume level properties (security style, quotas, NFS exports, CIFS shares, and so on) to the target volume. You may want to do this if this virtual volume will take the place of the source virtual volume and in other IT scenarios.

10 My client network slows down while replicating. Can I change the priority of replication against serving clients?

This is by design. Replication is a lower level process and takes priority over serving clients. Typically, replication finishes in under a minute.

11 Why can I not delete the replication policy from the target virtual volume?

This is by design. All configuration changes should be made on the source virtual volume. If the system in which the source volume resides cannot be reached (it is down, missing, and so on) you can delete the replication policy on the destination.

A

BPS Alarms

This chapter provides information about the external alarm conditions of the Dell backup power supply (BPS).

NOTE: The Dell BPS LED is solid amber with an audible alarm.

Table A-1. External Alarm Conditions

Alarm	Description	Audible	Corrective Action
Battery disconnected	Battery voltage is lower than the batteries disconnected level defined for this UPS. This may be due to a blown fuse, intermittent battery connection, or battery cable being disconnected. If EBMs are attached this alarm does not trigger unless the EBMs are also disconnected since they are paralleled with the battery bus.	Beeping	Reconnect the battery by following the steps in the *Getting Started Guide*.
Service battery	A faulted battery string has been detected and as a result the battery charger has been disabled until it is replaced.	Beeping	Battery needs to be replaced. Contact Dell.
Input AC over voltage	Utility RMS voltage greater than maximum valid utility threshold.	Beeping	Check the utility power.

Table A-1. External Alarm Conditions *(continued)*

Alarm	Description	Audible	Corrective Action
Site wiring problem	Site Fault detection is supported on LV and HV models anytime there is a Neutral connection and it is an LV model or has been manually enabled on the HV model. Alarm triggers when the difference between ground and neutral voltage is >= 25Vrms.	Beeping	Check the site wiring.
Output overload level L2	Load greater than level 2 threshold and less than level 3 threshold. Alarm clears when the load drops below 5% of the set point.	Beeping	Contact Dell.
Output overload level L3	Load greater than level 3 threshold. Alarm clears when the load drops below 5% of the set point.	Beeping	Contact Dell.
Battery DC over voltage	Battery voltage levels have exceeded the maximum allowable limits.	Beeping	Contact Dell.
Inverter AC over voltage	UPS has detected abnormally high inverter output voltage levels.	Beeping	Contact Dell.
Inverter AC under voltage	UPS has detected abnormally low inverter output voltage levels.	Beeping	Contact Dell.

Table A-1. External Alarm Conditions *(continued)*

Alarm	Description	Audible	Corrective Action
Output short circuit	Indicates that the UPS has detected abnormally low impedance placed on its output and considers it a short circuit.	Beeping	Contact Dell.
Heatsink over temperature	The UPS has detected that one of its heat sinks has exceeded the maximum operating temperature defined by Hardware.	Beeping	Contact Dell.
Fatal EEPROM fault	Set in parallel with EEPROM Range Check Failure, Incorrect Model EEPROM Map, and EEPROM Checksum Failure alarms.	Continuous	Contact Dell.
Fan failure	UPS has detected that one or more fans are not functioning properly.	Continuous	Contact Dell.

Table A-2. External Alarm Conditions

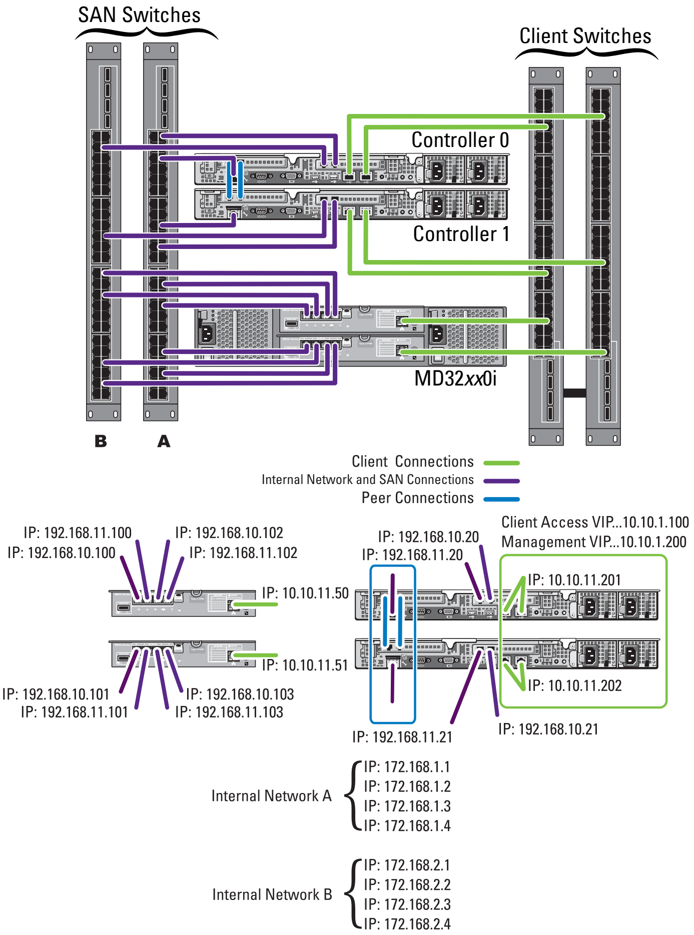
Alarm	Description	Audible	Corrective Action
Output overload	Load levels are at or have exceeded the configurable threshold limit for a Level 1 Overload condition. (Default 100% of nominal watts rating but is configurable from the LCD to be 10–100%). Alarm clears when the load drops below 5% of the set point.	Slow intermittent	Contact Dell.
Battery test failed	A weak battery string was detected during the last battery test.	Slow intermittent	Replace the battery. Contact Dell.
Input AC under voltage	Utility RMS voltage less than minimum valid utility threshold.	Slow intermittent	Check the utility power.
Input Under/Over Frequency	Utility frequency out of usable frequency range.	Slow intermittent	Check the utility power.

B

Cabling Recommendation

NOTE: The following cabling recommendation is applicable for existing MD-Series implementations.

Figure B-1. Dedicated SAN Solution in the High Availability Option



Index