Dell FluidFS NAS Solutions
Administratorhandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2013 - 03

Rev. A01

Inhaltsverzeichnis

1

Einführung

Die Dell FluidFS Network Attached Storage (NAS) Lösung ist eine Hochverfügbarkeitsspeicherlösung. Die Lösung fasst mehrere NAS-Controller in ein Cluster zusammen und stellt diese gegenüber UNIX-, Linux- und Microsoft Windows-Clients als einen einzigen virtuellen Dateiserver dar.

In diesem Dokument verwendete Begriffe

Bedingung	Beschreibung
Backup-Stromversorgung (BPS)	Versorgt das System im Falle eines Stromausfalls mit Akkustrom.
Client-Zugriffs-VIP	Virtuelle IP-Adresse, die Clients verwenden, um auf CIFS-Freigaben und NFS-Exporte zuzugreifen, die von der FluidFS NAS-Lösung gehostet werden. Die FluidFS NAS-Lösung unterstützt mehrere virtuelle Client-Zugriffs-IPs (VIPs).
NAS-Gerät	Zwei NAS-Controller, die als ein Paar in einem geclusterten FluidFS NAS-System konfiguriert sind. Cache-Daten werden zwischen den gepaarten NAS-Controllern innerhalb des Geräts gespiegelt.
Controller (NAS-Controller oder Knoten)	Die beiden Hauptkomponenten eines NAS-Geräts, wobei jeder der Controller ein separates Mitglied im FluidFS NAS-Cluster darstellt.
Datenverwaltungsanwendung (DMA)	Auch „Sicherungs-Anwendungsserver" genannt.
Dell PowerVault Modular Disk Storage Manager (MDSM)	Die Verwaltungssoftware, die zusammen dem Array der MD-Serie geliefert wird.
Enterprise Manager	Multi-Systemverwaltungssoftware, die zur Verwaltung von FluidFS mit Storage Center erforderlich ist.
Fluid File System (FluidFS)	Software für hochverfügbare, skalierbare Dateisysteme für die Installation auf NAS-Controllern.
Host-Anschlusskennung	Eindeutige Kennung zur Identifizierung von Hosts in einem Netzwerk.
LAN-/Client-Netzwerk (primäres Netzwerk)	Das Netzwerk, über das Clients auf NAS-Freigaben und Exporte zugreifen. Die FluidFS NAS-Lösung ist mit der IT-Umgebung des Kunden und ihren NAS-Clients über dieses Netzwerk verbunden. Es ist auch das Netzwerk, das der Speicheradministrator zum Verwalten der NAS-Lösung verwendet.
NAS-Speicherpool	Der NAS-Speicherpool ist eine virtualisierte Speicherschicht oben auf einem virtuellen Laufwerk. Die Größe des NAS-Speicherpools ist die Summe aller virtuellen Laufwerke, die im FluidFS NAS-Cluster verfügbar gemacht wurden.
NAS-Volume (NAS-Container oder virtuelles Volume)	Ein virtualisiertes Volume, das Speicherplatz im NAS-Speicherpool in Anspruch nimmt. Administratoren können CIFS-Freigaben und NFS-Exporte auf einem NAS-Volume erstellen und diese für autorisierte Benutzer freigeben. Eine FluidFS NAS-Lösung unterstützt mehrere NAS-Volumes.
NAS-Replikation	Replikation zwischen zwei FluidFS NAS-Lösungen oder zwischen zwei NAS-Volumes.

Bedingung	Beschreibung
NAS-Replikationspartner	FluidFS NAS-Lösungen, die an einer Replikation teilnehmen.
Network Data Management Protocol (NDMP)	Netzwerkdatenverwaltungsprotokoll, das für Sicherungen und Wiederherstellungen verwendet wird.
Peer-Controller	Der Peer-NAS-Controller, mit dem ein bestimmter NAS-Controller in einer FluidFS NAS-Lösung gekoppelt wird.
PowerVault MD3*xx*0i	Bezieht sich auf die folgenden Speicherlösungen: Dell PowerVault MD3200i, MD3220i, MD3600i und MD3620i iSCSI.
Storage Center	Compellent Storage Center-Lösungen der Serien 40 oder SC8000, die mindestens einen Fibre Channel-HBA für die FluidFS-Konnektivität enthalten.
Dell NAS Initial Deployment Utility (IDU)	Der Setup-Assistent zum erstmaligen Ermitteln und Konfigurieren einer FluidFS NAS-Lösung. Dieses Dienstprogramm wird nur für das erste Setup verwendet.
NAS Manager	Die webbasierte Benutzeroberfläche, die Teil der Software der NAS-Cluster-Lösung ist und zur Verwaltung der FluidFS NAS-Lösung verwendet wird.
FluidFS NAS-Lösung	Ein vollständig konfiguriertes, hochverfügbares und skalierbares NAS-Gerät, das NAS-Dienste (CIFS und/oder NFS) bereitstellt und aus einem Paar NAS-Controllern, einem Speichersubsystem und dem NAS-Manager besteht.
Standby-Controller	Ein NAS-Controller, der mit der FluidFS-Software installiert wird, aber nicht Teil des Clusters ist. Zum Beispiel wird ein neuer oder ein Ersatz-Controller von Dell als Standby-Controller bezeichnet.
SAN-Netzwerk	Das Netzwerk, das den Datenverkehr auf der Blockebene durchführt und mit dem das Speichersubsystem verbunden ist. **ANMERKUNG:** Es wird empfohlen, dieses Netzwerk isoliert vom LAN-oder Client-Netzwerk zu betreiben.

Architektur der Dell FluidFS NAS-Lösung

Die FluidFS NAS-Lösung, kombiniert mit Speicher-Arrays, bietet Ihnen eine einheitliche Speicherlösung. Durch diese Lösung erhalten Sie Zugriff sowohl auf Block- als auch auf Dateispeicher.

Die geclusterte FluidFS NAS-Lösung besteht aus einem NAS-Gerät mit einem Paar aus Controllern und Speicher-Arrays. Außerdem ist jeder NAS-Controller durch eine Backup-Stromversorgung (BPS) geschützt, die beim Schutz von Daten während eines Stromausfalls hilft.

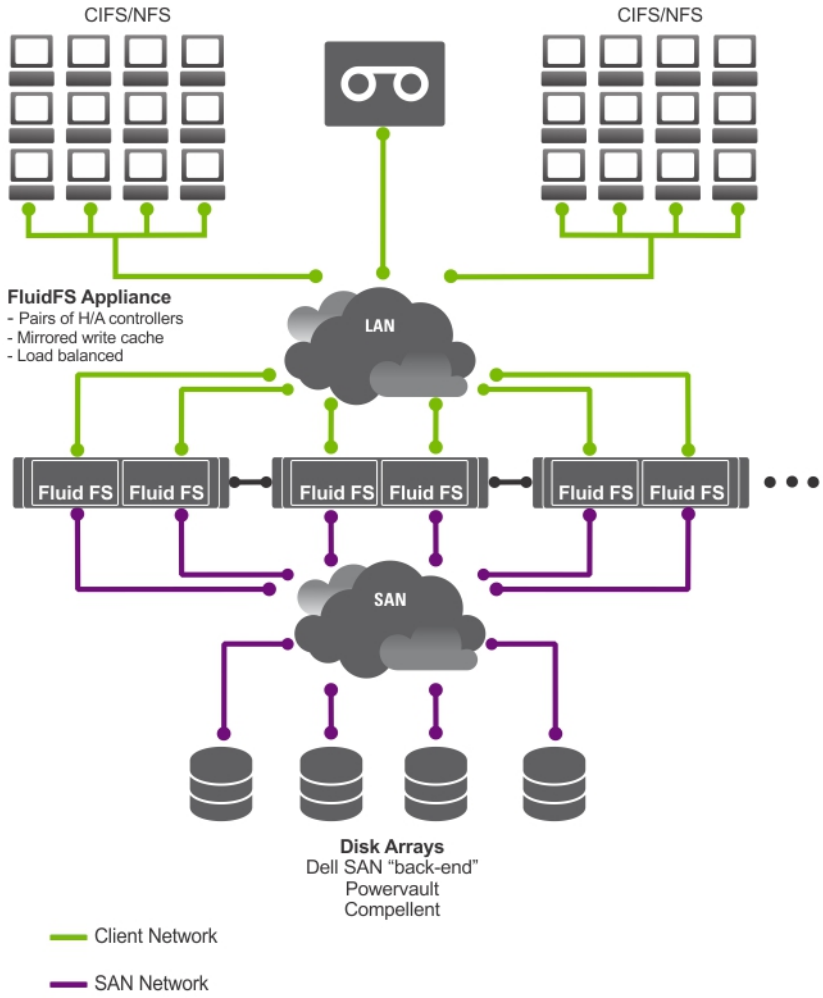

Abbildung 1. Architektur der FluidFS NAS-Cluster-Lösung

ANMERKUNG: Dell Compellent FS8600 NAS-Lösung verwendet ein zusätzliches Interconnect-Netzwerk, das in der Abbildung nicht gezeigt wird.

Anschlussbeschriftungen in FluidFS

Wenn ein Ethernet-Anschluss die Konnektivität verliert, veröffentlicht FluidFS ein Ereignis, das angibt, dass ein Kabel abgetrennt wurde, und es gibt an, welcher Anschluss nicht mehr verbunden ist. Die Anschlussbeschriftungen haben immer die Form von **eth** mit einer nachfolgenden Zahl, zum Beispiel **eth0**. Die folgenden Bilder zeigen, wie die physischen Anschlüsse mit den **eth**-Beschriftungen korrelieren, wie im FluidFS-Ereignisprotokoll gemeldet wird.

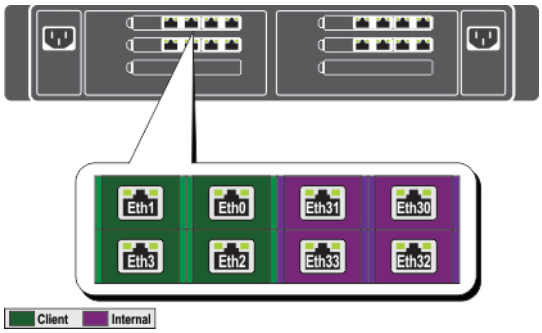

Abbildung 2. Anschlussbeschriftungen für 1GbE-Systeme

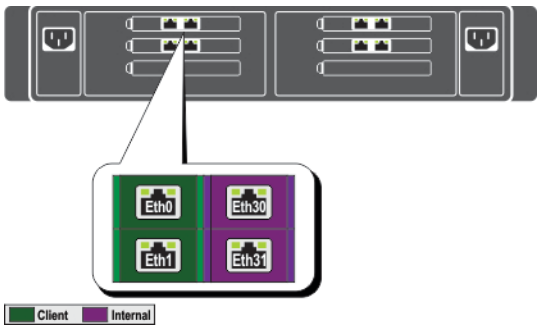

Abbildung 3. Anschlussbeschriftungen für 10GbE-Systeme

Wichtige Funktionen

Die NAS-Cluster-Lösung:

- Sie unterstützt Administratoren bei der Ausweitung der vorhandenen Kapazität und verbessert bedarfsgerecht die Leistung, ohne die Anwendungen und Benutzer negativ zu beeinträchtigen.
- Sie bietet administrative Funktionen für Speicheradministratoren, die für den alltäglichen Systembetrieb und die Speicherverwaltung zuständig sind.
- Ist mit einem verteilten Dateisystem ausgerüstet, das eine einzelne Schnittstelle für die Daten erstellt.
- Ist in der Lage, Daten im Terabyte-Bereich auf ein einzelnes Dateisystem zu speichern.
- Ermöglicht eine dynamische Erhöhung der Kapazität.
- Ist mit einer zentralen, intuitiven, webbasierten NAS-Verwaltungskonsole ausgestattet.
- Bietet eine bedarfsgerechte virtuelle Speicherbereitstellung.
- Ist in der Lage, benutzerzugängliche Snapshots zu einem bestimmten Zeitpunkt bereitzustellen.
- Ist in der Lage, Dateien für Microsoft Windows- , Linux-, UNIX- und Mac-Benutzer freizugeben.
- Bietet eine flexible, automatisierte Online-Replikation und Notfall-Wiederherstellung.
- Verfügt über eine integrierte Leistungsüberwachung und Kapazitätsplanung.

Ansichten NAS-Cluster-Lösungen

Abhängig von Ihrer Zugangsberechtigung können Sie als Client oder Administrator auf die NAS-Cluster-Lösung zugreifen.

ANMERKUNG: Es wird empfohlen, nicht zu versuchen, sich gleichzeitig an der Befehlszeilenschnittstelle und am NAS Manager anzumelden.

Client-Ansicht

Dem Client präsentiert sich die NAS-Cluster-Lösung als ein einziger Dateiserver mit einem einzigen Dateisystem, einer IP-Adresse und einem Namen. Das globale Dateisystem der NAS-Cluster-Lösung bedient alle Benutzer gleichzeitig ohne Leistungseinbußen. Es bietet dem Endbenutzer die Freiheit, sich mit der NAS-Cluster-Lösung zu verbinden und dabei die NAS-Protokolle seines jeweiligen eigenen Betriebssystems zu verwenden.

- NFS-Protokoll für Linux- und UNIX-Benutzer.
- CIFS-Protokoll für Windows-Benutzer.

Administratoransicht

Als Administrator können Sie entweder die Befehlszeilenschnittstelle (CLI) oder den NAS Manager verwenden, um die Systemeinstellungen zu konfigurieren oder zu ändern, so können Sie beispielsweise Protokolle konfigurieren, Benutzer hinzufügen oder Berechtigungen einrichten.

Der NAS Manager, über den Sie über einen Standard-Internet-Browser zugreifen können, bietet Zugang zu Systemfunktionen.

Systemkomponenten

Die NAS-Cluster-Lösung besteht aus:

- Hardware
  - einem oder mehreren NAS-Geräten
  - Speicher-Arrays
- Netzwerk
  - SAN-Netzwerk
  - Internes Netzwerk
  - LAN- oder Client-Netzwerk

NAS-Gerät

Die FluidFS NAS-Lösung besteht aus einem oder mehreren NAS-Geräten, die in einem Cluster konfiguriert sind. Jedes Gerät besteht aus einem Paar NAS-Controllern in einer aktiv-aktiv Konfiguration. Durch diese Konfiguration wird sichergestellt, dass Redundanz besteht. Die Controller erledigen den Lastenausgleich bei Client-Verbindungen, verwalten Lese-/Schreibvorgänge, führen Zwischenspeicherungen durch und verbinden mit Servern und Workstations. Das Cluster ist ein einzelner Speicherpool mit einem globalen Namensraum und der Zugriff geschieht über eine virtuelle IP (VIP).

Lese-/Schreibvorgänge werden über eine gespiegelte RAM vorgenommen. Durch das Spiegeln der Cache-Daten zwischen den gekoppelten NAS-Controllern wird eine schnelle Antwort auf Client-Anfragen sichergestellt, wobei die komplette Datenintegrität erhalten bleibt. Daten werden aus dem Cache zum permanenten Speicher asynchron durch optimierte Schemas zur Datenplatzierung übertragen.

Das Dateisystem verwendet den Cache effektiv, um schnelle und zuverlässige Lese- und Schreibvorgänge zu gewährleisten. Schreiben oder Ändern von Dateien geschieht zuerst im Cache. Dann werden die Daten zum Cache des Ziel-Controllers gespiegelt. Durch diese Funktion wird sichergestellt, dass alle Transaktionen dupliziert und gesichert werden.

Jeder Controller ist mit einer internen BPS ausgestattet, die für den Controller im Falle eines Stromausfalls mindestens 5 Minuten lang eine kontinuierliche Stromversorgung garantiert. Die Controller überwachen regelmäßig den Status der BPS-Batterie, sodass die BPS eine Mindeststromversorgung für den normalen Betrieb halten muss. Die BPS verfügt über genügend Batteriestärke, damit die Controller sicher herunterfahren können.

Die BPS ermöglicht es den Controllern, die NVRAM als Cache zu verwenden. Die BPS gibt der geclusterten Lösung ausreichend Zeit, um alle Daten aus dem Cache auf das Laufwerk zu speichern, wenn die Stromversorgung des Controllers ausfällt.

Speicher-Arrays

Die Controller sind mit einem Speicher-Array verbunden, welches ein RAID-Untersystem ist. RAID-Speicher-Untersysteme sind dafür ausgelegt, einzelne Fehlerpunkte zu beseitigen. Jede aktive Komponente im Speicher-Untersystem ist redundant und kann per Hot-Swap ausgetauscht werden. Die Lösung unterstützt typische RAID-Konfigurationen, inklusive RAID 1/10, RAID 5 und RAID 6.

SAN-Netzwerk

Das SAN-Netzwerk ist ein wichtiger Bestandteil der NAS-Cluster-Lösung. Das Controller-Paar befindet sich im SAN-Netzwerk und kommuniziert mit dem Speichersubsystem mithilfe des iSCSI-Protokolls bei Dell PowerVault NX3500/ NX3600/NX3610 oder mithilfe des Fibre-Channel-Protokolls bei Dell Compellent FS8600.

Interconnect-Netzwerk

Das Interconnect-Netzwerk besteht aus zwei unabhängigen Netzwerken. Das Interconnect-Netzwerk dient als Taktmechanismus und ermöglicht internen Datentransfer zwischen Controllern. In einem System mit zwei Controllern werden keine Switches verwendet. In einem System mit mehr als zwei Controllern enthält das Interconnect-Netzwerk zwei Switches. Alle Controller von Dell Fluid File System (FluidFS) sind mit beiden Interconnect-Switches verbunden. Diese verwenden duale Links für Redundanz und Lastenausgleich.

Um eine komplette Datenverteilung zu erreichen und hohe Verfügbarkeit zu erhalten, muss jeder Controller im Dell FluidFS Clustersystem Zugriff auf alle anderen Controller im System haben. Das Interconnect-Netzwerk erreicht dieses Ziel. Das Interconnect-Netzwerk bietet die Konnektivität zum Dell FluidFS Clustern, inklusive Taktüberwachung, Datentransfer, Informationsspiegelung zwischen Controller-Caches und gleicher Verteilung von Daten zu allen LUNs im System.

LAN- oder Client-Netzwerk

Nach der Erstkonfiguration wird die NAS-Cluster-Lösung über eine virtuelle IP-Adresse (VIP) mit dem Client oder dem LAN-Netzwerk verbunden.

Durch die virtuelle VIP-Adresse können Clients auf die NAS-Cluster-Lösung wie auf eine einzige Einheit zugreifen, wobei Zugriff auf das Dateisystem geboten wird. So kann die NAS-Cluster-Lösung einen Lastenausgleich zwischen Controllern vornehmen und sicherstellen, dass der Dienst weiter ausgeführt wird, auch wenn ein Controller ausfällt.

Das LAN oder Client-Netzwerk besteht aus Ports an jedem Controller, die mit den LAN- oder Client-Netzwerk-Switches verbunden sind. Die NAS-Cluster-Lösung wird unter Verwendung des LAN oder Client-Netzwerks auf der NAS-Verwaltungs-VIP gesteuert. Bei gerouteten Netzwerken hängt die Anzahl der VIPs, die das System bedienen, von der Anzahl der Ihnen verfügbaren Client-Ports ab, beispielsweise verfügt Dell Compellent FS8600 (1 GbE) mit vier Geräten über 32 Client-VIPs. Bei flachen Netzwerken reicht schon ein Client-VIP aus.

Weitere nützliche Informationen

WARNUNG: Beachten Sie die Hinweise zu Sicherheit und Betrieb, die mit dem Computer geliefert wurden. Garantieinformationen wurden möglicherweise als separates Dokument beigelegt.

- Das *Getting Started Guide* (Handbuch zum Einstieg) enthält eine Übersicht über die Einrichtung des Systems und technische Daten.
- Im *Owner's Manual (Benutzerhandbuch)* erhalten Sie Informationen über Systemfunktionen, zur Fehlerbehebung am System und zum Installieren oder Austauschen von Systemkomponenten.
- In der zusammen mit der Rack-Lösung gelieferten Rack-Dokumentation ist beschrieben, wie das System in einem Rack installiert wird.
- Das *Deployment Guide* (Bereitstellungshandbuch) enthält Informationen zur Hardware-Bereitstellung und die Erstbereitstellung des NAS-Geräts.
- Das *System Placemat (System-Platzset)* bietet Informationen zum Einrichten und Installieren der Software in Ihrer NAS-Lösung.
- Die *Online-Hilfe* bietet Informationen zum Konfigurieren und Steuern der Software. Die Online-Hilfe ist im System integriert und ist über die Web-Oberfläche des NAS-Managers erreichbar.
- Alle im Lieferumfang des Systems enthaltenen Medien mit Dokumentationen und Hilfsmitteln zur Konfiguration und Verwaltung des Systems, insbesondere in Bezug auf Betriebssystem, Systemverwaltungssoftware, System-Updates und mit dem System erworbene Komponenten.
- Die vollständigen Namen der in diesem Dokument verwendeten Abkürzungen und Akronyme finden Sie im Glossar unter **dell.com/support/manuals**.

ANMERKUNG: Wenn auf der Website **www.dell.com/support/manuals** aktualisierte Dokumente vorliegen, lesen Sie diese immer zuerst, denn frühere Informationen werden damit gegebenenfalls ungültig.

2

Überwachen der FluidFS NAS-Lösung

ANMERKUNG: Die Informationen in diesem Kapitel beziehen sich auf die Dateiverwaltung mithilfe des NAS-Managers. Blockverwaltung und Überwachung geschehen mithilfe von:

- **Dell PowerVault Modular Disk Storage Management** (MDSM) für die Dell PowerVault NX3500/NX3600/NX3610 NAS-Lösung
- **Enterprise Manager** für Dell Compellent FS8600 NAS-Lösung

Sie können den Status der NAS-Lösung mithilfe der Registerkarte **Monitor (Überwachen)** im NAS-Manager überwachen. Hier können Sie den Gesamtstatus des Systems auf der Seite **Dashboard (Instrumententafel)** ansehen und Kontingentnutzungsberichte und Statusberichte von Remote-Replikationsaufgaben empfangen.

Um auf die Überwachungsseiten zu gelangen, klicken Sie auf die Registerkarte **Monitor (Überwachen)**. Standardmäßig wird die Seite **Dashboard (Instrumententafel)** angezeigt.

Dashboard

Die Seite **Dashboard (Instrumententafel)** zeigt den Status des gesamten Systems in einer einzigen Ansicht an. Die Seite **Dashboard** umfasst fünf kurzfristige Echtzeit-Abschnitte:

- Status
- Kapazität
- Current Performance (Aktuelle Leistung)
- Recent Performance (Kürzliche Leistung)
- Load Balancing (Lastenausgleich)

ANMERKUNG: Die auf diesem Bildschirm angezeigten Daten werden alle fünf Sekunden automatisch aktualisiert.

ANMERKUNG: Um die Status-Parameter für jeden Abschnitt zu sehen, klicken Sie in **Dashboard** auf den jeweiligen Abschnitt.

Status

Der Abschnitt **Status** zeigt den Systemstatus und eine Liste der Hardware-Komponenten an. Jeder Hardware-Komponententyp zeigt die Gesamtzahl der Komponenten und die Anzahl der problematischen Komponenten an. Die Liste umfasst Controller und ihre zugewiesenen NAS-Geräte.

Kapazität

Der Abschnitt **Capacity (Kapazität)** zeigt eine Tabelle und ein Kreisdiagramm mit der gesamten Netzkapazität des Dell Fluid File System an.

Current Performance (Aktuelle Leistung)

Der Abschnitt **Current Performance (Aktuelle Leistung)** zeigt den aktuellen Netzwerkdurchsatz an. Der aktuelle Netzwerkdurchsatz umfasst den Durchsatz von Datenlese- / Schreibvorgängen (Mbit/s) und die Anzahl der Lese-/Schreibvorgänge pro Sekunde pro Protokoll.

Kürzliche Leistung

Im Abschnitt **Recent Performance (Kürzliche Leistung)** wird ein Diagramm mit dem Lese-/Schreibdurchsatz in den vergangenen 30 Minuten angezeigt.

Load Balancing (Lastenausgleich)

Im Abschnitt **Load Balancing** (Lastenausgleich) wird eine Tabelle mit Echtzeitdaten zum Controller-Status, zur Prozessornutzung und zur Anzahl der Verbindungen für jeden Controller angezeigt.

Ereignisanzeige

Mit der Ansicht **Events Viewer (Ereignisanzeige)** können Sie Ihr Fluid File System überwachen, denn sie zeigt sowohl Informationen als auch wichtige Ereignisse in Ihrem System an.

Um auf die Seite **Events Viewer (Ereignisanzeige)** zu gelangen, klicken Sie in der Registerkarte **Monitoring (Überwachung)** auf **Events (Ereignisse)**.

Auf der Seite **Events Viewer (Ereignisüberwachung)** können Sie:

- Ereignisse filtern
- Ereignisse ordnen
- Ereignisse in eine CSV-Datei exportieren

Ereignisse unter Event Viewer (Ereignisanzeige) ansehen

1. Wählen Sie **Monitor (Überwachen)** → **Overview (Übersicht)** → **Events (Ereignisse).**
   Die Seite **Event Viewer (Ereignisanzeige)** wird angezeigt.
2. Wählen Sie in den Listen **Show (Anzeigen)**, **events of (Ereignisse der Art)** und **from (von)** die gewünschten Filter aus und klicken Sie auf **Show (Anzeigen)**.
   Die Ereignisse werden in einer Tabelle gemäß den ausgewählten Parametern angezeigt.
3. Um die Ereignisse zu ordnen, klicken Sie auf die jeweilige Spaltenüberschrift in der Ereignistabelle.
4. Um Einzelheiten zum Ereignis anzuzeigen, wählen Sie das gewünschte Ereignis in der Ereignistabelle aus.
   Die Einzelheiten des ausgewählten Ereignisses werden im **View Pane (Fensterbereich Ansicht)** angezeigt.
5. Um die angezeigten Ereignisse in eine CSV-Datei zu exportieren, klicken Sie auf **Export to CSV file (In CSV-Datei exportieren)**.
   Ein neues Browserfenster mit den Ereignissen im CSV-Format wird angezeigt.
6. Kopieren Sie die Ereignisse in eine CSV-Datei und fügen Sie sie ein oder speichern Sie die Webseite als CSV-Datei.

Network Performance (Netzwerkleistung)

Die Seite **Network Performance Over Time (Zeitbezogene Netzwerkleistung)** zeigt die zeitbezogene Leistung des Dell Fluid File Systems an. Sie können die Netzwerkleistung von FluidFS für die folgenden Zeiträume ansehen:

- **Letzter Tag**
- **Letzte Woche**
- **Letzten Monat**
- **Letztes Jahr**

Klicken Sie auf jede Registerkarte, um die Netzwerkleistung während des gewünschten Zeitraums anzuzeigen. Sie können die folgenden Einzelheiten zur Netzwerkleistung ansehen:

- **Client-Netzwerkdurchsatz - Lesevorgänge**
- **Client-Netzwerkdurchsatz - Schreibvorgänge**
- **Vorgänge pro Sekunde**
- **Zusammengefasster Netzwerkdurchsatz**

ANMERKUNG: Weitere Informationen zur **Network Performance Over Time (Zeitbezogene Netzwerkleistung)** finden Sie in der *Online Help (Online-Hilfe)*.

Load Balancing (Lastenausgleich)

Sie können die folgenden Einzelheiten zum Lastenausgleich anzeigen:

- **Over time (Zeitbezogen)**
- **Client Connections (Client-Verbindungen)**
- **CIFS Connections (CIFS-Verbindungen)**

Zeitbezogenen Lastenausgleich anzeigen

1. Wählen Sie **Monitor (Überwachen)** → **Load Balancing (Lastenausgleich)** → **Over Time (Zeitbezogen).**

   Die Seite **Load Balancing Over Time (Zeitbezogener Lastenausgleich)** wird angezeigt. Die Seite **Load Balancing Over Time (Zeitbezogener Lastenausgleich)** zeigt **CPU Load (CPU-Last)**, **CIFS Connections (CFIS-Verbindungen)**, **Read Throughput (Lesedurchsatz)** und **Write Throughput (Schreibdurchsatz)** an.
2. Klicken Sie auf die entsprechende Registerkarte, um die Informationen zum Lastenausgleich für den gewünschten Zeitraum anzuzeigen.

   Sie können Informationen zum Lastenausgleich für folgende Zeiträume ansehen:

   - **Letzter Tag**
   - **Letzte Woche**
   - **Letzter Monat**
   - **Letztes Jahr**
3. Wählen Sie den Controller aus, für den Sie die Informationen zum Lastenausgleich anzeigen möchten und klicken Sie auf **Display (Anzeigen)**.

   ANMERKUNG: Standardmäßig sind alle Controller ausgewählt.
4. Um die angezeigten Ereignisse in eine CSV-Datei zu exportieren, klicken Sie auf **Export to CSV file (In CSV-Datei exportieren)**.

Ein neues Browserfenster mit den Ereignisse im CSV-Format wird angezeigt.

5. Kopieren Sie die Ereignisse in eine CSV-Datei und fügen Sie sie ein oder speichern Sie die Webseite als CSV-Datei.

Client Connections (Client-Verbindungen)

Mit der Seite **Client Connections (Client-Verbindungen)** können Sie:

- Verteilung von Clients auf die jeweiligen Controller anzeigen
- Spezifische Clients von einem Controller auf einen anderen Controller manuell migrieren
- Richtlinie für die automatische Client-Migration definieren

ANMERKUNG: Standardmäßig wird auf der Registerkarte **Clients** eine Liste aller Client-Verbindungen angezeigt.

Client-Verbindungen anzeigen

ANMERKUNG: Die Seite Client-Verbindungen zeigt nur Clients an, die zum selben Subnetz wie das System gehören (lokale Clients). Clients, die auf das System über einen Router (oder einen Layer-3-Switch) zugreifen, werden nicht auf dieser Seite angezeigt; stattdessen wird der Router angezeigt.

1. Wählen Sie **Monitor (Überwachen) → Load Balancing (Lastenausgleicht) → Client Connections (Client-Verbindungen).**

   Die Seite **Client Connections (Client-Verbindungen)** wird angezeigt. Standardmäßig zeigt die Registerkarte **Clients** eine Liste aller Client-Verbindungen an.

2. Wählen Sie in den Listen **Protocols (Protokolle)** und **Controller** die gewünschten Filter aus.

   Die Tabelle der Client-Verbindungen zeigt die Ereignisse gemäß den ausgewählten Parametern an.

3. Um die Client-Verbindungen zu ordnen, klicken Sie auf die jeweilige Spaltenüberschrift in der Tabelle der Client-Verbindungen.

Migrieren von Clients zu einem anderen Controller

Wenn es ein Ungleichgewicht in der Netzwerklast gibt, so kann das System das Gleichgewicht durch das manuelle oder automatische Migrieren von Clients zwischen Controllern wiederherstellen. Wählen Sie aus, ob die Clients oder Router in der Liste zu anderen Controllern migriert werden dürfen.

1. Wählen Sie **Monitor (Überwachen)→ Load (Lasten) Balancing (Ausgleich)→ Client Connections (Client-Verbindungen)**.

   Die Seite **Client Connections (Client-Verbindungen)** wird angezeigt. Standardmäßig zeigt die Registerkarte **Clients** eine Liste aller Client-Verbindungen an.

2. Wählen Sie in der Tabelle der Client-Verbindungen eine oder mehrere Client-Verbindungen, die Sie migrieren möchten, und klicken Sie auf **Assign Interface (Schnittstelle zuweisen)**.

   Die Seite **Assign Interface (Schnittstelle zuweisen)** wird angezeigt.

3. Unter **Move to (Verschieben nach)** können Sie entweder einen speziellen Controller als Ziel oder die Option **Assigned Controller (Zugewiesener Controller)** auswählen.

   – Wählen Sie zum Migrieren aller ausgewählten Clients auf einen bestimmten Controller einen speziellen Controller aus der Liste aus.

   – Um alle ausgewählten Clients zurück zu ihren ursprünglichen Controllern zu migrieren, nachdem ein ausgefallener Controller wieder verfügbar ist, wählen Sie Assigned Controller (Zugewiesener Controller) aus. Jeder Client kann einen anderen zugewiesenen Controller haben.

4. Wählen Sie in **Interface (Schnittstelle)** die entsprechende Zielschnittstelle aus oder erlauben Sie dem System, die Zielschnittstelle auf dem Controller automatisch zuzuweisen.

VORSICHT: Durch diesen Vorgang werden die CIFS-Verbindungen getrennt, wenn sie zu einem anderen Controller migriert werden.

