Dell FluidFS NAS Solutions Administrator's Guide

Notes, Cautions, and Warnings

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

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

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

© 2012 Dell Inc.

Trademarks used in this text: Dell™, the Dell logo, Dell Precision™ , OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

2012 - 06

Rev. A00

Contents

1

Introduction

The Dell FluidFS network attached storage (NAS) solution 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.

Terms Used In The Document

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 the FluidFS NAS solution. The FluidFS NAS solution supports multiple client access Virtual IPs (VIPs).
NAS appliance	Two NAS controllers that are configured as pair in a FluidFS NAS clustered system. Cache data is mirrored between the paired NAS controllers within the appliance.
Controller (NAS controller or nodes)	The two primary components of a NAS appliance, each of which functions as a separate member in the FluidFS NAS cluster.
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 MD Series array.
Enterprise Manager	Multi system management software required for managing FluidFS with Storage Center.
Fluid File System (FluidFS)	High-performance, scalable file system software installed on NAS controllers.
Host Port Identifier	Unique ID used to identify hosts in a network.
LAN or client network (primary network)	The network through which clients access NAS shares or exports. The FluidFS NAS solution is connected to customer’s IT environment and its NAS clients using this network. It is also the network used by the storage administrator to manage the NAS solution.
NAS storage pool	The NAS storage pool is a virtualized storage layer on top of the virtual disks. The size of the NAS storage pool is the sum of all virtual disks made available to the FluidFS NAS cluster.
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 FluidFS NAS solution supports multiple NAS volumes.
NAS replication	Replication between two FluidFS NAS solutions or between two NAS volumes.
NAS replication partners	FluidFS NAS solutions participating in a replication activity.

Term	Description
Network Data Management Protocol (NDMP)	Network Data Management Protocol used for backup and restore.
Peer controller	The peer NAS controller with which a specific NAS controller is paired in a FluidFS NAS solution.
PowerVault MD3*xx*0i	Refers to the Dell PowerVault MD3200i, MD3220i, MD3600i, MD3620i iSCSI storage solutions.
Storage Center	Series 40 or SC8000 Compellent Storage center solutions, containing at least one fibre channel HBA for FluidFS connectivity.
Dell NAS Initial Deployment Utility (IDU)	The setup wizard used to initially discover and configure a FluidFS NAS solution. This utility is only used for the initial setup.
NAS Manager	The web-based user interface, which is part of the NAS cluster solution software, used to manage the FluidFS NAS solution.
FluidFS NAS solution	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 storage subsystem, and the NAS Manager.
Standby controller	A NAS controller 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	The network that carries the block level traffic and to which the storage subsystem is connected. **NOTE:** It is recommended that this network be isolated from the LAN or client network.

Dell FluidFS NAS Solutions Architecture

The FluidFS NAS solutions combined with storage arrays provides you with a unified storage solution. This solution provides you with access to both block and file storage.

The FluidFS clustered NAS solution consists of a NAS appliance with a pair of controllers and storage arrays. In addition, each NAS controller is protected by a BPS, which helps protect data during power failure.

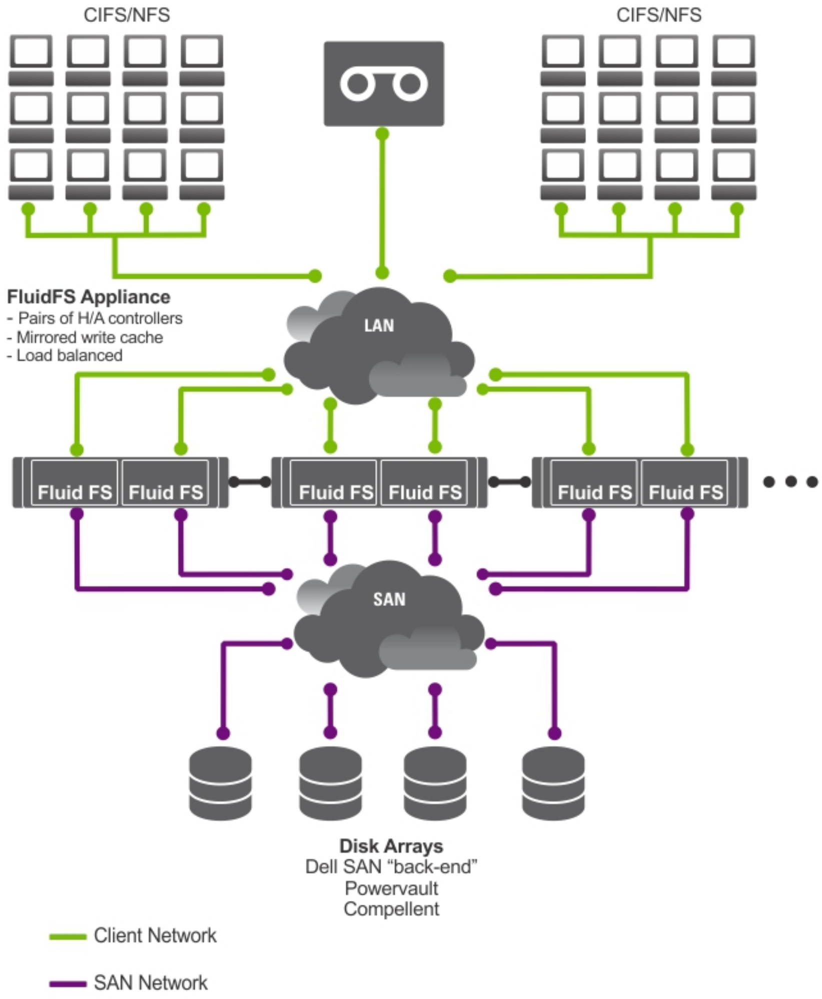

Figure 1. FluidFS NAS Cluster Solution Architecture

NOTE: Dell Compellent FS8600 NAS solution uses an additional Interconnect network, which is not represented in this illustration.

Key Features

The NAS cluster solution:

- 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.
- Is capable of storing terabytes of data 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.

- Is capable of providing user-accessible Point-In-Time snapshots.
- Is capable of sharing files with Microsoft Windows, Linux, UNIX, and Mac users.
- Offers flexible, automated online replication and disaster recovery.
- Features built-in performance monitoring and capacity planning.

NAS Cluster Solution Views

You can access the NAS cluster solution 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.

Client View

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

- NFS protocol for Linux and 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 NAS cluster solution system consists of:

- Hardware
  - One or more NAS appliances
  - Storage arrays
- Network
  - SAN network
  - Internal network
  - LAN or client network

NAS Appliance

The FluidFS NAS solution consists of one or more NAS appliances configured as a cluster. Each appliance consists of a pair of NAS Controllers in an active-active configuration. This configuration ensures that there is redundancy. The controllers handle load balancing of client connections, manage read-write operations, perform caching, and interface with servers and workstations. The cluster is a single pool of storage with a global name space, accessed using a virtual IP (VIP).

Read-write operations are handled through mirrored RAM. 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.

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.

Each controller is equipped with an internal BPS, which provides continuous power to the controllers for a minimum of five minutes in case of power failure. 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 NVRAM as cache. 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.

Storage Arrays

The controllers connect to a 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 1/10, RAID 5, and RAID 6.

SAN Network

The SAN network is a critical part of the NAS cluster solution. The controller pair resides on the SAN network and communicates to the storage subsystem using the iSCSI protocol for Dell PowerVault NX3500/NX3600/NX3610, or the fibre channel protocol for Dell Compellent FS8600.

Interconnect Network

The interconnect network is comprised of two independent networks. The interconnect network acts as the heartbeat mechanism and enables internal data transfer between controllers. In a two controller system, no switches are used. In configurations with more than two controllers, the interconnect network includes two switches. All Dell Fluid File System (FluidFS) controllers are connected to both interconnect switches. These employ dual links for redundancy and load balancing.

In order to achieve complete data distribution and to maintain high availability, each of the controllers in the Dell FluidFS cluster system must have access to all other controllers in the system. The interconnect network achieves this goal. The interconnect network provides the connectivity for Dell FluidFS clustering, including the heartbeat monitor, transferring data, mirroring information between the controllers' caches and distributing data evenly across all LUNs in the system.

LAN Or Client Network

After the initial configuration, a virtual IP (VIP) address connects the NAS cluster solution to the client or LAN network.

The VIP address allows clients to access the NAS cluster solution as a single entity, thereby providing access to the file system. It enables the NAS cluster solution 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 ports on each controller, which connect to the LAN or client network switches. The NAS cluster solution is administered using the LAN or client network on the NAS Management VIP. For routed networks, the number of VIPs that serve the system depends on the number of client ports available to you, for example, a Dell Compellent FS8600 (1 GbE) with four appliances has 32 Client VIPs. For flat networks, only one client VIP is sufficient.

Other Information You May Need

WARNING: See the safety and regulatory information that shipped with your system. Warranty information may be included within this document or as a separate document.

- The *Getting Started Guide* provides an overview of setting up your system and technical specifications.
- The *Owner's Manual* provides information about solution features and describes how to troubleshoot the system and install or replace system components.
- The rack documentation included with your rack solution describes how to install your system into a rack, if required.
- The *Deployment Guide* provides information on hardware deployment and the initial deployment of the NAS appliance.
- The *System Placemat* provides information on how to set up the hardware and install the software on your NAS solution.
- The *Online Help* provides information about configuring and managing the software. The online help is integrated with the system and can be accessed from the NAS Manager web interface.
- Any media that ships with your system that provides documentation and tools for configuring and managing your system, including those pertaining to the operating system, system management software, system updates, and system components that you purchased with your system.
- For the full name of an abbreviation or acronym used in this document, see the Glossary at **support.dell.com/manuals**.

NOTE: Always check for updates on **support.dell.com/manuals** and read the updates first because they often supersede information in other documents.

2

Monitoring The FluidFS NAS Solution

NOTE: The information in this chapter refers to file management using the NAS Manager. Block management and monitoring is done using:

- **Dell PowerVault Modular Disk Storage Management** (MDSM) for the Dell PowerVault NX3500/NX3600/NX3610 NAS solution
- **Enterprise Manager** for Dell Compellent FS8600 NAS solution

You can monitor the status of the NAS solution 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. By default, the **Dashboard** page is displayed.

Dashboard

The **Dashboard** page displays 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.

NOTE: To view detailed status parameters for each section, in the **Dashboard**, click each section.

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 their associated NAS appliances.

Capacity

The **Capacity** section displays a table and pie chart showing the total net capacity of the Dell Fluid File System.

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.

Recent Performance

The **Recent Performance** section displays a graph of the read-write throughput over the last 30 minutes.

Load Balancing

The **Load Balancing** section displays a table with real-time information about the controller's status, processor utilization, and the number of connections for each controller.

Events Viewer

The **Events Viewer** enables you to monitor your Fluid File System by displaying both informative and major events within your system.

To access the **Events Viewer** page, in the **Monitoring** tab, click **Events**.

In the **Events Viewer** page, you can:

- Filter events
- Sort events
- Export events to a CSV file

Viewing Events In The Event Viewer

1. Select **Monitor** → **Overview** → **Events.**
   The **Event Viewer** page is displayed.
2. Select the appropriate filters in the **Show**, **events of**, and **from** lists and click **Show**.
   An event viewer table displays the events depending on the parameters selected.
3. To sort the events, click the column headings of the event viewer table.
4. To view the details about the event, select the relevant event in the event viewer table.
   The details of the selected event is displayed in the **View Pane**.
5. To export the displayed events to a CSV file, on click **Export to CSV file**.
   A new browser window with the events in CSV format is displayed.
6. Copy and paste the events in a CSV file or save web page as a CSV file.

Network Performance

The **Network Performance Over Time** page displays Dell Fluid File System performance over time. You can view the network performance of FluidFS for the following periods of time:

- **Last Day**
- **Last Week**
- **Last Month**
- **Last Year**

Click on each tab to view the network performance over the appropriate period of time. You can view the following network performance details:

- **Client Network Throughput—Read**

- **Client Network Throughput—Write**
- **Operations Per Second**
- **Network Aggregated Throughput**

NOTE: For more information on **Network Performance Over Time**, see the *Online Help*.

Load Balancing

You can view the following load balancing details:

- **Over Time**
- **Client Connections**
- **CIFS Connections**

Viewing Load Balancing Over Time

1. Select **Monitor** → **Load Balancing** → **Over Time.**
   The **Load Balancing Over Time** page is displayed. The **Load Balancing Over Time** displays the **CPU Load**, **CIFS Connections**, **Read Throughput**, and **Write Throughput**.
2. Click the relevant tab to view the load balancing information for the required duration.
   You can view load balancing information for:
   - **Last Day**
   - **Last Week**
   - **Last Month**
   - **Last Year**
3. Select the controller for which you want to view the load balancing information and click **Display**.

NOTE: By default, all the controllers are selected.

4. To export the displayed events to a CSV file, click **Export to CSV file**.
   A new browser window with the events in CSV format is displayed.
5. Copy and paste the events in a CSV file or save the web page as a CSV file.

Client Connections

The **Client Connections** page enables you to:

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

NOTE: By default, the **Clients** tab displays a list of all the client connections.

Viewing Client Connections

NOTE: The client connections 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.

1. Select **Monitor** → **Load Balancing** → **Client Connections.**

The **Client Connections** page is displayed. By default, the **Clients** tab displays a list of all the client connections.

2. Select the appropriate filters in the **Protocols** and **Controller** lists.

   The client connections table displays the events depending on the parameters selected.

3. To sort the client connections, click the column headings of the client connections table.

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.

1. Select **Monitor→ Load Balancing→ Client Connections**.

   The **Client Connections** page is displayed. By default, the **Clients** tab displays a list of all the client connections.

2. In the client connections table, select one or more client connections that you want to migrate and click **Assign Interface**.

   The **Assign Interface** page is displayed.

3. In **Move to**, 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.

4. In **Interface**, choose the appropriate target interface or allow the system to assign the target interface on the controller automatically.

CAUTION: This operation disconnects CIFS connections if they are migrated to a different controller.

5. To enable **Automatic Rebalance**, select **Allow these clients to migrate to other controllers when rebalancing the network load**.

6. Click **Assign**.

Setting The Migration Policy

In case of a controller failure, the system automatically migrates each connection from the failed controller to another controller. This causes disconnections to CIFS clients, unless the **Migrate Manually** policy has been selected for CIFS. However, selection of this option requires you to manually migrate clients. Migration of CIFS clients in any circumstance, will interrupt I/O. Click the Windows **Cancel** button, and retry the transfer. When the failed controller restarts, the system rebalances 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. To optimize the fail-back operation, the system provides you with the following policies for migration on recovery:

- **Migrate Immediately** — Always keeps the system well balanced, at the cost of possibly disconnecting CIFS clients during work time.
- **Migrate Automatically** — Always keeps 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 a 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.