5. Wählen Sie zum Aktivieren des **automatischen Lastenausgleichs** die Option **Allow these clients to migrate to other controllers when rebalancing the network load (Diesen Clients die Migration zu anderen Controllern beim Neuausgleich der Netzwerklast ermöglichen)** aus.
6. Klicken Sie auf **Assign (Zuweisen)**.

Einrichten der Migrationsrichtlinie

Im Falle eines Controller-Fehlers migriert das System automatisch alle Verbindungen vom ausgefallenen Controller zu einem anderen Controller. Dadurch werden Verbindungen mit CIFS-Clients getrennt, wenn nicht die Richtlinie **Migrate Manually (Manuell migrieren)** für CIFS ausgewählt wurde. Mit Auswahl dieser Option müssen Sie die Clients manuell migrieren. Unter allen Umständen werden Ein-/Ausgaben bei der Migration von CIFS-Clients unterbrochen. Klicken Sie auf die Windows-Schaltfläche **Cancel** und versuchen Sie die Übertragung erneut. Wenn der ausgefallene Controller neu startet, gleicht das System die Last durch automatische Migration der Clients zurück auf den neu hochgefahrenen Controller aus. Dieser Vorgang nennt sich Failback.

Clients, die NFS verwenden, sind statuslos und sind von einem Failback nicht betroffen. Um den Failback-Vorgang zu optimieren, bietet Ihnen das System die folgenden Richtlinien zur Migration bei Wiederherstellung:

- **Migrate Immediately (Sofort migrieren)** - Hält das System stets in einem ausgeglichenen Zustand; dies kann möglicherweise bedeuten, dass die CIFS-Clients während der Arbeitszeit getrennt werden.
- **Migrate Automatically (Automatisch migrieren)** - Hält das System stets in einem ausgeglichenen Zustand, wenn der Controller-Fehler sehr kurz ist; dies kann bedeuten, dass die CIFS-Clients getrennt werden. Diese Option führt dazu, dass das System mehrere Tage lang nicht ausgeglichen ist, wenn der Fehler für längere Zeit besteht.

  Dieser Modus bewältigt kurzzeitige Controller-Fehler, da Clients während des kurzzeitigen Fehlers kein neues Material erstellt haben. Darum ist die beste Methode, die Clients so schnell wie möglich auszugleichen. Wenn der Fehler länger als 10 Minuten anhält, bleibt das System unausgeglichen, bis Sie es manuell neu ausgleichen.
- **Migrate Manually (Manuell migrieren)** - Clients werden niemals automatisch migriert. Zum Ausgleichen des Systems ist ein manueller Eingriff erforderlich. Wenn das System nach einem Failover einen manuellen Eingriff zum Ausgleichen erfordert, sendet es eine entsprechende E-Mail-Benachrichtigung an den Administrator.

So richten Sie die Migrationsrichtlinien ein:

1. Wählen Sie **Monitor (Überwachen)** → **Load Balancing (Lastenausgleicht)** → **Client Connections (Client-Verbindungen).**

   Die Seite **Client Connections (Client-Verbindungen)** wird angezeigt. Standardmäßig zeigt die Registerkarte **Clients** eine Liste aller Client-Verbindungen an.
2. Klicken Sie auf **Migration Policy (Migrationsrichtlinien)**.

   Die Seite **Migration Policy (Migrationsrichtlinien)** wird angezeigt.
3. Wählen Sie für jedes **Protocol (Protokoll)** die entsprechende Migrationsrichtlinien für das **Client Network (Client-Netzwerk)** aus.
4. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Verwalten von CIFS-Verbindungen

Die aktuellen **CIFS-Verbindungen** werden auf der Seite **CIFS Connections (CIFS-Verbindungen)** angezeigt.

So verwalten Sie CIFS-Verbindungen:

1. Wählen Sie **Monitor (Überwachen)** → **Load Balancing (Lastenausgleicht)** → **CIFS Connections (CIFS-Verbindungen).**

Daraufhin wird die Seite **CIFS Connection (CIFS-Verbindungen)** angezeigt.

2. Um einen Client vom CIFS-Protokoll zu trennen, wählen Sie den entsprechenden Client aus und klicken Sie **Disconnect (Trennen)** in der Leiste **Action (Aktion)**.
3. Um alle Verbindungen für einen bestimmten Controller zu trennen, wählen Sie den gewünschten Controller aus und klicken Sie auf **Disconnect (Trennen)** in der Leiste **Action (Aktion)**.
4. Klicken Sie auf **Refresh (Aktualisieren)**, um die angezeigten Informationen zu aktualisieren.

Hardware

Status der Systemvalidierung anzeigen

Sie können die Systemvalidierung ausführen, um die Systemkonfiguration inklusive Hardware und Netzwerkkonnektivität zu validieren.

ANMERKUNG: Die Systemvalidierung kann auch über die CLI-Oberfläche vorgenommen werden.

Sie bietet Informationen zu Prozessoren, Überwachungsverfügbarkeit, NICs, IPMI, Ethernet-Bandbreite, BPS-Überwachung usw.

So aktualisieren Sie den Status der Systemkomponenten:

1. Wählen Sie **Monitor (Überwachen)** → **Hardware** → **System Validation (Systemvalidierung).**
   Die Seite **System Validation (Systemvalidierung)** wird angezeigt.
2. Klicken Sie auf **Rerun (Erneut ausführen)**, um die Systemvalidierung auf allen Systemkomponenten erneut auszuführen, und aktualisieren Sie den Status jeder Systemkomponente.

Detaillierten Komponentenstatus anzeigen

Die Seite **Component Status (Komponentenstatus)** zeigt den aktuellen Status der NAS-Cluster-Lösung an. Sie bietet Informationen zu Status, interner Hardware, Konnektivität und Energie für jedes Gerät und seine Controller

So zeigen Sie zusätzliche Einzelheiten zum Status eines speziellen Controllers oder Geräts an:

1. Wählen Sie **Monitor (Überwachen)** → **Hardware** → **Component Status (Komponentenstatus).**
   Die Seite **Hardware Component Status Hardware-Komponentenstatus)** wird angezeigt.
2. Klicken Sie unter **Component (Komponente)** auf das gewünschte Gerät oder den gewünschten Controller.
   Eine Seite des Webbrowsers öffnet sich, die den Status jeder Komponente im ausgewählten Gerät oder Controller anzeigt.
3. Klicken Sie auf **Sample Hardware Components (Stichprobe Hardware-Komponente)**, um das Fenster so lange zu aktualisieren, bis es die neuen Stichprobenwerte anzeigt.

Geräte- und Controllernummern beginnen mit 0. Appliance0 (Gerät 0) enthält Controller0 und Controller1, Appliance1 (Gerät 1) enthält Controller2 und Controller3 usw. Um die physikalische Hardware zu identifizieren, müssen Sie auf **ApplianceX (GerätX)** klicken und den im Pop-Up-fenster angezeigten Service-Tag mit dem Service-Tag abgleichen, der auf einem Aufkleber an der vorderen rechten Lasche des Geräts angebracht ist.

Kapazität

Genutzten Speicherplatz anzeigen

Die Seite **Space Utilization (Speicherplatznutzung)** zeigt die aktuelle und die zeitbezogene Speicherplatznutzung des Dell Fluid File Systems an.

So zeigen Sie den genutzten Speicherplatz an:

1. Wählen Sie **Monitor (Überwachen)** → **Capacity (Kapazität)** → **Space Utilization (Speicherplatznutzung).**
   Die Seite **Space Utilization (Speicherplatznutzung)** zeigt eine Tabelle der Speicherplatznutzung für den ausgewählten Zeitraum an. Standardmäßig wird die **aktuelle** Speicherplatznutzung angezeigt.
2. Klicken Sie auf die entsprechende Registerkarte, um Informationen zum Lastenausgleich im gewünschten Zeitraum zu erhalten. Sie können sich Informationen zum Lastenausgleich für folgende Zeiträume ansehen:
   - **Letzter Tag**
   - **Letzte Woche**
   - **Letzten Monat**
   - **Letztes Jahr**
3. Um die Speicherplatznutzung zu ordnen, klicken Sie auf die jeweilige Spaltenüberschrift in der Tabelle zur Speicherplatznutzung.

Kontingentnutzung anzeigen

Die Seite **Quota Usage)Kontingentnutzung)** zeigt die Kontingente und die Nutzung für alle Benutzer an, auch für solche, für die kein Kontingent definiert wurde. Auch Benutzer, die aus dem System entfernt wurden, aber immer noch über Nutzung verfügen, sind eingeschlossen.

So zeigen Sie die Kontingentnutzung an:

1. Wählen Sie **Monitor (Überwachen)** → **Capacity (Kapazität)** → **Quota Usage (Kontingentnutzung).**
   Die Seite **Quota Usage (Kontingentnutzung)** zeigt die Tabelle der Kontingentnutzung für alle **NAS Volumes** an.
2. Wählen Sie unter **Show quota usage for NAS Volume (Kontingentnutzung für NAS-Volume anzeigen)** das gewünschte NAS-Volume oder **All NAS Volumes (Alle NAS-Volumes)** aus.
   Die Tabelle der Kontingentnutzung zeigt die Einzelheiten der Kontingentnutzung für das ausgewählte NAS-Volume an.
3. Um die Kontingentnutzung zu aktualisieren, klicken Sie auf **Refresh (Aktualisieren)**.

Replikation

Sie können den Status und den Fortschritt eines NAS-Replikationsvorgangs auf der Seite **NAS Replication (NAS-Replikation)** ansehen.

So zeigen Sie den Status und Fortschritt der NAS-Replikationsrichtlinien an:

1. Wählen Sie **Monitor (Überwachen)** → **Replication (Replikation)** → **NAS Replication (NAS-Replikation).**
   Die Seite NAS Replication zeigt eine Tabelle der NAS-Replikation für Replikationsrichtlinien an, deren Quell- oder Ziel-Volume oder beide sich in diesem Dell Fluid File System befinden.
2. Um die NAS-Replikation zu ordnen, klicken Sie auf die jeweilige Spaltenüberschrift in der Tabelle der NAS-Replikation.

3. Um den detaillierten Verlauf des Replikationsrichtlinienfortschritts anzuzeigen, klicken Sie auf den Status der gewünschten Replikationsrichtlinie.

NDMP

Sie können Status und Fortschritt der aktiven NDMP-Aufgaben auf der Seite **NDMP Active Jobs (Aktive NDMP-Aufgaben)** anzeigen.

3

Verwenden von Volumes, Freigaben und Kontingenten

Die Registerkarte **User Access (Benutzerzugriff)** ermöglicht es Ihnen, das Dell Fluid File System aus der Client-Perspektive zu definieren und zu verwalten.

NAS-Volumes

Ein NAS-Volume ist ein Teilbereich eines Speicher-Pools mit bestimmten Richtlinien, die den zugewiesenen Speicherplatz, den Schutz der Daten und die Sicherheitsart auf dem NAS-Volume überwachen.

NAS-Volumes können erstellt und konfiguriert werden. Administratoren können entweder ein großes NAS-Volume, das den gesamten NAS-Pool einnimmt, oder mehrere NAS-Volumes erstellen. Sie können diese NAS-Volumes in jedem Fall erstellen, in der Größe verändern oder löschen.

Dieser Abschnitt beschreibt, wie ein Administrator den Speicher der NAS-Cluster-Lösung mithilfe von NAS-Volumes zuweist und bereitstellt. Um NAS-Volumes dem Benutzer verfügbar zu machen, müssen sie separat freigegeben (exportiert) werden. Benutzer müssen jede Freigabe einzeln mounten.

Erwägungen zur Nutzung

Durch das Definieren von mehreren NAS-Volumes können Administratoren verschiedene Verwaltungsrichtlinien auf ihre Daten anwenden, wie z. B. Backup, Snapshots, Kontingente und Sicherheitsart. Ungeachtet der verwendeten Strategie wird der Speicher als ein Speicherpool verwaltet und freier Speicherplatz kann einfach zwischen NAS-Volumes durch Änderung des dem NAS-Volume zugewiesenen Speicherplatz migriert werden.

Berücksichtigen Sie die folgenden Faktoren, bevor Sie sich auf eine Strategie festlegen:

- Allgemeine Anforderungen
  - NAS-Volumes sind logisch; sie können auf einfache Weise und auf der Basis der Systemkapazität erstellt, gelöscht oder geändert (vergrößert oder verkleinert) werden.
  - Der Name von NAS-Volumes darf nicht mehr als 230 Zeichen enthalten. Er darf nur Buchstaben, Zahlen und Unterstriche (_) enthalten und muss entweder mit einem Buchstaben oder einem Unterstrich beginnen.
  - Sie können eine beliebige Anzahl an NAS-Volumes erstellen, die Gesamtkapazität darf dabei jedoch die gesamte Speicherkapazität nicht überschreiten.
  - Ein einzelnes Volume kann verschiedene Datentypen beherbergen; definieren Sie dazu mehrere Freigaben auf den Volumes.
  - Sie können die Größe eines virtuellen Laufwerks nach seiner Erstellung ändern.
  - Die Mindestgröße eines NAS-Volumes beträgt 20 MB. Wenn das Volume bereits verwendet wurde, richtet sich die Mindestgröße nach den auf dem Volume gespeicherten Daten.
  - Die Maximalgröße eines NAS-Volumes ist dann der verbleibende, nicht zugewiesene Speicherplatz.
- Geschäftsanforderungen - Eine Unternehmens- oder Anwendungsanforderung zur Trennung oder zur Nutzung eines einzelnen Volumes muss in Betracht gezogen werden. NAS-Volumes können dazu verwendet werden, Abteilungen Speicher auf Nachfrage zuzuweisen, mithilfe des Grenzwertmechanismus um Abteilungen zu benachrichtigen, wenn sie ihren zugewiesenen Speicherplatz verbraucht haben.

- Snapshots - Jedes NAS-Volume kann für den bestmöglichen Schutz des auf ihm gespeicherten Datentyps eine dedizierte Snapshot-Planungsrichtlinie haben.
- Sicherheitsart - In Umgebungen mit mehreren Protokollen kann es günstig sein, die Daten zu trennen und NAS-Volumes mit UNIX-Sicherheitsart für UNIX-basierte Clients und NTFS für Windows-basierte Clients zu definieren. So kann der Administrator die Sicherheitsart den Geschäftsanforderungen und verschiedenen Datenzugriffsmustern anpassen. Die Sicherheitsart kann auch als gemischt eingestellt werden, sodass sowohl POSIX-Sicherheit und Windows ACLs auf demselben Volume unterstützt werden.
- Kontingente - Kontingente werden auch pro NAS-Volume definiert. Verschiedene Kontingentrichtlinien können auf verschiedene NAS-Volumes angewendet werden, sodass der Administrator sich auf das Verwalten von Kontingenten konzentrieren kann, wenn passend.

Beispiele für die Verwendung sind Kopiervorgänge, Auflistungsvorgänge und Verschiebungsvorgänge. Die folgende Tabelle zeigt ein Beispiel für eine Organisation mit mehreren Abteilungen und wie NAS-Volumes erstellt werden können. Die richtige Lösung hängt von den Anforderungen des Kunden ab, da NAS-Volumes flexibel sind und bei Bedarf vergrößert oder verkleinert werden können.

Tabelle 1. NAS-Volume – Beispiel:

Abteilung	Bevorzugte Zugriffsverwaltungskontrolle	Snapshots	Replikation	Sicherung	CIFS- oder NFS-Clients und Mischung aus Lesen/Schreiben (Standard ist 80/20)	Stündliche Änderung in % der vorhandenen Daten (hoch ab 1 %)
Nachbearbeitung	NFS	Stündlich	Nein	Wöchentlich	20–20/80	1 %
Verwaltung und Finanzwesen	CIFS	Nein	Nein	Wöchentlich	10–50/50	Kein
Broadcast	Mixed (Gemischt)	Nein	Nein	Wöchentlich	10–90/10	Kein
Drücken Sie auf:	CIFS	Täglich	Nein	Nein	5–10/90	5 % (Schätzwert)
Marketing	CIFS	Täglich	Ja	Nein	5–50/50	Kein

Lösung 1

Erstellen Sie fünf NAS-Volumes, die auf der Abteilung basieren. Der Administrator unterteilt den Speicher und die Verwaltung logisch in Funktionsgruppen. In diesem Szenario sind die Abteilungsanforderungen recht unterschiedlich und das Design zum logischen Erstellen von NAS-Volumes gemäß den Abteilungslinien wird unterstützt.

Diese Lösung bietet die folgenden Vorteile:

- Es ist und logisch einfach, die NAS-Volumes zu verwalten.
- Die NAS-Volumes werden erstellt, um die exakten Anforderungen der Abteilung zu erfüllen.

Der Nachteil dieser Option liegt darin, dass die Verwaltung der NAS-Volumes erschwert wird, wenn die Anzahl der Abteilungen in der Organisation wächst.

Lösung 2

Gruppieren Sie Abteilungen mit ähnlichen Sicherheitsanforderungen zu NAS-Volumes. Der Administrator erstellt drei NAS-Volumes, eins für NFS, eins für CIFS und ein weiteres für Gemischtes. Der Vorteil besteht darin, dass die NAS-Volumes separat zwischen Windows und Linux arbeiten. Bei dieser Lösung gibt es folgende Nachteile:

- Alle Dateien in einem NAS-Volume werden gesichert.
- Manche Abteilungen können nicht gewünschte Dienste erhalten. Wenn ein CIFS-Volume erstellt wird, um Daten für die Verwaltungs- und die Finanzabteilung zu sichern, erhalten auch die Presse- und die Rechtsabteilung Sicherungen, auch wenn sie diese nicht benötigen.

Lösung 3

NAS-Volumes können auch auf Grundlage der Funktion erstellt werden. Der Nachteil dieser Lösung ist, dass Zuweisungen erforderlich sind. Ein Benutzer muss einen Sicherheitsstil, entweder NTFS oder UNIX, auswählen und auf Grundlage des ausgewählten Sicherheitsstils wird die korrekte Zuweisung für andere Benutzer eingerichtet.

Verwalten von NAS-Volumes

Sie können den derzeitigen Status aller NAS-Volumes anzeigen lassen, neue NAS-Volumes hinzufügen und vorhandene NAS-Volumes entfernen oder bearbeiten.

Hinzufügen eines NAS-Volumes

So fügen Sie ein NAS-Volume hinzu:

1. Wählen Sie **User Access (Benutzerzugriff) → NAS Volumes (NAS-Volumes) → Configuration (Konfiguration).**
   Die Seite **NAS Volumes Configuration (NAS-Volumes Konfiguration)** zeigt die Liste der NAS-Volumes an.
2. Klicken Sie auf **Add (Hinzufügen)**.
   Es wird die Seite **Add NAS Volume (NAS-Volume hinzufügen)** angezeigt.
3. Geben Sie in **NAS Volume** den NAS-Volume-Namen ein.
4. Geben Sie in **NAS volume allocated space (Zugewiesener Speicherplatz des NAS-Volumes)** den diesem NAS-Volume zugewiesenen Speicherplatz in MB, GB oder TB ein.

   ANMERKUNG: Ein NAS-Volume muss mindestens 20 MB groß sein und als Maximalgröße kann der gesamte verfügbare Speicherplatz angegeben werden.
5. Geben Sie in **Alert when used space reaches (Warnen, wenn verwendeter Speicherplatz folgende Grenze erreicht)** einen Prozentsatz des zugewiesenen Speicherplatzes ein.
6. Wählen Sie aus der Liste **Send email alerts to administrator (E-Mail-Warnungen an den Administrator senden)** einen Dell Fluid File System-Administrator aus, an dessen E-Mail-Adresse das System Warnmeldungen senden soll.

   ANMERKUNG: Diese Funktion ist nicht auf Dell Compellent FS8600 NAS-Lösungen verfügbar. Weitere Informationen zum Umgang mit Warnmeldungen bei diesen Lösungen finden Sie in der Dokumentation des **Enterprise Manager**.
7. Wählen Sie aus der Liste **Access time granularity (Granularität der Zugriffszeit)** die Auflösung der Genauigkeit des Dateisystemzeitstempels basierend auf der erforderlichen Systemleistung aus.
8. Wählen Sie aus der Liste **File Access Security Style (Sicherheitsstil des Dateizugriffs)** den Sicherheitsstil des NAS-Volumes aus.

Sie können **NTFS**, **MIXED** oder **UNIX** auswählen.

9. Definieren Sie in **Default UNIX permissions of Windows files (Standard-UNIX-Berechtigungen von Windows-Dateien)** die Standard-UNIX-Berechtigungen für neue, aus Windows-Clients erstellten Dateien.
10. Definieren Sie in **Default UNIX permissions of Windows directories (Standard-UNIX-Berechtigungen von Windows-Verzeichnissen)** die Standard-UNIX-Berechtigungen für neue, aus Windows-Clients erstellte Verzeichnisse.
11. Klicken Sie auf **Save Changes (Änderungen speichern)**, um das NAS-Volume zu erstellen.

Ändern eines NAS-Volumes

So ändern Sie die Parameter eines spezifischen NAS-Volumes:

1. Wählen Sie **User Access (Benutzerzugang) → NAS Volumes (NAS-Volumes) → Configuration (Konfiguration).**
   Die Seite **NAS Volumes Configuration (NAS-Volumes Konfiguration)** zeigt die Liste der NAS-Volumes an.
2. Klicken Sie in der Liste der verfügbaren NAS-Volumes in der Spalte **NAS Volume** auf das entsprechende NAS-Volume.
   Die Seite **Edit NAS Volume (NAS-Volume bearbeiten)** wird für das ausgewählte NAS-Volume angezeigt.
3. Ändern Sie die Parameter wie erforderlich und klicken Sie auf **Save Changes (Änderungen speichern)**.

   ANMERKUNG: Wenn Sie den zugewiesenen Speicherplatz des NAS-Volumes ändern, wird die neue Zuweisung durch deren verwendeten Speicherplatz (Minimum) und den verfügbaren Speicherplatz in NAS-Cluster-Lösung (Maximum) begrenzt.

Entfernen eines NAS-Volumes

Das ausgewählte NAS-Volume wird gelöscht. Der von dem gelöschten NAS-Volume verwendete Speicherplatz wird im Hintergrund zurückgefordert.

ANMERKUNG: Bitte beachten Sie außerdem, dass NFS-Exporte, CIFS-Freigaben, NAS-Replikation, bzw. jeder Verweis auf das zu löschende NAS-Volume vor der erfolgreichen Löschung eines NAS-Volumes zuerst entfernt werden müssen.

ANMERKUNG: Durch das Löschen eines NAS-Volumes werden sowohl alle Dateien und Verzeichnisse als auch seine Eigenschaften gelöscht, also Freigaben, Snapshot-Definitionen usw. Einmal gelöscht kann das NAS-Volume nur dann wiederhergestellt werden, wenn es von einem externen Backup neu definiert und wiederhergestellt wird.

So entfernen Sie ein NAS-Volume:

1. Stellen Sie sicher, dass das NAS-Volume nicht gemountet (geladen) ist und warnen Sie die betreffenden Benutzer, dass sie getrennt werden.
2. Wählen Sie **User Access (Benutzerzugriff) → NAS Volumes (NAS-Volumes) → Configuration (Konfiguration).**
   Die Seite **NAS Volumes Configuration (NAS-Volumes Konfiguration)** zeigt die Liste der NAS-Volumes an.
3. Wählen Sie aus der Liste der verfügbaren NAS-Volumes das gewünschte NAS-Volume aus und klicken Sie auf **Delete (Löschen)**.

Freigaben und Exporte

Sie können Zugriffsberechtigungen für Dateien im Dateisystem gemäß den Hosts und Benutzern zugewiesenen Berechtigungen definieren. Dies geschieht durch Freigeben von Verzeichnissen mithilfe von NFS-Exporten und CIFS-Freigaben.

Verwalten von NFS-Exporten

NFS-Exporte sind ein effektiver Weg, um Dateien und Daten über UNIX/Linux-Netzwerke freizugeben. NFS-Clients können nur Verzeichnisse laden, die exportiert wurden.

Um die NFS-Exportliste zu verwalten, wählen Sie in der Registerkarte **User Access (Benutzerzugriff)** unter **Shares (Freigaben) NFS Exports (NFS-Exporte)** aus. Die Seite **NFS Exports (NFS-Exporte)** wird angezeigt und zeigt eine Liste der derzeit definierten NFS-Exporte.

Hinzufügen eines NFS-Exports zur NAS-Cluster-Lösung

So fügen Sie einen NFS-Export hinzu:

1. Wählen Sie **Benutzerzugriff** → **Freigaben** → **NFS-Exporte** aus.
   Daraufhin wird die Seite **NFS-Exporte** angezeigt.
2. Klicken Sie auf **Hinzufügen**.
   Die Seite **NFS-Export hinzufügen** wird angezeigt. Sie besteht aus zwei Registerkarten, **Allgemein** und **Erweitert**. Standardmäßig wird die Registerkarte **Allgemein** angezeigt.
3. Wählen Sie in der **NAS Volume** -Liste das NAS-Volume aus, auf dem sich der NFS-Export befinden soll.
4. Geben Sie in **Exportiertes Verzeichnis** den Pfad zu dem Verzeichnis an, das Sie exportieren möchten ein, oder klicken Sie auf das Browse-Symbol und navigieren Sie zum entsprechenden Verzeichnis.
5. Wählen Sie **Exportiertes Verzeichnis erstellen, falls nicht vorhanden** aus, wenn das Verzeichnis nicht vorhanden ist.
6. Wählen Sie in der Liste **Diesen Benutzern vertrauen** die Benutzer aus, denen Sie vertrauen.

   ANMERKUNG: Andere Benutzer werden als Gäste identifiziert.
7. Definieren Sie die Client-Geräte, die auf diesen NFS-Export zugreifen dürfen. Wählen Sie eine der folgenden Optionen aus:
   - **Alle Client-Geräte.**
   - **Ein einzelnes Client-Gerät** – Sie müssen **IP oder Domänenname** für den Client eingeben.
   - **Alle Client-Geräte in einem spezifischen Netzwerk** – Sie müssen die **IP-Adresse und Netzmaske** für den Client eingeben.

     ANMERKUNG: Wenn Sie zum Beispiel allen Mitgliedern des Subnetzes `192.10.x.x/16` mit Netzmaske `255.255.0.0` Zugriff gewähren möchten, geben Sie `192.10.0.0` in das Feld **IP-Adresse** und `255.255.0.0` in das Feld **Subnetz** ein.
   - **Alle Client-Geräte in einer spezifischen Netgroup** – Sie müssen den **Netgroup-Namen** für die Clients eingeben.
8. Wählen Sie in **Zugriff zulassen für** die entsprechenden Zugangsberechtigungen für die Freigabe aus. Sie müssen entweder **Lesen/Schreiben** oder **Schreibgeschützt** auswählen.

   ANMERKUNG: Wenn die Zugangsberechtigungen für die Freigabe strenger sind als die für eine bestimmte Datei definierten, so werden die Zugangsberechtigungen der Datei von denen der Freigabe überschrieben.
9. Wählen Sie die Registerkarte **Erweitert**.
10. Stellen Sie in **Begrenzte gemeldete Größe** einen Grenzwert für die gemeldete Größe des NFS-Exports ein, um den Zugriff für Client-Geräte zuzulassen, die keine großen Dateisysteme handhaben können.

    ANMERKUNG: Wenn Sie **Begrenzte gemeldete Größe** leer lassen, ist die gemeldete Größe die wirkliche Größe.
11. Wählen Sie in**Sicherer Port erforderlich? Nein** aus, um den Zugriff über unsichere Ports (Ports über 1024) zuzulassen.

12. Fügen Sie in **Anmerkung** eine Anmerkung oder eine Beschreibung für den NFS-Export hinzu.
13. Klicken Sie auf **Änderungen speichern**.

NFS-Export ändern

So bearbeiten Sie die Parameter eines spezifischen NFS-Exports in der NFS-Export-Liste:

1. Wählen Sie **User Access Benutzerzugriff) → Shares (Freigaben) → NFS Exports (NFS-Exporte).**
   Die Seite NFS Exports (NFS-Exporte) wird angezeigt.
2. Klicken Sie in der Liste der verfügbaren NFS-Exporte in der Spalte **Exported Directory (Exportiertes Verzeichnis)** auf den gewünschten NFS-Export.
   Die Seite **Edit NFS Export (NFS-Export bearbeiten)** wird für den ausgewählten NFS-Export angezeigt.
3. Ändern Sie die Parameter wie in den Registerkarten **General (Allgemein)** und **Advanced (Erweitert)** vorgegeben und klicken Sie auf **Save Changes (Änderungen speichern)**.

Entfernen eines NFS-Exports

So entfernen Sie einen NFS-Export:

1. Wählen Sie **User Access (Benutzerzugriff) → Shares (Freigaben) → NFS Exports (NFS-Exporte).**
   Daraufhin wird die Seite NFS Exportes (NFS-Exporte) angezeigt.
2. Wählen Sie aus der Liste der verfügbaren NFS-Exporte den gewünschten NFS-Export aus und klicken Sie auf **Delete (Löschen).**

Zugriff unter Verwendung von NFS

Um auf einem NAS-Volume einen NFS-Exportordner zu mounten, verwenden Sie aus einem Shell in einem Client-System den Befehl `su`, um sich als root (Stamm) anzumelden und führen Sie den folgenden Befehl aus:

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

Ältere UNIX-/Linux-Versionen verwenden jedoch TCP nicht standardmäßig. Der folgende Mount-Befehl gibt die korrekten Argumente an.

Um auf einem NAS-Volume einen NFS-Exportordner zu mounten, verwenden Sie aus einem Shell in einem Client-System den Befehl `su`, um sich als `root (Stamm)` anzumelden und führen Sie den folgenden Befehl aus:

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

Um Abwärtskompatibilität mit FluidFS Version 1 herzustellen, kann ein NFS-Export auf dem Standard-NAS-Volume auch gemountet werden mit:

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

So mounten Sie einen NFS-Exportordner auf ein NAS-Volume von MAC:

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

ANMERKUNG: Die oben genannten Parameter sind empfohlene Parameter. Weitere Informationen und Optionen finden Sie der Seite im Benutzerhandbuch zum `mount`-Befehl.

Um eine UDP- oder TCP-Verbindung zu ermöglichen, können Sie die Firewall auf zwei mögliche Arten konfigurieren:

- Stellen Sie die Firewall-Einstellungen so ein, dass die Quellen-IP-Adresse von einem der beiden Controller und nicht der Client-VIP stammt.
- Öffnen Sie den Port-Bereich für UDP, so dass folgende Ports ermöglicht werden:

Dienstname	FluidFS Port
portmap	111
Statd	4000 bis 4008
NFS	2049 bis 2057
nlm (lock manager)	4050 bis 4058
mount (Einbinden)	5001 bis 5009
Quota (Kontingent)	5051 bis 5059

Verwalten von CIFS-Freigaben

CIFS-Freigaben stellen eine effektive Möglichkeit zur Freigabe von Dateien und Daten über ein Windows-Netzwerk dar.

Eigenschaften und Status von CIFS-Freigaben anzeigen

So zeigen Sie Informationen zu den vorhandenen CIFS-Freigaben an:

1. Wählen Sie **User Access (Benutzerzugriff) → Shares (Freigaben) → CIFS Shares (CIFS-Freigaben).**
   Die Seite **CIFS Share (CIFS-Freigabe)** wird angezeigt.
2. Wählen Sie aus der Liste **Show CIFS Shares for NAS Volumes (CIFS-Freigaben für NAS-Volumes anzeigen)** ein bestimmtes NAS-Volume oder **All NAS Volumes (Alle NAS-Volumes)** aus.
   Die Tabelle der CIFS-Exporte wird für das ausgewählte NAS-Volume angezeigt.

Hinzufügen einer CIFS-Freigabe

So fügen Sie eine CIFS-Freigabe hinzu:

1. Klicken Sie auf **Benutzerzugriff → Freigaben → CIFS-Freigaben.**
   Daraufhin wird die Seite **CIF-Freigabe)** angezeigt.
2. Klicken Sie auf der Seite **CIFS-Freigabe)** auf **Hinzufügen**.
   Die Seite **CIFS-Freigabe hinzufügen** wird angezeigt. Standardmäßig wird die Registerkarte **Allgemein** ausgewählt.
3. Wählen Sie aus der **NAS Volume**-Liste das entsprechende NAS-Volume aus.
4. Um ein Verzeichnis zu erstellen, auf das alle Benutzer zugreifen können, wählen Sie **Freigabe mit allgemeinem Zugriff** aus.
   a) Geben Sie in **Freigabenname** den Namen der CIFS-Freigabe ein.
   b) Geben Sie in **Verzeichnis** den Pfad zu dem Verzeichnis an, das Sie exportieren möchten oder klicken Sie auf die Schaltfläche **Durchsuchen** und navigieren Sie zum entsprechenden Verzeichnis.
   c) Wählen Sie **Exportiertes Verzeichnis erstellen, falls nicht vorhanden** aus, wenn das Verzeichnis nicht vorhanden ist.
5. Um ein benutzerbasiertes Verzeichnis zu erstellen, in dem jeder Benutzer über ein dezidiertes Verzeichnis verfügt, wählen Sie **CIFS-Freigabe mit benutzerbasierter Verzeichnisstruktur** aus.
   Weitere Informationen finden Sie unter Erstellen von Basisfreigaben.

a) Geben Sie in **Pfadvorlage** die Pfadvorlage (die Grundlage der Basisverzeichnisse) für das CIFS-Freigabe-Volume ein.
b) Wählen Sie Benutzer aus, um den Benutzernamen zum Basisverzeichnis hinzuzufügen, oder wählen Sie Gruppe/Benutzer, um die primäre Gruppe und Benutzer zum Basisverzeichnispfad hinzuzufügen.

6. Geben Sie in **Anmerkung** eine Beschreibung oder eine Anmerkung zur CIFS-Freigabe ein.

   VORSICHT: Wählen Sie Dateien sollen auf Viren überprüft werden nur dann aus, wenn Sie einen externen Antivirus-Server konfiguriert haben.

7. Wählen Sie **Dateien sollen auf Viren überprüft werden** aus, um anzugeben, ob das System überprüfen soll, ob die Dateien nicht mit Viren infiziert sind, bevor es den Zugriff erlaubt.
8. Klicken Sie auf die Registerkarte **Erweitert** und geben Sie in **Diese Dateien ausblenden** die Dateitypen ein, die ausgeblendet werden sollen, wenn die Freigabe durchsucht wird.

   ANMERKUNG: Geben Sie zum Beispiel *.tmp ein, um alle Dateien mit der Erweiterung .tmp auszublenden.

9. Wählen Sie in **Gäste zulassen Ja** aus, um unbekannten Benutzern den Zugriff auf die Freigabe als Gast zu erlauben.

   ANMERKUNG: Wenn Sie **Dateien sollen auf Viren überprüft werden** in der Registerkarte **Allgemein** auswählen, wird die Registerkarte **Antivirus** aktiviert.

10. Klicken Sie auf die Registerkarte **Antivirus** und wählen Sie in **Richtlinie zur Behandlung von mit Virus infizierten Dateien auswählen:** eine der folgenden Optionen aus:

    - **Nichts tun** – Zugriff durch den Client wird verweigert, aber die Datei bleibt an ihrem ursprünglichen Speicherort (Zugriff ist nur durch eine andere CIFS-Freigabe zulässig, die nicht auf Viren überprüft wurde).
    - **Datei in Quarantäne stellen** – Zugriff durch den Client wird verweigert und die Datei wird in den Ordner **.Quarantine** im Stammordner des NAS-Volumes verschoben.
    - **Datei entfernen** – Zugriff durch den Client wird verweigert und die Datei wird gelöscht.

    ANMERKUNG: Das System wendet die angegebene Option an, wenn eine mit einem Virus infizierte Datei gefunden wird und der Antivirus-Host sie nicht davon befreien konnte.

11. Wählen Sie unter **Angeben, welche Dateien auf Viren geprüft werden sollen** eine der folgenden Optionen aus:

    - **Alle Dateien außer die mit bestimmten Erweiterungen überprüfen**
    - **Nur Dateien mit bestimmten Erweiterungen überprüfen**

    ANMERKUNG: Verwenden Sie eine durch Kommas getrennte Liste mit den Erweiterungen. Zum Beispiel: tmp, jpg, jpeg.

12. Geben Sie in **Dateien in den folgenden Ordner ausschließen** die Ordnernamen ein, die nicht vom Antivirenprogramm überprüft werden sollen.

    ANMERKUNG: Verwenden Sie eine durch Kommas getrennte Liste mit den Ordnern und fassen Sie die Ordnernamen mit Anführungszeichen ein, wenn sie ein Leerzeichen oder ein Komma enthalten. Sie können Platzhalter für Ordner-Spezifikationen angeben. Zum Beispiel: /Marketing/temp*,/Secrets,"/All Finance".

13. Klicken Sie auf **Änderungen speichern**.

    ANMERKUNG: Versuchen Sie nicht, eine CIFs-Freigabe mithilfe der Microsoft Management Console (MMC) zu erstellen. Verwenden Sie die MMC nur, um Freigabeebenenberechtigungen (share level permissions, SLPs) einzurichten.

CIFS-Freigabe ändern

Nachdem Sie festgelegt haben, ob eine CIFS-Freigabe ein Verzeichnis mit allgemeinem Zugriff oder ein Benutzer-basiertes Verzeichnis ist, können Sie diese Einstellung nicht mehr ändern. So ändern Sie die Parameter einer spezifischen CIFS-Freigabe:

1. Klicken Sie auf **Benutzerzugriff → Freigaben → CIFS-Freigaben).**
   Daraufhin wird die Seite **CIFS-Freigabe** angezeigt.
2. Klicken Sie in der Liste der verfügbaren CIFS-Freigaben in der Spalte **Freigabe** auf die gewünschte CIFS-Freigabe.
   Die Seite **CIFS-Freigabe bearbeiten** wird für die ausgewählte CIFS-Freigabe angezeigt. Standardmäßig ist die Registerkarte **Allgemein** ausgewählt.
3. Ändern Sie in der Registerkarte **Allgemein** die Parameter der CIFS-Freigabe.
4. Klicken Sie auf **Erweitert**, um erweiterte CIFS-Freigabeparameter zu ändern.

   ANMERKUNG: Wenn Sie **Dateien sollen auf Viren überprüft werden** in der Registerkarte **Allgemein** auswählen, wird die Registerkarte **Antivirus** aktiviert.
5. Wenn aktiviert, klicken Sie auf **Antivirus** und ändern Sie die Antivirus-Richtlinien.
6. Klicken Sie auf **Änderungen speichern**.

Entfernen einer CIFS-Freigabe

So entfernen Sie eine CIFS-Freigabe:

1. Klicken Sie auf **User Access (Benutzerzugriff) → Shares (Freigaben) → CIFS Shares (CIFS-Freigaben).**
   Daraufhin wird die Seite **CIFS Share (CIFS-Freigabe)** angezeigt.
2. Wählen Sie aus der Liste der verfügbaren CIFS-Freigaben die gewünschte CIFS-Freigabe aus und klicken Sie auf **Delete (Löschen).**

Erstellen von Basisfreigaben

Wenn eine CIFS-Freigabe mit benutzerbasierter Verzeichnisstruktur (Basisfreigabe) erstellt wird, so kann auf die Freigabe zunächst nicht zugegriffen werden. Der Grund dafür ist, dass alle Verzeichnisse für jeden Benutzer vom Administrator erstellt werden müssen. Dies kann mit einem Script (vom Benutzer erstellt), einer Stapeldatei oder mit PowerShell cmdlet erreicht werden, vom Speicher-Administrator geschrieben. Alternativ kann der Administrator diese Ordner auch manuell erstellen. Dadurch erhält er stärkere Zugriffskontrollen. Der Administrator kann entweder manuell die Konten bestimmen, die eine Basisfreigabe erhalten sollen, oder er schreibt ein Script, das die Ordner automatisch für manche oder alle Benutzer in einem bestimmten Active Directory oder in einer lokalen Benutzerdatenbank generiert.

ANMERKUNG: Das folgende Verfahren darf nur von einem Domänenadministrator durchgeführt werden, der auch der NAS-Speicheradministrator ist.

So erstellen Sie die Ordner der CIFS-Basisfreigabe manuell:

1. Überprüfen Sie im **NAS Manager**, dass das System an Ihre Active Directory angebunden ist.
2. Wenn Sie Active Directory verwenden, wählen Sie im **NAS Manager Cluster Management (Cluster-Verwaltung) → CIFS Configuration (CIFS-Konfiguration)** aus und stellen Sie sicher, dass **Authenticate users' identity via Active Directory and local users database (Benutzeridentität über Active Directory und lokale Benutzerdatenbank authentifizieren)** ausgewählt ist.
3. Erstellen Sie im **NAS Manager** eine allgemeine Zugriffsfreigabe, die der Stamm für alle Benutzerordner ist.
   Erstellen Sie zum Beispiel eine allgemeine Zugriffsfreigabe mit dem Freigabenname `users` im Verzeichnis `/users`, und wählen Sie die Option zum Erstellen des Ordners aus, falls noch nicht vorhanden.
4. Laden Sie mithilfe des **Windows Explorer** die **users**-Freigabe als lokaler CIFS-Administrator.
5. Klicken Sie in den Sicherheitseinstellungen der geladenen Freigabe auf **Advanced (Erweitert)** und ändern Sie den Eigentümer auf `Domain Admins (Domänenadministrator)` oder das spezifische Domänenadministrator- oder Speicheradministratorkonto um, für das Sie die Eigentumsrechte wünschen.

Dies ist das Konto, das die Ordner für die Basisfreigabe eines jeden Benutzers erstellt (entweder mithilfe eines vom Benutzer erstellten Scripts oder manuell).

6. Trennen oder unmounten Sie die **user**-Freigabe und laden Sie sie erneut als Konto, das über die Eigentumsrechte darüber verfügt, wie vorher eingestellt (als Domänenadministrator, Speicheradministrator oder spezifisch eingestellte Kontoeigentumsrechte).
7. Erstellen Sie im **NAS Manager** eine neue CIFS-Freigabe und wählen Sie den Freigabetyp **CIFS share containing a user-based directory tree (CIFS-Freigabe mit einer benutzerbasierten Verzeichnisstruktur)** aus.
8. Vorher wurde die allgemeine Zugriffsfreigabe mit Namen **users** im Pfad **/users** erstellt. Geben Sie in **Path template (Pfadvorlage) /users** ein und wählen Sie dann aus, ob die Benutzerordner die Form **/users/username** oder **/users/domain/username** annehmen sollen.
9. Klicken Sie auf **Save Changes (Änderungen speichern)**.
10. Beim **Windows Explorer** erstellen Sie für jeden Benutzer, der eine Basisfreigabe erhalten soll, einen Ordner, der der Pfadvorlage entspricht, welche Sie im vorigen Schritt erstellt haben.

    Dies kann entweder manuell oder mithilfe eines vom Benutzer erstellten Scripts geschehen.

Zugriffskontrolllisten und Freigabeebenenberechtigungen auf FluidFS einstellen

FluidFS CIFS-Freigaben unterstützen Zugangssteuerungslisten (ACLs) und Freigabeebenenberechtigungen (SLP). Es wird empfohlen, dass ein Windows-Administrator den von Microsoft definierten bewährten Methoden folgt. SLPs sprechen Rechte zur Vollkontrolle, Modifizierung und zum Lesen für den jeweiligen Benutzer oder die jeweilige Gruppe auf der Freibagenebene an, während ACLs weitere Details auf der Verzeichnis- oder Dateiebene bereitstellen. Es wird empfohlen, die Standardeinstellungen für SLP (jeder hat vollständige Kontrolle) unverändert zu belassen und ACLs für die Steuerung des Zugriffs auf die Freigabe zu verwenden, es sei denn eine spezifische Anforderung für SLPs ist vorhanden, die mithilfe von ACLs nicht ausgeführt werden kann.

Lokales FluidFS-Administratorkonto

Ein integriertes lokales FluidFS-Administratorkonto bietet Ersteinrichtung-Berechtigungen und Eigentumsrecht für neue CIFS-Freigaben. Das Konto wird dazu verwendet, ACLs einzustellen, wenn der NAS-Dienst nicht an eine Active Directory-Domain angebunden ist. Dieses integrierte Konto verfügt aus Sicherheitsgründen über ein zufällig generiertes Kennwort. Ändern Sie dieses Kennwort, um dieses Konto zum Einstellen von ACLs oder SLPs verwenden zu können.

Benutzerkonto mit CIFS-Vollzugriff (Backup-Benutzer)

Die Funktion „Benutzerkonto mit Vollzugriff“ wird dazu verwendet, um einem **Active Directory** (AD)-Benutzer vollen Zugriff auf alle darunter liegenden NAS-Daten zu gewähren. Diese Funktion wird hauptsächlich dazu verwendet, wenn eine Speichervirtualisierungs-Anwendung mit dem FluidFS NAS-Gerät genutzt wird. Diese Art von Anwendung verwendet ein AD-Konto, um auf alle darunter liegenden NAS-Systeme zuzugreifen.

Das System muss Teil eines Active Directory (AD) sein, um diese Berechtigung mit einem AD-Konto zu verbinden. Die Berechtigungen des Benutzers mit Vollzugriff geben dem AD-Konto Vollzugriff auf alle Daten auf allen Freigaben und allen Volumes, ungeachtet der Datei-ACL-Definitionen. Die Einstellungen der SLPs (Freigabeebenenberechtigungen) jedoch gelten für das AD-Konto, das über die Berechtigungen des **Benutzers mit Vollzugriff** verfügt. Es ist die Aufgabe des NAS-Systemadministrators zu überprüfen, dass das AD-Konto mit Vollzugriff über alle wichtigen SLPs verfügt.

So verwalten Sie den Benutzer mit Vollzugriff:

1. Öffnen Sie eine Verbindung mit der CLI über eine direkte KVM-Verbindung oder über SSH zur Verwaltungs-VIP.
2. Um das Konto **Benutzer mit Vollzugriff** einzurichten oder den aktuellen Eintrag zu überschreiben, führen Sie in der CLI den folgenden Befehl aus:

```
system authentication full-access-account set DOMAIN+username
```

3. Um zu überprüfen, dass das Konto **Benutzer mit Vollzugriff** richtig eingerichtet ist, führen Sie den folgenden Befehl aus:
   ```
   system authentication full-access-account view
   ```
4. Um den **Benutzer mit Vollzugriff** zu löschen, führen Sie den folgenden Befehl aus:
   ```
   system authentication full-access-account delete
   ```

Active Directory-Konfiguration

FluidFS kann einem Active Directory-Domäne angeschlossen werden. Dies kann mit Hilfe des NAS-Manager unter Verwendung von **Clusterverwaltung** → **Authentifizierung** → **Systemidentität**oder dem CLI gemacht werden. Weitere Informationen über den Anschluss ans Active Directory mit dem CLI finden Sie im *FluidFS-Befehlszeilen-Referenzhandbuch* unter **dell.com/support/manuals**.

Damit das FluidFS NAS-Gerät an die Active Directory-Domäne angeschlossen werden kann, müssen Sie Anmeldeinformationen für den Anschlussvorgang bereitstellen.

ANMERKUNG: Der Anschlussvorgang ist das einzige Mal, dass diese Anmeldeinformationen erfordert werden. Die Anmeldeinformationen werden nicht vom FluidFS NAS-Gerät gespeichert oder gecacht.

Der Administrator hat drei Optionen zum Festlegen der Anmeldeinformationen, die zur Verbindung des FluidFS NAS-Geräts mit dem Active Directory verwendet werden:

- Schließen Sie den NAS-Cluster mit Hilfe eines Domänen-Adminkontos an.

  ANMERKUNG: Dies ist die empfohlene Methode.
- Verbinden Sie den NAS-Cluster mit der Active Directory-Domäne mit Hilfe eines Kontos, dem das Privileg **einen Computer einer Domäne anschließen** zugestanden wurde, sowie die vollständige Kontrolle über alle Computerobjekte in der Domäne.
- Falls ein Domänen-Adminkonto oder ein Konto mit vollständiger Kontrolle über alle Computerobjekte in der Domäne nicht zur Verfügung steht, ist die Mindestanforderung zum Anschluss des NAS-Geräts an die Active Directory-Domäne folgendes:
  - Ein organisatorische Einheit (OU)-Admin, dem das Privileg **einen Computer der Domäne anschließen** gewährt wurde.
  - Der OU-Admin muss auch vollständige Kontrolle über Objekte innerhalb der OU erhalten, einschließlich über die Computerobjekte.
  - Bevor das System der Domäne angeschlossen wird, muss ein Computerobjekt vom OU-Admin für das System erstellt werden; in der OU werden Privilegien zur Administration bereitgestellt.
  - Der NAS-Geräte-Computerobjektname und der NetBIOS-Name, die beim Anschluss verwendet werden, müssen übereinstimmen.
  - Wählen Sie bei der Erstellung des NAS-Gerätecomputerobjekts im Feld **Benutzer** oder **Gruppe** unter den Berechtigungen zum Anschluss an die Domäne das OU-Adminkonto. Dann kann das NAS-Gerät unter Verwendung der OU-Admin-Anmeldeinformationen angeschlossen werden.

ANMERKUNG: FluidFS NAS-Cluster brauchen Lesezugriff für das Attribut `tokenGroups` für alle Benutzer. Die Standardkonfiguration des Active Directory für alle Domänencomputer gewährt Lesezugriff zum Attribut `tokenGroups`. Falls die Berechtigung nicht erteilt wird, erhalten Active Directory-Domänenbenutzer in verschachtelten Gruppen oder OUs den Fehler **Zugriff verweigert**, und Benutzer, die nicht in verschachtelten OUs oder Gruppen sind, erhalten Zugriff.

Einrichten von ACLs oder SLPs auf einer CIFS-Freigabe

Die FluidFS NAS-Lösung unterstützt zwei Stufen von Zugangskontrolle auf Freigaben, Dateien und Ordner:

- Zugriffssteuerungsliste (ACL) – kontrolliert den Zugriff auf bestimmte Dateien und Ordner. Der Administrator kann einen großen Bereich von Vorgängen kontrollieren, die Benutzer und Gruppen ausführen können.
- Berechtigungen auf Freigabestufe (Share Level Permissions, SLP) – kontrolliert den Zugriff auf die ganzen Freigaben. Der Administrator kontrolliert den Zugriff für Nur-Lesen, ändern oder den vollständigen Zugriff auf eine ganze Freigabe.

ACLs bieten eine feinere Kontrolle und können viel mehr Vorgänge kontrollieren als Nur-Lesen/Ändern/Vollständiger Zugriff. Es wird empfohlen, die Standardeinstellung für SLP (jedermann hat vollständige Kontrolle) auf der Standardeinstellung zu belassen und ACLs zur Kontrolle des Zugriffs auf die Freigabe zu verwenden, außer es gibt eine bestimmte Anforderung für SLPs, die mit der Verwendung von ACLs nicht erfüllt werden kann.

Beim ersten Erstellen einer CIFS-Freigabe muss der Eigentümer der Freigabe geändert werden, bevor ACLs eingestellt werden oder versuchen können, auf die Freigabe zuzugreifen. Wenn die NAS-Cluster-Lösung einer Active Directory-Domäne angebunden ist, können die folgenden Methoden zum Einstellen von ACLs verwendet werden:

- Verwendung eines Active Directory Domain-Kontos, dessen primäre Gruppe als Admingruppe der Domain eingestellt ist.
- Verwendung des lokalen FluidFS-Administratorkontos (wird verwendet, wenn nicht am Active Directory angeschlossen oder die Admin-Anmeldeinformationen der Domäne nicht verfügbar sind).

Verwenden eines Active Directory, das als Mitglied der Domain-Admingruppe eingestellt ist

So verwenden Sie ein Active Directory Domain-Konto, dessen primäre Gruppe als Admingruppe der Domain eingestellt ist:

1. Öffnen Sie **Windows Explorer** und geben Sie in der Adressenleiste Folgendes ein: `\\<AccessVip>\C$`
   Eine Liste aller NAS-Volumes, auf die vom bestimmten FluidFS-System zugegriffen werden kann, wird als Verzeichnisse angezeigt.
2. Doppelklicken Sie auf das erforderliche Volume.
   Eine Liste aller CIFS-Freigaben für dieses NAS-Volume wird angezeigt.
3. Klicken Sie mit der rechten Maustaste auf die gewünschte CIFS-Freigabe (Ordner) und wählen Sie **Eigenschaften** aus.
4. Wählen Sie die Registerkarte **Sicherheit** aus und klicken Sie dann auf **Erweitert**.
5. Wählen Sie die Registerkarte **Besitzer** und wählen Sie anschließend die Registerkarte **Bearbeiten**.
6. Klicken Sie auf die Schaltfläche **Andere Benutzer oder Gruppen** und wählen Sie das Domain-Administratorkonto aus, das zum Einrichten der ACLs für diese Freigabe verwendet wird, oder wählen Sie die Gruppe Domain Admins (Domain-Administratoren) aus.
7. Stellen Sie sicher, dass **Besitzer von Subcontainern und Objekten ersetzen** aktiviert wurde und klicken Sie auf **Anwenden**.
8. Klicken Sie auf **Ok** und kehren Sie zum Fenster **Erweiterte Sicherheitseinstellungen** zurück.

Sie können die Registerkarte **Berechtigungen** und den besten Verfahren von Microsoft folgen, um dementsprechend dem CIFS-Freigabeordner ACL-Berechtigungen zuzuweisen.

ANMERKUNG: Wenn Sie auf dem gleichen NAS-Volume sowohl CIFS-Freigaben und auch NFS-Freigaben definiert haben, sehen Sie darin sowohl die NFS- wie auch die CIFS-Freigaben. Stellen Sie sicher, dass Sie nur die erforderliche CIFS-Freigabe auswählen.

Verwenden des Kontos für den lokalen FluidFS-Administrator

1. Starten Sie den Assistenten **Netzwerklaufwerk zuweisen**. Geben Sie unter **Ordner**: **\\<Zugriffs-VIP>\<Freigabenname>** ein.

ANMERKUNG: Sie können die Verbindung zur CIFS-Freigabe mithilfe des Client-Zugriffs-VIP- oder des DNS-Namens herstellen.

2. Wählen Sie **Verbindung unter anderen Anmeldeinformationen herstellen** aus.

   Verwenden Sie die folgenden Anmeldeinformationen: NetBIOS Name\Administrator

   Standardmäßig lautet der NetBIOS-Name **CIFSStorage**.

   ANMERKUNG: Sie können den NetBIOS-Namen im NAS-Manager ändern, indem Sie zu **Systemverwaltung** → **Authentifizierung** → **Systemidentität** navigieren.

3. Klicken Sie mit der rechten Maustaste auf die neu zugewiesene Freigabe und wählen Sie **Eigenschaften** aus.
4. Wählen Sie die Registerkarte **Sicherheit** aus und klicken Sie dann auf **Erweitert**.
5. Wählen Sie die Registerkarte **Benutzer** aus und wählen Sie anschließend die Registerkarte **Bearbeiten** aus.
6. Klicken Sie auf die Schaltfläche **Andere Benutzer oder Gruppen** und wählen Sie das Domain-Administratorkonto aus, das für diese Freigabe ACLs einrichten wird oder wählen Sie die Gruppe Domain-Administratoren aus. Alternativ dazu kann das lokale CIFS-Administratorkonto verwendet werden.
7. Stellen Sie sicher, dass **Besitzer von Subcontainern und Objekten ersetzen** aktiviert wurde und klicken Sie auf **Anwenden**.
8. Klicken Sie auf **Ok** und kehren Sie zum Fenster **Erweiterte Sicherheitseinstellungen** zurück.
9. Heben Sie die Zuweisung des Netzwerklaufwerks auf, nachdem der Besitzer eingestellt wurde.
10. Weisen Sie das Netzwerklaufwerk entweder dem als Besitzer eingestellten Domain-Administratorkonto neu zu, oder einem beliebigen Domain-Administrator. Falls der Besitzer auf die Domain-Administrator-Gruppe eingestellt wurde, folgen Sie den bewährten Methoden von Microsoft und weisen Sie Benutzern und Gruppen entsprechend ACL-Berechtigungen zu.

Wenn der NAS-Dienst nicht an eine Active Directory-Domain angebunden ist, muss das integrierte CIFS-Administratorkonto zur Einrichtung jeglicher ACLs verwendet werden. Um SLPs zu definieren, verwenden Sie MMC (Microsoft Management Console).

ANMERKUNG: Versuchen Sie nicht, eine CIFS-Freigabe unter Verwendung der MMC zu erstellen.

Zuweisen eines Netzlaufwerks zur CIFS-Freigabe

So weisen Sie ein Netzwerklaufwerk einer CIFS-Freigabe zu, auf der ACLs eingerichtet werden sollen:

1. Wählen Sie **Anderen Benutzernamen verwenden** aus.

   Verwenden Sie bei Aufforderung die folgenden Anmeldeinformationen:

   `<NetBios Name>\Administrator`

   Standardmäßig ist der Name des NetBios **CIFSStorage**. Wenn er nicht geändert wurde, geben Sie `CIFSStorage \Administrator` ein.

   ANMERKUNG: Sie können den NetBios-Namen im NAS-Manager ändern, indem Sie zu **Clusterverwaltung** → **Authentifizierung** → **Systemidentität** navigieren.

2. Befolgen Sie die Anweisungen, um den Besitzer der CIFS-Freigabe auf entweder ein Domain-Administrator-Benutzerkonto oder die Domain-Administratorengruppe einzustellen.
3. Heben Sie die Zuweisung des Netzwerklaufwerks auf, nachdem der Besitzer eingestellt wurde.
4. Weisen Sie das Netzlaufwerk neu mit einem Konto zu, das Teil der Benutzergruppe des Domänenadministrators ist, der vorher Eigentumsrechte zugeteilt wurden. Folgen Sie den bewährten Methoden von Microsoft und weisen Sie Benutzern und Gruppen entsprechend ACL-Berechtigungen zu.

   Wenn der NAS-Dienst nicht an eine Active Directory-Domain angebunden ist, muss das integrierte CIFS-*Administrator*konto zur Einrichtung jeglicher ACLs verwendet werden. Um SLPs zu definieren, verwenden Sie MMC.

ANMERKUNG: Versuchen Sie nicht, eine CIFS-Freigabe unter Verwendung der Microsoft Management Console (MMC) zu erstellen.

Zugriff unter Verwendung von CIFS

Microsoft Windows bietet mehrere Methoden, um sich mit CIFS-Freigaben zu verbinden.

Wählen Sie eine der folgenden Optionen, um von Windows aus zuzuweisen:

Option 1

Führen Sie den Befehl **net use** in der Eingabeaufforderung aus.

`net use` <*Laufwerkbuchstabe*>: \\< *NetBIOS-Name*> \< *Freigabenname* >

Option 2

1. Wählen Sie im **Start-**Menü die Option **Run (Ausführen)** aus.
   Das Fenster **Ausführen** wird angezeigt.
2. Geben Sie den Pfad zu der Freigabe ein, mit der Sie sich verbinden wollen:
   `\\Client Access VIP >\<share name>.`
3. Klicken Sie auf **OK**.
   Das **Explorer-**Fenster wird angezeigt.

Option 3

1. Öffnen Sie den **Windows Explorer** und wählen Sie **Tools (Extras)** → **Map Network Drive (Netzlaufwerk zuweisen).**
   Das Dialogfeld **Map Network Drive (Netzlaufwerk zuweisen)** wird angezeigt.
2. Wählen Sie aus der Dropdown-Liste **Drive (Laufwerk)** ein beliebiges verfügbares Laufwerk aus.
3. Geben Sie den Pfad in das Feld **Folder (Ordner)** ein und browsen Sie zum freigegebenen Ordner.
4. Klicken Sie auf **Finish (Fertigstellen)**.

Option 4

ANMERKUNG: Mit dieser Option können Sie eine Verbindung zur Freigabe herstellen, eine Zuweisung ist jedoch nicht möglich.

1. Klicken Sie im Windows **Desktop** auf **Netzwerknachbarschaft** und suchen Sie das NAS-Gerät.
2. Wählen Sie das NAS-Gerät aus und doppelklicken Sie auf das ausgewählte NAS-Gerät.
3. Wählen Sie aus der Liste **CIFS-Freigaben** die Freigabe aus, zu der Sie eine Verbindung herstellen möchten.

Konfigurieren von CIFS-Freigabeebenenberechtigungen

Das Konfigurieren von CIFS-Freigabeebenenberechtigungen (SLP) kann nur unter Verwendung der Microsoft Management Console (MMC) erfolgen.

Administratoren können eine vordefinierte MMC-Datei (.msc) vom Windows Server 2000/2003/2008 Startmenü aus verwenden und ein Snap-In für einen **freigegebenen Ordner** zur Verbindung mit dem NAS-Cluster verwenden.

In der MMC können Sie nicht auswählen, welchen Benutzer Sie mit einem Remote-Computer verbinden möchten. Standardmäßig verwendet die MMC der Benutzer, der auf dem Gerät zum Verbindungsaufbau angemeldet ist.

So verwenden Sie den richtigen Benutzer für die MMC-Verbindung:

- Wenn das NAS-Gerät, das Sie verwalten wollen, an ein Active Directory angebunden ist, dann melden Sie sich auf Ihrer Management-Station mit **<Domain>\Administrator** an.
- Bevor Sie die MMC verwenden, verbinden Sie sich mit der NAS-Cluster-Lösung unter Verwendung der Client-Zugriffs-VIP-Adresse in der Adressenleiste des Windows Explorers. Melden Sie sich mit dem Administratorkonto an und verbinden Sie sich dann zur MMC.

Wenn Sie den letzten Schritt ausführen, müssen Sie ggf. zuerst das lokale Administratorkennwort zurücksetzen.

Sollten keine vordefinierten MMC-Dateien vorhanden sein:

1. Klicken Sie auf **Start** → **Ausführen.**
2. Geben Sie `mmc` ein und klicken Sie auf **OK**.

   Das Fenster **Konsole 1 - [Konsolenstamm]** wird angezeigt.
3. Klicken Sie auf **Datei** → **Snap-In hinzufügen/entfernen**.
4. Wählen Sie **Freigegebene Ordner** aus und klicken Sie auf **Hinzufügen**.
5. Wählen Sie im Fenster **Freigegebene Ordner Anderer Computer** aus und geben Sie den Namen Ihrer NAS-Cluster-Lösung ein (wie im DNS konfiguriert). Alternativ können Sie die Client-Zugriffs-VIP-Adresse verwenden.
6. Klicken Sie auf **Fertigstellen**.

   Die neue Freigabenstruktur wird im Fenster **Konsolenstamm** angezeigt.
7. Klicken Sie mit der rechten Maustaste auf die gewünschte Freigabe und wählen Sie **Eigenschaften**, um die Freigabeebenenberechtigungen einzustellen.
8. Wählen Sie im Fenster **Freigabeeigenschaften** die Registerkarte **Freigabeberechtigungen** aus.

Auf Zugriff basierende Freigabenaufzählung

In Version v2 von Dell Fluid File System ist die auf SLP-Zugriff basierende Freigabenaufzählung standardmäßig aktiviert. Als Ergebnis werden Benutzer und Gruppen auf der Freigabe nur dann angezeigt, wenn Share Level Permissions (Freigabeebenenberechtigungen, SLPs) vorliegen. Wenn ein bestimmter Benutzer oder eine bestimmte Gruppe nicht über Freigabeberechtigungen für eine bestimmte Freigabe verfügt, wenn auf das NAS-Cluster direkt über **\\<client access VIP>** zugegriffen wird, dann erscheint die Freigabe nicht in der Liste der verfügbaren Freigaben. In der früheren Version, Dell Fluid File System v1, war die auf Zugriff basierende Freigabenaufzählung nicht aktiviert, darum wurde die Freigabe angezeigt, aber es konnte nicht auf sie zugegriffen werden.

Zurücksetzen des lokalen CIFS-Administratorkennworts

ANMERKUNG: Während der Installation wird ein zufälliges Kennwort erstellt. Setzen Sie das Kennwort zurück.

Sie können nun den Administratorbenutzer verwenden, um in MMC zu browsen. Dies wird auch als lokaler CIFS-Administrator bezeichnet.

So setzen Sie das lokale CIFS-Administratorkennwort zurück:

1. Melden Sie sich beim NAS-Manager an.
2. Wählen Sie **Clusterverwaltung** → **Authentifizierung** → **Lokale Benutzer** aus.

   Das Fenster **Lokale Benutzer** wird angezeigt.
3. Wählen Sie den Benutzer **Administrator**.
4. Wählen Sie **Kennwort ändern**.

Kontingente

Ein Laufwerkskontingent ist eine Sammlung von Richtlinien, die den Laufwerksspeicherplatz und die Anzahl der von einem Benutzer oder einer Gruppe verwendeten Dateien einschränken. Ein Kontingent kann auch den gesamten, in

einem NAS-Volume verwendeten Speicherplatz oder die Verwendung von Benutzern und Gruppen innerhalb eines NAS-Volumes einschränken. Kontingentwerte beziehen sich immer auf ein bestimmtes Volume und werden in Megabyte (MB) angegeben.