To set the migration policies:

1. Select **Monitor → Load Balancing → Client Connections.**

   The **Client Connections** page is displayed. By default, the **Clients** tab displays a list of all the client connections.
2. Click **Migration Policy**.

   The **Migration Policy** page is displayed.
3. For each **Protocol**, select the appropriate migration policy for the **Client Network**.
4. Click **Save Changes**.

Managing CIFS Connections

You can view current **CIFS Connections** in the **CIFS Connections** page.

To manage CIFS connections:

1. Select **Monitor → Load Balancing → CIFS Connections.**

   The **CIFS Connection** page is displayed.
2. To disconnect a client from the CIFS protocol, select the appropriate client and click **Disconnect** in the **Action** bar.
3. To disconnect all the connections for a specific controller, select the appropriate controller and click **Disconnect** in the **Action** bar.
4. Click **Refresh** to update the information displayed.

Hardware

Viewing System Validation Status

You can run system validation to validate the system configuration, including hardware and network connectivity.

NOTE: System validation can also be executed using the CLI interface.

It provides information about processors, monitoring availability, NICs, IPMI, Ethernet bandwidth, BPS monitoring, and so on.

To refresh the status of system components:

1. Select **Monitor → Hardware → System Validation.**

   The **System Validation** page is displayed.
2. Click **Rerun** to rerun system validation on each system component and refresh the status of each system component.

Viewing Detailed Component Status

The **Component Status** page displays the current status of the NAS cluster solution. It provides information about status, internal hardware, connectivity, and power for each appliance and its controllers.

To view additional details on the status of a specific controller or appliance:

1. Select **Monitor → Hardware → Component Status.**

   The **Hardware Component Status** page is displayed.
2. Under **Component**, click the appropriate appliance or controller.

   A web browser page opens, which displays the status of each component in the selected appliance or controller.
3. Click **Sample Hardware Components**, to refresh the screen until you see the new sampled values.

Appliance and Controller numbers start at 0. Appliance0 contains Controller0 and Controller1, Appliance1 contains Controller2 and Controller3, and so on. To identify the physical hardware, you must click **ApplianceX** and match the Service Tag shown in the popup window with the Service Tag printed on a sticker on the front right ear of the appliance.

Capacity

Viewing Space Utilized

The **Space Utilization** page displays the Dell Fluid File System space utilization and Dell Fluid File System space utilization over time.

To view the space utilized:

1. Select **Monitor** → **Capacity** → **Space Utilization.**

   The **Space Utilization** page displays the space utilization table for the selected period. By default, the **Current** space utilization is displayed.

2. Click the relevant tab to view the load balancing information for the required duration. You can view load balancing information for:

   - **Last Day**
   - **Last Week**
   - **Last Month**
   - **Last Year**

3. To sort the space utilization, click the column headings of the space utilization table.

Viewing 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:

1. Select **Monitor** → **Capacity** → **Quota Usage.**

   The **Quota Usage** page displays the quota usage table for **All NAS Volumes**.

2. From **Show quota usage for NAS Volume**, select the appropriate NAS volume or **All NAS Volumes**.

   The quota usage table displays the quota usage details for the selected NAS volume.

3. To refresh the quota usage, click **Refresh**.

Replication

You can view the status and progress of the NAS replication process in the **NAS Replication** page.

To view the status and progress of NAS replication policies:

1. Select **Monitor** → **Replication** → **NAS Replication.**

   The NAS Replication page displays the NAS replication table for replication policies whose source volume, destination volume, or both, reside on this Dell Fluid File System.

2. To sort the NAS replication, click the column headings of the NAS replication table.

3. To view a detailed history of the replication policy progress, click the status of the relevant replication policy.

NDMP

You can view the status and progress of the NDMP active jobs in the **NDMP Active Jobs** page.

3

Using Volumes Shares And Quotas

The **User Access** tab enables you to define and manage the Dell Fluid File System from the client perspective.

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 the NAS cluster solution 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.

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 must not contain more than 230 characters. It must contain only letters, digits and underscores (_) and must begin with either a letter or an underscore.
  - You can create as many NAS 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 20 MB (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 must 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. Security style can also be set to mixed which supports both POSIX security and Windows ACLs on the same volume.

- 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. The following table 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 1. 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 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.

Adding A NAS Volume

To add a NAS volume:

1. Select **User Access** → **NAS Volumes** → **Configuration.**

   The **NAS Volumes Configuration** page displays the list of NAS volumes.
2. Click **Add**.

   The **Add NAS Volume** page is displayed.
3. In **NAS Volume**, enter the NAS volume name.
4. In **NAS volume allocated space**, enter the space allocated to this NAS volume in MB, GB or TB.

NOTE: A NAS volume must have a minimal size of 20 MB and its maximum size can be all the available space.

5. In **Alert when used space reaches** , enter a percentage of the allocated space.
6. From the **Send email alerts to administrator** list, select a Dell Fluid File System administrator to whose email address the system sends alerts.

NOTE: This feature is not available on Dell Compellent FS8600 NAS solutions. For more information, see the **Enterprise Manager** documentation for alert handling on these solutions.

7. From the **Access time granularity** list, select the resolution of file access timestamp accuracy based on system performance requirements.
8. From the **File Access Security Style** list, select the NAS volume security style.

   You can select **NTFS**, **MIXED**, or **UNIX**.
9. In **Default UNIX permissions of Windows files**, define the default UNIX permissions for new files created from Windows clients.
10. In **Default UNIX permissions of Windows directories**, define the default UNIX permissions for new directories created from Windows clients.
11. Click **Save Changes** to create the NAS volume.

Modifying A NAS Volume

To modify the parameters of a specific NAS volume:

1. Select **User Access** → **NAS Volumes** → **Configuration.**

   The **NAS Volumes Configuration** page displays the list of NAS volumes.
2. From the list of available NAS Volumes, under the **NAS Volume** column, click the relevant NAS volume.

   The **Edit NAS Volume** page for the selected NAS volume is displayed.

3. 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 NAS cluster solution (maximum).

Removing A NAS Volume

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

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.

NOTE: Deleting a NAS volume deletes all the 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 external backup.

To remove a NAS volume:

1. Ensure that the NAS volume is not mounted and warn relevant users that they are disconnected.
2. Select **User Access** → **NAS Volumes** → **Configuration.**

   The **NAS Volumes Configuration** page displays the list of NAS volumes.
3. From the list of available NAS Volumes, select the relevant NAS volume and click **Delete**.

Shares And Exports

You can define access permissions to files in the file system, according to permissions assigned to hosts and users. This 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 The NAS Cluster Solution

To add an NFS export:

1. Select **User Access** → **Shares** → **NFS Exports.**

   The **NFS Exports** page is displayed.
2. Click **Add**.

   The **Add NFS Export** page is displayed. It consists of two tabs, **General** and **Advanced**. By default, the **General** tab is displayed.
3. From the **NAS Volume** list, select the NAS Volume on which the NFS export will be located.
4. In **Exported Directory,** enter the path to the directory you want to export or click the Browse icon, and navigate to the appropriate directory.
5. Select **Create the exported directory if it does not exist**, if the directory does not exist.
6. From the **Trust these users list,** select the users that are trusted.

NOTE: Other users are identified as guests.

7. Define the client machines that are allowed to access this NFS export. Select one of the following options:

   – **All Client Machines**.
   – **A Single Client Machine**—You must enter the **IP or Domain Name** for the client.
   – **All Client Machines in a Specific Network**—You must enter the **IP Address and Netmask** for the clients.

NOTE: For example, if you want to grant access to all members of the `192.10.x.x/16` subnet, with netmask `255.255.0.0`, enter `192.10.0.0` into the **IP address** field, and `255.255.0.0` in the **Subnet** field.

   – **All Client Machines in a Specific Netgroup**—You must enter the **Netgroup name** for the clients.

8. In **Allow access for,** select the appropriate access rights for the share. you must select either **Read/Write** or **Read only**.

NOTE: If the access rights for the share are stricter than those defined for a specific file, the file's access rights are overridden by those of the share.

9. Select the **Advanced** tab.
10. In **Limit reported size,** set a limit on the reported size of the NFS export to allow access by client machines that cannot handle large file systems.

NOTE: If you leave **Limited reported size** empty, the reported size will be the actual size.

11. In **Require secure port?**, select **No** to enable access through insecure ports (ports beyond 1024).
12. In **Comment**, add a comment or description for NFS export.
13. Click **Save Changes**.

Modifying An NFS Export

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

1. Select **User Access → Shares → NFS Exports.**
   The NFS Exports page is displayed.
2. From the list of available NFS Exports, under the **Exported Directory** column, click the relevant NFS export.
   The **Edit NFS Export** page for the selected NFS export is displayed.
3. Change the parameters as required in the **General** and **Advanced** tabs and click **Save Changes**.

Removing An NFS Export

To remove an NFS Export:

1. Select **User Access → Shares → NFS Exports.**
   The NFS Exports page is displayed.
2. From the list of available NFS Exports, select the relevant NFS export and click **Delete.**

Access Using NFS

To mount an NFS export folder on a NAS volume, from a shell on a client system, use the `su` command to log in as root and run the following command:

```
mount <FluidFS_client_VIP>:/<volume_name>/<exported_folder> <local_folder>
```

However, older versions of UNIX/Linux do not use TCP by default. The following mount command specifies the correct arguments.

To mount an NFS export folder on a NAS volume, from a shell on a client system, use the `su` command to log in as `root` and run the following command:

```
mount -o hard,tcp,nfsvers=3,timeo=3,retrans=10,rsize=32768,wsize=32768
<FluidFS_Client_VIP>:/<volume_name><exported_folder> <local_folder>
```

For backward compatibility with FluidFS version 1, an NFS export on the default NAS volume can also be mount by:

```
mount -o hard,tcp,nfsvers=3,timeo=3,retrans=10,rsize=32768,wsize=32768
<FluidFS_Client_VIP>:/<volume_name><exported_folder> <local_folder>
```

To mount an NFS export folder on a NAS volume from MAC:

```
mount_nfs -T -3 -r 32768 -w 32768 -P <FluidFS_Client_VIP>:/
<volume_name><exported_folder> <local_folder>
```

NOTE: The above parameters are recommended parameters. See the `mount` command manual page for more information and other options.

To allow a UDP or TCP connection, you can configure the firewall settings in two 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

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. Select **User Access** → **Shares** → **CIFS Shares.**
   The **CIFS Share** page is displayed.
2. From the **Show CIFS Shares for NAS Volumes** list, select a specific NAS volume or **All NAS Volumes**.
   The CIFS export table is displayed for the selected NAS volume.

Adding A CIFS Share

To add a CIFS share:

1. Click **User Access** → **Shares** → **CIFS Shares.**
   The **CIFS Share** page is displayed.
2. On the **CIFS Share** page, click **Add**.

The **Add CIFS Share** page is displayed. By default the **General** tab is selected.

3. From the **NAS Volume** list, select the appropriate NAS volume.
4. To set up a directory that can be accessed by all users, select **General-access Share**.
   a) In **Share name**, enter the CIFS share name.
   b) In **Directory**, enter the path to the directory you want to export or click the **Browse** button, and navigate to the appropriate directory.
   c) Select **Create the exported directory if it does not exist**, if the directory does not exist.
5. To set up a user-based directory where each user has a dedicated directory, select **CIFS Share containing a user-based directory tree**.

   For more information, see Creating Home Shares.

   a) In **Path template**, enter the path template (the base of the home directories) for the CIFS share volume.
   b) Select user, to add the user name to the home directory, or select group/user to add the primary group and user to the home directory path.
6. In **Comment**, enter a description or comment for the CIFS share.

⚠ **CAUTION: Do not select Files should be checked for viruses unless you have an external Antivirus server configured.**

7. Select **Files should be checked for viruses**, to specify whether or not the system checks and verifies that files are not infected by virus before allowing access.
8. Click the **Advanced** tab and in **Hide these files**, enter the file types you want to hide while the share is being browsed.

NOTE: For example, enter *.tmp to hide all files with a .tmp extension.

9. In **Allow guests**, select **Yes** to allow unknown users to access the share as guests.

NOTE: If you select **Files should be checked for viruses** in the **General** tab, the **Antivirus** tab is activated.

10. Click the **Antivirus** tab and in **Select the policy for handling of virus-infected files:**, select one of the following:

    – **Do nothing**—Deny access to the client, but keep the file in its original location (access is allowed only through another CIFS share that is not virus checked).
    – **Quarantine the file**—Deny access to the client and move the file to the **.Quarantine** folder in the NAS volume root folder.
    – **Remove the file**—Deny access to the client and delete the file.

NOTE: The system applies the specified option if a virus infected file is identified and the antivirus host was not able to cure it.

11. In **Specify which files should be checked for viruses**, select one of the following:

    – **Scan all files except files with specific extensions**
    – **Scan files with specific extensions only**

NOTE: Use comma-separated list of extensions. For example: tmp, jpg, jpeg.

12. In **Exclude files in the following folders**, enter the folder names that need not be checked by the antivirus.

NOTE: Use comma-separated list of folders, and enclose the folders with double-quotes if they contain a space or a comma. You may include wildcards for folder specification. For example, /Marketing/temp*,/Secrets,"/All Finance".

13. Click **Save Changes**.

NOTE: Do not attempt to create a CIFS share using the Microsoft Management Console (MMC). Use MMC only to set share level permissions (SLPs).

Modifying A CIFS Share

After you determine whether a CIFS share is a general access directory or user-based directory, you cannot change this setting. To modify the parameters of a specific CIFS share:

1. Click **User Access** → **Shares** → **CIFS Shares.**
   The **CIFS Share** page is displayed.
2. From the list of available CIFS share, under the **Share** column, click the relevant CIFS share.
   The **Edit CIFS Share** page for the selected CIFS share is displayed. By default, the **General** tab is selected.
3. In the **General** tab modify general CIFS share parameters.
4. Click **Advanced** and modify advanced CIFS share parameters.

NOTE: If you select **Files should be checked for viruses** in the **General** tab, the **Antivirus** tab is activated.

5. If active, click **Antivirus** and modify the antivirus policy.
6. Click **Save Changes**.

Removing A CIFS Share

To remove a CIFS share do the following:

1. Click **User Access** → **Shares** → **CIFS Shares.**
   The **CIFS Share** page is displayed.
2. From the list of available CIFS share, select the relevant CIFS share and click **Delete.**

Creating Home Shares

If creating a CIFS share with user-based directory structure (home share), the share will not be accessible initially. This is because all directories for each user must be created by the administrator. This can be accomplished with a script (user created script), batch file, or PowerShell cmdlet that is written by the storage administrator. Alternatively, the administrator can manually create these folders. This is to provide stronger access controls to the administrator. The administrator can either manually determine the accounts to be given a home share, or can write a script that automatically generates the folders, for some or all of the users in a particular Active Directory or local user database.