ANMERKUNG: Benutzer und Gruppen, für die kein eigenes Kontingent definiert wird, verwenden das Standardkontingent für Benutzer bzw. Gruppen.

Quotenerwägungen

- Quotenerwägungen bei der Verwendung von Datenträgern verschiedener Arten – Für NAS-Datenträger mit gemischten Sicherheitsstilen muss eine eindeutige Quote für Windows (Active Directory)-Benutzer sowie UNIX-Benutzer (LDAP oder NIS) eingestellt werden. Die Quoten für die Windows- und UNIX-Benutzer sind unabhängig voneinander, auch wenn die Benutzer (automatisch oder manuell) zugewiesen wurden.
- Quotenerwägungen beim Zugriff auf CIFS und NFS – Für NAS-Datenträger mit Berechtigungen des Stils NTFS oder UNIX muss nur eine eindeutige Quote eingestellt werden. Die Benutzerzuweisungsfunktion sorgt für die Interoperabilität über Protokolle hinweg. Der UNIX- und der Windows-Benutzer teilen dieselbe Quote für die Windows- sowie die UNIX-Konten, die zugewiesen wurden.

Verwalten von Standardkontingenten

So verwalten Sie die Standardkontingente auf einem Volume:

ANMERKUNG: Das Standardkontingent kann durch benutzer- oder gruppenspezifische Kontingente überschrieben werden.

1. Wählen Sie **User Access (Benutzerzugriff) → Quota (Kontingent) → Default (Standard).**

   Das Fenster **Default Quota (Standardkontingente)** wird angezeigt.
2. Wählen Sie aus der Liste **NAS Volume** das entsprechende NAS-Volume, auf dem das Kontingent hinzugefügt oder modifiziert werden kann.
3. Unter **Default quota per user (Standardkontingent pro Benutzer)** wählen Sie das gewünschte Benutzerkontingent aus und geben es in MB ein oder wählen **Unlimited (Unbegrenzt)**.

   ANMERKUNG: Wenn dieser Grenzwert überschritten wird, ist das Schreiben auf das NAS-Volume nicht mehr zulässig.
4. Unter **Alert administrator when quota reaches (Administrator benachrichtigen, wenn Kontingent folgenden Wert erreicht)** wählen Sie das gewünschte Benutzerkontingent aus und geben es in MB ein oder wählen **Disabled (Deaktiviert)**.

   ANMERKUNG: Wenn dieser Grenzwert überschritten wird, wird eine Warnmeldung an die E-Mail-Adresse des Empfängers gesendet. Diese Standardeinstellung wird bei Benutzern verwendet, für die kein individuelles Kontingent definiert ist.
5. Unter **Default quota per user (Standardkontingent pro Benutzer)** wählen Sie das gewünschte Benutzerkontingent aus und geben es in MB ein oder wählen **Unlimited (Unbegrenzt)**.

   ANMERKUNG: Wenn dieser Grenzwert überschritten wird, ist das Schreiben auf das NAS-Volume nicht mehr zulässig.
6. Unter **Alert administrator when quota reaches (Administrator benachrichtigen, wenn Kontingent folgenden Wert erreicht)** wählen Sie das gewünschte Gruppenkontingent aus und geben es in MB ein oder wählen **Disabled (Deaktiviert)**.

   ANMERKUNG: Wenn dieser Grenzwert überschritten wird, wird eine Warnmeldung an die E-Mail-Adresse des Administrators gesendet. Diese Standardeinstellung wird bei Benutzern verwendet, für die kein individuelles Kontingent definiert ist.
7. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Verwalten von benutzer- oder gruppenspezifischen Kontingenten

Vorhandene benutzer-/gruppenspezifische Kontingente anzeigen

So zeigen Sie die Einzelheiten für ein spezifisches Benutzer- oder Gruppenkontingent an:

1. Wählen Sie **User Access (Benutzerzugriff) → Quota (Kontingent) → User/Group (Benutzer/Gruppe).**
   Die Seite **User/Group Quota (Benutzer-(Gruppenkontingent)** wird angezeigt.
2. Wählen Sie aus der Liste **Show quotas for NAS Volume (Kontingente für NAS-Volume anzeigen)** das gewünschte NAS-Volume oder **All NAS Volumes (Alle NAS-Volumes)** aus.
   Die Liste der verfügbaren Benutzer-/Gruppenkontingente für das ausgewählte NAS-Volume wird angezeigt. Standardmäßig werden Informationen zu Benutzer-/Gruppenkontingenten für **All NAS Volumes (Alle NAS-Volumes** angezeigt**.**

Kontingenttypen

Die folgenden Kontingenttypen sind verfügbar:

- User (Benutzer) - Pro Benutzerkontingent.
- All of group (Gesamte Gruppe) - Gesamtkontingent der ganzen Gruppe.
- Any user in group (Jeder Benutzer in der Gruppe) - Kontingent für jeden Benutzer, der der Gruppe angehört.

Benutzer-/gruppenspezifische Kontingente hinzufügen

So fügen Sie ein Kontingent hinzu:

1. Wählen Sie **User Access (Benutzerzugriff) → Quota (Kontingent) → User/Group (Benutzer/Gruppe).**
   Die Seite **User/Group Quota (Benutzer-/Gruppenkontingent)** wird angezeigt.
2. Klicken Sie auf **Add (Hinzufügen)**.
   Es wird die Seite **Create Quota** (Kontingent erstellen) angezeigt.
3. Wählen Sie aus der Liste **NAS Volume** das gewünschte NAS-Volume aus, dem Sie das Kontingent hinzufügen möchten.
4. Wählen Sie aus der Liste **Quota for (Kontingent für)** den gewünschten Beschränkungstyp für das Kontingent aus und gegen Sie den entsprechenden Benutzer- bzw. Gruppennamen ein oder klicken Sie auf die Schaltfläche Browse (Durchsuchen), um den gewünschten Benutzer oder die Gruppe auszuwählen.

   ANMERKUNG: Das Auflisten von Benutzern kann einige Zeit in Anspruch nehmen, je nach Anzahl der Benutzer in Ihrer Active Directory-Domäne. Während dieser Wartezeit kann es zu sporadischen Authentifizierungsfehlern kommen. Wenn Sie den Benutzernamen kennen, können Sie ihn eingeben, anstatt alle Benutzer aufzulisten.

5. Wählen Sie in **Quota (Kontingent)** das Kontingent in MB aus und geben es ein oder klicken Sie auf **Unlimited (Unbegrenzt)**.

   ANMERKUNG: Wenn der Benutzer oder die Gruppe bereits diese Datenmenge verwendet, werden neue Schreibvorgänge verweigert.

6. Unter **Alert administrator when quota reaches (Administrator benachrichtigen, wenn Kontingent folgenden Wert erreicht)** wählen Sie das gewünschte Gruppenkontingent aus und geben es in MB ein oder wählen **Disabled (Deaktiviert)**.

   ANMERKUNG: Wenn die Höchstgrenze überschritten wird, wird eine Warnmeldung an die E-Mail-Adresse des Administrators gesendet.

ANMERKUNG: Diese Standardeinstellung wird für Benutzer verwendet, für die kein eigenes Kontingent definiert wurde.

7. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Benutzer-/gruppenspezifische Kontingente

So bearbeiten Sie ein vorhandenes Kontingent:

1. Wählen Sie **User Access (Benutzerzugriff) → Quota (Kontingent) → User/Group (Benutzer/Gruppe).**
   Die Seite **User/Group Quota (Benutzer-/Gruppenkontingent** wird angezeigt.
2. Wählen Sie aus der Liste **NAS Volume** das entsprechende NAS-Volume.
   Die Tabelle **User/Group Quota (Benutzer-/Gruppenkontingent)** zeigt die Liste mit verfügbaren **User/Group Quotas (Benutzer-/Gruppenkontingenten)** für das ausgewählte NAS-Volume an.
3. Klicken Sie in der Liste der verfügbaren Benutzer-/Gruppenkontingente in der Spalte **Name/ID** auf das gewünschte Benutzer-/Gruppenkontingent.
   Es wird die Seite **Edit Quota (Kontingent bearbeiten)** angezeigt.
4. Bearbeiten Sie die Kontingentregeln wie gewünscht und klicken Sie auf **Save Changes (Änderungen speichern)**.

Löschen eines Kontingents

So löschen Sie eine Kontingentrichtlinie:

1. Wählen Sie **User Access (Benutzerzugriff) → Quota (Kontingent) → User/Group (Benutzer/Gruppe).**
   Die Seite **User/Group Quota (Benutzer-/Gruppenkontingent)** wird angezeigt.
2. Wählen Sie aus der **NAS Volume**-Liste das entsprechende NAS-Volume aus.
   Die Tabelle **User/Group Quota (Benutzer-/Gruppenkontingent)** zeigt die Liste mit verfügbaren **User/Group Quotas (Benutzer-/Gruppenkontingenten)** für das ausgewählte NAS-Volume an.
3. Wählen Sie aus der Liste der verfügbaren Benutzer-/Gruppenkontingente die angemessene Kontingentrichtlinie aus und klicken Sie auf **Delete (Löschen)**.

4

Schutz von Daten in der FluidFS NAS-Cluster-Lösung

Der Schutz von Daten ist wichtiger und integrierter Bestandteil einer jeden Speicherinfrastruktur. Sie können verschiedene Methoden zum Datenschutz in Ihrem Dell Fluid File System konfigurieren, inklusive:

- Snapshots
- Replikation
- Systemwiederherstellung von einem Backup aus
- Konfiguration des Backup-Agents

Snapshots

Die Snapshot-Technologie erstellt ein Zeitpunkt-Backup der Daten, die sich auf einem Volume befinden. Zur Erstellung eines Snapshots können verschiedene Richtlinien erstellt werden, darunter wann ein Snapshot gemacht werden soll, wie viele Snapshots behalten werden und wie viel Speicherplatz auf dem NAS-Volume genutzt werden kann, bevor Snapshots gelöscht werden. Snapshots basieren auf Änderungen. Nachdem der erste Snapshot eines NAS-Volumes erstellt ist, sind alle danach erstellten Snapshots Deltas (Änderungen) des vorherigen Snapshots.

Weitere Informationen zu Snapshots finden Sie in der *Online-Hilfe*.

Hinzufügen oder Bearbeiten einer Snapshot-Richtlinie

1. Wählen Sie **Data Protection (Datenschutz)** → **Snapshots** → **Policies (Richtlinien).**

   Die Seite **Snapshot Policies (Snapshot-Richtlinien)** wird angezeigt.
2. Wählen Sie aus der Liste **NAS Volume** das entsprechende NAS-Volume.
3. Geben Sie in **Alert the administrator when snapshot space is % of total volume (Administrator benachrichtigen, wenn Snapshot-Speicherplatz % des gesamten Volumes beträgt** den gewünschten Prozentsatz am gesamten NAS-Volume-Speicherplatz ein.

   Wenn dieser Grenzwert überschritten wird, werden Snapshots automatisch gelöscht.

   ANMERKUNG: Lassen Sie dieses Feld leer, um Ereignisse zum Snapshot-Speicherplatz zu deaktivieren.

   ANMERKUNG: Es werden sowohl geplante als auch vom Benutzer erstellte Snapshots gelöscht. Replikations-Snapshots werden nicht gelöscht.
4. Wählen Sie **Periodic (Periodisch)** aus, um Snapshots in einer Periode von weniger als einer Stunde zu erstellen:
   a) Wählen Sie die Minutenfrequenz aus der Liste **Every Minutes (Alle Minuten)** aus.
   b) Geben Sie die **Number of snapshots to keep (Anzahl der zu behaltenden Snapshots)** ein.
5. Wählen Sie **Hourly (Stündlich)** aus, um jede Stunde einen Snapshot zu erstellen:
   a) Wählen Sie entweder **Every hour (Jede Stunde)** oder **At (Um)** und die gewünschte Uhrzeit **inklusive Minuten** aus, zu der die Snapshots erstellt werden sollen.
   b) Geben Sie die **Number of snapshots to keep (Anzahl der zu behaltenden Snapshots)** ein.
6. Wählen Sie **Daily (Täglich)** aus, um Snapshots je nach Tag zu erstellen.
   a) Wählen Sie entweder **Every day (Jeden Tag)** oder **On (Am)** und die gewünschten Tagen aus.

b) Wählen Sie in **At (Um)** die Uhrzeit aus, zu der der Snapshot erstellt werden soll.
c) Geben Sie die **Number of snapshots to keep (Anzahl der zu behaltenden Snapshots)** ein.

7. Wählen Sie **Weekly (Wöchentlich)** aus, um Snapshots jede Woche zu erstellen.
   a) Wählen Sie aus der Liste **On (Am)** den Tag und die Uhrzeit aus, zu der der Snapshot erstellt werden soll.
   b) Geben Sie die **Number of snapshots to keep (Anzahl der zu behaltenden Snapshots)** ein.
8. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Erstellen eines Snapshots (ohne Richtlinie)

1. Wählen Sie **Data Protection (Datenschutz) → Snapshots → List (Liste).**
   Die Seite **Snapshots List (Snapshot-Liste)** zeigt eine Liste der vorhandenen Snapshots an. Standardmäßig werden Snapshots für alle NAS-Volumes angezeigt.
2. Klicken Sie auf **Create (Erstellen)**.
   Es wird die Seite **Create Snapshot (Snapshot erstellen)** angezeigt.
3. Wählen Sie aus der **NAS Volume**-Liste das entsprechende NAS-Volume aus.
4. Geben Sie in **Snapshot name (Snapshot-Name)** den Namen des neuen Snapshots ein.
5. Klicken Sie auf **Create (Erstellen)**.
   Der neue Snapshot wird erstellt und der Liste mit den Snapshots auf der Seite **Snapshots List (Snapshot-Liste)** hinzugefügt.

Zugreifen auf Snapshots

Nachdem der Snapshot erstellt wurde, können Sie auf einen bestimmten Ordner unter „Export“ oder „Freigabe“ zugreifen.

Greifen Sie auf den speziellen Ordner über UNIX unter dem Verzeichnis mit der Bezeichnung **.snapshots** unter jedem NFS-Export zu.

Greifen Sie in Microsoft Windows auf den speziellen Ordner unter dem Verzeichnis .**snapshots** unter jeder Freigabe zu. (Dies integriert Schattenkopien und aktiviert frühere Versionen.)

Snapshots behalten den gleichen Sicherheitsstil wie das Active-Dateisystem bei. Darum können Benutzer, selbst wenn sie Snapshots verwenden, nur auf ihre eigenen Dateien gemäß den bestehenden Berechtigungen zugreifen. Die Daten, die beim Zugriff auf einen bestimmten Snapshot verfügbar sind, sind auf der gleichen Ebene wie die bestimmte Freigabe und ihre Unterverzeichnisse; so wird sichergestellt, dass Benutzer nicht auf andere Teile des Dateisystems zugreifen können.

Modifizieren eines Snapshots

ANMERKUNG: Sie können nur den **Snapshot-Namen** modifizieren.

1. Wählen Sie **Data Protection (Datenschutz) → Snapshots → List (Liste).**
   Die Seite **Snapshots List (Snapshot-Liste)** zeigt eine Liste der vorhandenen Snapshots an. Standardmäßig werden Snapshots für alle NAS-Volumes angezeigt.
2. Wählen Sie aus der Liste **Show Snapshots for NAS Volume (Snapshots für NAS-Volume anzeigen)** das entsprechende NAS-Volume aus oder wählen Sie **All NAS volumes (Alle NAS-Volumes).**
   Vorhandene Snapshots für das ausgewählte NAS-Volume werden angezeigt.
3. Klicken Sie in der Liste der verfügbaren Snapshots in der Spalte **Name** auf den gewünschten Snapshot.
   Das Fenster **Edit Snapshot (Snapshot bearbeiten)** wird angezeigt.

4. Ändern Sie in **Snapshot name (Snapshot-Name)** den vorhandenen Namen.
5. Klicken Sie auf **Calculate Snapshot Delta (Snapshot-Delta berechnen)**, um den tatsächlichen Speicherplatz zu berechnen, der durch Entfernen eines Snapshots frei gemacht wird.
6. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Wiederherstellen von Daten

Sie können Daten auf zwei verschiedene Arten wiederherstellen:

- Kopieren und Einfügen: Für die Wiederherstellung einer einzelnen Datei.
  Wenn Sie eine Datei aus Versehen gelöscht oder verändert haben und Sie sie wiederherstellen möchten, gehen Sie zum Snapshot-Verzeichnis auf dem aktuellen NFS-Export oder der NFS-Freigabe, suchen Sie den gewünschten Snapshot (gemäß seines Erstellungszeitpunktes) und kopieren Sie die Datei an ihren ursprünglichen Speicherort zurück. Diese Methode ist bei alltäglichen Wiederherstellungen von einzelnen Dateien sinnvoll.
- Ein NAS-Volume aus einem Snapshot wiederherstellen
  Wenn Sie ein gesamtes Volume wiederherstellen müssen (z. B. im Fall eines Anwendungsfehlers oder eines Virenangriffs), bei dem das Kopieren und Einfügen von großen Datenmengen zu zeitaufwändig ist, haben Sie die Möglichkeit, das gesamte NAS-Volume wiederherzustellen.

Löschen eines Snapshots

1. Wählen Sie **Data Protection (Datenschutz)** → **Snapshots** → **List (Liste).**
   Die Seite **Snapshots List (Snapshot-Liste)** zeigt die Liste der vorhandenen Snapshots an. Standardmäßig werden Snapshots von allen NAS-Volumes angezeigt.
2. Wählen Sie aus der Liste **Show Snapshots for NAS Volume (Snapshots für NAS-Volume anzeigen)** das entsprechende NAS-Volume aus oder wählen Sie **All NAS volumes (Alle NAS-Volumes).**
   Vorhandene Snapshots für das ausgewählte NAS-Volume werden angezeigt.
3. Wählen Sie aus der Liste der verfügbaren Snapshots den gewünschten Snapshot aus und klicken Sie auf **Delete (Löschen)**.

Ein NAS-Volume aus einem Snapshot wiederherstellen

1. Wählen Sie **Data Protection (Datenschutz)** → **Snapshots** → **Restore (Widerherstellen).**
   Die Seite **Snapshot Restore (Snapshot wiederherstellen)** wird angezeigt.
2. Wählen Sie in **Choose the volume to be reverted (Volume zum Wiederherstellen auswählen)** das entsprechende NAS-Volume aus.
   Die Liste **Choose a snapshot for revision (Snapshot zur Wiederherstellung auswählen)** zeigt die Snapshots für das ausgewählte NAS-Volume an.
3. Wählen Sie in **Choose a snapshot for revision (Snapshot zur Wiederherstellung auswählen)** den Snapshot aus, auf den das Volume wiederhergestellt werden soll.
4. Klicken Sie auf **Next (Weiter).**
   Eine Meldung zeigt Ihnen Anweisungen an, die Sie befolgen müssen, bevor Sie den Wiederherstellungsvorgang starten können.
5. Um das NAS-Volume auf den ausgewählten Snapshot wiederherzustellen, klicken Sie auf **Yes (Ja)**.
   Das NAS-Volume wird auf den Snapshot wiederhergestellt.

VORSICHT: Der Vorgang Restore (Wiederherstellen) kann nicht rückgängig gemacht werden. Alle Daten, die in der Zeit zwischen Snapshoterstellung und Abschluss des Wiederherstellungsvorgangs erstellt oder verändert wurden, werden gelöscht.

Replikation

Die Replikation in der Dell FluidFS NAS-Lösung basiert auf Blöcken und ist asynchron.

- Auf Blöcken basierend – nur Blöcke, die eine Veränderung aufweisen, werden repliziert und nicht die gesamte Datei
- Asynchron – die Kommunikation mit dem Client besteht auch dann, wenn Daten repliziert werden

Replikation wird in unterschiedlichen Szenarien verwendet, um verschiedene Niveaus von Datenschutz zu erreichen. Manche davon beinhalten:

Schnelle Sicherung und Wiederherstellung	Verwaltung von ganzen Datenkopien zum Schutz vor Datenverlust, Beschädigung oder Benutzerfehlern.
Notfallwiederherstellung	Spiegelungsdaten zu Remote-Speicherorten für Failover.
Remote-Datenzugriff	Anwendungen können auf gespiegelte Daten im schreibgeschützten oder im Lese-/Schreibmodus zugreifen.
Online Datenmigration	Minimierung der mit Datenmigration verbundenen Ausfallzeit

Replikation nutzt die Snapshot-Technologie im Dateisystem der NAS-Cluster-Lösung. Nach der ersten Replikation werden nur noch Änderungen (Deltas) repliziert. So werden schnellere Replikation und effiziente Verwendung der Prozessor-Zyklen ermöglicht. Außerdem wird Speicherplatz eingespart, während die Daten konsistent bleiben.

Replikation basiert auf dem Volume und kann zum Replizieren von Volumes auf demselben NAS-Gerät oder von einem Volume auf einem anderen NAS-Gerät verwendet werden. Beim Replizieren eines Volumes auf ein anderes NAS-Gerät muss das andere NAS-Gerät als Replikationspartner eingestellt werden.

Replication Partners (Replikationspartner)

Wenn eine Replikationsbeziehung aufgebaut ist, so verläuft die Replikation in beide Richtungen. Ein System kann sowohl Ziel-Volumes für das andere System als auch Quell-Volumes zur Replikation auf das andere System enthalten. Die Replikationsdaten fließen durch einen sicheren SSH-Tunnel zum anderen System über das Client-Netzwerk.

Eine Replikationsrichtlinie kann so eingerichtet werden, dass sie zu verschiedenen Zeitplänen oder auch nach Bedarf ausgeführt wird. Alle Systemkonfigurationen (Benutzerkontingente, Snapshot-Richtlinien usw.) werden auf jedem Volume gespeichert. Wenn ein Volume repliziert wird, erhält das Ziel-Volume die identischen Informationen. Wenn eine Replikationsrichtlinie entfernt wird, wird eine Option zur Übertragung der Volume-Konfiguration angeboten.

ANMERKUNG: Replikationspartner müssen die gleiche Anzahl an Controllern haben. Versuchen Sie darum beispielsweise nicht, ein Gerät mit vier Controllern auf ein Gerät mit zwei Controllern zu replizieren.

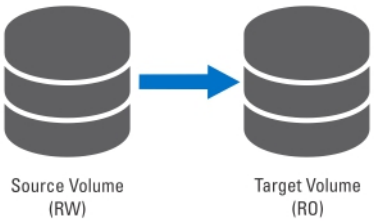

Abbildung 4. Lokale Replikation

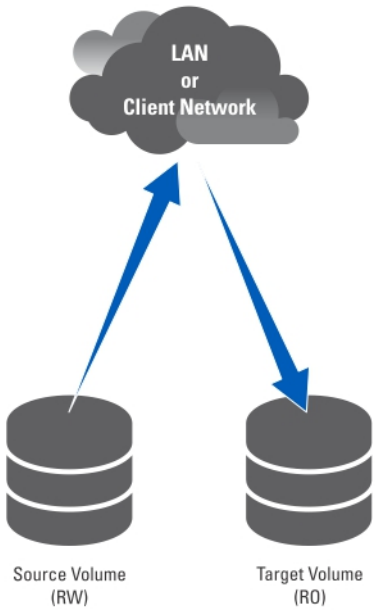

Abbildung 5. Partner-Replikation

Anzeigen von vorhandenen Replikationspartnern

Sie können sich eine Liste der Replikationspartner anzeigen lassen. Um die Replikationspartner anzuzeigen, denen vom ausgewählten System vertraut wird, wählen Sie **Datenschutz** → **Replikation** → **Replikationspartner** aus. Das Fenster **Replikationspartner** zeigt die Liste mit den Namen der vorhandenen Replikationspartner an.

Einrichten eines Replikationspartners

Auf dem Remote-System wird das Quellsystem nun auch zum Partner. Dies ist eine Vertrauensstellung in beide Replikationsrichtungen. Quell- und Ziel-Volumes können sich in beiden Systemen befinden.

So fügen Sie Replikationspartner hinzu:

1. Wählen Sie **Data Protection (Datenschutz)** → **Replication (Replikation)** → **Replication Partners (Replikationspartner).**

   Die Seite **Replication Partners (Replikationspartner)** wird angezeigt.

2. Klicken Sie auf **Add (Hinzufügen)**.

   Die Seite **Add Replication Partner (Replikationspartner hinzufügen)** wird angezeigt.

3. Geben Sie in **Remote NAS management VIP (Remote-NAS-Verwaltungs-VIP)** die VIP-Adressen der Remote-System-NAS-Verwaltung ein.

4. Geben Sie in **User name (Benutzername)** und **Password (Kennwort)** den Benutzernamen und das Kennwort eines Administratorkontos im Remote-System ein.

   ANMERKUNG: Diese Werte werden nicht im Dell Fluid File System gespeichert.

5. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Konfiguration eines Replikationspartners modifizieren

Sie können die Konfiguration eines Replikationspartners durch Ändern seiner Parameter modifizieren.

So modifizieren Sie die Parameter eines Replikationspartners:

1. Wählen Sie **Data Protection (Datenschutz) → Replication (Replikation) → Replication Partners (Replikationspartner).**

   Die Seite **Replication Partners (Replikationspartner)** zeigt eine Liste der vorhandenen Replikationspartnernamen an.

2. Wählen Sie unter **Replication Partner Name (Replikationspartnername)** den gewünschten Replikationspartner aus.

   Die Seite **Edit Replication Partner (Replikationspartner bearbeiten)** wird angezeigt.

3. Ändern Sie in **Remote NAS management VIP (Remote-NAS-Verwaltungs-VIP)** die VIP-Adresse wie gewünschte um.
4. Ändern Sie in **User name (Benutzername)** und **Password (Kennwort)** die Benutzeranmeldeinformationen wie gewünscht um.
5. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Entfernen eines Replikationspartners

Sie können einen Replikationspartner eines Systems entfernen, indem Sie ihn aus der Liste der Replikationspartner löschen. Wenn Sie einen Replikationspartner löschen, vergewissern Sie sich, dass beide Systeme eingeschaltet sind und funktionieren. Wenn ein System ausgeschaltet oder nicht erreichbar ist, wird eine Warnmeldung angezeigt.

So löschen Sie die Konfiguration eines Replikationspartners:

1. Wählen Sie **Datenschutz → Replikation → Replikationspartner** aus.

   Die Seite **Replikationspartner** zeigt eine Liste der vorhandenen Replikationspartnernamen an.

2. Wählen Sie aus der Liste der vorhandenen Replikationspartner die gewünschten Partner aus und klicken Sie auf **Löschen**.

Richtlinien der NAS-Replikation

Die Replikation zwischen Volumes wird durch Richtlinien gesteuert. So erstellen Sie eine NAS-Replikationsrichtlinie, auch als verbundene Volumes bezeichnet, über den NAS-Manager:

1. Erstellen Sie eine Vertrauensstellung zwischen dem Quell- und dem Zielsystem.

   Dazu müssen Sie die IP-Adresse des Remote-Systems und Benutzername und Kennwort eines Administrators angeben.

2. Fügen Sie die Replikationsrichtlinie hinzu.

   Dazu müssen Sie das Quell-Volume und das Ziel-Volume auswählen und einen periodischen Zeitplan für die Replikation angeben.

   Wenn das Zielsystem über Daten verfügt, die auf dem Quellsystem nicht verfügbar sind, wird eine Warnmeldung ausgegeben und Sie werden dazu aufgefordert, dem Datenverlust zuzustimmen.

3. Überwachen Sie den Replikationsfortschritt.

   Überprüfen Sie, ob die Replikation reibungslos abläuft.

   Sie können die Replikationsrichtlinie löschen und dadurch das Zielsystem beschreibbar machen. Weitere Informationen zu NAS-Replikationsrichtlinien finden Sie in der *Online Help (Online-Hilfe)*.

ANMERKUNG: Ziel-Volumes in einer Replikation sind **schreibgeschützt**, wenn sie einer Replikationsrichtlinie zugewiesen sind.

Hinzufügen einer Replikationsrichtlinie

1. Wählen Sie **Data Protection (Datenschutz) → Replication (Replikation) → NAS Replication (NAS-Replikation).**
   Die Seite **NAS Replication (NAS-Replikation)** zeigt eine Liste der vorhandenen NAS-Replikationsrichtlinien an.
2. Klicken Sie auf **Add (Hinzufügen)**.
   Die Seite **Add NAS Replication Policy (NAS-Replikationsrichtlinie hinzufügen)** wird angezeigt.
3. Geben Sie in **Source NAS volume (NAS-Quell-Volume)** das NAS-Quell-Volume ein oder klicken Sie auf die Schaltfläche **Browse (Durchsuchen)** und wählen Sie das gewünschte NAS-Volume aus.
4. Wählen Sie aus der Liste **Destination cluster (Ziel-Cluster)** eine der folgenden Optionen aus:
   - **localhost** um das Quell-Volume in diesem System zu replizieren.
   - einen anderen verfügbaren Dell Fluid File System-Replikationspartner.
5. Geben Sie in **Destination NAS volume (NAS-Ziel-Volume)** das NAS-Ziel-Volume ein oder klicken Sie auf die Schaltfläche **Browse (Durchsuchen)** und wählen Sie das gewünschte NAS-Volume aus.
6. Wählen Sie eine der folgenden Optionen für den Zeitplan des Wiederherstellungspunktes aus:
   - **Jede Stunde replizieren nach**
   - **Jeden Tag replizieren um**
   - **Jede Woche replizieren am**
   - **Nach Bedarf replizieren (ohne Zeitplan)**
7. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Modifizieren von Replikationsrichtlinien

1. Wählen Sie **Data Protection (Datenschutz) → Replication (Replikation) → NAS Replication (NAS-Replikation).**
   Die Seite **NAS Replication (NAS-Replikation)** zeigt eine Liste der vorhandenen NAS-Replikationsrichtlinien an.
2. Wählen Sie das gewünschte NAS-Volume in der Spalte **Source NAS Volume (NAS-Quell-Volume)** aus.
   Die Seite **Edit NAS Replication Policy (NAS-Replikationsrichtlinie bearbeiten)** wird angezeigt.
3. Geben Sie in **Source NAS Volume (NAS-Quell-Volume)** das NAS-Quell-Volume ein oder klicken Sie auf die Schaltfläche **Browse (Durchsuchen)** und wählen Sie das entsprechende NAS-Volume aus.
4. Wählen Sie aus der Liste **Destination cluster (Ziel-Cluster)** eine der folgenden Optionen aus:
   - **localhost** um das Quell-Volume in diesem System zu replizieren.
   - einen anderen verfügbaren Dell Fluid File System-Replikationspartner.
5. Geben Sie in **Destination NAS volume (NAS-Ziel-Volume)** das NAS-Ziel-Volume ein oder klicken Sie auf die Schaltfläche **Browse (Durchsuchen)** und wählen Sie das gewünschte NAS-Volume aus.
6. Wählen Sie eine der folgenden Optionen für den Zeitplan des Wiederherstellungspunktes aus:
   - **Jede Stunde replizieren nach**
   - **Jeden Tag replizieren um**
   - **Jede Woche replizieren am**
   - **Nach Bedarf replizieren (ohne Zeitplan)**
7. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Anhalten, wieder aufnehmen und ausführen der NAS-Replikation

Sie können die NAS-Replikation nach Bedarf je nach Status des ausgewählten NAS-Volumes anhalten, wieder aufnehmen oder ausführen.

1. Wählen Sie **Data Protection (Datenschutz) → Replication (Replikation) → NAS Replication (NAS-Replikation).**
   Die Seite **NAS Replication (NAS-Replikation)** zeigt eine Liste der vorhandenen NAS-Replikationsrichtlinien an.
2. Wählen Sie aus der Liste der vorhandenen NAS-Volumes das gewünschte NAS-Volume aus.
3. Klicken Sie auf **Pause (Anhalten)**, um das ausgewählte NAS-Volume anzuhalten.
4. Klicken Sie auf **Resume (Wieder aufnehmen)**, um die NAS-Replikation für das ausgewählte NAS-Volume fortzuführen.
5. Klicken Sie auf **Replicate Now (Jetzt replizieren)**, um die Replikation für das ausgewählte NAS-Volume sofort zu starten.

Löschen einer Replikationsrichtlinie

Wenn Sie eine Replikationsrichtlinie löschen, enthalten beide Volumes die Systemkonfiguration des Quellsystems. Es ist optional, die Quellsystemkonfiguration auf das Zielsystem-Volume zu übertragen. Diese Konfiguration schließt Benutzer, Kontingente, Snapshot-Richtlinien, Sicherheitstypen und andere Einstellungen ein. Diese Option ist bei der Notfallwiederherstellung hilfreich.

ANMERKUNG: Wenn die Replikationsrichtlinie vom System des Ziel-Volumes gelöscht wird, wird eine Warnung ausgegeben und die Richtlinie muss auch vom Quellsystem gelöscht werden.