NOTE: The following procedure must be completed only by a domain administrator who is also the NAS storage administrator.

To create the CIFS home share folders manually:

1. In the **NAS Manager**, verify that the system is joined to your Active Directory.
2. If you are using Active Directory, in **NAS Manager**, select **Cluster Management** → **CIFS Configuration** and ensure that **Authenticate users' identity via Active Directory and local users database** is selected.
3. In the **NAS Manager**, create a general access share that is the root of all the users folders.
   For example, create a general access share with share name `users`, at directory `/users`, and select the option to create the folder if not already present.
4. Using **Windows Explorer**, mount the **users** share as the CIFS local administrator.
5. In the security setting of the mounted share, click on **Advanced**, and change owner to `Domain Admins`, or the specific Domain Administrator or Storage Administrator account you wish to have ownership.

This is the account that creates the folders (either using a user create script or manually) for each users home share.

6. Disconnect or unmount the **user** share, and remount it as an account that has ownership of it, as previously set (as a Domain Admin, Storage Admin, or specific account ownership was set to).
7. In the **NAS Manager**, create a new CIFS share, and select the share type **CIFS share containing a user-based directory tree**.
8. Previously, the general access share titled **users** was created at the path **/users**. In **Path template**, enter **/users** and then select if you want the users folders to take the form of **/users/username** or **/users/domain/username**.
9. Click **Save Changes**.
10. Using **Windows Explorer**, for each user that you wish to be given a home share, create a folder for them that conforms to the Path template: you selected in the previous step.

    This can be done manually or with a user create script.

Setting Access Control Lists And Share Level Permissions On FluidFS

You can set up access control lists (ACLs) and share level permissions (SLP) on Fluid File System (FluidFS). It is recommended that a Windows administrator follows 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.

CIFS Full Access User Account (Backup User)

The **Full Access User** account is a special purpose account that is to be used by backup administrators. The system must be a member of an **Active Directory** (AD) to associate this privilege with an AD account. The Full Access User privilege gives the AD account full access to all data on all shares, and all volumes, regardless of the file ACL definitions. However, the SLP settings do apply on the AD account granted **Full Access User** privilege. It is the job of the NAS system administrator to verify the AD account set for full access user has all relevant SLPs.

To manage the Full Access User:

1. Open a connection to the CLI using a direct KVM connection or through SSH to the management VIP.
2. To set the **Full Access User** account, or overwrite the current entry, in the CLI, run the command:
   ```
   system authentication full-access-account set DOMAIN+username
   ```
3. To verify if **Full Access User** account is properly set, run the command:
   ```
   system authentication full-access-account view
   ```
4. To delete the **Full Access User**, run the command:
   ```
   system authentication full-access-account delete
   ```

Active Directory Configuration

FluidFS has the ability to join an Active Directory domain. This can be done using the NAS Manager or the CLI.

Setting ACLs Or SLPs On A CIFS Share

The first time a CIFS share is created, the owner of the share must be changed before setting any ACLs or attempting to access this share. If the NAS cluster solution 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.

Using An Active Directory Account Set As The Domain Administrators Group

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

Mapping A Network Drive To The CIFS Share

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>\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 **Cluster 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 *Administrator* 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

Microsoft Windows offers several methods to connect to CIFS shares.

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

Option 1

Execute the **net use** command from the command prompt.

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 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** and 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 NAS appliance.
2. Select the NAS appliance, and double click the selected NAS appliance.
3. From the **CIFS shares** list, select the share that you want to connect to.

Configuring CIFS Shares Level Permissions

Configuring CIFS 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 NAS cluster.

The MMC does not let you chose which user to connect with to a remote computer. By default, the MMC uses the user logged on to the machine to form the connection.

To use the correct user in the MMC connection:

- If the NAS appliance that 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 the NAS cluster solution 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.

If there are no predefined MMC files:

1. Click **Start → Run.**
2. Type `mmc` and click **OK**.

   The **Console 1 - [Console Root]** window is displayed.
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 NAS cluster solution 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.

Access Based Share Enumeration

In the v2 release of the Dell Fluid File System, SLP access based share enumeration is enabled by default. The result is that when Share Level Permissions (SLP) are not given, users and groups are not presented the share. If a certain user or group does not have Share Permissions for a particular share, when the NAS cluster is accessed directly at **\\<client access VIP>**, the share will not be presented at all in the list of available shares. Previously, in Dell Fluid File System v1, access based share enumeration was not enabled, therefore the share would be presented, but could not be accessed.

Resetting CIFS Local Administrator Password

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

To reset the CIFS local administrator 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.

1. Log in to the NAS Manager.
2. Select **Cluster Management** → **Authentication** → **Local Users.**
   The **Local Users** screen is displayed.
3. Choose **Administrator** user.
4. Choose **Change password**.

Quotas

A disk quota is a set of rules that restrict disk space and the number of files used by a user or a group. A quota can also restrict the total space used in a NAS volume or the usage of users and groups within an NAS Volume. Quota values always relate to a specific volume and are specified in units of MB.

NOTE: Users and groups for which an individual quota is not defined will use the default user/group quota.

Managing Default Quotas

To manage the default quotas of a volume:

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

1. Select **User Access** → **Quota** → **Default.**
   The **Default Quota** screen is displayed.
2. From the **NAS Volume** list, select the appropriate NAS Volume where the quota can be added or modified.
3. In **Default quota per user**, select and enter the desired user quota in MB or select **Unlimited**.

   NOTE: When this limit is exceeded, writing to the NAS Volume is not permitted.

4. In **Alert administrator when quota reaches**, select and enter the desired user quota in MB or select **Disabled**.

   NOTE: When this limit is exceeded, a warning message is sent to the mail recipient's address. This default is used for users for which an individual quota is not defined.

5. In **Default quota per group**, select and enter the desired user quota in MB or select **Unlimited**.

   NOTE: When this limit is exceeded, writing to the NAS Volume is not permitted.

6. In **Alert administrator when quota reaches**, select and enter the desired group quota in MB or select **Disabled**.

NOTE: When this limit is exceeded, a warning message is sent to the administrator's e-mail address. This default is used for users for whom an individual quota is not defined.

7. Click **Save Changes**.

Managing User Or Group Specific Quotas

Viewing Existing User/Group Specific Quotas

To view the details for a specific user or group quota:

1. Select **User Access** → **Quota** → **User/Group.**

   The **User/Group Quota** page is displayed.
2. From the **Show quotas for NAS Volume** list, select the appropriate NAS volume or **All NAS Volumes**.

   The list of available User/Group Quota for the selected NAS volume is displayed. By default, User/Group Quota information for **All NAS Volumes** is displayed.

Quota Types

The following quota types are available:

- 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 User/Group Specific Quotas

To add a quota:

1. Select **User Access** → **Quota** → **User/Group.**

   The **User/Group Quota** page is displayed.
2. Click **Add**.

   The **Create Quota** page is displayed.
3. From the **NAS Volume** list, select the appropriate NAS volume to which you want to add the quota.
4. From the **Quota for** list, select the type of quota restriction you want and enter the appropriate user or group name or click the Browse button to select the appropriate user or group.

NOTE: Listing users may take some time, depending on the number of users in your Active Directory domain. During this time, sporadic authentication failures may occur. If you know the user name, you can type it instead of listing all users.

5. In **Quota**, select and enter the quota in MB, or click **Unlimited**.

NOTE: If the user or group already uses this amount of data, new writes are denied.

6. In **Alert administrator when quota reaches**, select and enter the desired group quota in MB or select **Disabled**.

NOTE: When this limit is exceeded, a warning message is sent to the administrator's e-mail address.

NOTE: This default is used for users for which an individual quota has not been defined.

7. Click **Save Changes**.

Modifying User/Group Specific Quotas

To modify an existing quota:

1. Select **User Access** → **Quota** → **User/Group.**

The **User/Group Quota** page is displayed.

2. From the **NAS Volume** list, select the appropriate NAS volume.

   The **User/Group Quota** table displays the list of available **User/Group Quota**s for the selected NAS volume.

3. From the list of available User/Group Quotas, under the **Name/ID** column, click the relevant User/Group Quota.

   The **Edit Quota** page is displayed.

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

Deleting A Quota

To delete a quota rule:

1. Select **User Access** → **Quota** → **User/Group.**

   The **User/Group Quota** page is displayed.

2. From the **NAS Volume** list, select the appropriate NAS volume.

   The **User/Group Quota** table displays the list of available **User/Group Quota**s for the selected NAS volume.

3. From the list of available User/Group Quotas, select the appropriate quota rule and click **Delete**.

4

Protecting Data On The FluidFS NAS Cluster Solution

Data protection is an important and integral part of any storage infrastructure. You can configure various methods for protecting the data in your Dell Fluid File System, including:

- Snapshots
- Replication
- System Restore from Backup
- Backup Agent Configuration

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 are a delta from the previous snapshot.

For more information on snapshots, see the *Online Help*.

Adding Or Modifying A Snapshot Policy

1. Select **Data Protection → Snapshots → Policies.**

   The **Snapshot Policies** page is displayed.
2. From the **NAS Volume** list, select the appropriate NAS volume.
3. In **Alert the administrator when snapshot space is % of total volume**, enter the percentage of total NAS volume space.

   When this limit is exceeded, snapshots are automatically deleted.

NOTE: Leave this field empty to disable snapshot space events.

NOTE: Both scheduled and user-created snapshots are deleted. Replication snapshots are not be deleted.

4. Select **Periodic** to take snapshots for periods shorter than an hour:
   a) Select the minute frequency from the **Every Minutes** list.
   b) Enter the **Number of snapshots to keep**.
5. Select **Hourly** to take snapshots on an hourly basis:
   a) Either select **Every hour** or select **At** and the specific hour **and minutes** when the snapshots must be taken.
   b) Enter the **Number of snapshots to keep**.
6. Select **Daily** to take snapshots according to the day.
   a) Either select **Every day** or select **On** and specific days.
   b) In **At**, select the time at which the snapshot is generated.
   c) Enter the **Number of snapshots to keep**.

7. Select **Weekly** to take Snapshots on a weekly basis.
   a) From the **On** list, select which day and at what time the snapshot is generated.
   b) Enter the **Number of snapshots to keep**.

8. Click **Save Changes**.

Creating A Snapshot (Without A Policy)

1. Select **Data Protection → Snapshots → List.**

   The **Snapshots List** page displays the list of existing snapshots. By default, snapshots for all the NAS volumes is displayed.

2. Click **Create**.

   The **Create Snapshot** page is displayed.

3. From the **NAS Volume** list, select the appropriate NAS volume.

4. In **Snapshot name**, enter the name of the new snapshot.

5. Click **Create**.

   The new snapshot is created and added to the list of snapshots in the **Snapshots List** page.

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.

Modifying A Snapshot

NOTE: You can only modify the **Snapshot name**.

1. Select **Data Protection → Snapshots → List.**

   The **Snapshots List** page displays the list of existing snapshots. By default, snapshots for all the NAS volumes is displayed.

2. From the **Show Snapshots for NAS Volume list**, select the appropriate NAS volume or select **All NAS volumes.**

   Existing snapshots for the selected NAS volume is displayed.

3. From the list of available snapshots, under the **Name** column, click the relevant snapshot.

   The **Edit Snapshot** screen is displayed.

4. In **Snapshot name**, change the existing name.

5. Click **Calculate Snapshot Delta** to calculate the actual space freed by removing a snapshot.

6. Click **Save Changes**.

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.

Deleting A Snapshot

1. Select **Data Protection** → **Snapshots** → **List.**
   The **Snapshots List** page displays the list of existing snapshots. By default, snapshots for all the NAS volumes are displayed.
2. From the **Show Snapshots for NAS Volume** list, select the appropriate NAS volume or select **All NAS volumes.**
   Existing snapshots for the selected NAS volume is displayed.
3. From the list of available snapshots, select the relevant snapshot and click **Delete**.

Restoring A NAS Volume From A Snapshot

1. Select **Data Protection** → **Snapshots** → **Restore.**
   The **Snapshot Restore** page is displayed.
2. In **Choose the volume to be reverted**, select the appropriate NAS volume.
   The **Choose a snapshot for revision** list displays the snapshots for the selected NAS volume.
3. In **Choose a snapshot for revision**, select the snapshot to which you want the volume to be reverted.
4. Click **Next**.
   A message prompts you with instructions that you must follow before starting the restore process.
5. To restore the NAS volume to the selected snapshot, click **Yes**.
   The NAS volume is restored to the snapshot.

⚠ **CAUTION: The Restore operation cannot be undone. Any data created or changed between the time of the snapshot and when the restore operation is completed, is erased.**

Replication

Replication in the Dell FluidFS NAS solutions is block-based and asynchronous.

- Block-based—only blocks that have any changes are replicated and not the entire file
- Asynchronous—communication with the client continues even when the data is being replicated

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.

Replication leverages the snapshot technology in the NAS cluster solution 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 NAS appliance or a volume on another NAS appliance. When replicating a volume to another NAS appliance, the other NAS appliance must be setup as a replication partner.

Replication Partners

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.

NOTE: Replication partners must have the same controller count. Do not, for example, attempt to replicate a 4 controller appliance to a 2 controller appliance.

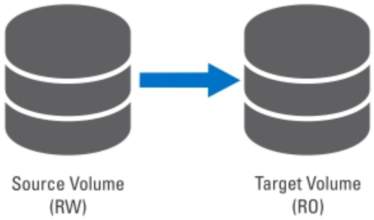

Figure 2. Local Replication

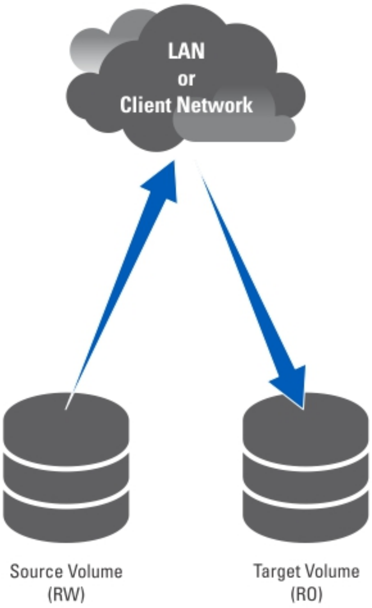

Figure 3. Partner Replication

Viewing Existing Replication Partners

You can view a list of the replication partners. To view the replication partners trusted by the selected system, select **Data Protection** → **Replication** → **Replication Partners,** the **Replication Partners** screen displays the list of existing replication partner names.