So löschen Sie die Replikationsrichtlinie:

1. Wählen Sie **Data Protection (Datenschutz) → Replication (Replikation) → NAS Replication (NAS-Replikation).**
   Die Seite **NAS Replication (NAS-Replikation)** zeigt eine Liste der vorhandenen NAS-Replikationsrichtlinien an.
2. Wählen Sie aus der Liste der vorhandenen NAS-Volumes das gewünschte NAS-Volume aus und klicken Sie auf **Delete (Löschen)**.

Notfallwiederherstellung mithilfe von Replikation

Sie können die Replikationsfunktionen dazu verwenden, um einen Quell-Cluster (Cluster A) von seinem Backup-Cluster (Cluster B) wiederherzustellen.

ANMERKUNG:

- **Cluster A** – das Quell-Cluster, in dem sich die zu sichernden Daten befinden.
- **Cluster B** – das Backup-Cluster, das voll konfiguriert aber ohne Volumes ist und die Daten aus Quell-Cluster A sichert.

Bevor Sie die Notfallwiederherstellung mithilfe von Replikation einrichten, vergewissern Sie sich, dass die folgenden Bedingungen erfüllt sind:

- Sowohl Cluster A als auch Cluster B sind vom gleichen Typ und haben die gleiche Konfiguration.

  ANMERKUNG: Wenn z. B. das Cluster A ein NX3600 mit vier Vierkern-Prozessoren ist, dann muss auch das Cluster B ein NX3600 mit vier Vierkern-Prozessoren sein.
- Die Replikationsversion von Cluster B ist die gleiche wie Cluster A.
- Cluster B verfügt über ausreichend Speicherplatz, um alle Daten aus Cluster A zu replizieren.

- Cluster B hat andere Netzwerkeinstellungen (Client, SAN, IC usw.) als das Quell-Cluster A, allerdings müssen beide Cluster miteinander kommunizieren können, sodass der Replikationsvorgang durchgeführt werden kann.

Beim Einrichten der Notfallwiederherstellung mithilfe von Replikation gibt es drei Phasen:

- Phase 1 – Replikationsstruktur zwischen Cluster A und Cluster B wird aufgebaut
- Phase 2 – Cluster A fällt aus und der Client fordert ein Failover zu Cluster B an
- Phase 3 – Failback von Cluster A wird von Cluster B auf Cluster A wiederhergestellt

DNS-Konfiguration für Failover für einzelne Datenträger

Für Failover für einzelne Datenträger ist es wichtig, dass die Umgebung dazu eingestellt ist, Benutzer der NAS-Datenträger, für die Sie ein Failover planen, ordnungsgemäß zu migrieren, ohne Benutzer anderer NAS-Datenträger, für die kein Failover geplant ist, zu unterbrechen.

Wenn ein Failover eines NAS-Datenträgers von einem NAS-Cluster zu einem anderen ausgeführt wird, ändern sich die IP-Adressen, mit denen darauf zugegriffen wird, von den IP-Adressen von Cluster A in die IP-Adresse von Cluster B. Es wird empfohlen, dass diese Änderung mit Hilfe von DNS ausgeführt wird. Wenn ein Failover für einzelne Datenträger erforderlich ist, wird die Einstellung eines DNS-Eintrags zur Korrelation mit jedem NAS-Datenträger und die Änderung des DNS-Eintrags für einzelne Datenträger nach deren Failover empfohlen.

Beispiel: Marketing und Vertrieb haben ihre eigenen NAS-Datenträger, mit einer CIFS-Freigabe auf dem NAS-Datenträger mit den Namen *marketing_share* und *sales_share*. Ein DNS-Eintrag mit Namen *FluidFSmarketing* wird für Marketing erstellt und ein anderer DNS-Eintrag für den Vertrieb mit Namen *FluidFSsales*. Beide Datenträger verweisen auf denselben Satz von Client-Zugriffs-VIPs auf dem Quell-Cluster A. Marketing kann unter Verwendung von **\\FluidFSmarketing\marketing** auf den Marketing-Datenträger oder die -Freigabe zugreifen, und der Vertrieb kann mit **\\FluidFSsales\sales** auf den Vertriebs-Datenträger oder die -Freigabe zugreifen.

Anfänglich verweisen beide DNS-Einträge *FluidFSmarketing* und *FluidFSsales* auf denselben Satz von Client-Zugriffs-VIP. Dann kann der Zugriff auf die Freigaben *marketing* und *sales* von einem beliebigen der DNS-Namen *FluidFSmarketing* oder *FluidFSsales* aus erfolgen. Wenn Sie ein Failover für einen einzelnen Datenträger möchten (zum Beispiel *Marketing*), ändern Sie die DNS-Einträge für *FluidFSmarketing*, um die Client-Zugriffs-VIPs auf Cluster B aufzulösen.

Es wird empfohlen, dass Sie eine Tabelle führen, um zu verfolgen, welche DNS-Einträge für den Zugriff auf die einzelnen NAS-Datenträger verwendet werden. Dies hilft bei der Ausführung der Failover und der Einrichtung von Gruppenrichtlinien.

ANMERKUNG: Ein einzelner FluidFS NAS-Cluster darf keine zwei Sätze von Startfreigaben enthalten. Sehen Sie z. B., dass Cluster A und Cluster B beide Startfreigaben haben, für verschiedene Sites oder Benutzerbasen. Cluster A und Cluster B dienen beide als Replikationsziele für den NAS-Datenträger des anderen, der die Startfreigaben enthält. Im Fall dass der Administrator ein Failover des NAS-Datenträgers mit Startfreigaben von Cluster A auf Cluster B machen möchte, weist Cluster B diesen Vorgang zurück, weil bereits Startfreigaben auf ihm definiert sind.

Phase 1 – Replikationsstruktur zwischen Quell-Cluster A und Backup-Cluster B wird aufgebaut

1. Melden Sie sich in Cluster A an.
2. Richten Sie eine Replikationsbeziehung zwischen Quell-Cluster A und Backup-Cluster B ein.
   Weitere Informationen zum Einrichten von Replikationspartnern finden Sie unter Einrichten eines Replikationspartners.
3. Erstellen Sie eine Replikationsrichtlinie für alle Quell-Volumes in Cluster A nach Ziel-Volumes in Cluster B.
   Weitere Informationen zum Erstellen von Replikationsrichtlinien finden Sie unter Hinzufügen einer Replikationsrichtlinie.

ANMERKUNG: Die Replikationsrichtlinie ist eine eins-zu-eins-Übertragung auf Volume-Basis, zum Beispiel:

Quell-Volume A1 (Cluster A) nach Ziel-Volume B1 (Cluster B)

Quell-Volume A2 (Cluster A) nach Ziel-Volume B2 (Cluster B)

.....

Quell-Volume A*n* (Cluster A) nach Ziel-Volume B*n* (Cluster B)

ANMERKUNG: FluidFS v2 unterstützt die automatische Erstellung von Ziel-Volumes während dem Hinzufügen der Replikationsrichtlinie. Bei FluidFS 1.0 müssen Sie die Ziel-Volumes in Cluster B erstellen und sicherstellen, dass die Volume-Größe groß genug ist, um die entsprechenden Daten des Quell-Volumes in Cluster A zu beherbergen.

4. Starten Sie den Replikationszeitplaner um sicherzustellen, dass für alle Quell-Volumes in Cluster A mindestens eine erfolgreiche Replikation durchgeführt wurde.

   Wenn die Replikation fehlschlägt, beheben Sie das gefundene Problem und starten Sie den Replikationsvorgang neu. So wird sichergestellt, dass alle Quell-Volumes in Cluster A über mindestens eine erfolgreiche Replikationskopie in Cluster B verfügen. Richten Sie einen regelmäßigen Replikationszeitplan ein, sodass die Ziel-Volumes in Cluster B immer über die aktuellsten Replikationskopien von Cluster A verfügen.

VORSICHT: Die Replikationswiederherstellung ist keine komplette BMR-Wiederherstellung (Bare-metal Restore), Einstellungen wie Netzwerkkonfiguration (Client, SAN und IC) können mit dieser Replikationsmethode nicht gesichert und wiederhergestellt werden. Notieren Sie sich für die spätere Verwendung alle Einstellungen von Cluster A (zur Verwendung beim Wiederherstellen von Cluster A), inklusive Netzwerkkonfiguration, Einstellungen für das gesamte Cluster wie z. B. Volume-Name, Warnungseinstellungen usw. Wenn der Vorgang zur Systemwiederherstellung diese Einstellungen nicht wiederherstellen kann, können Sie die Einstellungen von Cluster A manuell zurück auf ihre ursprünglichen Werte wiederherstellen.

Phase 2 – Cluster A fällt aus und der Client fordert ein Failover zu Backup-Cluster B an

Wenn Quell-Cluster A aufhört zu antworten aufgrund eines unerwarteten Fehlers (Hardware, Laufwerk usw.), gehen Sie wie folgt vor:

1. Melden Sie sich auf Backup-Cluster B an.
2. Löschen Sie die bestehende Replikationsrichtlinie für alle Replikationsziel-Volumes.

   - Beim Löschen der Replikationsrichtlinie vom Zielcluster B – Der FluidFS Replikationsmanager versucht Quell-Cluster A zu kontaktieren, was fehlschlägt. Der Datenträger auf Zielcluster B muss seine Konfiguration unter Verwendung von **Clusterverwaltung → NASDatenträger-Konfiguration wiederherstellen.**
   - Beim Löschen der Replikationsrichtlinie vom Zielcluster A – Sie haben die Option, die Quelldatenträgerkonfiguration auf den Zieldatenträger anzuwenden. Falls Sie nicht daran denken, diese auszuwählen, oder falls es fehlschlägt, kann die Konfiguration des Quelldatenträgers von Cluster A unter Verwendung von **Clusterverwaltung → NAS-Datenträgerkonfiguration wiederherstellen** auf dem Zieldatenträger auf Cluster B wiederhergestellt werden.

3. Bestätigen Sie das Löschen der Replikationsrichtlinie auf Backup-Cluster B und das Anwenden der Konfiguration des Quelldatenträgers von Cluster A.

   Derzeit können die folgenden Volume-Konfigurationen wiederhergestellt werden:

   - NFS-Exporte
   - CIFS-Freigaben
   - Kontingentregeln
   - Snapshot-Zeitplan
   - NAS-Volume-Warnmeldungen, Sicherheitsstil und damit verbundene Parameter
   - Name des NAS-Volumes

– Größe des NAS-Volumes

So werden Ziel-Volumes (B1, B2, .. B*n*) zu eigenständigen Volumes. Wiederholen Sie diesen Vorgang, um aus allen Ziel-Volumes in Cluster B eigenständige Volumes mit der von Cluster A übernommenen Konfiguration zu machen.

4. Stellen Sie von der Web-Oberfläche des NAS-Managers die NAS-Systemkonfiguration von Cluster A wieder her.

   Weitere Informationen zum Wiederherstellen der NAS-Systemkonfiguration finden Sie unter Cluster-Konfiguration wiederherstellen.

   Dies stellt die Konfiguration von Cluster B auf die Einstellungen von Cluster A wieder her. Derzeit können die folgenden Cluster-Systemkonfigurationen wiederhergestellt werden:

   – Protokollkonfigurationen
   – Benutzer und Gruppen
   – Benutzerzuordnungen
   – Überwachungskonfiguration
   – Zeitkonfiguration
   – Antivirus-Hosts

5. Stellen Sie sicher, dass Cluster B dazu verwendet wird, für die Dauer des Failovers vorübergehend Client-Anfragen zu bedienen

   Administratoren müssen die folgenden Schritte durchführen, um DNS und Authentifizierung einzurichten:

   a) Weisen Sie die DNS-Namen des DNS-Kundenservers Cluster B anstatt Cluster A zu.

      Stellen Sie sicher, dass der DNS-Server in Cluster B derselbe DNS-Server wie in Cluster A ist oder er sich in derselben DNS-Farm befindet. Vorhandene Client-Verbindungen können abbrechen und müssen eventuell neu errichtet werden. Sie müssen NFS-Exporte auf dem Client unmounten und neu mounten.

      ANMERKUNG: Beenden Sie die Schritte b, c und d nur für Failover einzelner Datenträger.

   b) Aktualisieren Sie den DNS-Eintrag für den NAS-Datenträger, auf dem ein Failover ausgeführt wurde, auf DNS manuell.

      Diese Schritt soll Endbenutzer wieder ausrichten, die von Cluster A zu Cluster B auf diesen Datenträger zugreifen, während die Endbenutzer weiterhin mit demselben DNS-Namen darauf zugreifen.

      ANMERKUNG: Clientsysteme müssen evtl. den DNS-Cache aktualisieren.

   c) Um CIFS- und NFS-Clients auf Cluster B zu zwingen, müssen wir auch die CIFS-Freigaben und NFS-Exporte auf Cluster A löschen.

      Dies zwingt die CIFS- und NFS-Clients zur Wiederverbindung, zu einer Zeit, zu der sie mit Cluster B verbunden sind. Nach der Wiederherstellung der Konfiguration des Quelldatenträgers auf Cluster B sind alle Freigaben und Exporte auf dem Zieldatenträger (auf Cluster B) vorhanden, und daher gehen keine Freigaben-/Exportkonfigurationsinformationen verloren.

   d) Es kann jetzt auf den Datenträger, an dem ein Failover vorgenommen wurde, zugegriffen werden, und zwar mit dem genau gleichen DNS-Namen und Freigabennamen wie beim Hosting auf Cluster A, nur dass er jetzt auf Cluster B gehostet wird.

      ANMERKUNG: NFS-Einrichtungen müssen abmontiert und wieder montiert werden. Aktive CIFS-Übertragungen schlagen während diesem Vorgang fehl, aber wenn CIFS-Freigaben als lokale Laufwerke zugeordnet werden, werden sie beim Löschen der Replikation automatisch neu verbunden, DNS wird aktualisiert, und NFS/CIFS-Freigaben werden auf Cluster A gelöscht.

   e) Ordnen Sie AD-Server oder LDAP/NIS zu.

      Vergewissern Sie sich, dass sich AD und LDAP in derselben AD/LDAP-Farm oder auf demselben Server befinden.

Phase 3 – Failback von Cluster A von Cluster B auf Cluster A wiederherstellen

1. Beheben Sie den Fehler, wegen dem Cluster A fehlgeschlagen ist (Hardware austauschen, Laufwerk austauschen usw.) und installieren Sie FluidFS neu, falls erforderlich.
2. Erstellen Sie das Cluster neu (verwenden Sie dazu die Einstellungen für Cluster A, die Sie vorher gespeichert haben), formatieren Sie die NAS-Reserve und richten Sie das Netzwerk (Client, SAN und IC) so ein wie zuvor.
3. Melden Sie sich in Cluster B an und richten Sie die Replikationspartnerschaft zwischen Cluster B und Cluster A ein.

   Weitere Informationen zum Einrichten von Replikationspartnern finden Sie unter Einrichten eines Replikationspartners.
4. Erstellen Sie die Replikationsrichtlinien für alle Quell-Volumes in Cluster B nach Ziel-Volumes in Cluster A.

   Weitere Informationen zum Erstellen von Replikationsrichtlinien finden Sie unter Hinzufügen einer Replikationsrichtlinie.

   ANMERKUNG: Die Replikationsrichtlinie ist eine eins-zu-eins-Übertragung auf Volume-Basis, zum Beispiel:

   Quell-Volume B1 (Cluster B) nach Ziel-Volume A1 (Cluster A)

   Quell-Volume B2 (Cluster B) nach Ziel-Volume A2 (Cluster A)

   .....

   Quell-Volume B*n* (Cluster B) nach Ziel-Volume A*n* (Cluster A)

   ANMERKUNG: FluidFS v2 unterstützt die automatische Erstellung von Ziel-Volumes während dem Hinzufügen der Replikationsrichtlinie. Bei FluidFS 1.0 müssen Sie die Ziel-Volumes in Cluster B erstellen und sicherstellen, dass die Volume-Größe groß genug ist, um die entsprechenden Daten des Quell-Volumes in Cluster A zu beherbergen.
5. Wählen Sie in der Internetschnittstelle des NAS Managers **Datenschutz → Replikation → NAS-Replikation** aus und klicken Sie auf **Jetzt replizieren** für alle Volumes in Cluster B (B1, B2, .., B*n*).

   Wenn die Replikation fehlschlägt, beheben Sie die gefundenen Probleme und starten Sie den Replikationsvorgang neu. Stellen Sie sicher, dass alle Volumes erfolgreich nach Cluster A repliziert werden.
6. Löschen Sie die Replikationsrichtlinien für alle Volumes (B1, B2, .. B*n*) und wenden Sie die Quell-Volume-Konfiguration von Cluster B auf Cluster A an.

   Wiederholen Sie diesen Vorgang, um alle Replikationsrichtlinien zu löschen und alle Ziel-Volumes in Cluster A auf eigenständige Volumes zu bringen.

   - Beim Löschen der Replikationsrichtlinie vom Zielcluster B – Der FluidFS Replikationsmanager versucht Quell-Cluster A zu kontaktieren, was fehlschlägt. Das Volume auf Zielcluster B muss seine Konfiguration unter Verwendung von **Clusterverwaltung → NAS-Volume-Konfiguration wiederherstellen** wiederherstellen.
   - Beim Löschen der Replikationsrichtlinie vom Zielcluster A – Sie haben die Option, die Quelldatenträgerkonfiguration auf den Zieldatenträger anzuwenden. Falls Sie nicht daran denken, diese auszuwählen, oder falls es fehlschlägt, kann die Konfiguration des Quelldatenträgers von Cluster A unter Verwendung von **Clusterverwaltung → NAS-Datenträgerkonfiguration wiederherstellen** auf dem Zieldatenträger auf Cluster B wiederhergestellt werden.
7. Melden Sie sich in Cluster A an.
8. Stellen Sie von der Internetschnittstelle des NAS Managers die NAS-Systemkonfiguration von Cluster B wieder her.

   Weitere Informationen zum Wiederherstellen der NAS-Systemkonfiguration finden Sie unter Cluster-Konfiguration wiederherstellen.

   So werden die globalen Konfigurationseinstellungen von Cluster A auf die Einstellungen von Cluster B geändert, wie z. B. Protokolleinstellungen, Zeiteinstellungen, Authentifizierungsparameter usw.

ANMERKUNG: Wenn die Systemkonfigurationswiederherstellung fehlschlägt, stellen Sie sie manuell auf die ursprünglichen Einstellungen zurück (verwenden Sie dafür die Einstellungen für Cluster A, die Sie vorher gespeichert haben).

Die ursprünglichen Einstellungen für Cluster A werden wiederhergestellt.

9. Beginnen Sie damit, Cluster A zu verwenden, um Client-Anfragen zu bedienen.

   Administratoren müssen die folgenden Schritte durchführen, um DNS und Authentifizierung einzurichten:

   a) Richten Sie die DNS-Namen des Kunden-DNS-Servers auf Cluster A anstatt auf Cluster B aus.

      Vergewissern Sie sich, dass der DNS-Server in Cluster A der gleiche DNS-Server wie der DNS-Server in Cluster B ist oder er sich in derselben DNS-Farm befindet. Bestehende Client-Verbindungen können abbrechen und müssen während dieses Prozesses neu hergestellt werden.

      ANMERKUNG: Beenden Sie die Schritte b, c und d nur für Failover einzelner Datenträger.

   b) Aktualisieren Sie den DNS-Eintrag für den NAS-Datenträger, auf dem ein Failover ausgeführt wurde, auf DNS manuell.

      Dieser Schritt soll Endbenutzer wieder ausrichten, die von Cluster B zu Cluster A auf diesen Datenträger zugreifen, während die Endbenutzer weiterhin mit demselben DNS-Namen darauf zugreifen.

      ANMERKUNG: Clientsysteme müssen evtl. den DNS-Cache aktualisieren.

   c) Um CIFS- und NFS-Clients auf Cluster A zu zwingen, müssen wir auch die CIFS-Freigaben und NFS-Exporte auf Cluster B löschen.

      Dies zwingt die CIFS- und NFS-Clients zur Wiederverbindung, zu einer Zeit, zu der sie mit Cluster A verbunden sind. Nach der Wiederherstellung der Konfiguration des Quelldatenträgers auf Cluster A sind alle Freigaben und Exporte auf dem Zieldatenträger (auf Cluster A) vorhanden, und daher gehen keine Freigaben-/Exportkonfigurationsinformationen verloren.

   d) Es kann jetzt auf den Datenträger, an dem ein Failover vorgenommen wurde, zugegriffen werden, und zwar mit dem genau gleichen DNS-Namen und Freigabennamen wie beim Hosting auf Cluster B, nur dass er jetzt auf Cluster A gehostet wird.

      ANMERKUNG: NFS-Einrichtungen müssen abmontiert und wieder montiert werden. Aktive CIFS-Übertragungen schlagen während diesem Vorgang fehl, aber wenn CIFS-Freigaben als lokale Laufwerke zugeordnet werden, werden sie beim Löschen der Replikation automatisch neu verbunden, DNS wird aktualisiert, und NFS/CIFS-Freigaben werden auf Cluster B gelöscht.

   e) Ordnen Sie AD-Server oder LDAP/NIS zu.

      Vergewissern Sie sich, dass sich AD und LDAP in derselben AD/LDAP-Farm oder auf demselben Server befinden.

10. Bauen Sie eine Replikationsstruktur zwischen Quell-Cluster A und Backup-Cluster B auf, um eine Replikationsrichtlinie zwischen Cluster A und Cluster B einzurichten; verwenden Sie Volumes aus Cluster B als Replikationsziel-Volumes zur Vorbereitung auf die nächste Notfallwiederherstellung.

Sichern und Wiederherstellen von Daten

ANMERKUNG: Es wird empfohlen, Ihre Daten regelmäßig zu sichern.

Die NAS-Cluster-Lösung unterstützt Sicherung und Wiederherstellung mithilfe des Network Data Management Protocol (NDMP, Netzwerkdatenverwaltungsprotokoll). Ein in der NAS-Cluster-Lösung installierter NDMP-Agent stellt sicher, dass gespeicherte Daten gesichert und wiederhergestellt werden können, unter Verwendung der Data Management Application (DMA, Datenverwaltungsanwendung), welche wiederum das NDMP-Protokoll unterstützt, ohne dass Hersteller-spezifische Agenten auf dem NAS-Gerät installiert werden müssen.

Um Sicherungs- und Wiederherstellungsvorgänge durchzuführen, muss eine DMA so konfiguriert sein, dass sie auf das NAS-Gerät über das LAN oder das Client-Netzwerk zugreifen kann. Die NAS-Cluster-Lösung verwendet keine dedizierte

Adresse für Sicherungsvorgänge, es können alle konfigurierten LAN- oder Client-Netzwerk-Adressen für Sicherungs- und Wiederherstellungsvorgänge verwendet werden.

NDMP-Sicherungen in der NAS-Cluster-Lösung werden mithilfe des LAN oder des Client-Netzwerkes durchgeführt. Die DMA muss so konfiguriert sein, dass sie auf eine der Client-VIPs (oder einen DNS-Namen) der NAS-Cluster-Lösung zugreifen kann.

Die NAS-Cluster-Lösung unterstützt keine dedizierte Backup-IP-Adresse, die im LAN oder im Client-Netzwerk konfiguriert ist. Alle virtuellen IPs, die im LAN oder im Client-Netzwerk konfiguriert sind, können von Sicherungssoftware zum Erstellen von Sicherungen und Durchführen von Wiederherstellungen verwendet werden.

Die NAS-Cluster-Lösung stellt eine allgemeine Benutzerschnittstelle zur Aktivierung des NDMP-Agents zur Verfügung und ist für einen vom installierten NDMP-Agenten unabhängigen Betrieb programmiert.

Sichern von Replikationsziel-NAS-Volumes

Wenn Sie eine Sicherung von Replikationsziel-Volumes durchführen, erstellt FluidFS keinen dezidierten NDMP-Snapshot. FluidFS verwendet stattdessen den Basisreplikat-Snapshot aus der letzten erfolgreichen Replikation.

Wenn sich der Zeitplan für Replikation und NDMP-Sicherung überschneidet, so ist es möglich, dass, während die NDMP-Sicherung der Ziel-Volumes durchgeführt wird, ein neuer Replikationsvorgang ausgeführt und abgeschlossen wird, bevor die NDMP-Sicherung fertig gestellt wurde. In diesem Fall löscht der Replikationsvorgang den vorigen Basisreplikat-Snapshot und erstellt ein neues Basisreplikat

VORSICHT: Dadurch wird die NDMP-Sicherung beendet. Um dieses Szenario zu verhindern, planen Sie Ihre Replikations- und Sicherungsvorgänge so, dass die Replikation endet, bevor die NDMP-Sicherung startet.

Erwägungen zum NDMP-Design

- Verwenden Sie den DNS-Namen für den NDMP-Server, wenn Sie Sicherungen auf DMAs einrichten, sodass der Lastenausgleich verwendet wird.
- Begrenzen Sie die Anzahl gleichzeitig ausgeführter Sicherungsaufgaben für eine schnellere Datenübertragung auf einen Vorgang pro Controller.
- Ihre Lösung unterstützt nur ein Dreiwege-Backup, in dem der DMA-Server die Datenübertragung zwischen NAS-Gerät und Speichergerät vermittelt. Stellen Sie sicher, dass der DMA-Server über ausreichend Bandbreite verfügt.

Unterstützte Anwendungen

Die NAS-Cluster-Lösung ist dazu zertifiziert, mit den folgenden DMAs zu arbeiten:

- Symantec BackupExec 2010 R3 und Symantec BackupExec 2012
- Symantec NetBackup 7.0 oder höher
- CommVault Simpana 9.0 oder höher
- IBM Tivoli 6.3

Aktivieren der NDMP-Unterstützung

NDMP-Sicherungen werden mithilfe des Client-Netzwerkes durchgeführt. Die DMA muss so konfiguriert sein, dass sie auf eine der Client-VIPs (oder einen DNS-Namen) des NAS-Clusters zugreifen kann.

ANMERKUNG: Bevor Sie die NDMP-Unterstützung aktivieren, muss eine Client-VIP im System konfiguriert werden. Überprüfen Sie, ob die Client-VIP konfiguriert ist, indem Sie **Systemverwaltung → Netzwerk → Subnetze** auswählen und überprüfen, ob das **Primäre** Subnetz eingerichtet ist.

So aktivieren Sie die NDMP-Unterstützung:

1. Wählen Sie **Datenschutz → NDMP → NDMP-Konfiguration** aus.
   Die Seite **NDMP-Konfiguration** wird angezeigt.
2. Wählen Sie **NDMP aktivieren** aus.

   ANMERKUNG: Zu Beginn ist das Kennwort für den **backup_user** nicht eingerichtet. Nachdem Sie den Benutzernamen ändern oder den Standardnamen verwenden, muss auch das Kennwort eingerichtet werden.

   ANMERKUNG: Standardmäßig ist der NDMP-Client-Port 10000.
3. Geben Sie in **DMA-Server** die IP-Adresse eines autorisierten DMA-Servers ein.

   ANMERKUNG: DNS-Namen werden nicht unterstützt.
4. Klicken Sie auf **Änderungen speichern**.

Ändern des NDMP-Kennworts und des Backup-Benutzernamens

Beim Konfigurieren eines NDMP-Servers in der DMA ist ein Benutzername und ein Kennwort erforderlich. Standardmäßig ist der Benutzername **backup_user**. Das Standardkennwort wird zufällig erstellt und muss vor Verwendung von NDMP geändert werden.

So ändern Sie das NDMP-Kennwort:

1. Wählen Sie **Data Protection (Datenschutz) → NDMP → NDMP Configuration (NDMP-Konfiguration).**
   Die Seite **NDMP Configuration (Budget-/Redundanzkonfiguration)** wird angezeigt.
2. Bei Bedarf ändern Sie in **Backup username (Backup-Benutzername)** den aktuellen Backup-Benutzernamen und klicken Sie auf **Save Changes (Änderungen speichern)**.
   Der Backup-Benutzername wurde geändert.
3. Klicken Sie auf **Change Backup User Password (Kennwort für Backup-Benutzer ändern)**.
   Die Seite **Change Password (Kennwort ändern)** zeigt den aktuellen Backup-Benutzernamen an.
4. Geben Sie in **admin password (Administratorkennwort)** das gültige Administratorkennwort ein.
5. Geben Sie unter dem Backup-Benutzernamen in **New password (Neues Kennwort)** das neue Kennwort ein.
6. Geben Sie in **Retype password (Kennwort erneut eingeben)** das genaue Kennwort ein, das Sie schon in **New password** eingegeben haben.
7. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Bearbeiten der DMA-Serverliste

Um eine NDMP-Sicherung der NAS-Cluster-Lösung zu erstellen, muss der Backup Application Server (Sicherungsanwendungsserver) in der Whitelist der DMA-Server enthalten sein.

Hinzufügen von DMA-Servern

So fügen Sie einen DMA-Server zur Liste hinzu:

1. Wählen Sie **Data Protection (Datenschutz) → NDMP → NDMP Configuration (NDMP-Konfiguration).**

Die Seite **NDMP Configuration (Budget-/Redundanzkonfiguration)** wird angezeigt.

2. Wenn keine leeren Felder des Typs **DMA server (DMA-Server)** verfügbar sind, klicken Sie auf **Add DMA server (DMA-Server hinzufügen)**.

   Ein zusätzliches Feld **DMA server** wird hinzugefügt.

3. Geben Sie in das leere Feld **DMA server** die IP-Adresse des DMA-Servers ein.

   ANMERKUNG: DNS-Namen werden nicht unterstützt.

4. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Entfernen von DMA-Servern

So entfernen Sie einen DMA-Server von der Liste:

1. Wählen Sie **Data Protection (Datenschutz) → NDMP → NDMP Configuration (NDMP-Konfiguration).**

   Die Seite **NDMP Configuration (NDMP-Konfiguration)** wird angezeigt.

2. Wählen Si den entsprechenden DMA-Server aus und klicken Sie auf **Remove DMA Server (DMA-Server entfernen)**.

   ANMERKUNG: Das Entfernen des DMA-Servers von der Whitelist unterbricht den bereits auf bzw. von diesem DMA-Server aus laufenden Sicherungs-/Wiederherstellungsvorgang nicht.

Angabe eines NAS-Volumes für die Sicherung

Die meisten Backup-Anwendungen listen die verfügbaren Volumes automatisch auf. In Symantec NetBackup 7.0 können Sie den Volume-Pfad manuell eingeben.

Die NAS-Cluster-Lösung macht die Backup-Volumes im folgenden Pfad verfügbar:

/<NASVolumeName>

wobei **<NASVolumeName>** der genaue Name ist, wie er in der Benutzeroberfläche erscheint.

Anzeigen von aktiven NDMP-Aufgaben

Alle Sicherungs- und Wiederherstellungsvorgänge, die die NAS-Cluster-Lösung durchführt, werden auf der Seite **Aktive NDMP-Aufgaben** angezeigt. Um die aktiven NDMP-Aufgaben anzusehen, wählen Sie **Datenschutz → NDMP → Aktive NDMP-Aufgaben** oder **Überwachen → Aktive NDMP-Aufgaben** aus.

Beenden einer aktiven NDMP-Aufgabe

Sie können eine aktive NDMP-Aufgabe beenden. So beenden Sie eine aktive NDMP-Aufgabe:

1. Wählen Sie **Data Protection (Datenschutz) → NDMP → NDMP Active Jobs (Aktive NDMP-Aufgaben).**

   Die Seite **Aktive NDMP-Aufgaben** zeigt alle aktiven NDMP-Aufgaben an.

2. Wählen Sie die Sitzung aus, die beendet werden soll.

3. Klicken Sie auf **Kill Active NDMP Job (Aktive NDMP-Aufgaben abbrechen)**.

   ANMERKUNG: Es können mehrere Sitzungen gleichzeitig ausgewählt werden.

Verwenden von Antivirus-Anwendungen

Die NAS-Cluster-Lösung enthält eine Integration mit nach Industriestandard ICAP-aktivierter Antivirus-Software, um sicherzustellen, dass von CIFS-Clients geschriebene Dateien virusfrei sind. Der Antivirus-Host muss mit Symantec ScanEngine 5.2 ausgeführt werden oder Symantec Protection Engine für Cloud Services 7.0, welches ICAP-aktiviert ist.

Vorhandene Antivirus-Hosts anzeigen

Um die für das System definierten Antivirus-Hosts anzuzeigen, wählen Sie **Datenschutz → Antivirus → Antivirus-Hosts** aus. Die Seite **Antivirus-Hosts** zeigt die Einzelheiten der bereits definierten Antivirus-Hosts, seine IP-Adressen (oder Namen) und den ICAP-Port an.

Hinzufügen von Antivirus-Hosts

Es wird empfohlen, mehrere Antivirus-Hosts zu definieren, um Hochverfügbarkeit bei der Virenprüfung zu erreichen und Verzögerungen beim Dateizugriff zu reduzieren. Wenn kein Antivirus-Host verfügbar ist, wird der Dateizugriff eventuell aufgrund fehlender Dienste verweigert.

So aktivieren Sie die Antivirus-Option:

1. Wählen Sie **Data Protection (Datenschutz) → Antivirus → Antivirus Hosts.**
   Die Seite **Antivirus Hosts** zeigt eine Liste der vorhandenen Antivirus-Hosts an.
2. Wenn keine leeren **Antivirus host**-Felder verfügbar sind, klicken Sie auf **Add (Hinzufügen)**.
   Ein zusätzliches **Antivirus host**-Feld wird hinzugefügt.
3. Geben Sie in **Antivirus host** die IP-Adresse (oder den Namen) des Antivirus-Hosts ein.
4. Geben Sie in **Port** den Port ein, über den das Host-ICAP-Protokoll kommuniziert.
   Standardmäßig ist der ICAP-Port 1344.
5. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Entfernen eines Antivirus-Hosts

So entfernen Sie einen Host aus der Liste der Antivirus-Hosts:

1. Wählen Sie **Data Protection (Datenschutz) → Antivirus → Antivirus Hosts.**
   Die Seite **Antivirus Hosts** zeigt eine Liste der verfügbaren Antivirus-Hosts an.
2. Wählen Sie aus der Liste der verfügbaren Antivirus-Hosts den gewünschten Antivirus-Host aus und klicken Sie auf **Delete (Löschen)**.

Antivirus-Unterstützung pro CIFS-Freigabe aktivieren

Antivirus-Unterstützung steht auf einer pro-CIFS-Freigabe Basis zur Verfügung.

So aktivieren Sie Antivirus-Support für CIFS-Freigaben:

1. Klicken Sie auf **Benutzerzugriff → Freigaben → CIFS-Freigaben.**
2. Klicken Sie auf die CIFS-Freigabe, für die Sie Antivirus-Unterstützung aktivieren möchten.
3. Aktivieren Sie das Kontrollkästchen **Dateien auf Viren überprüfen** unten auf der Seite.
4. Klicken Sie auf den Link **Antivirus**, der oben auf der Seite neben **Allgemein** und **Erweitert** angezeigt wird.
5. Konfigurieren Sie das Verhalten für die Handhabung von virusinfizierten Dateien (optional).
6. Konfigurieren Sie, welche Dateien auf Viren geprüft werden sollen (optional).
7. Konfigurieren Sie die Ausschlussliste (optional).
8. Klicken Sie auf **Änderungen speichern**.

5

Verwalten der FluidFS NAS-Lösung

Über die Registerkarte **Cluster Management (Clusterverwaltung)** können Sie allgemeine Systeminformationen einsehen und einstellen, Dateisystem und Netzwerkparameter konfigurieren und die erforderlichen Protokolle einstellen. Außerdem können Sie die Authentifizierungseinstellungen konfigurieren.

Zum Zugreifen auf die Optionen von **Cluster Management** starten Sie den NAS-Manager. Klicken Sie auf die Registerkarte **Cluster Management**. Die Seite **General Information (Allgemeine Informationen)** wird angezeigt.

Verwalten des Systems

Sie können die Verwaltungsvorgänge auf dem Cluster mithilfe des NAS-Managers durchführen.

Eine virtuelle IP-Adresse zur NAS-Verwaltung ist erforderlich, um auf den NAS-Manager zuzugreifen. Durch diese IP-Adresse können Sie das Cluster als eine Einheit verwalten.

Zusätzliche IP-Adressen werden sowohl für einzelne Controller im System als auch für das System selbst benötigt. Auf diese IP-Adressen dürfen Clients nicht direkt zugreifen.

Verwalten des Client-Zugangs

Über die Seite **Subnets (Subnetze)** können Sie eine oder mehrere virtuelle IP-Adressen einrichten, über die die Clients auf Freigaben und Exporte des Systems zugreifen können. Wenn Ihr Netzwerk geroutet ist, so wird empfohlen, mehr als eine virtuelle IP-Adresse zu definieren.

Sie können mehrere Subnetze definieren, damit Clients auf die NAS-Cluster-Lösung direkt zugreifen können und nicht über einen Router. Konfigurieren Sie für jedes Subnetz jeweils einen Namen auf Ihren DNS-Servern, um einen Lastenausgleich zwischen diesen IP-Adressen zu ermöglichen.

ANMERKUNG: Alle virtuellen IP-Adressen müssen gültige IP-Adressen auf den Netzwerken sein, die durch den Systemadministrator vor Ort zugewiesen wurden.

Auf der Seite **Subnets (Subnetze)** können Sie außerdem die IP-Adressbereiche aktualisieren, die intern durch das System für Verwaltungs- und Verbindungszwecke verwendet werden.

Sie können die aktuelle Konfiguration der Systemsubnetze anzeigen, neue Subnetzinformationen hinzufügen und vorhandene Subnetze entfernen oder ändern. Konfigurieren Sie für jedes Subnetz jeweils einen Namen auf Ihren DNS-Servern, um einen Lastenausgleich zwischen diesen IP-Adressen zu ermöglichen.

Anzeigen von definierten Subnetzen

Um die definierten Subnetze anzuzeigen, wählen Sie **Cluster Management (Clusterverwaltung)** → **Network (Netzwerk)** → **Subnets (Subnetze),** die Seite **Subnets (Subnetze)** zeigt eine Liste der vorhandenen Subnetze an.

Hinzufügen eines Subnetzes

1. Wählen Sie **Clusterverwaltung** → **Netzwerk** → **Subnetze** aus.

Die Seite **Subnetze** zeigt eine Liste der vorhandenen Subnetze an.

2. Klicken Sie auf **Hinzufügen**.
   Die Seite **Subnetz hinzufügen/bearbeiten** wird angezeigt.
3. Geben Sie in **Subnetzname** den entsprechenden Namen für das Subnetz ein.
4. Wählen Sie aus der Liste **Physikalisches Netzwerk** das gewünschte Netzwerk aus.
5. Geben Sie in **Subnetzmaske** die Adresse der Subnetzmaske ein.
6. Geben Sie die VLAN-ID für das Subnetz an, falls erforderlich.

   ANMERKUNG: Wenn ein VLAN mehrere Switche umfasst, wird die **VLAN-ID** dazu verwendet, anzugeben, an welche Ports und Schnittstellen Broadcast-Pakete übertragen werden sollen.
7. Geben Sie in **VIP der Verwaltungskonsole** die IP-Adresse der Systemverwaltungskonsole an.
8. Geben Sie in **Private IP** die IP-Adressen der einzelnen Systemcontroller für jeden Controller ein.

   ANMERKUNG: Diese IP-Adressen werden für die Controllerverwaltung vom technischen Support verwendet.
9. Geben Sie in **VIP-Adresse** die virtuellen IP-Adressen für einen oder mehrere Clients ein.

   ANMERKUNG: Diese VIPs werden für den Zugriff auf Dateien im System verwendet.

   ANMERKUNG: Die optimale Anzahl an VIPs hängt von Ihrer Netzwerkkonfiguration ab; weitere Informationen finden Sie in der Online-Hilfe.
10. Klicken Sie auf **Änderungen speichern**.

Ändern eines Subnetzes

ANMERKUNG: Sie können das primäre Subnetz oder ein internes Subnetz (Interconnect und Management) nicht ändern. Wenn Sie die IP-Adressen eines internen Subnetzes ändern müssen, dann müssen Sie zuerst das Dateisystem anhalten, bevor Sie die gewünschten IP-Adressen bearbeiten.

ANMERKUNG: Ändern Sie nicht nach der Erstbereitstellung die Interconnect- oder Management-Subnetze. Die Art und Weise, wie diese Subnetze während der Erstbereitstellung konfiguriert werden, sind von entscheidender Bedeutung für eine optimale Funktionalität.

1. Wählen Sie **Clusterverwaltung** → **Netzwerk** → **Subnetze** aus.
   Die Seite **Subnetze** zeigt eine Liste der vorhandenen Subnetze an.
2. Wählen Sie in der Liste der angezeigten Subnetze in der Spalte **Subnetzname** das gewünschte Subnetz aus.
   Die Seite **Subnetz hinzufügen/bearbeiten** wird für das ausgewählte Subnetz angezeigt.
3. Ändern Sie die Parameter nach Bedarf.
4. Klicken Sie auf **Änderungen speichern**.

Entfernen eines Subnetzes

ANMERKUNG: Es ist nicht möglich, das Subnetz mit der Bezeichnung „Primär“ oder ein anderes internes Subnetz (Interconnect und Management) zu löschen.

1. Wählen Sie **Clusterverwaltung** → **Netzwerk** → **Subnetze** aus.
   Die Seite **Subnetze** zeigt eine Liste der vorhandenen Subnetze an.
2. Wählen Sie aus der Liste der angezeigten Subnetze das entsprechende Subnetz aus und klicken Sie auf **Löschen**.

Verwalten von Administratorbenutzern

Administratoren können das Dell Fluid File System mithilfe der Dell Fluid File System-CLI oder der Web-Oberfläche verwalten.

Administratorbenutzer anzeigen

Um die vorhandenen Administratorbenutzer anzuzeigen, wählen Sie **Clusterverwaltung** → **Allgemein** → **Administratoren** aus. Die Seite **Administratoren** zeigt eine Liste der derzeit definierten Administratoren an.

Hinzufügen eines Administrators

Beim Definieren eines Administrators geben Sie die Berechtigungsebene des Administrators an. Berechtigungsebenen sind im System vordefiniert.

Die definierten Berechtigungsebenen lauten wie folgt:

- Administrator
- Nur Anzeige

Die Berechtigungsebenen definieren die Aktionen, die durch den Benutzer auf dieser Ebene ausgeführt werden können.

So fügen Sie einen Administrator hinzu:

1. Wählen Sie im NAS Manager **Clusterverwaltung** → **Allgemein** → **Administratoren** aus.
   Die Seite **Administratoren** wird angezeigt.
2. Klicken Sie auf **Hinzufügen**.
   Die Seite **Administrator hinzufügen** wird angezeigt. Standardmäßig wird die Registerkarte **Eigenschaften** angezeigt.
3. Geben Sie in **Benutzername** einen Namen für den Administrator ein.
4. Geben Sie in **Kennwort** ein Kennwort mit mindestens 6 Zeichen ein.
5. Geben Sie in **Kennwort erneut eingeben** das genaue Kennwort ein, dass Sie bereits in das Feld Password eingegeben haben.

   ANMERKUNG: Wenn das Kennwort zu einfach ist, werden Sie dazu aufgefordert, ein komplexeres Kennwort einzugeben.
6. Geben Sie in **Benutzer-ID** die Benutzer-ID (UID) ein oder verwenden Sie die vom System zur Verfügung gestellte Standard-UID.
7. Wählen Sie aus der Liste **Ebene** die Berechtigungsebene für den Administrator aus. Sie können **3-Administrator** oder **4-Nur Anzeige** auswählen.

   ANMERKUNG: Sie können andere Administratoren nur mit Berechtigungsebenen definieren, die in der Hierarchie unter der Ihrigen stehen.
8. Geben Sie in **E-Mail-Adresse** die E-Mail-Adresse des Administrators in dem verfügbaren **E-Mail-Adressenfeld** ein.
   Das System verwendet diese E-Mail-Adresse, um Warnmeldungen an den Administrator zu senden. Sie können zusätzliche E-Mail-Adressen hinzufügen, indem Sie auf **E-Mail-Adresse hinzufügen** klicken. Sie können die Arten der E-Mail-Warnmeldungen, die an den Administrator gesendet werden, mithilfe der Registerkarte **Filter** einstellen.
9. Wählen Sie die Registerkarte **Filter** aus, um Filterregeln für SNMP-Traps zu definieren.
10. Definieren Sie den Mindest-Trap-Schweregrad, der für jede Trap-Kategorie versendet wird.

    ANMERKUNG: Die Standardoption besteht darin, **wichtige** Traps für alle Kategorien zu senden.

11. Klicken Sie auf **Änderungen speichern**.

Ändern eines Administrators

1. Wählen Sie **Cluster Management → General (Allgemein) → Administrators (Administratoren).**
   Daraufhin wird die Seite **Administrator (Administratoren)** angezeigt, auf der eine Liste der derzeit definierten Administratoren angezeigt wird.
2. Klicken Sie in der Liste der verfügbaren Administratoren in der Spalte **User Name (Benutzername)** auf den gewünschten Administrator.
   Die Seite **Edit Administrator (Administrator bearbeiten)** wird angezeigt. Standardmäßig ist die Registerkarte **Properties (Eigenschaften)** ausgewählt.
3. Sie können **Level (Ebene)** und **Email address (E-Mail-Adresse)** für den ausgewählten Administrator ändern.
4. In der Registerkarte **Filters (Filter)** können Sie die Filterregeln für SNMP-Traps in jeder Kategorie verändern.
5. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Ändern des Administratorkennworts

VORSICHT: Wenn Sie bei Dell Compellent FS8600 das Administrator-Kennwort ändern, schlägt die Verbindung zwischen dem Enterprise Manager und dem Cluster fehl. Um die Verbindung zwischen dem Enterprise Manager und dem Cluster wiederherzustellen, klicken Sie im Enterprise Manager auf Wieder mit FluidFS-Cluster verbinden, nachdem Sie das Administrator-Kennwort geändert haben.

1. Wählen Sie **Clusterverwaltung → Allgemein → Administratoren** aus.
   Daraufhin zeigt die Seite **Administratoren** eine Liste der derzeit definierten Administratoren an.
2. Klicken Sie in der Liste der verfügbaren Administratoren in der Spalte **Benutzername** auf den gewünschten Administrator.
   Die Seite **Administrator bearbeiten** wird angezeigt. Standardmäßig ist die Registerkarte **Eigenschaften** ausgewählt.
3. Klicken Sie auf **Kennwort ändern**.
   Daraufhin wird das Fenster **Kennwort ändern** angezeigt.
4. Geben Sie in **Administrator-Kennwort** das aktuelle Kennwort für den ausgewählten Administrator ein.
5. Geben Sie unter **admin** in **Neues Kennwort** das neue Kennwort ein.
6. Geben Sie in **Kennwort erneut eingeben** das genaue Kennwort ein, dass Sie bereits in das Feld **Neues Kennwort** eingegeben haben.
7. Klicken Sie im Fenster **Kennwort ändern** auf **Änderungen speichern**.
   Es wird die Seite **Administrator bearbeiten** angezeigt.
8. Klicken Sie auf **Änderungen speichern**.

Entfernen eines Administrators

1. Wählen Sie **Cluster Management (Clusterverwaltung) → General (Allgemeine) → Administrators (Administratoren).**
   Daraufhin zeigt die Seite **Administrators (Administratoren)** eine Liste der derzeit definierten Administratoren an.
2. Wählen Sie aus der Liste der verfügbaren Administratoren den gewünschten Administrator aus und klicken Sie auf **Delete (Löschen).**

Verwalten von lokalen Benutzern für CIFS- und NFS-Zugriff

ANMERKUNG: Überspringen Sie diesen Abschnitt, wenn Ihre Einrichtung mit einer externen NIS/LDAP-Datenbank konfiguriert ist.

Sobald lokale Benutzer konfiguriert sind, können sie selbst dann auf das Cluster zugreifen, wenn ein externer NIS, LDAP oder Active Directory eingeführt wird.

Bei lokalen Benutzern richtet sich der Zugang zum Dateisystem nach Volumes, Freigaben und Exporten.

So gestatten Sie der NAS-Cluster-Lösung, lokale Benutzerdefinitionen zu verwenden:

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Authentication (Authentifizierung) → Identity Management Database (Identifikationsverwaltungsdatenbank).**

   Es wird die Seite **Identity Management Database (Identitätsverwaltungsdatenbank)** angezeigt.
2. Wählen Sie die Option **Users are not defined in an external user database (Benutzer sind nicht in einer externen Benutzerdatenbank definiert)**.
3. Bei CIFS-Benutzern wählen Sie **Cluster Management (Clusterverwaltung) → Protocols (Protokolle) → CIFS Configuration (CIFS-Konfiguration)**.

   Die Seite **CIFS Agent Configuration (Konfiguration des CIFS-Agenten)** wird angezeigt.
4. Wählen Sie den Modus aus, der zur Authentifizierung der Benutzeridentität verwendet werden soll. Sie können zwischen Folgendem auswählen:

   - **Authenticate users' identity via Active Directory and local user database (Benutzeridentität über Active Directory und lokale Benutzerdatenbank authentifizieren)**
   - **Authenticate users' identity via local users database (Benutzeridentität über lokale Benutzerdatenbank authentifizieren)**
5. Um die Liste **Local Users (Lokale Benutzer)** zu verwalten, wählen Sie **Cluster Management (Clusterverwaltung) → Authentication (Authentifizierung) → Local Users (Lokale Benutzer).**

Lokale Benutzer anzeigen

Um ein Liste der vorhandenen Benutzer anzuzeigen, wählen Sie **Clusterverwaltung → Authentifizierung → Lokale Benutzer** aus. Die Seite **Lokale Benutzer** zeigt eine Liste der vorhandenen Benutzer an.

Hinzufügen von lokalen Benutzern

1. Wählen Sie **Clusterverwaltung → Authentifizierung → Lokale Benutzer** aus.

   Die Seite **Lokale Benutzer** wird angezeigt.
2. Klicken Sie auf **Hinzufügen**.

   Die Seite **Benutzer hinzufügen** wird angezeigt. Standardmäßig wird die Registerkarte **Allgemein** der Seite **Benutzer hinzufügen** angezeigt.
3. Geben Sie in **Benutzername** den lokalen Benutzernamen ein.
4. Geben Sie in **Kennwort** das Kennwort ein (mindestens 6 Zeichen), das dem lokalen Benutzer zugeordnet werden soll.
5. Geben Sie in **Kennwort erneut eingeben** das gleiche Kennwort ein, dass Sie bereits in das Feld **Password** eingegeben haben.
6. Geben Sie in **Benutzer-ID** eine eindeutige UNIX-Benutzer-ID ein oder verwenden Sie die Standard-ID, die vom System angeboten wird.
7. In **Primäre Gruppe**:

- Geben Sie entweder den Namen der primären Gruppe für den lokalen Benutzer ein; oder
- klicken Sie auf die Schaltfläche **Durchsuchen**, um zur Liste der primären Gruppen zu browsen; oder
- verwenden Sie die vom System angebotene Standardgruppe.

8. Geben Sie in **Zusätzliche Gruppen** entweder den Namen einer anderen Gruppe ein, zu der der lokale Benutzer gehört, oder klicken Sie auf die Schaltfläche **Durchsuchen**, um zur Gruppenliste zu browsen (optional).

   ANMERKUNG: Sie können mehr als eine Gruppe hinzufügen.

9. Wählen Sie die Registerkarte **Erweitert** aus, um zusätzliche Informationen und optionale Felder abzurufen.
10. Geben Sie in **Echter Name** den echten Namen des Benutzers an.
11. Geben Sie in **Anmerkungen** Kommentare zum Benutzer an (optional).
12. Klicken Sie auf **Änderungen speichern**.

Ändern von lokalen Benutzern

1. Wählen Sie **Cluster Management → Authentication (Authentifizierung) → Local Users (Lokale Benutzer).**

   Die Seite **Local User (Lokale Benutzer)** zeigt eine Liste der vorhandenen lokalen Benutzer an.
2. Klicken Sie in der Liste der vorhandenen Benutzer unter **User Name (Benutzername)** auf den entsprechenden **User Name (Benutzernamen)**.

   Die Seite **Edit User (Benutzer bearbeiten)** wird angezeigt. Standardmäßig ist die Registerkarte **General (Allgemein)** ausgewählt.

   ANMERKUNG: Sie können die Gruppeninformationen für den ausgewählten Benutzer nur in der Registerkarte **General (Allgemein)** ändern.
3. In **Primary group (Primäre Gruppe)**:
   - Geben Sie entweder den Namen der primären Gruppe für den lokalen Benutzer ein; oder
   - klicken Sie auf die Schaltfläche **Browse (Durchsuchen)**, um zur Liste der primären Gruppen zu browsen; oder
   - verwenden Sie die vom System gestellte Standardgruppe.
4. Geben Sie in **Additional groups (Zusätzliche Gruppen)** entweder den Namen einer anderen Gruppe ein, zu der der lokale Benutzer gehört, oder klicken Sie auf die Schaltfläche **Browse (Durchsuchen),** um zu browsen und aus der Gruppenliste auszuwählen (optional).
5. Wählen Sie die Registerkarte **Advanced (Erweitert)** aus, um zusätzliche Informationen und optionale Felder abzurufen.
6. Geben Sie in **Real name (Echter Name)** den echten Namen des Benutzers an.
7. Geben Sie in **Remarks (Anmerkungen)** Kommentare zum Benutzer an (optional).
8. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Löschen von lokalen Benutzern

1. Wählen Sie **Cluster Management (Clusterverwaltung → Authentication (Authentifizierung) → Local Users (Lokale Benutzer).**

   Die Seite **Local User (Lokale Benutzer)** zeigt eine Liste der vorhandenen lokalen Benutzer an.
2. Wählen Sie aus der Liste der vorhandenen Benutzer den Benutzernamen aus und klicken Sie auf **Delete (Löschen)**.

Ändern des Kennworts

Sie können das Kennwort eines lokalen Benutzers über die Seite **Edit User (Benutzer bearbeiten)** ändern.

So ändern Sie das Kennwort eines lokalen Speicherbenutzers:

1. Wählen Sie **Cluster Management → Authentication (Authentifizierung) → Local Users (Lokale Benutzer).**
   Die Seite **Local User (Lokale Benutzer)** zeigt eine Liste der vorhandenen lokalen Benutzer an.
2. Klicken Sie in der Liste der vorhandenen Benutzer unter **User Name (Benutzername)** auf den entsprechenden User Name (Benutzernamen).
   Die Seite **Edit User (Benutzer bearbeiten)** wird angezeigt. Standardmäßig ist die Registerkarte **General (Allgemein)** ausgewählt.
3. Geben Sie in **admin password (Administrator-Kennwort)** das aktuelle Kennwort für den ausgewählten Administrator ein.
4. Geben Sie unter **admin** in **New password (Neues Kennwort)** das neue Kennwort ein.
5. Geben Sie in **Retype password (Kennwort erneut eingeben)** das genaue Kennwort ein, dass Sie bereits in das Feld **New Password (Neues Kennwort)** eingegeben haben.
6. Klicken Sie im Fenster **Change Password (Kennwort ändern)** auf **Save Changes (Änderungen speichern)**.
   Es wird die Seite **Edit Administrator (Administrator bearbeiten)** angezeigt.
7. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Verwalten von lokalen Gruppen

Wenn Ihr Standort mit einer externen NIS-Datenbank konfiguriert ist, können Sie diesen Abschnitt übergehen.

Sie müssen nur dann lokale Gruppen definieren, wenn Sie nur sehr wenige Linux/UNIX-Endbenutzer haben, die auf die NAS-Cluster-Lösung mithilfe von NFS zugreifen müssen, und nur dann, wenn keine externe NIS-Datenbank vorhanden ist.

Die Gruppen der NAS-Cluster-Lösung helfen bei der Organisation und Verwaltung von Benutzern. Beim Definieren von Benutzern können Sie lokale Speicherbenutzer einer oder mehreren Gruppen zuweisen. Die NAS-Cluster-Lösung kann auch extern definierte Gruppen oder Benutzer enthalten, wie z. B. in einem UNIX-System definierte Gruppen.

Lokale Gruppen anzeigen

Um die vorhandenen **Lokale Gruppen** anzuzeigen, wählen Sie **Clusterverwaltung → Authentifizierung → Lokale Gruppen** aus. Die Seite **Lokale Gruppen** zeigt eine Liste der vorhandenen lokalen Gruppen an.

Hinzufügen einer lokalen Gruppe

1. Wählen Sie **Cluster Management (Clusterverwaltung → Authentication (Authentifizierung) → Local Groups (Lokale Gruppen).**
   Die Seite **Local Groups (Lokale Gruppen)** wird angezeigt.
2. Klicken Sie auf **Add (Hinzufügen)**.
   Die Seite **Add Group (Gruppen hinzufügen)** wird angezeigt.
3. Geben Sie in **Group Name (Gruppenname)** den Namen der Gruppe ein.
4. Geben Sie in **Group ID (Gruppen-ID)** die Kennnummer der Gruppe ein.

   ANMERKUNG: Dell Fluid File System-Gruppen tragen Kennnummern über 200.

   ANMERKUNG: Der Gruppe wird automatisch die nächste verfügbare Kennnummer zugewiesen. Sie können sie bei Bedarf ändern.
5. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Löschen einer lokalen Gruppe

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Authentication (Authentifizierung) → Local Groups (Lokale Gruppen).**

   Die Seite **Local Groups (Lokale Gruppen)** zeigt eine Liste der vorhandenen lokalen Gruppen an.
2. Wählen Sie aus der Liste der vorhandenen lokalen Gruppen die gewünschte Gruppe aus und klicken Sie auf **Delete (Löschen)**.

Authentifizierung

Der Authentifizierungseintrag erlaubt es Ihnen, die Authentifizierungsstellen zu konfigurieren, wie z. B. Network Information Services (NIS), Active Directory (AD) und Light-weight Directory Access Protocol (LDAP). Außerdem können Sie lokale Benutzer und Gruppen verwalten und Benutzernamen von Windows SIDs zu UNIX UIDs zuweisen.

Die NAS-Cluster-Lösung unterstützt die folgenden Konfigurationsmodi:

- Gemischter und nativer Active Directory-Authentifizierungsmodus
- Nur NIS-Authentifizierung
- Nur LDAP-Authentifizierung
- Nur lokale interne Benutzer
- NIS oder LDAP und Active Directory

Konfigurieren einer Identitätsverwaltungsdatenbank

Durch eine **Identity Management Database (Identitätsverwaltungsdatenbank)** kann das System die Zugriffskontrolle auf Benutzerebene authentifizieren und verwalten. Diese Datenbank ist für die Verwaltung der Benutzer und ihrer Kennwörter, für die Gruppen und die Beziehungen zwischen Benutzern und Gruppen verantwortlich.

Wenn das System zu einer Active Directory-Domain gehört, dann dient es auch als Identitätsverwaltungsdatenbank. Sie können bei Bedarf zusätzliche UNIX-Datenbanken definieren.

Zu den UNIX-Identitätsverwaltungsdatenbanken gehören NIS und LDAP, und sie sind nur dann relevant, wenn Clients über das NFS-Protokoll (UNIX-/Linux-Clients) auf das System zugreifen.

Sie können entsprechend Ihrer Netzwerkumgebung eine der folgenden Optionen auswählen:

- Enable user authentication through an NIS database (Benutzerauthentifizierung über eine NIS-Datenbank aktivieren)
- Enable user authentication through an LDAP database (Benutzerauthentifizierung über eine NIS-Datenbank aktivieren)
- Disable the use of an external UNIX identity management database (Verwendung einer externen UNIX-Identitätsverwaltungsdatenbank deaktivieren)

Aktivieren der Benutzerauthentifizierung über eine NIS-Datenbank

1. Wählen Sie **Clusterverwaltung → Authentifizierung → Identifikationsverwaltungsdatenbank** aus.

   Es wird die Seite **Identitätsverwaltungsdatenbank** angezeigt.
2. Wählen Sie **Benutzer und Gruppen sind in einer NIS-Datenbank definiert.**
3. Geben Sie in **Domänenname** den Domänenname der NIS-Datenbank ein.
4. In allen leeren **NIS-Servern**, geben Sie den Namen oder die IP-Adresse des NIS-Servers ein.
5. Um einen NIS-Server zu Redundanzzwecken hinzuzufügen, klicken Sie auf **NIS-Server hinzufügen**.

Ein zusätzlicher **NIS-Server** wird in der Liste der NIS-Server angezeigt.

6. Wählen Sie zum Entfernen eines NIS-Servers aus der Liste den NIS-Server aus, den Sie löschen möchten, und klicken Sie dann auf **NIS-Server löschen**.
7. Klicken Sie auf **OK**, wenn Sie dazu aufgefordert werden, die Änderungen zu bestätigen.
8. Klicken Sie auf **Änderungen speichern**.

Aktivieren der Benutzerauthentifizierung über eine LDAP-Datenbank

1. Wählen Sie **Clusterverwaltung → Authentifizierung → Identitätsverwaltungsdatenbank** aus.
   Es wird die Seite **Identitätsverwaltungsdatenbank** angezeigt.
2. Wählen Sie **Benutzer und Gruppen sind in einer LDAP-Datenbank definiert** aus.
3. Geben Sie in **LDAP-Server** den Namen oder die IP-Adresse des LDAP-Servers ein.
4. Geben Sie in **unterscheidbaren Basisnamen** den unterscheidbaren Basisnamen (DN) ein, den Sie zur Authentifizierung verwenden möchten.
   Der unterscheidbarer Basisname ist eine eindeutige LDAP-Zeichenfolge, die die Domäne zur Authentifizierung repräsentiert. Normalerweise ist das Format wie folgt:
   `dc=domain`
   `dc=com`
5. Klicken Sie auf **Änderungen speichern**.

Deaktivieren der Verwendung einer externen UNIX-Identitätsverwaltungsdatenbank

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Authentication (Authentifizierung) → Identity Management Database (Identitätsverwaltungsdatenbank).**
   Es wird die Seite **Identity Management Database (Identitätsverwaltungsdatenbank)** angezeigt.
2. Wählen Sie die Option **Users are not defined in an external user database (Benutzer sind nicht in einer externen Benutzerdatenbank definiert)**.
3. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Active Directory

Der Dienst Active Directory speichert Informationen zu allen Objekten in dem Computernetzwerk und macht diese Informationen für Administratoren und Benutzer zum Suchen und Anwenden verfügbar. Mithilfe von Active Directory können Benutzer von überall im Netzwerk mit einer einzigen Anmeldung auf Ressourcen zugreifen.

Genauso verfügen Administratoren über eine einzige Verwaltungsstelle für alle Objekte im Netzwerk, die in einer hierarchischen Struktur angezeigt werden. Der Active Directory-Eintrag ermöglicht es Ihnen, die Active Directory-Einstellungen zu konfigurieren und Optionen zur Benutzerauthentifizierung einzustellen. Außerdem können Sie die Active Directory-Domäne verknüpfen.

Synchronisieren der NAS-Cluster-Lösung mit dem Active Directory-Server

Wenn Ihr Standort Active Directory verwendet und die NAS-Cluster-Lösung Teil des Windows-Netzwerkes ist, synchronisieren Sie die Zeituhr mit dem Active Directory-Server. Um die Uhr mit dem Active Directory-Server zu synchronisieren, wählen Sie **Cluster Management (Clusterverwaltung) → General (Allgemein) → Time Configuration (Zeitkonfiguration).**

Konfigurieren des Active Directory-Dienstes

1. Wählen Sie **Clusterverwaltung** → **Authentifizierung** → **Systemidentität** aus.

   Die Seite **Systemidentität** wird angezeigt. Diese Seite zeigt die aktuelle Konfiguration an und ob die NAS-Cluster-Lösung bereits mit einer Active Directory-Domäne verbunden ist.

2. Geben Sie in **Systemname** den Systemnamen ein.

   Dieser Name identifiziert das Dell Fluid File System in Warnmeldungen, die das System ausgibt, und ist außerdem der Standardname für das Dell Fluid File System, wenn Sie Active Directory konfigurieren.

3. Wählen Sie **Das System ist Mitglied eines Microsoft Windows-Netzwerkes** aus, wenn das Dell Fluid File System mit einer Active Directory-Domäne verbunden werden soll, und fahren Sie mit dem nächsten Schritt fort. Ist dies nicht der Fall, so lassen Sie dieses Feld leer und klicken Sie auf **Änderungen speichern**.

4. Geben Sie in **Name des System-NetBIOS** den Namen des Dell Fluid File System-NetBIOS ein, der in der Netzwerknachbarschaft angezeigt wird.

   Dieser Name ist auf 15 Zeichen beschränkt. Verwenden Sie den Systemnamen, wenn Sie nicht zu etwas anderem aufgefordert werden.

5. Geben Sie in **Domäne** die Domäne ein, zu der das Dell Fluid File System gehört.

   Verwenden Sie den Fully Qualified Domain Name (FQDN), nicht den NetBIOS-Domänenname. Zum Beispiel: mydomain.company.com

6. Geben Sie in **Benutzername** den Benutzernamen des Administrators ein, der zum Verbinden der Active Directory-Domäne verwendet werden soll.