Setting Up a Replication 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.

To add replication partners:

1. Select **Data Protection** → **Replication** → **Replication Partners.**
   The **Replication Partners** screen is displayed.
2. Click **Add**.
   The **Add Replication Partner** screen is displayed.
3. In **Remote NAS management VIP**, enter the VIP addresses of the remote system NAS manager.
4. In **User name** and **Password**, enter the username and password of an administrator account on the remote system.

NOTE: These values are not stored in Dell Fluid File System.

5. Click **Save Changes**.

Modifying A Replication Partner Configuration

You can modify a replication partner's configuration by changing its parameters.

To modify the parameters of a replication partner:

1. Select **Data Protection** → **Replication** → **Replication Partners.**
   The **Replication Partners** screen displays the list of existing replication partner names.
2. Under **Replication Partner Name**, select the appropriate replication partner.

The **Edit Replication Partner** page is displayed.

3. In **Remote NAS management VIP**, change the VIP address as required.
4. In **User name** and **Password**, change the admin credentials as required.
5. Click **Save Changes**.

Removing A Replication Partner

You can remove a system's replication partner by deleting it from the replication partner list. When deleting a replication partner, ensure that both systems are up and running. If one of the systems is down or unreachable, a warning message is displayed.

To delete a replication partner's configuration:

1. Select **Data Protection → Replication → Replication Partners.**

   The **Replication Partners** screen displays the list of existing replication partner names.

2. From the list of existing replication partners, select the appropriate replications partner and click **Delete**.

NAS Replication Policies

Replication between volumes is managed through policies. You can create a NAS replication policy, also known as attaching volumes, through the NAS Manager by:

1. Creating a trust between the source and destination systems.

   This requires entering the IP address of the remote system and specifying an administrator's user name and password.

2. Add the replication policy.

   This requires selecting the source volume, the destination volume, and specifying a periodic schedule for the replication.

   If the destination system has data that is not available on the source system, a warning is issued, and you are asked to approve losing this data.

3. Monitor the replication progress.

   Verify if the replication is running smoothly.

   You can delete the replication policy, thus making the destination system writable. For more information on NAS replication policies, see the *Online Help*.

NOTE: Replication destination volumes are **read only** when associated with a replication policy.

Adding A Replication Policy

1. Select **Data Protection → Replication → NAS Replication.**

   The **NAS Replication** page displays a list of existing NAS replication policies.

2. Click **Add**.

   The **Add NAS Replication Policy** page is displayed.

3. In **Source NAS volume**, enter the source NAS volume or click the **Browse** button and select the appropriate NAS volume.
4. From the **Destination cluster** list, select one of the following:

   – **localhost** to replicate the source volume in this system.

   – another available Dell Fluid File System replication partner.

5. In **Destination NAS volume**, enter the destination NAS volume or click the **Browse** button and select the appropriate NAS volume.
6. Select one of the following recovery point schedule options:
   - **Replicate every hour after**
   - **Replicate every day at**
   - **Replicate every week on**
   - **Replicate on demand (not scheduled)**
7. Click **Save Changes**.

Modifying Replication Policies

1. Select **Data Protection → Replication → NAS Replication.**

   The **NAS Replication** page displays a list of existing NAS replication policies.
2. Select the appropriate NAS volume under the **Source NAS Volume** column.

   The **Edit NAS Replication Policy** page is displayed.
3. In **Source NAS Volume**, enter the source NAS volume or click the **Browse** button and select the appropriate NAS volume.
4. From the **Destination cluster** list, select one of the following:
   - **localhost** to replicate the source volume in this system.
   - another available Dell Fluid File System replication partner.
5. In **Destination NAS volume**, enter the destination NAS volume or click the **Browse** button and select the appropriate NAS volume.
6. Select one of the following recovery point schedule options:
   - **Replicate every hour after**
   - **Replicate every day at**
   - **Replicate every week on**
   - **Replicate on demand (not scheduled)**
7. Click **Save Changes**.

Pausing, Resuming, And Running The NAS Replication

You can pause, resume, or run the NAS replication on demand depending on the status of the selected NAS volume.

1. Select **Data Protection → Replication → NAS Replication.**

   The **NAS Replication** page displays a list of existing NAS replication policies.
2. From the list of existing NAS volumes, select the appropriate NAS volume.
3. Click **Pause**, to place the selected NAS replication on hold.
4. Click **Resume**, to continue the NAS replication for the selected NAS replication.
5. Click **Replicate Now**, to immediately start the replication for the selected NAS volumes.

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. 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.

To delete the replication policy:

1. Select **Data Protection** → **Replication** → **NAS Replication.**

   The **NAS Replication** page displays a list of existing NAS replication policies.

2. From the list of existing NAS volumes, select the appropriate NAS volume and click **Delete**.

Disaster Recovery Using Replication

Before you set up disaster recovery using replication, ensure that the following conditions are met:

NOTE:

  - **Cluster A** is the source cluster containing the data that must be backed up.
  - **Cluster B** is the backup cluster, which is fully configured but with no volumes created and backs up the data from source cluster A.

- Both the source and backup clusters are of the same type and configuration.

NOTE: For example, if the source cluster A is an NX3600 with a four quad core processors then the backup cluster B must also be an NX3600 with four quad core processors.

- Cluster B replication version is same as cluster A.
- Cluster B has enough space to replicate all the data in cluster A.
- Backup cluster B has different network settings (client, SAN, IC, and so on) than source cluster A, however, both clusters must be able to communicate with each other so that the replication process can occur.

NOTE: Ideally cluster B must serve as a pure back up cluster for cluster A and contain only the backup data from cluster A. Apart from the replication volume from cluster A, cluster B must not have any additional volumes configured.

There are three phases involved in setting up disaster recovery using replication:

1. Phase 1—Build up replication structure between source cluster A and backup cluster B
2. Phase 2—Cluster A fails and client requests fail over to backup cluster B
3. Phase 3—Restore cluster A fail back from cluster B to cluster A

Phase 1—Build Replication Partnership Between Source Cluster A And Backup Cluster B

1. Log on to cluster A.

2. Set up replication partnership between source cluster A and backup cluster B.

   For more information on setting up replication partners, see Setting Up A Replication Partner.

3. Create a replication policy for all the source volumes in cluster A to target volumes in cluster B.

   For more information on creating replication policies, see Adding A Replication Policy.

NOTE: Replication policy is a one to one match on a volume basis, for example:

Source volume A1 (cluster A) to target volume B1 (cluster B)

Source volume A2 (cluster A) to target volume B2 (cluster B)

....

Source volume A*n* (cluster A) to target volume B*n* (cluster B)

NOTE: FluidFS 1.1 supports auto generate target volume during addition of the replication policy. For FluidFS 1.0, you must create the target volumes in cluster B and make sure that the volume size is big enough to accommodate the corresponding source volume data in cluster A.

4. Start the replication scheduler to ensure that at least one successful replication has occurred for all the source volumes in cluster A.

   If the replication fails, fix the problems encountered and restart the replication process. This ensures that all source volumes in cluster A have at least one successful replication copy in cluster B. Set up a regular replication schedule, so the target volumes in cluster B always have most up to date replication copy for cluster A.

CAUTION: Replication restore is not a complete BMR restore, settings such as network configuration (client, SAN, and IC) cannot be backed up and restored using the replication method. Note all cluster A settings (for use when restoring cluster A) including network configuration, cluster wide settings such as volume name, alert settings, and so on for future use. If the system restore operation fails to restore these settings, you can manually restore the cluster A settings back to their original values.

Phase 2—Cluster A Fails And Client Requests Fail Over To Backup Cluster B

If source cluster A stops responding because of an unexpected failure (hardware, disk, and so on), you must:

1. Log on to backup cluster B.
2. Delete the existing replication policy for all replication target volumes.

   FluidFS replication manager tries to contact source cluster A, which fails.
3. Confirm replication policy deletion on backup cluster B and apply the source volume configuration from cluster A.

   Currently the following volume configurations can be restored:

   – NFS exports
   – CIFS shares
   – Quota rules
   – Snapshot schedule
   – NAS volume alerting, security style and related parameters
   – NAS volume name
   – NAS volume size

   This transforms target volumes (B1, B2, .. B*n*) to standalone volumes. Repeat this procedure to bring all target volumes in cluster B to standalone volumes with volume configuration applied from cluster A.
4. From the NAS Manager web interface, restore the NAS system configuration from cluster A.

   For more information on restoring the NAS system configuration, see Restoring Cluster Configuration.

   This restores cluster B configuration to cluster A settings. Currently the following cluster system configuration can be restored:

   – Protocols configuration
   – Users and Groups
   – User mappings
   – Monitoring configuration
   – Time configuration
   – Antivirus hosts
5. Ensure that cluster B is used to temporarily serve client requests during the fail over time.

   Administrators must perform the following steps to set up DNS and authentication:

   a) Point the DNS names from customer DNS server to cluster B instead of cluster A.

Ensure that the DNS server on cluster B is the same as the DNS server or in the same DNS farm as the DNS server of cluster A. Existing client connections may break and may need to be re-established. You must unmount and remount the NFS Exports on the client.

b) Join AD server or LDAP/NIS.

Ensure that the AD and LDAP are in the same AD/LDAP farm or same server.

Phase 3—Restore Cluster A Fail Back From Cluster B To Cluster A

1. Fix the reason that caused cluster A to fail (replace hardware, replace disk, and so on), and if required reinstall FluidFS.
2. Rebuild the cluster (use the settings for cluster A that you saved earlier), format the NAS reserve, and set up the network (client, SAN, and IC) as before.
3. Log on to cluster B and set up the replication partnership between cluster B and cluster A.

   For more information on setting up replication partners, see Setting Up A Replication Partner.
4. Create replication policy for all the source volumes in cluster B to target volumes in cluster A.

   For more information on creating replication policies, see Adding A Replication Policy.

NOTE: Replication policy is a one to one match on volume base, for example:

Source volume B1 (cluster B) to target volume A1 (cluster A)

Source volume B2 (cluster B) to target volume A2 (cluster A)

…………………………

Source volume B*n* (cluster B) to target volume A*n* (cluster A)

NOTE: FluidFS 1.1 supports auto generate target volume during addition of the replication policy. For FluidFS 1.0, you must create the target volumes in cluster B and make sure that the volume size is big enough to accommodate the corresponding source volume data in cluster A.

5. In the NAS Manager web interface, select **Data Protection** → **Replication** → **NAS Replication** and click **Replicate Now** for all the volumes in cluster B (B1, B2, .., B*n*).

   If the replication fails, fix the problems encountered and restart the replication process. Ensure that all the volumes are successfully replicated to cluster A.
6. Delete the replication policy for all the volumes (B1, B2, .. B*n*) and apply source volume configuration from cluster B to cluster A.

   Repeat this procedure to delete all the replication policies and bring all target volumes in cluster A to standalone volumes.
7. Log on to cluster A.
8. From the NAS Manager web interface, restore the NAS system configuration from cluster B.

   For more information on restoring the NAS system configuration, see Restoring Cluster Configuration.

   This changes cluster A global configuration settings, like, protocol setting, time setting, authentication parameters, and so on to cluster B settings.

NOTE: If system configuration restore fails, manually set them back to the original settings (use the settings for cluster A that you saved earlier).

   Cluster A is restored to its original settings.
9. Start using cluster A to serve client requests.

   Administrators must perform the following steps to set up DNS and authentication:

   a) Point the DNS names from customer DNS server to cluster A instead of cluster B.

   Ensure that the DNS server on cluster A is the same as the DNS server or in the same DNS farm as the DNS server of cluster B. Existing client connections may break and need to re-establish during this process.

b) Join AD server or LDAP/NIS.

Ensure that the AD and LDAP are in the same AD/LDAP farm or same server.

10. Build up replication structure between source cluster A and backup cluster B, to set up replication policy between cluster A and cluster B, use cluster B volumes as replication target volumes, to prepare for next disaster recover.

Backing Up And Restoring Data

NOTE: It is recommended that you back up your data at regular intervals.

The NAS cluster solution supports backup and restore using Network Data Management Protocol (NDMP). An NDMP agent installed on the NAS cluster solution 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 must be configured to be able to access the NAS appliance using the LAN or client network. The NAS cluster solution does not use a dedicated address for backup operations, any configured LAN or client network address can be used for backup and restore operations.

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

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

Backing Up Replication Target NAS Volumes

When performing a backup of replication target volumes, FluidFS does not create a dedicated NDMP snapshot. FluidFS instead uses the base replica snapshot from the last successful replication.

If the schedules for replication and NDMP backup overlap, it is possible that while NDMP backup of target volumes is in process, a new replication operation will execute and complete before the NDMP backup has finished. In this case the replication operation deletes the previous base replica snapshot and create a new base replica.

CAUTION: Doing this terminates the NDMP backup. To avoid this scenario schedule your replication and backup operations such that replication completes before the NDMP backup starts.

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.

Supported Applications

The NAS cluster solution is certified to work with the following DMAs:

- Symantec BackupExec 2010 R3 and Symantec BackupExec 2012
- Symantec NetBackup 7.0 or later
- CommVault Simpana 9.0 or later

Enabling NDMP Support

NDMP backups are performed using the client network. The DMA must be configured to access one of the client VIPs (or a DNS name) of the NAS cluster.

NOTE: Before enabling the NDMP support, a client VIP must be configured on the system. Verify if the client VIP is configure by selecting **System Management** → **Network** → **Subnets** and verifying if the **Primary** subnet is set.

To enable NDMP support:

1. Select **Data Protection** → **NDMP** → **NDMP Configuration.**
   The **NDMP Configuration** page is displayed.
2. Select **Enable NDMP**.

NOTE: Initially, the **backup_user** password is not set. After changing the user name, or using the default, the password must also be set.

NOTE: By default, the NDMP client port is 10000.

3. In **DMA server**, enter the IP address of an authorized DMA server.

NOTE: DNS names are not supported.

4. Click **Save Changes**.

Changing NDMP Password And Backup Username

A username and password are required when configuring an NDMP server in the DMA. By default, the username is **backup_user**. The default password is randomized and must be changed prior to using NDMP.

To change the NDMP password:

1. Select **Data Protection** → **NDMP** → **NDMP Configuration.**
   The **NDMP Configuration** page is displayed.
2. If required, in **Backup username**, change the current backup username and click **Save Changes**.
   The backup username is changed.
3. Click **Change Backup User Password.**
   The **Change Password** window displays the current backup username.
4. In **admin password**, enter the existing administrator password.
5. Under the backup username, in **New password**, enter the new password.
6. In **Retype password**, enter the exact password that you entered in **New password**.
7. Click **Save Changes**.