   ANMERKUNG: Dieser Benutzername wird nicht im Dell Fluid File System gespeichert.

7. Geben Sie in **Kennwort** das Administratorkennwort ein.

   ANMERKUNG: Dieses Kennwort wird nicht im Dell Fluid File System gespeichert.

   VORSICHT: „Erweiterte Konfiguration" darf nur markiert sein, wenn Sie dazu vom Dell Support angewiesen wurden. Mit diesem Feld können Sie weitere Parameter zu Active Directory konfigurieren.

   Mithilfe der Option **Erweiterte Konfiguration** können Sie einen Domain-Controller so definieren, dass er den durch das System ausgewählten Standard-Controller überschreibt.

8. Klicken Sie auf **Änderungen speichern**.

Netzwerkkonfiguration – Überblick

Definieren Sie für den Zugriff auf das System eine IP-Adresse, auf die Ihre Clients zugreifen können. Es wird empfohlen, diese IP-Adresse auch zu Ihrem DNS-Server hinzuzufügen, damit Clients neben der IP-Adresse auch über einen Namen auf das System zugreifen können.

ANMERKUNG: Sie müssen CIFS konfigurieren, um Benutzer nach Beitritt zur Domäne zu authentifizieren. Um Benutzer zu authentifizieren, gehen Sie zu **Clusterverwaltung** → **Protokolle** → **CIFS-Konfiguration.** Wählen Sie **Benutzeridentität über Active Directory und lokale Benutzerdatenbank authentifizieren** aus.

ANMERKUNG: Die Client-Zugriffs-VIP wird während der Erstkonfiguration mithilfe des **Dienstprogramm zur ersten Bereitstellung von Dell NAS** konfiguriert. Die Adresse, die Sie konfiguriert haben, finden Sie im NAS-Manager unter **Clusterverwaltung** → **Netzwerk** → **Subnetze**. Klicken Sie auf **Primär** unten auf der Seite, um die als Zugriffs-VIP gekennzeichnete **VIP-Adresse** anzuzeigen.

Da die Architektur des Systems ein Cluster aus zwei oder mehr Controllern ist, ist diese IP-Adresse eine VIP, die jeden Controller im Cluster bedient. So können Clients auf das System als eine Einheit zugreifen, das System kann einen

Lastenausgleich zwischen den Controllern durchführen und außerdem können Dienste weiter ausgeführt werden, auch wenn ein Controller ausfällt. Clients profitieren von der hohen Verfügbarkeit und der starken Leistung des Systems.

Client-Benutzer greifen auf das System über verschiedene Netzwerktopologien zu. Je nach den physikalischen Funktionen der Netzwerkinfrastruktur gilt Folgendes:

- Die NAS-Cluster-Lösung gehört allen LAN- oder Client-Subnetzen. In Hinblick auf die Leistung ist dies die optimalste Konfiguration. In solchen Netzwerkkonfigurationen ist es ausreichend, eine Client-Zugriffs-VIP für jedes Subnetz zu definieren.
- Die NAS-Cluster-Lösung gehört keinem der LAN- oder Client-Subnetze, in diesem Fall werden alle Clients als geroutet betrachtet. In diesen Fällen greifen die Clients auf die Daten über einen Router oder einen Layer-3-Switch zu. In solchen Netzwerkkonfigurationen wird empfohlen, mehrere Client-Zugriffs-VIPs in einem Subnetz zu definieren und einen Mechanismus zur Verfügung zu stellen, mit dem die Clients eine IP-Adresse aus dieser Liste auswählen können.
- Die NAS-Cluster-Lösung gehört zu einigen der LAN- oder Client-Subnetze, in diesem Fall sind manche Clients flach und manche geroutet. In solchen Netzwerkkonfigurationen wird empfohlen, beide oben beschriebenen Methoden zu verwenden und die Benutzer über die VIPs zu informieren, die sie verwenden müssen, je nachdem, ob sie flach oder geroutet sind.

Es wird empfohlen, einen Eintrag ins DNS für jedes Subnetz zu definieren, zu dem das System gehört, sodass Clients auf die Daten zugreifen können, ohne sich an die VIPs zu erinnern. Wenn es im Subnetz mehrere VIPs gibt, definieren Sie einen einzelnen Namen in Ihrem DNS-Server, der IP-Adressen aus der Liste im Roundrobin-Verfahren ausgibt, und alle Clients können auf das System zugreifen.

ANMERKUNG: Vermischen Sie niemals VIPs aus unterschiedlichen Subnetzen in einem einzigen DNS-Namen.

Leistung und statische Routen

Geroutete Netzwerke bieten die Möglichkeit, die Leistung durch eine Funktion namens statische Routen zu erweitern. Mit dieser Funktion können Sie die genauen Pfade konfigurieren, in denen das System mit verschiedenen Clients in einem gerouteten Netzwerk kommuniziert.

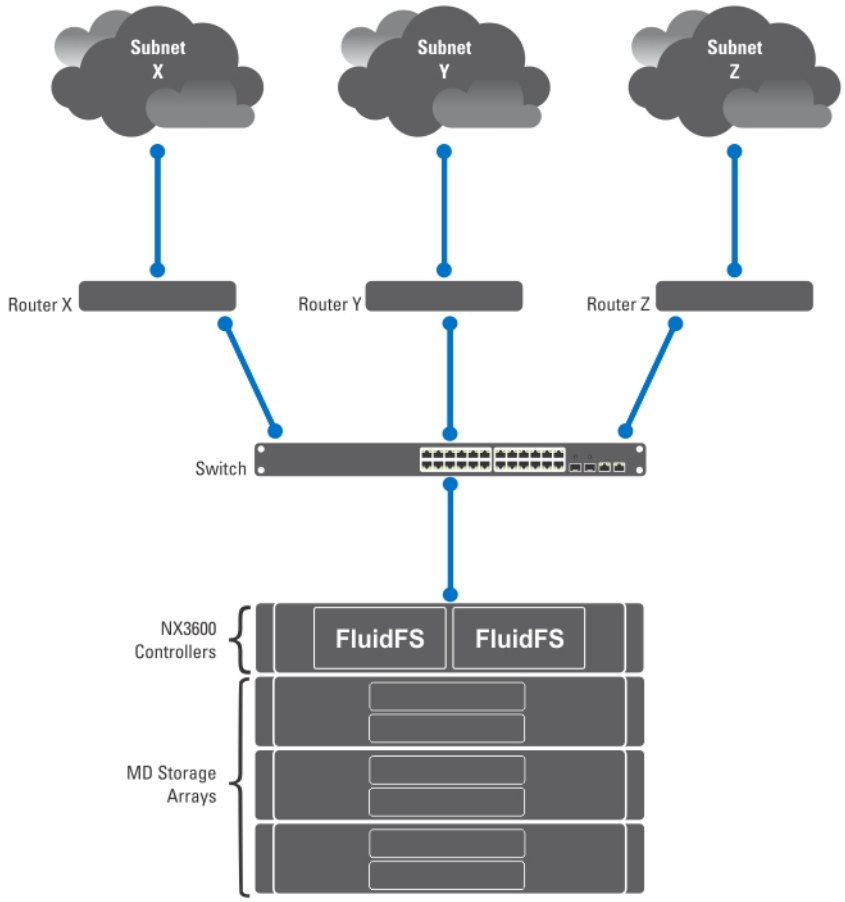

Abbildung 6. Netzwerkkonfiguration

Es kann im Netzwerk oben nur ein Standard-Gateway für das System geben. Nehmen Sie an, dass Sie den *Router X* auswählen.

Pakete, die zu Clients in Subnetz Y gesendet werden, werden zu Router X geroutet und dann (über den Switch) zurück zu Router Y gesendet. Diese Pakete wandern unnötigerweise durch Router X und verringern dadurch den Datendurchsatz für alle Subnetze in Ihrem Netzwerk.

Die Lösung besteht darin, neben einem Standard-Gateway ein spezielles Gateway für bestimmte Subnetze konfigurierende statische Routen zu definieren. Dazu müssen Sie jedes Subnetz in Ihrem Netzwerk beschreiben und das geeignetste Gateway für den Zugriff auf das Subnetz identifizieren.

Sie müssen dies nicht für das gesamte Netzwerk machen, ein Standard-Gateway ist durchaus angebracht, wenn die Leistung kein Problem ist. Sie können auswählen, wann und wo statische Routen genutzt werden sollen, um Ihren Leistungsansprüchen voll gerecht zu werden.

Konfigurieren von DNS

Domain Name System (DNS) ist der Dienst zur Namensauflösung, durch den Benutzer Computer in einem Netzwerk oder im Internet (TCP/IP-Netzwerk) mithilfe des Domänennamens auffinden können. Der DNS-Server verwaltet eine Datenbank mit Domänennamen (Hostnamen) und ihren entsprechenden IP-Adressen und bietet so Auflösungsdienste der Arten Name-zu-Adresse und Adresse-zu-Name im IP-Netzwerk. Sie können einen oder mehrere externe DNS-

Server (außerhalb des NAS-Clusters, aber am selben Standort) konfigurieren, die zur Namensauflösung verwendet werden sollen.

DNS-Server anzeigen

Um eine Liste der vorhandenen DNS-Server und ihrer Parameter anzuzeigen, wählen Sie **Clusterverwaltung** → **Netzwerk** → **DNS-Konfiguration** aus. Die Seite **DNS-Konfiguration** zeigt eine Liste der vorhandenen DNS-Server und ihrer Parameter an.

Hinzufügen von DNS-Servern und DNS-Erweiterungen

1. Wählen Sie **Cluster Management (Clusterverwaltung)** → **Network (Netzwerk)** → **DNS Configuration (DNS-Konfiguration).**
   Die Seite **DNS Configuration (DNS-Konfiguration)** wird angezeigt.
2. Um einen DNS-Server hinzuzufügen, klicken Sie auf **Add DNS Server (DNS-Server hinzufügen)**.
   Es wird eine neue leere Zeile zur Liste der DNS-Server hinzugefügt.
3. Legen Sie die IP-Adresse für die primäre DNS der Client-Umgebung fest.
4. Um eine DNS-Erweiterung hinzuzufügen, klicken Sie auf **Add DNS Suffix (DNS-Erweiterung hinzufügen)**.
   Es wird eine neue leere Zeile zur Liste der DNS-Erweiterungen hinzugefügt.
5. Geben Sie die DNS-Erweiterungen nach Priorität ein.
6. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Entfernen von DNS-Servern und DNS-Erweiterungen

1. Wählen Sie **Cluster Management** → **Network (Netzwerk)** → **DNS Configuration (DNS-Konfiguration).**
   Die Seite **DNS Configuration (DNS-Konfiguration)** zeigt eine Liste der vorhandenen DNS-Server und ihre Parameter an.
2. Wählen Sie den entsprechenden DNS-Server und/oder die DNS-Erweiterung aus und klicken Sie auf **Delete (Löschen)**.
   Eine Meldung fordert Sie auf, zu bestätigen, dass der gelöschte DNS-Server alle anderen vorgenommenen Änderungen speichert.
3. Klicken Sie auf **OK**.

Verwalten von statischen Routen

Um das Auftreten von Hops zwischen Routern zu minimieren, werden statische Routen in gerouteten Netzwerken empfohlen, wenn es mehrere direkte Pfade von der NAS-Cluster-Lösung zu verschiedenen Routern gibt.

Statische Routen anzeigen

Wählen Sie **Clusterverwaltung** → **Netzwerkverwaltung** → **Statische Routen** aus. Die Seite **Statische Routen** zeigt eine Liste der derzeit definierten statischen Routen an.

Hinzufügen von statischen Routen

Wenn Sie eine statische Route definieren, müssen Sie auch die Subnetz-Eigenschaften und das Gateway angeben, über das der Zugriff auf das Subnetz erfolgen soll.

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Network Management (Netzwerkverwaltung) → Static Routes (Statische Routen).**

   Die Seite **Static Routes (Statische Routen)** wird angezeigt.
2. Klicken Sie auf **Add (Hinzufügen)**.

   Die Seite **Add Static Routes (Statische Routen hinzufügen)** wird angezeigt.
3. Wählen Sie aus der Liste **Network (Netzwerk) d**as Netzwerk aus, von dem aus auf das Subnetz zugegriffen werden kann.
4. Geben Sie in **Gateway IP (Gateway-IP)** die IP-Adresse des Gateways zum Subnetz ein, das den besten Zugriff auf das Ziel-Subnetz bietet.
5. Geben Sie in **Destination Subnet (Ziel-Subnetz)** das Subnetz des Ziels ein, um über eine statische Route zugreifen zu können.
6. Geben Sie in **Netmask (Netzmaske)** die Netzmaske ein, um dieses Subnetz von anderen Subnetzen zu trennen.
7. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Ändern einer statischen Route

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Network Management (Netzwerkverwaltung) → Static Routes (Statische Routen).**

   Die Seite **Static Routes** zeigt eine Liste der derzeit definierten statischen Routen an.
2. Wählen Sie aus der Liste der vorhandenen statischen Route die gewünschte statische Route aus und klicken Sie auf **Edit (Bearbeiten)**.

   Daraufhin werden die Eigenschaften der ausgewählten statischen Route angezeigt.
3. Ändern Sie die Eigenschaften nach Bedarf.

Löschen einer statischen Route

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Network Management (Netzwerkverwaltung) → Static Routes (Statische Routen).**

   Die Seite **Static Routes (Statische Routen)** zeigt eine Liste der derzeit definierten statischen Routen an.
2. Wählen Sie aus der Liste der vorhandenen statischen Routen die gewünschte Route aus und klicken Sie auf **Delete (Löschen)**.

Definieren von Dateisystemprotokollen

Dateisystemprotokolle sind Netzwerkprotokolle, die Dienste zur Dateisystemfreigabe bieten. Die NAS-Cluster-Lösung dient als ein Dateisystemserver, indem sie die folgenden Protokolle erfüllt:

- CIFS: Das Common Internet File System ist für Microsoft Windows-Benutzer oder andere CIFS-Benutzer. Verzeichnisse werden mithilfe von CIFS-Freigaben freigegeben.
- NFS: Das Network File System-Protokoll ist für UNIX-Clients oder -Dienste. Es wird auf der NFS-Ebene ausgeführt. Verzeichnisse werden mithilfe von NFS-Exporten freigegeben.

Mithilfe der Einträge **Protocol (Protokoll)** können Sie die CIFS- und NFS-Protokolle auf Systemebene verwalten.

Konfigurieren von CIFS-Parametern

Durch die **CIFS-Protokollkonfiguration** können Windows-Benutzer sich mit der NAS-Cluster-Lösung verbinden. Sie können auch Linux-Benutzer dazu aktivieren, auf das System über das CIFS-Protokoll zuzugreifen und sie durch NIS, LDAP oder die lokalen Benutzer der NAS-Cluster-Lösung zu authentifizieren.

In der Registerkarte **Allgemein** können Sie auswählen, ob die Benutzer mithilfe der Active Directory-Domäne oder mithilfe einer internen Benutzerdatenbank authentifiziert werden sollen. Sie können auch die Verwendung des CIFS-Protokolls aktivieren oder deaktivieren.

Konfigurieren von allgemeinen CIFS-Parametern

1. Wählen Sie **Clusterverwaltung** → **Protokolle** → **CIFS-Konfiguration** aus.

   Die Seite **CIFS-Protokollkonfiguration** wird angezeigt. Standardmäßig wird die Registerkarte **Allgemein** ausgewählt.
2. Wählen Sie **Clients den Zugriff auf Dateien über das CIFS-Protokoll genehmigen** aus, um das CIFS-Dateifreigabeprotokoll zu aktivieren.
3. Geben Sie in **Systembeschreibung** eine kurze Beschreibung für den Server ein.

   Diese Beschreibung wird in der Windows Explorer-Titelleiste angezeigt.
4. Wählen Sie die Methode aus, mit der das System die Benutzeridentität authentifizieren soll. Sie können zwischen Folgendem auswählen:

   – Um Benutzer über die Active Directory-Domäne, der das System angebunden ist, zu identifizieren, wählen Sie **Benutzeridentität über Active Directory und lokale Benutzerdatenbank authentifizieren** aus.

   – Um Benutzer über eine interne Benutzerdatenbank zu identifizieren, wählen Sie **Benutzeridentität über lokale Benutzerdatenbank authentifizieren** aus.
5. Klicken Sie auf **Änderungen speichern**.

   Durch diesen Vorgang werden alle Benutzerverbindungen neu gestartet.

Benutzern den Zugriff auf Dateien über das CIFS-Protokoll verweigern

1. Wählen Sie **Cluster Management (Clusterverwaltung)** → **Protocols (Protokolle)** → **CIFS Configuration (CIFS-Konfiguration).**

   Die Seite **CIFS Protocol Configuration (CIFS-Protokoll-Konfiguration)** wird angezeigt. Standardmäßig ist die Registerkarte **General (Allgemein)** ausgewählt.
2. Entfernen Sie die Markierung von **Allow clients to access files via the CIFS protocol (Clients erlauben, auf Dateien über das CIFS-Protokoll zuzugreifen)**.
3. Klicken Sie auf **Save Changes (Änderungen speichern)**.

   Durch diesen Vorgang werden alle Benutzerverbindungen neu gestartet.

Konfigurieren von erweiterten CIFS-Parametern

Auf der Registerkarte **Erweitert** können Sie Folgendes festlegen:

- Der Zeichensatz, der von DOS-Code-Seiten verwendet wird.
- Der UTF-8-Zeichensatz, der von der NAS-Cluster-Lösung verwendet wird.

So konfigurieren Sie erweiterte CIFS-Parameter:

1. Wählen Sie **Clusterverwaltung** → **Protokolle** → **CIFS-Konfiguration** aus.

   Die Seite **CIFS-Protokoll-Konfiguration** wird angezeigt. Standardmäßig wird die Registerkarte **Allgemein** ausgewählt.
2. Wählen Sie die Registerkarte **Erweitert**.
3. Wählen Sie aus der Liste **DOS-Code-Seite** den Zeichensatz aus, der von Clients verwendet wird, die nicht UNICODE unterstützen.
4. Wählen Sie aus der Liste **Unix-Zeichensatz** die Version des UTF-8-Zeichensatzes aus, die vom System verwendet wird. So kann Text richtig in den Zeichensatz des verbundenen Clients konvertiert werden.
5. Klicken Sie auf **Änderungen speichern**.

   ANMERKUNG: Durch diesen Vorgang werden alle Benutzerverbindungen neu gestartet.

Konfigurieren von Systemzeitparametern

Sie können auf dieser Seite die Systemuhr konfigurieren, festlegen, wie die Uhrzeit automatisch mit einem NTP-Server aktualisiert werden soll und die Zeitzone für Ihr System konfigurieren. Das Synchronisieren der Uhr ist sehr wichtig für die korrekte Funktion des Systems.

Dadurch werden die folgenden Funktionen aktiviert:

- Windows-Clients zum Laden des Systems.
- Geplante Aktivitäten, wie z. B. Snapshot- und Replikationsaufgaben, die zur entsprechenden Uhrzeit ausgeführt werden.
- Die korrekte Uhrzeit, die im Systemprotokoll erfasst wird.

Ändern der Zeitzone

1. Wählen Sie **Cluster Management (Clusterverwaltung)** → **General (Allgemein)** → **Time Configuration (Zeitkonfiguration).**

   Die Seite **Time Configuration (Zeitkonfiguration)** wird angezeigt.
2. Wählen Sie aus der Liste **Time zone (Zeitzone)** die korrekte Zeitzone für die Region aus, in der sich das Cluster befindet.
3. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Manuelles Konfigurieren des Tagesdatums und der aktuellen Uhrzeit

Wenn in Ihrer Umgebung keine Zeitsynchronisierungsserver verwendet werden, müssen Sie das Tagesdatum und die aktuelle Uhrzeit manuell konfigurieren.

So führen Sie eine manuelle Konfiguration von Tagesdatum und aktueller Uhrzeit durch:

1. Wählen Sie **Clusterverwaltung** → **Allgemein** → **Zeitkonfiguration** aus.

   Die Seite **Zeitkonfiguration** wird angezeigt.
2. Wählen Sie **Es sind keine NTP-Server für die Synchronisation der Zeit vorhanden** aus.
3. Geben Sie in **Datum** das aktuelle Datum ein.

   ANMERKUNG: Verwenden Sie das Format: TT/MM/JJJJ, wobei TT den Tag, MM den Monat und JJJJ das Jahr angibt. Zum Beispiel: *30/05/2012*.
4. Geben Sie in **Uhrzeit** die aktuelle Uhrzeit ein.

   ANMERKUNG: Verwenden Sie das Format: HH:MM:SS, wobei HH die Stunde im 24-Stunden-Zeitformat angibt. Zum Beispiel: *17:38:23*.

5. Klicken Sie auf **Änderungen speichern**.

Entfernen eines NTP-Servers

Wenn sich ein NTP-Server nicht mehr im LAN-oder Client-Netzwerk befindet, können Sie den NTP-Server entfernen.

So entfernen Sie einen NTP-Server:

1. Klicken Sie auf **Cluster Management → General (Allgemein) → Time Configuration (Zeitkonfiguration).**
   Die Seite **Time Configuration (Zeitkonfiguration)** zeigt eine Liste der verfügbaren NTP-Server an.
2. Wählen Sie den entsprechenden NTP-Server aus und klicken Sie auf **Delete NTP server(s) (NTP-Server löschen)**.
3. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Synchronisieren der NAS-Cluster-Lösung mit einem lokalen NTP-Server

Das Netzwerkzeitprotokoll (NTP) hilft bei der Synchronisierung und Koordinierung der Zeitverteilung. Der NTP-Server trägt zur Synchronisierung der Uhren innerhalb des Netzwerkes bei.

Wenn das System nicht Teil eines Windows-Netzwerkes ist, konfigurieren Sie es so, dass es sich entweder mit eine lokalen NTP-Server (falls vorhanden) oder mit einem NTP-Server im Internet synchronisiert. Wenn das System jedoch Teil eines Windows-Netzwerkes ist, kann das Active Directory als NTP-Server dienen.

So konfigurieren Sie das Cluster-System für die Synchronisation mit einem lokalen NTP-Server oder einem NTP-Server im Internet:

1. Wählen Sie **Clusterverwaltung → Allgemein → Zeitkonfiguration** aus.
   Die Seite **Zeitkonfiguration** wird angezeigt.
2. Wählen Sie die Option **Uhrzeit muss mit einem NTP-Server synchronisiert werden**.
3. Wählen Sie **NTP-Server** aus.
4. Geben Sie im **NTP-Server** den Namen des lokalen NTP-Servers oder des Internet-NTP-Servers ein.
5. Um einen redundanten NTP-Server hinzuzufügen, klicken Sie auf **NTP-Server hinzufügen**, und geben Sie den Namen des redundanten NTP-Servers in das Feld **NTP-Server** ein.
6. Klicken Sie auf **Änderungen speichern**.

Lizenzenverwaltung

Installierte Lizenzen können in der NAS-Verwaltungssoftware angezeigt und verwaltet werden.

Lizenzen anzeigen

Um installierte Lizenzen anzuzeigen, wählen Sie **Clusterverwaltung → Allgemein → Lizenzen** . Die Seite **Lizenzierte Funktionen** zeigt eine Liste der installierten Lizenzen an.

Hinzufügen einer Lizenz

Die Funktion(en) aus der Lizenzdatei wird/werden im Lizenzfenster angezeigt, nachdem das System die Datei validiert und den Bildschirm aktualisiert hat.

So fügen Sie eine Lizenz hinzu:

1. Wählen Sie **Clusterverwaltung → Allgemein → Lizenzen** aus.

Die Seite **(Lizenzierte Funktionen** wird angezeigt.

2. Geben Sie in **XML-Lizenzdatei hochladen** den Pfad der XML-Lizenzdatei ein oder klicken Sie auf die Schaltfläche **Durchsuchen,** um zum Speicherort der XML-Lizenzdatei zu navigieren.
3. Klicken Sie auf **Hochladen**, um die Lizenzdatei hochzuladen.

   Die Funktion(en) aus der Lizenzdatei wird/werden im Lizenzfenster angezeigt, nachdem das System die Datei validiert und den Bildschirm aktualisiert hat.

Entfernen einer Lizenz

VORSICHT: Eine Lizenz darf nur auf Anweisung des technischen Supports von Dell entfernt werden.

Die Funktion(en) aus der Lizenzdatei wird/werden im Lizenzfenster angezeigt, nachdem das System die Datei validiert und den Bildschirm aktualisiert hat.

1. Wählen Sie **Cluster Management → General (Allgemein) → Licensing (Lizenzen).**

   Die Seite **Licensed Features (Lizenzierte Funktionen)** zeigt eine Liste der installierten Lizenzen an.
2. Wählen Sie aus der Liste der installierten Lizenzen die gewünschte Funktion aus und klicken Sie auf **Delete License for feature (Lizenz für Funktion löschen)**.

Konfigurieren von E-Mail-Parametern in PowerVault NX3500/ NX3600/NX3610 NAS-Lösungen

ANMERKUNG: Diese Funktion wird in Dell Compellent FS8600 NAS-Lösungen nicht unterstützt. Dell Compellent FS8600 verwendet Enterprise Manager für alle E-Mail-Warnmeldungen. Weitere Informationen finden Sie unter *Enterprise Manager Users Guide (Benutzerhandbuch des Enterprise Managers)*.

Dell Fluid File System verwendet E-Mails als Grundlage für Warnmeldungen und Remote-Support. Sie können bestimmen, wer manche oder alle der folgenden Nachrichtenarten erhalten soll, die das Dell Fluid File System versendet:

- Takte – Takte werden alle fünf Minuten an den E-Mail-Empfänger gesendet. So kann das Remote-Support-Team auf Systemausfälle reagieren.
- Systemprotokolle – Systemprotokolle werden regelmäßig an den E-Mail-Empfänger gesendet. So kann das Remote-Support-Team leichte Systemfehler identifizieren und sie bei Bedarf beheben.
- Warnmeldungen – E-Mail-Warnmeldungen, die über den Systemdienst Auskunft geben.

Sie können bei Bedarf zusätzliche Empfänger hinzufügen. Wenn Sie Administratoren als Empfänger hinzufügen, so wird empfohlen, das System so konfigurieren, dass Systemwarnmeldungen nur an sie gesendet werden.

Sie können das System auch manuell dazu auffordern, bei Bedarf einen Systeminformationsbericht zu senden.

SMTP-Server anzeigen

Um eine Liste der konfigurierten SMTP-Server anzuzeigen, wählen Sie **Clusterverwaltung → Überwachungskonfiguration → E-Mail-Konfiguration**. Die Seite **E-Mail-Konfiguration** zeigt eine Liste der konfigurierten SMTP-Server an.

Konfigurieren eines SMTP-Servers

SMTP-Server erlauben es Ihnen, E-Mails an Benutzer zu senden, die sich nicht in derselben Domäne befinden. Ein SMTP-Server lässt Sie Trap-Meldungen von der Kundendomäne an ein Postfach zum Remote-Support weiterleiten.

So fügen Sie SMTP-Server hinzu:

1. Wählen Sie **Clusterverwaltung → Überwachungskonfiguration → E-Mail-Konfiguration** aus.
   Die Seite **E-Mail-Konfiguration** wird angezeigt. Standardmäßig wird die Registerkarte **Allgemein** ausgewählt.
2. Klicken Sie auf **SMTP-Server hinzufügen**.
   Die Seite **SMTP-Server hinzufügen** wird angezeigt.
3. Geben Sie in **SMTP-Server** die IP-Adresse oder den Namen des E-Mail-Servers ein.
4. Geben Sie in **Description (Beschreibung)** eine Beschreibung des Servers ein.
5. Wählen Sie **SMTP-Server erfordert Authentifizierung** aus, um alle E-Mails auf dem SMTP-Server durch die Eingabe von Benutzername und Kennwort in die Felder **Benutzername** und **Kennwort** zu authentifizieren.
6. Klicken Sie auf **Änderungen speichern**.

Modifizieren einer SMTP-Server-Konfiguration

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Monitoring Configuration (Überwachungskonfiguration) → Email Configuration (E-Mail-Konfiguration).**
   Die Seite **Email Configuration (E-Mail-Konfiguration)** zeigt eine Liste der vorhandenen SMTP-Server an.
2. Klicken Sie in der Liste der vorhandenen SMTP-Server unter **SMTP server** auf den gewünschten Server.
   Die Seite **Edit SMTP server (SMTP-Server bearbeiten)** wird angezeigt.
3. Geben Sie in **SMTP server** die aktualisierte IP-Adresse oder den Namen des E-Mail-Servers ein.
4. Geben Sie in **Description (Beschreibung)** die aktualisierte Beschreibung des Servers ein.
5. Wählen Sie **The SMTP server requires authentication (SMTP-Server erfordert Authentifizierung)** aus, um alle E-Mails auf dem SMTP-Server durch Benutzername und Kennwort zu authentifizieren, einzugeben in die Felder **User name (Benutzername)** und **Password (Kennwort)**.
6. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Löschen eines E-Mail-Absenders

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Monitoring Configuration (Überwachungskonfiguration) → Email Configuration (E-Mail-Konfiguration).**
   Die Seite **Email Configuration (E-Mail-Konfiguration)** zeigt eine Liste der vorhandenen SMTP-Server an.
2. Wählen Sie aus der Liste der vorhandenen SMTP-Server einen oder mehrere SMTP-Server aus und klicken Sie auf **Delete SMTP Server(s) (SMTP-Server löschen)** .

Konfigurieren eines E-Mail-Absenders

Manche E-Mail-Systeme verhindern die Sendung von E-Mails, wenn der Sender nicht zu einer bestimmten Domäne gehört. Sie können das System so konfigurieren, dass alle E-Mails von einem bestimmten Benutzer in der erforderlichen Domäne gesendet werden.

Um die E-Mail-Adresse zu bestimmen, die beim Absenden von E-Mails im Feld **From (Von)** angezeigt wird, geben Sie in **Send E-mails From (E-Mails senden von)** eine E-Mail-Adresse ein, die zur erforderlichen Domäne gehört.

Konfigurieren von erweiterten Optionen

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Monitoring Configuration (Überwachungskonfiguration) → Email Configuration (E-Mail-Konfiguration).**

Die Seite **Email Configuration (E-Mail-Konfiguration)** wird angezeigt. Standardmäßig ist die Registerkarte **General (Allgemein)** ausgewählt.

2. Klicken Sie auf die Registerkarte **Advanced (Erweitert)**.

   Die Seite **Add SMTP server (SMTP-Server hinzufügen)** wird angezeigt.

3. Geben Sie in **Maximum mail size (kB) (Maximale Mailgröße, kB)** die Maximalgröße jeder E-Mail ein.
4. Geben Sie in **Messages sent in intervals of (seconds) (Nachrichten versenden im Intervall von (Sekunden))** die maximale Zeit ein, die eine Warnmeldung warten kann, bevor sie gesendet wird.
5. Klicken Sie auf **Save Changes (Änderungen speichern)**.

Konfigurieren von SNMP

Dell Fluid File System unterstützt das Simple Network Management Protocol (SNMP), ein häufig verwendetes Netzwerkverwaltungsprotokoll, das SNMP-kompatible Verwaltungsfunktionen wie z. B. Geräteermittlung, Überwachung und Ereigniserzeugung ermöglicht.

Mit der SNMP-Seite können Sie SNMP-kompatible Verwaltungsfunktionen konfigurieren.

So konfigurieren Sie SNMP-Eigenschaften:

1. Wählen Sie **Clusterverwaltung** → **Überwachungskonfiguration** → **SNMP-Konfiguration** aus.

   Die Seite **SNMP-Konfiguration** wird angezeigt. Standardmäßig ist die Registerkarte **Eigenschaften** ausgewählt.

2. Geben Sie in **Systemkontakt** einen Namen für die erforderliche Kontaktperson ein.
3. Geben Sie in **Systemstandort** eine Beschreibung zum Standort des Systems ein.
4. Geben Sie in **Lesecommunity** die SNMP-Community für Geräte ein, die SNMP-Variablen aus dem Dell Fluid File System lesen oder verwenden Sie den Standardwert.
5. Geben Sie in **Trap-Empfänger** die IP-Adresse oder den Hostnamen des Netzwerkverwaltungsservers oder eines anderen Hosts ein, der vom Dell Fluid File System generierte SNMP-Traps empfängt.
6. Zum Hinzufügen von zusätzlichen Trap-Empfängern klicken Sie auf **Hinzufügen.**

   Der Trap-Empfänger wird zur Liste hinzugefügt.