Modifying DMA Servers List

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

Adding DMA Servers

To add a DMA server to the list:

1. Select **Data Protection** → **NDMP** → **NDMP Configuration.**

The **NDMP Configuration** page is displayed.

2. If no empty **DMA server** fields are available, click **Add DMA server**.
   An additional **DMA server** field is added.
3. In the empty **DMA server**, enter the IP address of the DMA server.

NOTE: DNS names are not supported.

4. Click **Save Changes**.

Removing DMA Servers

To remove a DMA server from the list:

1. Select **Data Protection → NDMP → NDMP Configuration.**
   The **NDMP Configuration** page is displayed.
2. Select the appropriate DMA server and click **Remove DMA Server**.

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 NAS cluster solution exposes backup volumes at the following path:

/<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 NAS cluster solution can be viewed on the NDMP Active Jobs page. To view the active NDMP jobs, select **Data Protection → NDMP → NDMP Active Jobs** or **Monitor → NDMP Active Jobs.**

Terminating An Active NDMP Job

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

1. Select **Data Protection → NDMP → NDMP Active Jobs.**
   The **NDMP Active Jobs** page displays all the active NDMP jobs.
2. Select the session to be terminated.
3. Click **Kill Active NDMP Job**.

NOTE: Multiple sessions can be selected at a time.

Using Antivirus Applications

The NAS cluster solution contains integration with industry standard ICAP-enabled antivirus software to ensure files written from CIFS clients are virus-free. The antivirus host must run Symantec ScanEngine 5.2, which is ICAP-enabled.

Viewing Existing Antivirus Hosts

To view the antivirus hosts defined for the system, select **Data Protection** → **Antivirus** → **Antivirus Hosts,** the **Antivirus Hosts** page displays the details of the antivirus hosts already defined, its IP address (or name), and the ICAP port.

Adding Antivirus Hosts

It is recommended to define multiple antivirus hosts to achieve high-availability of virus scanning, and reduce the latencies for file access. If no antivirus host is available, file access might be denied causing lack of service.

To enable the Antivirus option:

1. Select **Data Protection** → **Antivirus** → **Antivirus Hosts.**
   The **Antivirus Hosts** page displays a list of existing antivirus hosts.
2. If no empty **Antivirus host** fields are available, click **Add**.
   An additional **Antivirus host** field is added.
3. In **Antivirus host**, enter the IP addresses (or name) of the antivirus host.
4. In **Port**, enter the port on which the host ICAP protocol is listening.
   By default, the ICAP port is 1344.
5. Click **Save Changes**.

Removing An Antivirus Host

To delete a host from the list of antivirus hosts:

1. Select **Data Protection** → **Antivirus** → **Antivirus Hosts.**
   The **Antivirus Hosts** page displays a list of existing antivirus hosts.
2. From the list of available antivirus hosts, select the appropriate antivirus host and click **Delete**.

Enabling Antivirus Support Per CIFS Share

Antivirus support is available on per-CIFS share basis. To enable antivirus support for CIFS shares:

1. Click **User Access** → **Shares** → **CIFS Shares.**
2. Click on the CIFS share you would like to enable antivirus 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 are checked for viruses (optional).
7. Configure the exclusion list (optional).
8. Click **Save Changes**.

5

Managing The FluidFS NAS Solution

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

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

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 NAS cluster solution 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.

Viewing The Defined Subnets

To view the defined subnets, select **Cluster Management** → **Network** → **Subnets,** the **Subnets** page displays the list of existing subnets.

Adding A Subnet

1. Select **Cluster Management** → **Network** → **Subnets.**
   The **Subnets** page displays the list of existing subnets.
2. Click **Add**.
   The **Add/Edit Subnet** page is displayed.

3. In **Subnet name**, enter a relevant name for the subnet.
4. From the **Physical network** list, select the relevant network.
5. In **Subnet mask**, enter the subnet mask address.
6. Specify the VLAN ID for the subnet, if applicable.

NOTE: When a VLAN spans multiple switches, the **VLAN ID** is used to specify which ports and interfaces to send broadcast packets to.

7. In **Management console VIP**, enter the IP address for the system management console.
8. In **Private IP**, enter the IP addresses of the individual system controllers for each controller.

NOTE: These IP addresses are used for controller management by the technical support.

9. In **VIP address**, enter the virtual IP addresses for one or more clients.

NOTE: These VIPs are used to access files on the system.

NOTE: The optimal number of virtual IP addresses (VIPs) depends on your network configuration, and more information is available in the online help.

10. Click **Save Changes**.

Modifying A Subnet

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.

1. Select **Cluster Management → Network → Subnets.**
   The **Subnets** page displays the list of existing subnets.
2. From the list of displayed subnets, under the Subnet Name column, click the appropriate subnet.
   The **Add/Edit Subnet** page for the selected subnet is displayed.
3. Change the parameters as required.
4. Click **Save Changes**.

Removing A Subnet

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

1. Select **Cluster Management → Network → Subnets.**
   The **Subnets** page displays the list of existing subnets.
2. From the list of displayed subnets, select the appropriate subnet and click Delete.

Managing Administrator Users

Administrators can manage the Dell Fluid File System using the Dell Fluid File System CLI or the Web interface.

Viewing Administrator Users

To view existing administrator users, select **Cluster Management → General → Administrators,** the **Administrators** page displays a list of currently defined administrators.

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. In the NAS Manager, select **Cluster Management** → **General** → **Administrators.**
   The **Administrators** page is displayed.
2. Click **Add**.
   The **Add Administrator** page is displayed. By default, the **Properties** tab is displayed.
3. In **User name**, enter a name for the administrator.
4. In **Password**, enter a password containing at least six characters.
5. In **Retype password**, enter the exact password that you entered in the password field.

NOTE: If the password is too simple you are prompted to enter a more complex password.

6. In **User ID**, enter the UID or use the default UID provided by the system.
7. From the **Level** list, select the permission level for the administrator. You can select, **3-Administrator** or **4-View only**.

NOTE: You can only define other administrators with permission levels that are hierarchically lower than your own.

8. In **E-mail address**, enter the e-mail address of the administrator in each available E-mail address field.
   The system uses this E-mail address to send alerts to the administrator. You can add additional E-mail addresses by clicking **Add Email address**. You can set the types of E-mail alerts to send to the administrator using the **Filters** tab.
9. Select the **Filters** tab to define filter rules for SNMP traps.
10. Define the minimum trap severity that is sent for each category of traps.

NOTE: The default option is to send **Major** traps for all categories.

11. Click **Save Changes**.

Modifying An Administrator

1. Select **Cluster Management** → **General** → **Administrators.**
   The **Administrators** page displays the list of currently defined administrators.
2. From the list of available administrators, under the **User Name** column, click the relevant administrator.
   The **Edit Administrator** page is displayed. By default, the **Properties** tab is selected.
3. You can change the **Level** and **Email address** for the selected administrator.
4. In the **Filters** tab, you can change the filter rules for SNMP traps for each category.
5. Click **Save Changes**.

Changing The Administrator Password

WARNING: For Dell Compellent FS8600, if you change the administrator password, the connection between the Enterprise Manager and cluster fails. To re-establish the connection between Enterprise Manager and the cluster, in Enterprise Manager, click Reconnect to FluidFS Cluster after changing the admin password.

1. Select **Cluster Management** → **General** → **Administrators.**

   The **Administrators** page displays the list of currently defined administrators.
2. From the list of available administrators, under the **User Name** column, click the relevant administrator.

   The **Edit Administrator** page is displayed. By default, the **Properties** tab is selected.
3. Click **Change Password**.

   The **Change Password** window is displayed.
4. In **admin password**, enter the current password for the selected administrator.
5. Under **admin**, in **New password**, enter the new password.
6. In **Retype password**, enter the exact password that you entered in the **New password** field.
7. In the **Change Password** window, click **Save Changes**.

   The **Edit Administrator** page is displayed.
8. Click **Save Changes**.

Removing An Administrator

1. Select **Cluster Management** → **General** → **Administrators.**

   The **Administrators** page displays the list of currently defined administrators.
2. From the list of available administrators, select the relevant administrator and click **Delete.**

Managing Local Users For CIFS And NFS Access

NOTE: Skip this section if your site is configured with an external NIS/LDAP database.

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

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

To allow the NAS cluster solution to use local user definitions:

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

   The **Identity Management Database** page is displayed.
2. Select **Users are not defined in an external user database**.
3. For CIFS users, select **Cluster Management** → **Protocols** → **CIFS Configuration**.

   The **CIFS Protocol Configuration** page is displayed.
4. Select the mode that is used to authenticate the user’s identity. You can select:

   – **Authenticate users' identity via Active Directory and local users database**

   – **Authenticate users' identity via local users database**
5. To manage the **Local Users** list, select **Cluster Management** → **Authentication** → **Local Users.**

Viewing Local Users

To view the list of existing users, select **Cluster Management** → **Authentication** → **Local Users**, the **Local User** page displays the list of existing users.

Adding Local Users

1. Select **Cluster Management** → **Authentication** → **Local Users.**
   The **Local Users** page is displayed.
2. Click **Add.**
   The **Add User** page is displayed. By default, the **General** tab of the **Add User** page is displayed.
3. In **User name**, enter the local user's name.
4. In **Password**, enter the password (consisting of at least 6 characters) to assign to the local user.
5. In **Retype password**, enter the same password that you entered in the **Password** field.
6. In **User ID**, enter a unique UNIX UID or use the default ID provided by the system.
7. In **Primary group**, either:
   - Enter the name of the primary group for the local user.
   - Click the browse button to browse to the list of primary groups.
   - Use the default group provided by the system.
8. In **Additional groups**, either enter the name of another group to which the local user belongs or click the browse button to browse to the list of groups (optional).

NOTE: You can add more than one group.

9. Select the **Advanced** tab for additional and optional fields.
10. In **Real name**, enter the real name of the user.
11. In **Remarks**, enter comments about the user (optional).
12. Click **Save Changes.**

Modifying Local Users

1. Select **Cluster Management** → **Authentication** → **Local Users.**
   The **Local User** page displays a list of existing local users.
2. From the list of existing users, under **User Name,** click the appropriate **User Name**.
   The **Edit User** page is displayed. By default the **General** tab is selected.

NOTE: You can only change the group information for the selected user in the **General** tab.

3. In **Primary group**, either:
   - Enter the name of the primary group for the local user
   - Click the **Browse** button to browse to the list of primary groups.
   - Use the default group provided by the system.
4. In **Additional groups**, either enter the name of another group to which the local user belongs or click the **Browse** button to browse to select from the list of groups (optional).
5. Select the **Advanced** tab for additional and optional fields.
6. In **Real name,** enter the real name of the user.

7. In **Remarks**, enter comments about the user (optional).
8. Click **Save Changes.**

Deleting Local Users

1. Select **Cluster Management** → **Authentication** → **Local Users.**
   The **Local User** page displays a list of existing local users.
2. From the list of existing users, select the user name and click **Delete**.

Changing The Password

You can change the password of a local user from the **Edit User** page.

To change the password of a local storage user:

1. Select **Cluster Management** → **Authentication** → **Local Users.**
   The **Local User** page displays a list of existing local users.
2. From the list of existing users, under **User Name,** click the appropriate User Name.
   The **Edit User** page is displayed. By default, the **General** tab is selected.
3. In **admin password**, enter the current password for the selected administrator.
4. Under **admin**, in **New password**, enter the new password.
5. In **Retype password**, enter the exact password that you entered in the **New password** field.
6. In the **Change Password** window, click **Save Changes**.
   The **Edit Administrator** page is displayed.
7. Click **Save Changes**.

Managing Local Groups

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

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

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

Viewing Local Groups

To view the existing **Local Groups**, select **Cluster Management** → **Authentication** → **Local Groups**, the **Local Groups** page displays the list of existing local groups.

Adding A Local Group

1. Select **Cluster Management** → **Authentication** → **Local Groups.**
   The **Local Groups** page is displayed.
2. Click **Add.**
   The **Add Group** page is displayed.

3. In **Group Name,** enter the name of the group.
4. In **Group ID**, enter the identification number of the group.

NOTE: Dell Fluid File System groups have ID numbers above 200.

NOTE: The group is automatically assigned the next available identification number. You can modify it if required.

5. Click **Save Changes**.

Deleting A Local Group

1. Select **Cluster Management** → **Authentication** → **Local Groups.**

   The **Local Groups** page displays a list of existing local groups.
2. From the list of existing local groups, select the appropriate local group and click **Delete**.

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.

The NAS cluster solution 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

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

   The **Identity Management Database** page is displayed.
2. Select **Users and groups are defined in a NIS database.**
3. In **Domain name**, enter the domain name of the NIS database.

4. In any blank **NIS server**, enter the name or IP address of the NIS server.
5. To add an NIS server for redundancy purposes, click **Add NIS server** .

   An additional **NIS server** is displayed in the list of NIS servers.
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**.

Enabling User Authentication Through An LDAP Database

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

   The **Identity Management Database** page is displayed.
2. Select **Users and groups are defined in an LDAP database**.
3. In **LDAP server**, enter the name or IP address of the LDAP server.
4. In **Base DN,** enter the base DN (distinguishable name) that you want to use for authentication purposes.

   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
   ```
5. Click **Save Changes**.

Disabling The Use Of An External UNIX Identity Management Database

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

   The **Identity Management Database** page is displayed.
2. Select **Users are not defined in an external user database**.
3. Click **Save Changes**.

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 domain.

Synchronizing The NAS Cluster Solution With The Active Directory Server

If your site uses Active Directory and the NAS cluster solution is part of the Windows network, synchronize the time clock to the Active Directory server. To synchronize the time clock to the Active Directory server, select **Cluster Management → General → Time Configuration.**

Configuring The Active Directory Service

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

The **System Identity** page is displayed. This page shows the current configuration and whether the NAS cluster solution is already joined to an Active Directory domain.

2. In **System name**, enter the system name.

   This name identifies the Dell Fluid File System in alerts that the system sends and is also the default name for the Dell Fluid File System when you configure Active Directory.

3. Select **The system is a member of a Microsoft Windows Network** if you want Dell Fluid File System to join an Active Directory domain and proceed to the next step. Otherwise, leave this field unselected and click **Save Changes**.

4. In **System NetBIOS name**, enter the Dell Fluid File System NetBIOS name that is displayed in the network neighborhood.

   This name is limited to 15 characters. Use the system name unless otherwise instructed.

5. In **Domain**, enter the domain to which Dell Fluid File System belongs.

   Use the fully qualified domain name (FQDN), not the NetBIOS domain name. For example: mydomain.company.com

6. In **User name**, enter the administrator user name to be used to join the Active Directory domain.

NOTE: This user name is not saved in Dell Fluid File System.

7. In **Password**, enter the administrator password.

NOTE: This password is not saved in Dell Fluid File System.

CAUTION: Advanced Configuration must be deselected, unless otherwise instructed by Dell support. This field allows configuring more Active Directory related parameters.

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

8. Click **Save Changes**.

Network Configuration Overview

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: You must configure CIFS to authenticate users after joining the Domain. To authenticate users, **Cluster Management → Protocols → CIFS Configuration.** Select the radial for **Authenticate users' identity using Active Directory and local user database**.

NOTE: The Client Access VIP is configured during initial configuration using the **Dell NAS Initial Deployment Utility**. You can see the address you configured by going to the NAS Manager **Cluster 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 or more 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.

Client users access the system through a variety of network topologies. Depending on the physical capabilities of the network infrastructure, the NAS cluster solution:

- 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.
- 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.

- 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 issues 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.

Performance And Static Routes

Routed networks provide an 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.

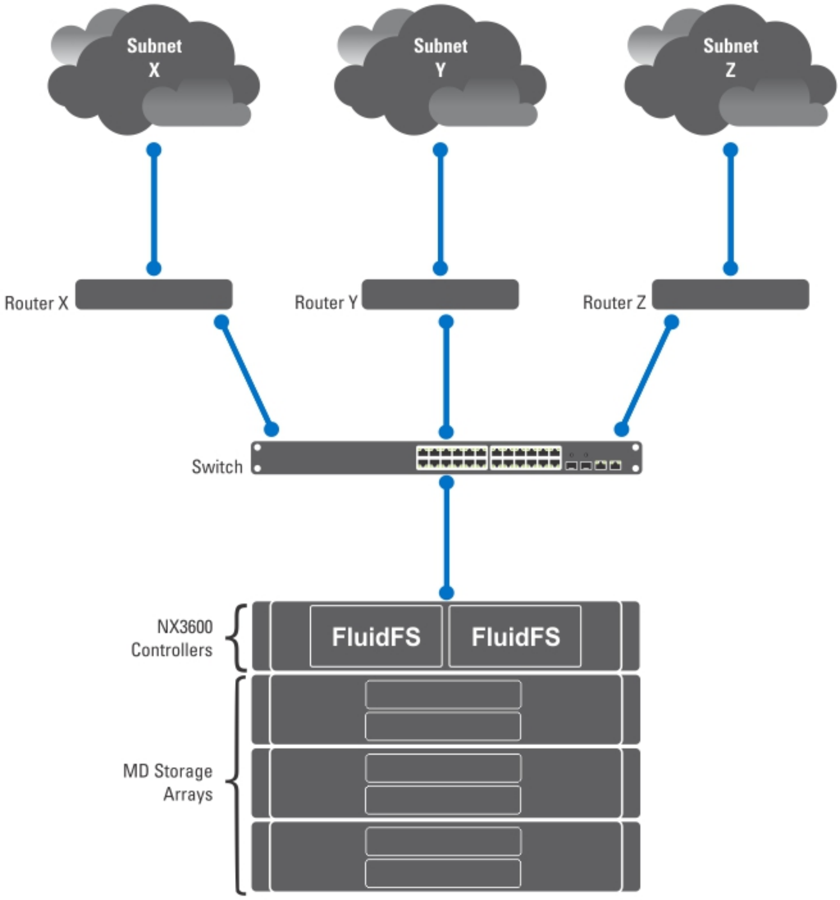

Figure 4. Network Configuration

Consider the above network, there can be only one default gateway for the system. Assume that 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. 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 must 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.

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 NAS cluster solution but within the site) to be used for name resolutions.

Viewing DNS Servers

To view a list of existing DNS servers and their parameters, select **Cluster Management** → **Network** → **DNS Configuration**, the **DNS Configuration** page displays the list of existing DNS servers and their parameters.

Adding DNS Servers And DNS Suffixes

1. Select **Cluster Management** → **Network** → **DNS Configuration.**
   The **DNS Configuration** page is displayed.
2. To add a DNS server, click **Add DNS Server**.
   A new empty row is added to the list of DNS servers.
3. Set the IP address of the client environment primary DNS.
4. To add a DNS suffix, click **Add DNS Suffix**.
   A new empty row is added to the list of DNS suffixes.
5. Enter the DNS suffixes in order of precedence.
6. Click **Save Changes**.

Removing DNS Servers And DNS Suffixes

1. Select **Cluster Management** → **Network** → **DNS Configuration.**
   The **DNS Configuration** page displays the list of existing DNS servers and their parameters.
2. Select the appropriate DNS server and/or DNS suffix and click **Delete**.
   A message prompts you that the deleted DNS server saves all other changes that have been made.
3. Click **OK**.

Managing Static Routes

To minimize hops between routers, static routes are suggested in routed networks when there are multiple direct paths from the NAS cluster solution to various routers.

Viewing Static Routes

Select **Cluster Management** → **Network Management** → **Static Routes,** the **Static Routes** page displays 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.

1. Select **Cluster Management** → **Network Management** → **Static Routes.**

   The **Static Routes** page is displayed.
2. Click **Add**.

   The **Add Static Routes** page is displayed.
3. From the **Network** list, select the network on which the subnet is accessible.
4. In **Gateway IP**, enter the IP address of the gateway to the subnet that best provides access to the destination subnet.
5. In **Destination Subnet**, enter the subnet of the destination to access through a static route.
6. In **Netmask**, enter the netmask to separate this subnet from other subnets.
7. Click **Save Changes**.

Modifying A Static Route

1. Select **Cluster Management** → **Network Management** → **Static Routes.**

   The **Static Routes** page displays the list of currently defined static routes.
2. From the list of existing static routes, select the appropriate static route and click **Edit**.

   The properties of the selected static route are displayed.
3. Modify the properties as required.

Deleting A Static Route

1. Select **Cluster Management** → **Network Management** → **Static Routes.**

   The **Static Routes** page displays the list of currently defined static routes.
2. From the list of existing static routes, select the appropriate static route and click **Delete**.

Defining File System Protocols

File system protocols are networking protocols that provide file system sharing services. The NAS cluster solution 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 NAS cluster solution system. You can also enable Linux users to access the system using the CIFS protocol, and authenticate them through NIS, LDAP or the NAS cluster solution local users.

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.

Configuring General CIFS Parameters

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

   The **CIFS Protocol Configuration** page is displayed. By default, the **General** tab is selected.
2. Select **Allow clients to access files via the CIFS protocol** to enable the CIFS file sharing protocol.
3. In **System description**, enter a short description for the server.

   This description is displayed in the Windows Explorer title.
4. Choose the way the system authenticates users' identity. You can select one of the following methods:

   – To authenticate users using the Active Directory domain to which the system is joined, select **Authenticate users' identity via Active Directory and local user database**.

   – To authenticate users using an internal user database, Select **Authenticate users' identity via local users database**.
5. Click **Save Changes**.

   This restarts all user connections.

Denying Users From Accessing Files Using The CIFS Protocol

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

   The **CIFS Protocol Configuration** page is displayed. By default, the **General** tab is selected.
2. Deselect **Allow clients to access files via the CIFS protocol**.
3. Click **Save Changes**.

   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 NAS cluster solution.

To configure advanced CIFS parameters:

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

   The **CIFS Protocol Configuration** page is displayed. By default, the **General** tab is selected.
2. Select the **Advanced** tab.
3. From the **DOS Code Page** list, select the character set used by clients that do not support UNICODE.
4. From the **Unix Charset** list, Choose the version of UTF8 character set that is used by the system. This enables text to be properly converted to the character sets of the connected client.

5. Click **Save Changes**.
   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

1. Select **Cluster Management** → **General** → **Time Configuration.**
   The **Time Configuration** page is displayed.
2. From the **Time zone** list, select the correct time zone for the region that the cluster is located in.
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.

To configure the current date and time manually:

1. Select **Cluster Management** → **General** → **Time Configuration.**
   The **Time Configuration** page is displayed.
2. Select **There is no NTP server to synchronize time with**.
3. In **Date**, enter the current date.

NOTE: Use the format: DD/MM/YYYY, where DD indicates the day, MM indicates month, and YYYY indicates the year. For example, *30/05/2012*.

4. In **Time**, enter the current time.

NOTE: Use the format: HH:MM:SS, where HH indicates a 24-hour format. For example, *17:38:23*.

5. 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. Click **Cluster Management** → **General** → **Time Configuration.**
   The **Time Configuration** page displays a list of available NTP servers.
2. Select the appropriate NTP server and click **Delete NTP server(s)**.
3. Click **Save Changes**.

Synchronizing The NAS Cluster Solution 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 NAS cluster solution to be synchronized with a local NTP server or an NTP server on the Internet:

1. Select **Cluster Management** → **General** → **Time Configuration.**
   The **Time Configuration** page is displayed.
2. Select **Time should be synchronized with an NTP server.**
3. Select **NTP server**.
4. In the **NTP server**, enter the name of the local NTP server or Internet NTP server.
5. 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**.

Managing Licenses

Installed licenses can be viewed and managed from the NAS Management software.

Viewing Licenses

To view installed licenses, select **Cluster Management** → **General** → **Licensing,** the **Licensed Features** page displays a list of installed licenses.

Adding A License

The feature(s) from the license file is displayed on the licensing screen after the system validates the file and refreshes the screen.

To add a license:

1. Select **Cluster Management** → **General** → **Licensing.**
   The **Licensed Features** page is displayed.
2. In **Upload the license XML file**, enter the path of the license XML file or click the **Browse** button to navigate to the license XML file location.
3. Click **Upload** to upload the license file.
   The feature(s) from the license file is/are displayed on the licensing screen after the system validates the file and refreshes the screen.

Removing A License

⚠ **CAUTION: Removal of licenses must only be performed at the direction of Dell Technical Support.**

The feature(s) from the license file are displayed on the licensing screen after the system validates the file and refreshes the screen.

1. Select **Cluster Management** → **General** → **Licensing.**

   The **Licensed Features** page displays a list of installed licenses.

2. From the list of installed licenses, select the appropriate feature and click **Delete License for feature**.

Configuring E-mail Parameters On PowerVault NX3500/NX3600/ NX3610 NAS Solutions

NOTE: This feature is not supported on Dell Compellent FS8600 NAS Solutions. Dell Compellent FS8600 utilizes Enterprise Manager for all e-mail alerts. For more information, see the *Enterprise Manager Users Guide*.

Dell Fluid File System uses e-mail as the basis for alerting and remote support. You can determine who receives one or all of the following types of messages that Dell Fluid File System sends:

- Heartbeats—Heartbeats are sent every five minutes to the e-mail recipient. This enables the remote support team to respond to system failures.
- System logs—System logs are periodically sent to the e-mail recipient. This enables the remote support team to identify mild system errors and correct them if necessary.
- Alerts—Alert e-mail messages that report on the system service.

You can add additional recipients if necessary. If you add the Administrator as a recipient, it is recommended that you configure the system to only send them system alerts.

You can also manually request the system to send a system information report, as required.

Viewing SMTP Servers

To view the list of configured SMTP servers, select **Cluster Management** → **Monitoring Configuration** → **Email Configuration**, the **Email Configuration** page displays the list of configured SMTP servers.

Configuring An SMTP Server

SMTP servers let you send e-mail to users who are not in the same domain. An SMTP server lets you forward trap messages from the customer's domain to a remote support mailbox.

To add SMTP servers:

1. Select **Cluster Management** → **Monitoring Configuration** → **Email Configuration.**

   The **Email Configuration** page is displayed. By default, the **General** tab is selected.

2. Click **Add SMTP server**.

   The **Add SMTP server** page is displayed.

3. In **SMTP server**, enter the IP address or name of the e-mail server.

4. In **Description**, enter a description of the server.

5. Select **The SMTP server requires authentication** to authenticate all e-mail on the SMTP server using the username and password that you enter in **User name** and **Password**.

6. Click **Save Changes.**

Modifying An SMTP Server Configuration

1. Select **Cluster Management** → **Monitoring Configuration** → **Email Configuration.**

   The **Email Configuration** page displays a list of existing SMTP servers.
2. From the list of existing SMTP servers, under **SMTP server**, click the appropriate SMTP server.

   The **Edit SMTP server** page is displayed.
3. In **SMTP server**, enter the updated IP address or name of the e-mail server.
4. In **Description**, enter the updated description of the server.
5. Select **The SMTP server requires authentication** to authenticate all e-mail on the SMTP server using the user name and password that you enter in **User name** and **Password**.
6. Click **Save Changes.**

Delete An E-mail Sender

1. Select **Cluster Management** → **Monitoring Configuration** → **Email Configuration.**

   The **Email Configuration** page displays a list of existing SMTP servers.
2. From the list of existing SMTP servers, select one or more SMTP server(s) and click **Delete SMTP Server(s)**.

Configuring An E-mail Sender

Some e-mail systems prevent e-mail messages from being sent if the sender does not belong to a specific domain. You can configure the system to send all e-mail messages from a specific user in the required domain.

To determine the e-mail address that must be displayed in the **From** field when sending e-mail messages, In **Send E-mails From**, type an e-mail address belonging to the required domain.

Configuring Advanced Options

1. Select **Cluster Management** → **Monitoring Configuration** → **Email Configuration.**

   The **Email Configuration** page is displayed. By default, the **General** tab is selected.
2. Click the **Advanced** tab.

   The **Add SMTP server** page is displayed.
3. In **Maximum mail size (kB),** enter the maximum size of each E-mail message.
4. In **Messages sent in intervals of (seconds)**, enter the maximum time an alert may wait before it is sent.
5. Click **Save Changes.**

Configuring SNMP

Dell Fluid File System supports the Simple Network Management Protocol (SNMP), a commonly used network management protocol that allows SNMP-compatible management functions such as device discovery, monitoring, and event generation.

The SNMP page allows you to configure SNMP-compatible management functions.

To configure SNMP properties:

1. Select **Cluster Management** → **Monitoring Configuration** → **SNMP Configuration.**

The **SNMP Configuration** page is displayed. By default, the **Properties** tab is selected.

2. In **System contact**, enter a name for the required contact person.
3. In **System location**, enter a description for the location of the system.
4. In **Read community**, enter the SNMP community for devices reading SNMP variables from Dell Fluid File System or use the default value.
5. In **Trap recipient**, enter the IP address or host name of the Network Management Server or of another host that receives the Dell Fluid File System-generated SNMP traps.
6. To add additional trap recipients, click **Add.**

   The trap recipient is added to the list.
7. Enter the IP address or host name of the network management server.
8. To remove a trap recipient from the list, select the appropriate trap recipient and click **Delete**.

   The trap recipient is removed from the list.
9. Select the **Filter** tab and select the minimum trap severity that must be sent, for various categories of traps.

NOTE: The default is to send all traps for all categories.

10. Click **Save Changes**.

6

Troubleshooting

Troubleshooting CIFS Issues

Misconfigured AV Host Settings Result In Access Denied To CIFS files

Description	The Dell NAS cluster solution supports antivirus scans on a per CIFS share basis. When a file on a share is opened by a client application the NAS cluster solution sends the file to an antivirus host to be scanned. 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 NAS cluster solution, 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 NAS cluster solution 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. Verify that you set the ACL's as the owner of the files, directories, and shares. In case you cannot redefine your ACLs since you currently do not have permissions, perform the following steps:

1. Restore the files from snapshots or backup.
2. 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.
3. 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 NX3600 appliance is limited to 200 concurrent CIFS connections and each NX3610 and FS8600 is limited to 1500 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 another NAS appliance. • 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 client access VIP and share name: **\\<Client_VIP>\<CIFS_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 must 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.
- appliance not responding due to port mapper failure - RPC timed out or input/output error.
- appliance 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 appliance could not recognize the client system through NIS, or the appliance does not accept the identity you provided.
- The NAS cluster solution 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 NAS appliance.
- 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 appliance not responding due to a port mapper failure:

- Check the NAS cluster solution status.

- Check the network connection by trying to NFS mount from some other system.
- Verify if other users experience the same problem.

If the appliance 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 appliance exported file systems using the command:
  `showmount -e <FluidFS 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 NAS cluster solution 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:
3. `% showmount -e <Server name/IP>`
4. `Export list for <Server name/IP>:`
5. `/abc 10.10.10.0`
6. `/xyz 10.10.10.0`
7. 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:
3. Try pinging the NAS from a client located in the same subnet as the NIS/LDAP server.
4. Try pinging the NIS/LDAP server from a client located in the same subnet as the NAS.
5. If a packet loss is evident on one of the above, resolve the network issues in the environment.
6. 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 a mount path that does not exists 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 must 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 NAS cluster solution which is down. Verify the source and destination, both the source and destination have the same number of NAS controllers.

NOTE: You cannot replicate between a 4 node NAS cluster and 2 node NAS cluster.

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 must 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 must check if the file system is down in the destination system using the monitoring section of the NAS Manager. If the NAS cluster solution file system is not responding, administrators must 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 must 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 must 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 must 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 must 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 source NAS cluster is higher than the system version of the destination cluster.

Workaround

Administrators must 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 must 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 must verify that the replication 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 must check if the NAS cluster solution is down in the source system, by checking the monitoring section of the NAS Manager. If the NAS cluster solution is down, the administrators must start the file 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 must check the file 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 must verify that the replication 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 NAS cluster solution 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 must be listed. Click the group and then click the **Set Primary Group** button.

Now quotas takes 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 NAS cluster solution 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 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 must 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: 3. Verify there is enough free space on the NAS volume or expand it. 4. 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 NAS cluster solution 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 NAS cluster solution 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 NAS cluster solution. 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 NAS cluster solution 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 NAS cluster solution subnet and verify it responds.
2. Issue a request to the server from a client on the NAS cluster solution 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 NAS Cluster Solution

Description

Users (new or old), accessing from specific network(s), cannot access the NAS cluster solution.

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 NAS cluster solution 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 NAS cluster solution controller is configured to the correct DNS server.
3. Contact DNS server administrator to verify the DNS record creation.

Determining The IQN Of The NAS Cluster Solution Controllers Using CLI

Description

Determining the IQN of the NAS cluster solution controllers using CLI.

Workaround

Using an ssh client and the NAS Management VIP, log in to the NAS cluster 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 NAS cluster solution 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 NAS cluster solution 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.
- Wrong IP address was specified in the backup job.

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 must not exceed 20 snapshots per hour per system.
- Check the total number of snapshots in the system. If the number is in thousands, delete a few snapshots and retry.
- Ensure the Client virtual IP address is specified in the backup job.

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.
4. On the NAS Manager, the **Enabled** check box must be checked.
5. In the NAS CLI, type `view` and ensure that **State** is set to **Enabled**.
6. If NDMP is not enabled, enable it.
7. Verify that backup application IP address is configured in NDMP.
8. On the NAS Manager, the DMA server list must include the IP address of the backup application.
9. 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 `data-protection ndmp configuration set-Password <new_password>` 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 NAS cluster solution 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 must 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 Dell NAS Initial Deployment Utility (IDU).
- 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 NAS IDU:

1. Verify that the MD discovery IP used while running the NAS IDU 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:`system maintenance luns configuration iscsi-view`

This command shows the MD discovery IP.

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:

To change the discovery IP in the CLI, run the following command:

```
system maintenance luns configuration
iscsi-set -iSCSIDiscoveryIPs <IP
Address> none none
```

After the command is complete, refresh the host port identifiers. You can now run the configuration wizard from the NAS Manager again.

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 NAS Manager are virtual disks in the Modular Disk Storage Manager.

Workaround

Open the NAS Manager web interface and go to **Cluster Management** → **Maintenance** → **Add Luns.** This page displays all LUNs that the NAS cluster solution has access to (assigned to the NAS cluster solution 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.

NAS IDU Failed To Discover Any Controllers

Description

NAS IDU failed to discover any controllers.

Cause

IPV6 may not be enabled on your workstation.

Workaround

Enable IPV6 support on your management workstation.

Attach Operation Fails

Description

The operation to attach the controller to NAS cluster fails.

Workaround

- Connect a keyboard and monitor to the controller that failed the attach operation, and view the error message to determine why the attach operation failed.
- Verify the following:
  - While the controller was detached, the IP assigned to it on the client network was not allocated to another host. While the controller is detached, it loses its identity, including IP addresses. When it is attached, its identity is applied back to the controller, including the IP addresses.
  - Verify the default gateway is in the **Primary** subnet by using the NAS Manager. In **Cluster Management** →

Network Configuration view the default gateway. In **Cluster Management → Subnets** to view the **Primary** subnet on the client network. If the default gateway is not in the **Primary** subnet, change the default gateway. For attach to succeed, the default gateway must be **pingable**.

- After an attach operation fails, the controller must manually be reset to standby mode. This is done by connecting a keyboard and monitor to the controller that failed attach, and pressing the system identification button key ⓘ, as directed by the on-screen instructions.

Controller Taking Long Time To Boot Up After Service Pack Upgrade

Description

The controller takes a long time to boot up after upgrading the service pack of the controller firmware.

Workaround

- Connect a keyboard and monitor to the controller that is taking a long time to boot up.
- If the system is booting, and is at the boot phase , let the upgrades finish. This can take up to 60 minutes to complete.
- Do not reboot the controller manually if it is in the boot phase **Executing System Upgrades**.

Troubleshooting Dell NAS Initial Deployment Utility (IDU) Issues

Error Received While Running The Dell NAS Initial Deployment Utility

Description

Error occurred while running the Dell NAS Initial Deployment Utility (IDU).

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. Verify that the management station running **NAS IDU** has a network connection to the client switch of the NAS cluster.

NOTE: It is mandatory that there must be no router connecting the NAS controllers and the system running NAS IDU.

2. Check if IPv6 is enabled on the management station where the NAS IDU is running.
3. Connect a USB keyboard and monitor to the NAS cluster controllers and verify that there are repeated messages printing the controller MAC address with a message stating **Press "i" -re-install standby node"**.

If the failure is in the configuration NAS cluster page:

1. Capture the failure message screenshot from the NAS IDU window during clusterization.
2. Collect the cluster configuration file, the NAS IDU log file, and the result file from the installation directory and zip the config folder from the installation directory.
3. The NAS IDU must 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 IDU.
5. If the failure still persists, collect all the files in a bundle package and contact Dell support.

Cannot Launch Dell NAS Initial Deployment Utility (IDU)

Description	Cannot launch Dell NAS Initial Deployment Utility.
Cause	Probable causes maybe: • NAS Initial Deployment Utility installer failed to install. • JAVA runtime environment is not properly installed.
Workaround	Perform the following: • Determine if the NAS ID Utility installer completed successfully. • Check to see if the minimum of JRE1.6x is installed successfully. • On Microsoft Windows, run java -version from command console to display a valid JRE version.

7

Maintaining The NAS Cluster Solution

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 FluidFS NAS Solutions Owner's Manual* on **support.dell.com**, for information on hardware service and maintenance.

Shutting Down The NAS Cluster Solution

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 **Cluster Management** → **Maintenance** → **System Stop/Start.**

   The **System Stop/Start** page displays the system status.
3. From the **System action to perform** list, select **Stop**.
4. Click **Next**.
5. When prompted to continue with the stop procedure, click **OK**.

   This operation copies the file-system cache to the disks and stops the file system.
6. Press and release the recessed power button at the back of each controller to shut down the controller.

NOTE: Pressing and holding the power button down for several seconds will not power down the system.

Turning On The NAS Cluster 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. Storage arrays

   – Turn on all the 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.
2. NAS cluster solution

   To start the controllers, connect each NAS controller or appliance to a power source.
3. From the NAS Manager, select **Cluster Management** → **Maintenance** → **System Stop/Start.**

   The **System Stop/Start** page displays the system status.
4. From the **System action to perform** list, select **Start**.

5. Click **Next**.

Restoring NAS Volume Configuration

Restoring the NAS volumes configuration provides an effective way for the system administrator to restore all NAS volume settings (exports, shares, snapshots schedule, quota rules, and so on) without having to manually reconfigure them. This is useful after creating a new NAS volume, after a fresh installation of the system, or after recovering a system.

A NAS volume can be restored by restoring the configuration of one NAS volume (even if it is only a saved configuration) to another NAS volume on the same system or on another system. The administrator must copy the configuration to the NAS volume from its backup or from another NAS volume.

Whenever a change in the volume's configuration is made, it is automatically saved in a format that allows you to restore it later. The configuration is stored in the **.clusterConfig** folder, which is located in the NAS volume's root folder.

This folder can be backed up, either individually, or with the volume's user data, and later restored. In order for the stored configuration in the folder to take effect, the administrator must first copy the **.clusterConfig** folder to the NAS volume to be restored and then use the Restore NAS Volume Configuration screen to apply the configuration on the NAS volume.

NOTE: When you restore a NAS volume, it overwrites and replaces the existing configuration. Users that are currently connected to the system are disconnected.

The following parameters can be restored:

- NFS exports
- CIFS shares
- Quota rules
- Snapshot schedule
- NAS volume alerting, security style and related parameters
- NAS volume name
- NAS volume size

To restore a NAS volume configuration:

NOTE: When using a backup from another system, the restore operation works only if the saved configuration was taken from a system using the same software release.

1. Select **Cluster Management** → **Maintenance** → **Restore NAS Volume Configuration.**
   The **Restore NAS Volume Configuration** page is displayed.
2. From the **Update the configuration of** list, select the system whose configuration you want to update.
3. From the **Configuration taken from system** list, select the source cluster for the configuration information.
4. Select one or more options, from the list of system-wide parameters that can be restored.
5. Click **Apply**.

Restoring Cluster Configuration

Restoring the system configuration provides an effective way for you to restore most of the system settings (such as protocol configuration and local users and groups) without having to manually reconfigure the settings. This can be useful after upgrading a system with a new software release, after a fresh installation of the system, or after recovering a system.

The system configuration can be restored by taking the configuration stored on the most updated NAS volume in the cluster and restoring in on the current system. You must copy the configuration to the NAS volume from its backup or from another system.

Whenever a change in the system's configuration is made, it is automatically saved in a format that will allow restoring it afterwards. The configuration is stored in the **.clusterConfig** folder, which is located in every NAS volume root folder.

This folder can be backed up, either individually or together with the volume's user data, and later restored. In order for the stored configuration in the folder to take effect, the administrator must first copy the **.clusterConfig** folder to one of the NAS volumes on the system and then apply the configuration to the system.

NOTE: When you restore a system configuration, it overwrites and replaces the existing configuration. Users that are currently connected to the system are disconnected.

The following parameters can be restored:

- Protocols Configuration
- Users and Groups
- User Mappings
- Monitoring configuration
- Time Configuration
- Antivirus hosts

1. Select **Cluster Management** → **Maintenance** → **Restore Cluster Configuration.**
   The **Restore Cluster Configuration** page is displayed.
2. From the **Configuration taken from system** list, select the system whose configuration you want to update.
3. Select one or more options, from the list of system-wide parameters that can be restored.
4. Click **Apply**.

Formatting File System

NOTE: Only NX3600 and NX3610 support formatting of file systems using the **NAS Manager**. For FS8600, **File System Format** is performed by **Enterprise Manager** when initially deploying the FS8600 using **Enterprise Manager**.

A file system format installs the file system on the LUNs mapped to the NAS. The format erases any existing data contained on the LUNs. A file system format must occur before a NAS Volume can be created. The file system format is usually a onetime event unless the NAS is redeployed and existing data is no longer needed.

To format the file system, select **Cluster Management** → **Maintenance** → **File System Format** and click **Format**.

Installing The Service Pack

The NAS cluster solution 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**.

Upgrading The Service Pack Using The NAS Manager

Service packs keep your Dell FluidFS NAS solution up to date with the latest firmware and software. Visit **support.dell.com** and download the latest service packs to keep your system running safely and efficiently.

WARNING: If upgrading the NAS solution software from version 1.x to version 2.x use the service pack with filename format DellFS-2.0.xxxx-SP.sh. When upgrading the NAS solution software from version 2.0 and above, use the service pack with the filename format DellFluidFS-2.0.xxxx-SP.sh.

⚠ **CAUTION: Do not modify the service pack filename.**

⚠ **CAUTION: Installing a service pack causes the NAS controllers to reboot during the installation process. This may cause interruptions in client connections. It is therefore recommended that service pack installations occur during scheduled maintenance windows.**

⚠ **WARNING: The service pack installation process is irreversible. Your system cannot be reverted back to a previous version once updated.**

To install a service pack:

1. Download the service pack from **support.dell.com/downloads**.
2. In the NAS Manager, select **Cluster Management** → **Maintenance** → **Service Pack.**
   The **Service Pack** page is displayed.
3. Click **Browse**.
4. Navigate to the latest service pack and click **Open**.
5. Click **Upload**.
6. After the service pack file is uploaded to the system click **Install**.

Expanding The NAS Cluster Storage Capacity

Expanding The NAS Pool On The Dell PowerVault NX3500/NX3600/NX3610 NAS Solution

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 NAS cluster solution.

The MD Storage Array must have additional capacity to allocate to the NAS cluster solution. For more information on disk group and virtual disk expansion, see the Modular Disk Storage Manager Administrator's Guide, at **support.dell.com/manuals**.

To expand the NAS cluster solution storage capacity:

1. Start the **NAS Manager** on your management station and log on as **admin**.

   NOTE: By default, the admin password is **Stor@ge!**.
2. Select **Cluster Management** → **Maintenance** → **Expand Luns.**
   The **Expand Luns** page is displayed.
3. Click **Expand Luns** from the lower right of the page.
   The **Status** page is displayed indicating the progress of the Expand LUNs operation.
4. Click **Finish**.

Expanding The NAS Pool On The FS8600 NAS Solution

1. Log on to the **Enterprise Manager Client**.
2. Click **Storage** from the left pane.
3. Click **Expand NAS Pool** from the top menu.
4. Enter the NAS pool size.

NOTE: Maximum limit is 512 TB per Storage Center. NAS Pools can only be expanded, shrinking a NAS pool is not allowed.

NOTE: The NAS Pool can also be expanded by adding a second Storage Center. For more information on how to add a second Storage Center array to the FluidFS cluster, see the *Enterprise Manager Administrator's Guide*.

Adding LUNs To The PowerVault NX3500/NX3600/NX3610 NAS Cluster Solution

This procedure requires the MD Storage Array has additional capacity to allocate to the NAS cluster solution. For more information on disk group and virtual disk expansion on the MD array, see the MD Series Storage Array Administrator's Guide, at **support.dell.com/manuals**.

WARNING: FluidFS supports a maximum of 32 LUNs and maximum LUN size of 32 TB; however, this limit can be exceeded using the MDSM. Exceeding the maximum number of supported LUNs may result in performance and/or access issues.

NOTE: It is recommended that you use fewer LUNs of larger size instead of using a larger number of smaller LUNs. expand existing LUNs when possible to increase the NAS pool size.

1. In MDSM, create additional virtual disks in pairs.

   NOTE: For more information, see the MD Series Storage Array Administrator's Guide, at **support.dell.com/manuals**.
2. Add the virtual disks that you just created to the cluster's **Host Group**.
3. Start **NAS Manager** on your management station and log on as **admin.**

   NOTE: By default, the admin password is **Stor@ge!**.
4. Select **Cluster Management** → **Maintenance** → **Add LUNs.**

   The page may take a few minutes to display. It runs the iSCSI discovery for all Virtual Disks/LUNs allocated to the NAS cluster solution.

   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 worldwide name.

   The **Add Luns** page is displayed.
5. Click **Add LUNs** to add the new LUNs to the NAS cluster solution. The system performs an incremental file system format on the new LUNs.

   This process takes some time depending on the size and the number of the LUNs.

   When complete, the new space is available for use.
6. Click **Finish**.

Running Diagnostics

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. The following diagnostic options are available:

- **General**
- **File System**
- **Networking**
- **Performance**
- **Protocols - collect logs**
- **Protocols - single client**
- **Protocols - single file**

To run any of these diagnostics:

1. Select **Cluster Management** → **Maintenance** → **Diagnostics.**
   The **Diagnostics** page is displayed.
2. From the **Diagnostics type** list, select the appropriate option and click **Start**.
   On completion of the diagnostics, links to the compressed archive of diagnostic files are displayed.
3. Click the appropriate link under **Download diagnostics archive** files.
   A message prompts you to either open or save the selected diagnostics file.
4. Click **Done**.

Offline Diagnostics

NOTE: Connect a keyboard 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 controllers 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.

Running The Embedded System Diagnostics

CAUTION: Use the embedded system diagnostics to test only your system. Using this program with other systems may cause invalid results or error messages.

1. Connect a keyboard, monitor, and mouse to the controller's VGA port and USB ports.
2. To reboot the controller, press and release the power button (at the back of the controller) to shut down the controller and press and release the power button (at the back of the controller) again to turn the controller back on.
3. As the system boots, press <F10>.
4. Use the arrow keys to select **System Utilities** → **Launch Dell Diagnostics.**
   The **ePSA Pre-boot System Assessment** window is displayed, listing all devices detected in the system. The diagnostics starts executing the tests on all the detected devices.
5. When completed, remove the keyboard, monitor, and mouse from the controller and reboot the controller.

Reinstalling The NAS Cluster Solution

⚠ **WARNING: Reinstalling the NAS cluster software reverts your system to factory defaults. All data on the NAS solution will be erased after performing this procedure.**

NOTE: Install the latest service pack updates after reinstalling the NAS solution software.

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

To reinstall the NAS cluster solution software:

1. Power OFF the controller using the recessed power button located at the back of the system.
2. Power ON the controller using the recessed power button located at the back of the system.
3. When the BIOS starts, press <F11> to access the pop-up menu.
4. Select **Generic Storage Device**.
5. From the pop-up menu select **FluidFS Reinstall**.
6. Type `resetmysystem` at the prompt.

   The software starts installation automatically.
7. When the software installation is complete, the controller will reboot into standby mode.

NOTE: The NAS cluster solution software cannot be installed on unsupported hardware.

Expanding The NAS Cluster

You can expand the number of appliances in a NAS cluster. Expanding the number of appliances in the existing cluster, increases the overall NAS cluster performance by allowing additional client connections and evenly distributes data flow between all controllers and back-end storage. The original appliance pair no longer dedicates all its system resources for NAS cluster operations, but reduces its system resource utilization due to other appliance pairs contributing their resources.

A NAS appliance consists of two NAS controllers within a single chassis. You can add a maximum of one appliance at a time. Depending on the Dell NAS solution version, the maximum number of appliances in a cluster solution is four (total eight controllers).

- For Dell PowerVault NX3600, the maximum number of supported appliances is 1 (2 controllers).
- For Dell PowerVault NX3610, the maximum number of supported appliances is 2 (4 controllers).
- For Dell Compellent FS8600, the maximum number of supported appliances is 4 (8 controllers).

Add a NAS appliance is a seamless operation that does not interrupt current NAS cluster operations. After the appliance(s) are successfully added, new client connections will be automatically distributed to all controllers, ensuring that there is efficient load balancing between all controllers.

Adding An Additional NAS Appliance To The NAS Cluster

Before adding an additional NAS appliance, ensure that:

- The additional NAS appliance is racked, cabled, and powered ON.
- Appliance service tags are recorded.
- New IP addresses are available (to be added to the add on appliance).

To add an additional NAS appliance:

1. Select **Cluster Management** → **Hardware** → **Add NAS Appliance Wizard.**

   The **Add NAS Appliance Wizard** is displayed.

2. Click **Next**.

   The **Add NAS Appliance Wizard (Scan Network for NAS Appliances)** page is displayed.

3. From the **Chassis number** list, select the NAS appliance that you want to add to the NAS cluster and click **Next**.

   The **Add NAS Appliance Wizard (Subnets)** page is displayed.

4. Use the suggested IP addresses or enter new ones for the additional pair of controllers for all required subnets and click **Next**.

NOTE: Clicking **Next** displays the next subnet until the IP addresses for all the subnets are entered.

   After IP addresses for all the subnets area entered, a message prompts you that the system is saving the entered IP addresses.

5. Click **Next**.

   The **Add NAS Appliance Wizard (Prepare Controllers To Add Appliance)** page is displayed.

6. To validate the necessary hardware conditions for the expansion process, click **Next**.

   The **Add NAS Appliance Wizard (System Validation)** page is displayed. Various components and parameters are checked and the status for each component and parameter of the new NAS appliance is displayed.

7. To skip the validation, click **Skip**.

8. After the validation is complete, click Rerun to restart the validation or click Next.

   If you click **Rerun**, the validation process restarts. If you click **Next**, the **Add NAS Appliance Wizard (Attach New Member)** page is displayed.

9. Click **Next**.

   The **Add NAS Appliance Wizard (Controller Management)** page is displayed. The controllers on the newly added NAS appliance are attached to the NAS cluster. After the NAS appliance is successfully attached to the cluster, the **Add NAS Appliance Wizard (LUNs Configuration)** page is displayed.

   - For the PowerVault NX3500/NX3600/NX3610 solutions, the new IQN's are displayed. From the **Modular Data Storage Manager** (MDSM), create two new virtual hosts in the existing host group and associate the new IQNs to the virtual hosts. For more information, see Creating A Host In PowerVault NX3500/NX3600/NX3610.

NOTE: For more information on virtual host creation and IQN associations, see the *Modular Disk Storage Manager Administrator's Guide*, at **support.dell.com/manuals**.

   - For the Dell Compellent FS8600 NAS solution, apart from the **LUN configuration**, you can also view the **Fibre Channel WWNs Configuration**.

10. For Dell Compellent FS8600 NAS solution, the WWN information for the newly added controllers are listed in the upper table under FC WWNs. Note the new WWNs and define the necessary FC zoning conditions on the fibre channel switch before proceeding further.

NOTE: Skip the next step if you are adding an additional appliance to the Dell PowerVault NX3610 NAS solution.

11. For Dell Compellent FS8600 NAS solution, click **Rescan**.

    Ensure the additional controllers are now listed in the lower table under Accessible Controllers. If all controllers are not listed, verify your storage connections by clicking the **Verify Storage Connection** button in **Enterprise Manager**.

12. Click **Next**.

    The **Add NAS Appliance Wizard (Add NAS Appliance)** page is displayed.

13. Click **Next**.

    A message prompts you that the system expansion is complete and displays the number of appliances in the NAS cluster.

Creating A Host In PowerVault NX3500/NX3600/NX3610

For PowerVault NX3500/NX3600/NX3610 NAS solutions, you can create hosts manually using Modular Disk Storage Manager (MDSM).

To create a host in the host group you created:

1. Right-click the host group you created.
2. Click **Define** → **Host**.
   The **Specify Host Name (Define Host)** screen is displayed.
3. Type the name of the new host in **Host name**.
4. Click **Next**.
   The **Specify Host Port Identifiers (Define Host)** screen is displayed.
5. Select the host port identifier from the **Add by selecting a known unassociated host port identifier** list.
6. Type the host name in **User label** and suffix the host name with IQN.
7. Click **Add**.
8. Click **Next**.
   The **Specify Host Type (Define Host)** screen is displayed.
9. Select **Linux** from the **Host type (operating system)** list.
10. Click **Next**.
    The **Preview (Define Host)** screen is displayed.
11. Click **Finish**.
    The **Creation Successful (Define Host)** screen is displayed.
12. Click **Yes** to define another host.
    Repeat step 2 to step 10 to create another host.

Replacing A NAS Cluster Solution Controller

You must replace the controller in the event of a catastrophic failure where the existing controller cannot be brought back online.

Prerequisites

Before replacing the controller ensure that:

- You have physical access to the controllers.
- The controller is verified as failed (if it is replaced with a new one).

The procedure for replacing a controller involves:

- Detaching the controller.
- Removing and replacing the controller.
- Attaching the new controller.

Detaching The FluidFS NAS Cluster Solution Controller

In order to bring the cluster into the journalling 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 no downtime.

You may have to detach the controller under the following circumstances:

- A controller needs to be replaced with a new standby controller.
- The administrator wants to attach a working controller to another (more critical) cluster.

Detaching A Controller Using The NAS Manager

1. Select **Cluster Management** → **Hardware** → **Controllers Management.**

   The **Controllers Management** page is displayed.
2. From the list of available controllers, select the appropriate controller and click **Detach**.

   The selected controller is detached from the cluster, and powered off. This operation takes around 10 to 15 minutes.

Removing And Replacing The NAS Cluster Solution Controller

To remove and replace the NAS cluster solution controller:

1. Label all the cables correctly before disconnecting any cables.
2. Disconnect all cables from the back of the controller.
3. Remove the failed controller from the appliance chassis.
4. Install the new controller in the appliance chassis.
5. Connect all cables to the new controller.

NOTE: For more information on removing and installing the controller, see the *Dell FluidFS NAS Solution Owner's Manual*, at **support.dell.com/manuals**.

6. Ensure that the cables are reconnected to the same ports when installing the controller.
7. Power ON the new system by inserting the power cable.

Attaching The NAS Cluster Solution Controller

Before completing this procedure, verify that the controller being attached is in standby mode and powered up. You can verify that the controller is ON and in standby mode, if the power LED of the new controller is flashing green at around 2 flashes per second.

Attaching A Controller Using The NAS Manager

1. Select **Cluster Management** → **Hardware** → **Controllers Management.**

   The **Controllers Management** page is displayed.
2. From the list of available controllers, select the appropriate controller and click **Attach**.

NOTE: The following are additional steps required for the Dell Compellent FS8600 NAS Solutions.

NOTE: Fabric zoning must be updated manually on the fibre optic switch.

3. After the attach operation completes, the NAS Manager displays the WWN's for the newly attached controller, for fibre channel switch zoning.

NOTE: To view the WWNs at any time using the CLI, execute the following command:

```
system maintenance Luns configuration Fc-view
```

NAS Manager Features In Degraded Mode

When the NAS appliance is in degraded mode, the status of the following features in the NAS Manager are either **View only** or **Fail**.

Tab	Feature	Status in degraded mode
Access	Delete NAS volume	Fails
	NFS exports	View only
	CIFS shares	View only
Data Protection	Snapshot restore	Fails
	Replication Partners	View only
System Management	Time configuration	View only
	Network configuration	View only
	Subnets	View only
	Local hosts	View only
	Static routes	View only
	CIFS configuration	View only
	NIS/LDAP	View only
	Local users/groups	View only
	Mapping	Mapping
	SNMP	View only
	Restore Cluster Config	Fails
	Format	Fails
	Expand LUNS	Fails
	Add LUNs	Fails
	Add nodes	Fails

8

Internationalization

Overview

The NAS cluster solution 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 NAS cluster solution 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 NAS cluster solution.

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 NAS cluster solution's 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.

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 must be used.

Unicode Configuration Parameters

The following configuration parameters may contain Unicode characters.

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.

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)
OVERLINE (￣)	U+FFE3 (FULLWIDTH MICRON)	U+FFE3 (FULLWIDTH MICRON)	U+203E (OVERLINE)

Character	UNIX	Windows	Macintosh
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 NAS cluster solution 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 NAS cluster solution. This ensures that in any case correct and incorrect characters are mapped correctly.

9

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 NAS cluster solution. 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. The administrator can monitor the progress of the replication by clicking on **Refresh**. The screen displays an approximate percentage completion.

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 is no longer 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 takes 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. The administrator can monitor the progress of the replication by clicking on **Refresh**. The screen displays an approximate percentage completion.

11. Why can I not delete the replication policy from the target virtual volume?

    This is by design. All configuration changes must 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.

10

Getting Help

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit **support.dell.com**.
2. Select your support category.
3. If you are not a U.S. customer, select your country code at the bottom of the **support.dell.com** page, or select **All** to see more choices.
4. Select the appropriate service or support link based on your need.