7. Geben Sie die IP-Adresse oder den Hostnamen des Netzwerkverwaltungsservers ein.
8. Um einen Trap-Empfänger aus der Liste zu entfernen, wählen Sie den gewünschten Trap-Empfänger aus und klicken Sie auf **Löschen**.

   Der Trap-Empfänger wird aus der Liste entfernt.

9. Wählen Sie die Registerkarte **Filter** und wählen Sie den Mindest-Trap-Schweregrad aus, der für jede Trap-Kategorie versendet wird.

   ANMERKUNG: Standardmäßig werden alle Traps für alle Kategorien gesendet.

10. Klicken Sie auf **Änderungen speichern**.

6

Fehlerbehebung

Fehlerbehebung – CIFS-Fehler

Falsch konfigurierte Antivirus-Host-Einstellungen führen zur Zugriffsverweigerung auf CIFS-Dateien

Beschreibung	Die Dell NAS-Cluster-Lösung unterstützt Antivirusprüfungen auf Grundlage einer jeden CIFS-Freigabe. Wenn eine Datei auf einer Freigabe von einer Client-Anwendung geöffnet wird, sendet die NAS-Cluster-Lösung die Datei zur Prüfung an einen Antivirus-Host. Wenn kein Antivirus-Host verfügbar ist, wird der Zugriff auf die Datei und die gesamte Freigabe verhindert.
Ursache	Da keine Antivirus-Hosts auf der NAS-Cluster-Lösung verfügbar sind, können Dateien auf einer für Antivirus aktivierte CIFS-Freigabe nicht geöffnet werden.
Problemumgehung	Stellen Sie sicher, dass dieses Problem nur auf für Antivirus aktivierten Freigaben auftritt, nicht aber, wenn Clients auf andere Freigaben zugreifen. Überprüfen Sie den Status der Antivirus-Hosts sowie den Netzwerkpfad zwischen der NAS-Cluster-Lösung und den Antivirus-Hosts.

CIFS-Zugriff verweigert

Beschreibung	Der CIFS-Zugriff auf eine Datei oder einen Ordner wurde verweigert.
Ursache	Ein Client ohne ausreichende Berechtigungen führt einen Vorgang in einer Datei oder einem Ordner aus.
Problemumgehung	Überprüfen Sie die Berechtigungen in einer Datei/einem Ordner, und legen Sie die erforderlichen Berechtigungen fest.

Beschädigung der CIFS-Zugangskontrollliste (ACL)

Beschreibung	Die CIFS-Zugangskontrollliste (ACL) ist beschädigt.
Ursache	• Die Zugriffskontrolllisten (ACLs) wurden versehentlich durch einen Benutzer oder ein Skript geändert. • Die Zugriffskontrollliste wurde beschädigt, nachdem eine Antivirus-Anwendung die

	entsprechenden Dateien in der Quarantäne abgelegt hat. • Die Zugriffskontrollliste wurde durch eine Backup-Anwendung nach einer Datenwiederherstellung aufgrund von Kompatibilitätsproblemen beschädigt. • Die Zugriffskontrollliste wurde nach der Migration von Daten von einem anderen Speicherplatz mithilfe einer Drittanbieteranwendung, z. B. *RoboCopy*, beschädigt.
Problemumgehung	Überprüfen Sie die aktuellen ACL-Einstellungen im Windows-Client. Definieren Sie die ACLs für die Dateien neu, indem Sie einen Windows-Client so verwenden wie ursprünglich definiert. Vergewissern Sie sich, dass Sie die ACLs als Besitzer der Dateien, Verzeichnisse und Freigaben eingestellt haben. Falls Sie Ihre ACLs nicht neu definieren können, da Sie derzeit nicht über Berechtigungen dazu verfügen, führen Sie die folgenden Schritte durch: 1. Stellen Sie die Dateien aus Snapshots oder einem Backup wieder her. 2. Sollten Sie die Daten mithilfe der **RoboCopy-**Anwendung aus verschiedenen Speicherorte migriert haben, ist die Wahrscheinlichkeit recht groß, dass Sie die ACLs einfach durch das Kopieren der Metadaten für die ACLs wiederherstellen können, anstatt die gesamten Daten neu kopieren zu müssen. 3. Sollten die gesamten Zugriffskontrolllisten für das Dateisystem beschädigt sein, können Sie alle Daten über den NAS-Replikationspartner wiederherstellen.

Uhrzeitversatz auf dem CIFS-Client

Beschreibung	Es liegt ein Uhrzeitversatz auf dem CIFS-Client vor.
Ursache	Die Uhrzeit auf dem Client muss mit der Uhrzeit auf dem Kerberos-Server (als dem Active Directory) übereinstimmen. Dabei ist eine Toleranz von 5 Minuten zulässig.
Problemumgehung	Konfigurieren Sie den Client so, dass die Uhrzeit mit dem Active Directory (als NTP-Server) synchronisiert wird. Auf diese Weise vermeiden Sie Fehler, die durch einen Uhrzeitversatz auftreten.

CIFS-Client-Verbindung beim Datei-Lesevorgang unterbrochen

Beschreibung	Die CIFS-Client-Verbindung wurde beim Datei-Lesevorgang unterbrochen.
Ursache	Während eines Controller-Failovers ist eine außergewöhnlich hohe CIFS-Arbeitsauslastung aufgetreten.

Problemumgehung	Stellen Sie die Verbindungen für die Clients neu her, und öffnen Sie die Datei erneut.

Allgemeiner Verlust der CIFS-Client-Verbindung

Beschreibung	Es ist ein Verlust der CIFS-Client-Verbindung aufgetreten.
Ursache	Wenn das System einen allgemeinen Fehler beim CIFS-Dienst erkannt hat, wird es automatisch wiederhergestellt, der Fehler führt jedoch dazu, dass die Verbindung zu allen Benutzern getrennt und das oben beschriebene Ereignis ausgelöst wird.
Problemumgehung	Sollte dieses Problem wiederholt auftreten, wenden Sie sich bitte an Dell.

Fehler beim Anmelden am CIFS-Client

Beschreibung	Beim Anmelden am CIFS-Client ist ein Fehler aufgetreten.
Ursache	Der Benutzer hat nach dem Verbindungsaufbau das falsche Kennwort eingegeben.
Problemumgehung	Interaktive Benutzer können die Anmeldung mit dem korrekten Kennwort erneut versuchen. Anwendungen und Server brauchen eventuell besondere Aufmerksamkeit, da Benutzer/Kennwort, welche normalerweise in einem Script oder einer Konfigurationsdatei festgelegt sind, wahrscheinlich abgelaufen sind.

CIFS-Verbindungsfehler

Beschreibung	Der Zugriff auf die CIFS-Client-Freigabe wurde verweigert.
Ursache	Der Benutzer ist dem Active Directory-Server nicht bekannt und das NAS-System hat diesen Benutzer einem Gast zugeordnet. Wenn die Freigabe keinen Gastzugriff zulässt, so erhält der Benutzer eine Warnmeldung des Typs Zugriff verweigert.
Problemumgehung	Stellen Sie sicher, dass der Benutzer in dem Active Directory-Server gelistet ist, den der NAS verwendet. Alternativ können Sie auch die Zugriffbegrenzung für Gäste auf der Freigabe entfernen. Wenn der Benutzer dann auf die Freigabe als Gast zugreifen kann, sind die neu erstellten Dateien im Besitz von niemandem/Gast.

Löschen beim Schließen von CIFS-Datei verweigert

Beschreibung	Die Dateien sollen gelöscht werden, während sie noch verwendet werden.
Ursache	Wenn eine Datei gelöscht wird, während sie geöffnet ist, so wird sie zum Löschen markiert und wird erst dann gelöscht, wenn sie geschlossen wird. Bis dahin erscheint

	die Datei an ihrem ursprünglichen Speicherplatz, aber das System verweigert jeden Versuch, sie zu öffnen.
Problemumgehung	Benachrichtigen Sie den Benutzer, der versucht hat, die Datei zu öffnen, darüber, dass die Datei gelöscht wurde.

Zugriff auf CIFS-Datei verweigert

Beschreibung	Der Zugriff auf die CIFS-Datei wurde verweigert.
Ursache	Der Client verfügt nicht über ausreichende Berechtigungen, um den gewünschten Vorgang für die Datei auszuführen.
Problemumgehung	Dies ist ein informatives Ereignis. Der Benutzer kann anfragen, die Datei-ACL zu modifizieren, um den Zugriff zu gestatten.

Konflikt bei der Freigabe der CIFS-Datei

Beschreibung	Bei der Freigabe der CIFS-Datei ist ein Konflikt aufgetreten.
Ursache	Wenn eine Datei über das CIFS-Protokoll geöffnet wird, gibt die öffnende Anwendung den Freigabemodus weiter, der verwendet werden muss, während diese Datei geöffnet ist. Dieser Freigabemodus beschreibt, welche anderen Benutzeraktivitäten in Bezug auf diese – geöffnete – Datei zulässig sind. Diese Definition wird durch die Anwendung versendet; der Benutzer kann diese Definition weder steuern noch konfigurieren. Nachdem diese Freigabedefinition verletzt wird, erhält der Benutzer einen Zugriffsverweigerungsfehler und dieses Ereignis wird ausgegeben.
Problemumgehung	Hierbei handelt es sich um ein rein informatives Ereignis. Der Administrator kann den blockierenden Benutzer kontaktieren und ihn auffordern, die Anwendung zu schließen, die sich auf diese Datei bezieht. Es ist möglich, dass die Anwendung, welche die Datei geöffnet hat, nicht korrekt heruntergefahren ist. Es wird empfohlen, den Client wenn möglich neu zu starten.

CIFS-Gastkonto ungültig

Beschreibung	CIFS-Dienst konnte nicht gestartet werden.
Ursache	Für die CIFS-Funktion wird ein gültiges CIFS-Gastkonto benötigt.
Problemumgehung	Konfigurieren Sie das Gastkonto des Systems mit einem gültigen Konto.

CIFS-Arretierinkonsistenz

Beschreibung	Der CIFS-Dienst wurde aufgrund von CIFS-Arretierfehlern unterbrochen.
Ursache	Arretierszenarien für den CIFS-Client.
Problemumgehung	Das System führt automatisch eine Selbstwiederherstellung durch und gibt nach der Wiederherstellung den oben genannten Fehler aus.

Maximale Anzahl der CIFS-Verbindungen erreicht

Beschreibung	Die maximale Anzahl an CIFS-Verbindungen pro NAS-Controller ist erreicht.
Ursache	Jedes NX3600-Gerät ist auf 200 gleichzeitige CIFS-Verbindungen beschränkt und jedes NX3610 und FS8600 auf 1500 Verbindungen. • Das System befindet sich in einem optimalen Status und die Anzahl der CIFS-Clients, die auf einen der Controller zugreifen, erreicht die Höchstgrenze. In solch einem Szenario sollten Sie erwägen, ein weiteres NAS-Gerät hinzuzufügen. • Das System befindet sich in einem optimalen Status, aber die Clients sind höchst ungleichmäßig zwischen den NAS-Controllern verteilt. Gleichen Sie in diesem Fall die Client-Verteilung mithilfe des NAS-Managers neu aus. • Das System befindet sich im heruntergestuften Modus (einer oder mehrere NAS-Controller sind aus) und die CIFS-Clients bleiben auf den verbleibenden Controllern zurück. Warten Sie in diesem Fall darauf, dass das System wieder in den optimalen Status zurückkehrt oder senken Sie die Anzahl der CIFS-Clients im System.
Problemumgehung	Wenn sich beide NAS-Controller in einem optimalen Modus befinden, werden die vorhandenen Verbindungen auf die beiden Controller aufgeteilt.

CIFS-Freigabe nicht vorhanden

Beschreibung	Der Client versucht, eine Verbindung mit einer nicht vorhandenen Freigabe aufzubauen.
Ursache	• Rechtschreibfehler auf der Client-Seite. • Zugriff auf den falschen Server.
Problemumgehung	Listen Sie die verfügbaren NAS-Freigaben auf und stellen Sie sicher, dass alle Freigaben angezeigt und keine nicht geplanten Veränderungen vorgenommen werden.

Stellen Sie sicher, dass Sie über einen Windows-Client Zugang zu der Freigabe haben, bei der die Probleme auftreten:

1. Klicken Sie auf **Ausführen**.
2. Geben Sie die Zugriffs-VIP des Clients und den Freigabennamen ein: **\\<Client_VIP>\<CIFS_share_name>**

CIFS-Pfadfreigabe nicht gefunden

Beschreibung	Der Client hat auf eine Freigabe zugegriffen, die sich auf ein nicht vorhandenes Verzeichnis auf dem NAS-Container bezieht.
Ursache	• Das NAS-System wird von einer Backup- oder einer Remote-Replikation wiederhergestellt. In der Wiederherstellungszeit ist die Verzeichnisstruktur nicht komplett und einige Verzeichnisse sind eventuell nicht vorhanden. Leiten Sie den Status weiter und warten Sie, bis der Wiederherstellungsprozess abgeschlossen ist. • Ein Client mit einer Berechtigung löscht oder ändert ein Verzeichnis, das durch einen anderen Client gemountet wurde. Wenn mehrere Benutzer auf den gleichen Datensatz zugreifen, wird empfohlen, ein strenges Berechtigungssystem anzuwenden, um derartige Konflikte zu vermeiden.
Problemumgehung	Listen Sie alle im NAS verfügbaren Freigaben auf und identifizieren Sie die problematische Freigabe. Sie muss einen Hinweis darauf enthalten, dass auf sie nicht zugegriffen werden kann. 1. Stellen Sie den Pfad, auf dem die Probleme auftreten, aus einem Backup wieder her. 2. Erstellen Sie die fehlenden Verzeichnisse manuell. Richten Sie Berechtigungen zur Zugriffskontrolle je nach Bedarf ein. 3. Entfernen Sie die Freigabe, und nehmen Sie die Kommunikation mit dem Client auf.

CIFS-Schreibvorgang auf schreibgeschütztem Volume

Beschreibung	Der Client versucht, eine Datei auf einem schreibgeschützten Volume zu ändern.
Ursache	Ein NAS-Volume wird schreibgeschützt gesetzt, wenn es das Ziel einer Replikation ist.

Im Folgenden werden die häufigsten Gründe für dieses Ereignis genannt:

- Der Benutzer wollte auf das System zu Lesezwecken zugreifen, er hat dabei jedoch versehentlich versucht, eine Datei zu ändern.
- Der Benutzer greift aufgrund ähnlicher Namen bzw. IP-Adressen auf das falsche System zu.
- Der Benutzer greift auf einen NAS-Container zu, der ohne das Wissen des Benutzers in ein Replikationsziel umgewandelt wurde.

Problemumgehung

Um auf dieses Volume zu schreiben, muss zuerst die Replikation getrennt werden. Leiten Sie den Benutzer zum korrekten Speicherort.

Fehlerbehebung – NFS-Fehler

NFS-Export kann nicht geladen werden

Beschreibung

Beim Versuch, einen NFS-Export zu laden, kann beim Aufrufen des Mount-Befehls einer der folgenden Fehler auftreten:

- Fehlende Berechtigung.
- Das Gerät antwortet aufgrund eines Portmapper-, RPC-Zeitüberschreitungs- oder E/A-Fehlers nicht.
- Das Gerät antwortet aufgrund eines nicht registrierten Programms nicht.
- Zugriff verweigert.
- Kein Verzeichnis.

Ursache

- Der Client verbindet sich über NFS/UDP und eine Firewall verhindert den Zugriff.
- Der Client ist nicht in der Exportliste enthalten, das Gerät konnte das Client-System über NIS nicht erkennen oder das Gerät akzeptiert die von Ihnen bereitgestellte Identität nicht.
- Die NAS-Cluster-Lösung ist ausgeschaltet oder es bestehen interne Dateisystemprobleme.
- Der Mount-Befehl ist bis zum Portmapper vorgedrungen, der NFS-Mount-Daemon **rpc.mountd** war jedoch nicht registriert.
- Die IP-Adresse des Client-Systems, der IP-Bereich, der Domänenname oder die Netgroup sind nicht in der Exportliste für das Volume enthalten, auf das der Mount-Vorgang vom NAS-Gerät aus erfolgen soll.
- Entweder der Remote-Pfad oder der lokale Pfad ist kein Verzeichnis.
- Der Client verfügt nicht über Stammbefugnis oder ist kein Mitglied der Systemgruppe. NFS-Mount- und Unmount-Vorgänge sind nur für Stammbenutzer und Mitglieder der Systemgruppe zulässig.

Problemumgehung	Wenn das Problem auf NFS/UDP und Firewall beruht, überprüfen Sie, ob der Client mithilfe von UDP mountet (dies ist normalerweise die Standardeinstellung) und es eine Firewall in dem Pfad gibt. Wenn eine Firewall vorhanden ist, fügen Sie der Firewall eine geeignete Ausnahme hinzu. Wenn das Problem aus fehlenden Berechtigungen resultiert: • Überprüfen Sie, ob der von Ihnen genannte Pfad korrekt ist. • Stellen Sie sicher, dass der Mount-Vorgang als Root durchgeführt wird. • Stellen Sie sicher, dass die IP-Adresse des Systems, der IP-Bereich, der Domänenname oder die Netgroup in der Export-Liste enthalten sind. Das Gerät reagiert nicht aufgrund eines Portmapper-Fehlers: • Überprüfen Sie den Status der NAS-Cluster-Lösung. • Überprüfen Sie die Netzwerkverbindung, indem Sie versuchen, den NFS-Mount-Vorgang von einem anderen System aus zu starten. • Überprüfen Sie, ob bei anderen Benutzern ähnliche Probleme auftreten. Wenn das Gerät aufgrund eines nicht registrierten Programms nicht reagiert, überprüfen Sie, ob der Portmapper auf Ihrem Client betriebsbereit ist. Der Fehler ist aufgrund nicht erteilter Zugriffsberechtigungen aufgetreten: • Rufen Sie über den folgenden Befehl eine Liste der durch das Gerät exportierten Dateisysteme ab: `showmount –e <FluidFS hostname>` • Stellen Sie sicher, dass der Systemname oder der Name der Netgroup nicht in der Benutzerliste für das Dateisystem enthalten sind. • Verwenden Sie die Benutzerschnittstelle der NAS-Cluster-Lösung, um die mit dem NFS in Verbindung stehenden Dateisysteme zu überprüfen. Wenn das Verzeichnis die Ursache des Problems ist, überprüfen Sie die Syntax in Ihrem Befehl und versuchen Sie, den Mount-Befehl in beiden Verzeichnissen auszuführen.

NFS-Export nicht vorhanden

Beschreibung	Versuch, ein nicht vorhandenen Export zu laden.
Ursache	Dieser Fehler wird häufig durch Rechtschreibfehler auf dem Client-System hervorgerufen oder wenn auf den falschen Server zugegriffen wird.

Problemumgehung	1. Überprüfen Sie die verfügbaren Exporte auf dem NAS, und stellen Sie sicher, dass alle benötigten Exporte vorhanden sind. 2. Stellen Sie auf einem Client, auf dem Probleme aufgetreten sind, sicher, dass der entsprechende Export auf diesem Client verfügbar ist: 3. `% showmount -e <Servername/IP-Adresse>` 4. `Export list for (Exportliste für) <Servername/IP-Adresse>:` 5. `/abc 10.10.10.0` 6. `/xyz 10.10.10.0` 7. Wenn der Export verfügbar ist, überprüfen Sie die Schreibweise des Exportnamens im entsprechenden Mount-Befehl auf dem Client. Es wird empfohlen, den Exportnamen aus der Ausgabe showmount in den Mount-Befehl zu kopieren.

Zugriff auf NFS-Datei verweigert

Beschreibung	Dieses Ereignis wird ausgegeben, wenn ein NFS-Benutzer nicht über ausreichende Berechtigungen für eine Datei in einem NAS-Container verfügt.
Ursache	Das Dateieigentumsrecht lautet UID/UNIX, und der Benutzer ist nicht berechtigt, auf die Datei zuzugreifen, oder das Dateieigentumsrecht lautet SID/ACL, und die Berechtigung gewährt nach der Umwandlung in UID/UNIX keinen Zugriff auf die Datei.
Problemumgehung	Bei nativem Zugriff (wenn der CIFS-Benutzer auf die SID/ACL-Datei oder der NFS-Benutzer auf die UID/UNIX-Datei zugreift) lautet die Standardeinstellung, dass die fehlende Berechtigung verstanden wird. Bei einem nicht-nativen Zugriff kommen die Umwandlungsregeln zum Einsatz, und es wird empfohlen, Kontakt mit dem technischen Support von Dell aufzunehmen.

Unsicherer NFS-Zugriff für sicheren Export

Beschreibung	Der Benutzer hat versucht, über einen unsicheren Anschluss auf einen sicheren Export zuzugreifen.
Ursache	Eine sichere Exportanforderung bedeutet, dass es sich bei den zugreifenden Clients um einen bekannten Port handeln muss (unterhalb von 1024); dies bedeutet in der Regel, dass es sich um einen Root (UID=0) auf dem Client handelt.
Problemumgehung	• Identifizieren Sie den entsprechenden Export, und stellen Sie sicher, dass dieser als sicher eingestellt ist (erfordert einen sicheren Client-Anschluss). • Wenn der Export dauerhaft sicher bleiben soll, finden Sie weitere Informationen in der

Dokumentation zum NFS-Client, um die Mount-Anfrage von einem bekannten Anschluss aus zu stellen (unterhalb von 1024).

- Wenn kein sicherer Export benötigt wird (wenn das Netzwerk beispielsweise nicht öffentlich ist), müssen Sie sicherstellen, dass der Export unsicher ist; versuchen Sie dann erneut, auf den Export zuzugreifen.

Fehler beim Ausführen des Mount-Befehls für NFS aufgrund von Exportoptionen

Beschreibung	Dieses Ereignis wird ausgegeben, wenn der Mount-Befehl für NFS aufgrund der eingestellten Exportoptionen fehlschlägt.
Ursache	Die Exportliste filtert den Client-Zugriff nach IP-Adresse, Netzwerk oder Netgroup und zeigt den zugreifenden Client auf dem Bildschirm an.
Problemumgehung	1. Überprüfen Sie die entsprechenden Einzelheiten des Exports. Notieren Sie alle vorhanden Optionen, damit Sie darauf zurückgreifen können. 2. Heben Sie die Beschränkungen des Exports in Bezug auf die IP-Adresse oder den Client auf, und versuchen Sie erneut, den Mount-Vorgang durchzuführen. 3. Wenn das Mounten erfolgreich ist, überprüfen Sie, ob die IP oder die Domäne explizit angegeben ist und das sie Teil des definierten Netzwerks oder der Netzwerkgruppen ist. Beachten Sie Sonderszenarien, in denen die Netzmaske nicht intuitiv ist, zum Beispiel ist 192.175.255.254 Teil von192.168.0.0/12, aber nicht von 192.168.0.0/16. 4. Nachdem der Ladevorgang erfolgreich abgeschlossen wurde, passen Sie die ursprünglichen Optionen entsprechend an.

Fehler beim Mount-Vorgang für NFS aufgrund von Netgroup-Fehler

Beschreibung	Dieses Ereignis wird ausgegeben, wenn beim Laden des NFS-Exports durch den Clients ein Fehler auftritt, da die benötigten Netgroup-Daten nicht abgerufen werden konnten.
Ursache	Dieser Fehler entsteht in der Regel durch einen Kommunikationsfehler zwischen dem NAS-System und dem NIS/LDAP-Server. Dies kann das Ergebnis eines Netzwerkproblems, einer Überladung des Verzeichnisservers oder einer Fehlfunktion der Software sein.
Problemumgehung	Wiederholen Sie den unten genannten Prozess für jeden konfigurierten NIS-Server und verwenden Sie dabei jeweils nur einen NIS. Beginnen Sie mit dem NIS-Server, auf dem die Probleme aufgetreten sind:

1. Überprüfen Sie die NIS/LDAP-Serverprotokolle, und ermitteln Sie, ob der Grund für den Fehler in den Protokollen enthalten ist.
2. Schließen Sie den Netzwerk-Test ab, indem Sie das NAS von einem Client auf dem gleichen Subnetz wie der NIS/LDAP-Server aus anpingen.
3. Pingen Sie den NIS/LDAP-Server von einem Client auf dem gleichen Subnetz wie das NAS aus an.
4. Wenn der Paketverlust auf einem der oben genannten Entitäten aufgetreten ist, müssen Sie die Netzwerkprobleme in der Umgebung lösen.
5. Verwenden Sie einen Linux-Client, der sich im selben Subnetz wie der NAS befindet und zur Verwendung desselben Verzeichnisservers konfiguriert ist, und fragen Sie die Netgroup-Einzelheiten vom NIS/LDAP-Server mithilfe der entsprechenden Befehle ab. Vergewissern Sie sich, dass Sie die Antwort zeitnah (nach bis zu 3 Sekunden) erhalten.

Sie können das Problem übergangsweise beheben, indem Sie die Netgroup-Beschränkung auf dem Export entfernen und/oder einen alternativen Verzeichnisserver definieren.

Identifizieren Sie den entsprechenden Export und seine definierten Optionen, wobei Sie sich auf die Netgroup-Definition konzentrieren. Dokumentieren Sie die verwendete Netgroup, um sie wiederherzustellen, sobald das Problem behoben ist und heben Sie die Netgroup-Beschränkungen auf.

NFS-Ladepfad nicht vorhanden

Beschreibung	Der Client versucht, einen Ladepfad zu mounten, der in keinem NAS-Container vorhanden ist.
Ursache	Dieser Fehler tritt in der Regel bei den folgenden Szenarien auf: • Beim Zugriff auf ein System, das von einer Backup- oder Remote-Replikation wiederhergestellt wird. Die komplette Verzeichnisstruktur ist erst dann verfügbar, wenn die Wiederherstellung abgeschlossen ist. • Wenn ein Client mit einer Berechtigung für den Zugriff auf ein höheres Verzeichnis auf dem gleichen Pfad ein Verzeichnis löscht oder ändert, das durch einen anderen Client gemountet wurde. • Wenn mehrere Benutzer auf den gleichen Datensatz zugreifen, wird empfohlen, ein strenges Berechtigungssystem anzuwenden, um derartige Konflikte zu vermeiden.
Problemumgehung	1. Wenn das NAS-System wiederhergestellt wird, leiten Sie den aktuellen Status an den Client weiter, und weisen Sie ihn an, zu warten, bis der Vorgang abgeschlossen ist. 2. Im anderen Fall gibt es drei Optionen:

- Stellen Sie den Pfad, auf dem die Probleme auftreten, aus einem Backup wieder her.
- Erstellen Sie manuell die fehlenden Verzeichnisse, um das Laden zu ermöglichen. Clients erhalten Fehlermeldungen, wenn sie versuchen, auf vorhandene Daten in einem gelöschten Pfad zuzugreifen.
- Entfernen Sie den Export und leiten Sie dies an den Client weiter.

3. Listen Sie alle im NAS verfügbaren Exporte auf und identifizieren Sie den problematischen Export. Er muss einen Hinweis darauf enthalten, dass auf ihn nicht zugegriffen werden kann.
4. Löschen Sie den Export oder erstellen Sie das Verzeichnis, auf das sich der Export bezieht.

Beschränkter Vorgang für den NFS-Eigentümer

Beschreibung	Der NFS-Client ist nicht berechtigt, die angeforderte Aktion in der angegebenen Datei durchzuführen.
Ursache	Der NFS-Benutzer hat versucht, einen `chmod`- oder `chgrp`-Vorgang auszuführen, obwohl er nicht der Eigentümer der Datei ist.
Problemumgehung	Dies ist ein kleineres Problem auf Benutzerebene. Häufige Ereignisse dieser Art können auf einen bösartigen Versuch zum Zugriff auf eingeschränkte Daten hinweisen.

NFS-Schreibvorgang auf schreibgeschütztem Export

Beschreibung	Der NFS-Client versucht, Änderungen auf einem schreibgeschützten Export vorzunehmen.
Ursache	Ein NFS-Export kann als ein schreibgeschützter Export definiert werden. Ein Client, der auf einen schreibgeschützten Export zugreift, kann weder Schreibvorgänge ausführen noch enthaltene Dateien modifizieren.
Problemumgehung	Für dieses Ereignis ist kein administrativer Benutzereingriff erforderlich.

NFS-Schreibvorgang auf schreibgeschütztem Volume

Beschreibung	Ein NFS-Benutzer versucht, eine Datei auf einem schreibgeschütztem Volume zu ändern.
Ursache	Ein NAS-Volume wird schreibgeschützt, wenn es als Ziel in einer Replikationsbeziehung festgelegt ist. Das Modifizieren eines schreibgeschützten Volumes ist so lange nicht zulässig, bis die Replikationsbeziehung entfernt wird und das Volume in einen einfachen, normalen Status zurückkehrt.

Problemumgehung	Informieren Sie den/die Benutzer zum Status des NAS-Volumes.

NFS-Schreibvorgang auf Snapshot

Beschreibung	Ein NFS-Benutzer versucht, eine Datei auf einem Snapshot zu ändern.
Ursache	NAS-Volume-Snapshots können per Design nicht geändert werden.
Problemumgehung	Snapshot-Daten können nicht modifiziert werden. Ein Snapshot ist die genaue Darstellung der NAS-Volume-Daten zum Zeitpunkt ihrer Erstellung.

NFS-Zugriff auf eine Datei oder ein Verzeichnis verweigert

Beschreibung	Der Benutzer kann nicht auf die NFS-Datei oder das Verzeichnis zugreifen, obwohl der Benutzer zu der Gruppe gehört, die im Besitz des NFS-Objekts ist und die Gruppenmitglieder berechtigt sind, diesen Vorgang auszuführen.
Ursache	NFS-Server (Versionen 2 und 3) verwenden das Remote Procedure Call (RPC)-Protokoll zur Authentifizierung von NFS-Clients. Die meisten RPC-Clients verfügen absichtlich über eine Beschränkung von bis zu 16 Gruppen, die an den NFS-Server weitergegeben werden. Wenn ein Benutzer zu mehr als 16 UNIX-Gruppen gehört, wie von manchen UNIX-Derivaten unterstützt, werden manche der Gruppen nicht weitergegeben und nicht vom NFS-Server überprüft und darum wird der Benutzerzugriff eventuell verweigert.
Problemumgehung	Eine Möglichkeit, dieses Problem zu überprüfen, ist, den Befehl `newgrp` (Neue Gruppe) zu verwenden, um die primäre Gruppe des Benutzers vorübergehend zu ändern und damit sicherzustellen, dass sie an den Server weitergeleitet wird. Bei dieser einfachen Ausweichmaßnahme, die jedoch nicht immer umsetzbar ist, wird der Benutzer aus nicht benötigten Gruppen entfernt, so dass höchstens 16 Gruppen übrig bleiben.

Fehlerbehebung – Replikationsfehler

Fehler bei der Replikationskonfiguration

Beschreibung	Die Replikation zwischen den Quell- und Ziel-NAS-Volumes schlägt fehl, da die Topologien der Quell- und Zielsystemen nicht kompatibel sind.
Ursache	Die Quell- und Zielsysteme sind für Replikationszwecke nicht kompatibel.

Problemumgehung	Aktualisieren Sie die NAS-Cluster-Lösung, die jetzt ausgeschaltet ist. Überprüfen Sie, dass sowohl Quelle als auch Ziel die gleiche Anzahl an NAS-Controllern haben. **ANMERKUNG:** Sie können nicht zwischen einem NAS-Cluster mit vier Knoten und einem NAS-Cluster mit zwei Knoten replizieren.

Replikations-Zielcluster ausgelastet

Beschreibung	Die Replikation zwischen dem Quell-NAS-Volume und dem Ziel-NAS-Volume schlägt fehl, da das Zielcluster nicht verfügbar ist, um die erforderliche Replikation zu leisten.
Ursache	Die Replikationsaufgabe schlägt fehl, da das Zielcluster nicht verfügbar ist, um die erforderliche Replikation zu leisten.
Problemumgehung	Administratoren müssen den Replikationsstatus auf dem Zielsystem überprüfen.

Replikations-Ziel-Dateisystem ausgelastet

Beschreibung	Die Replikation zwischen dem Quell-NAS-Volume und dem Ziel-NAS-Volume schlägt fehl.
Ursache	Die Replikationsaufgabe schlägt fehl, da das Zielcluster derzeit nicht verfügbar ist, um die erforderliche Replikation zu leisten.
Problemumgehung	Die Replikation wird automatisch weitergeführt, wenn das Dateisystem einen Teil der Ressourcen freigibt. Administratoren müssen überprüfen, dass die Replikation automatisch nach einer bestimmten Frist weitergeht (eine Stunde).

Replikationsziel ist ausgefallen

Beschreibung	Die Replikation zwischen dem NAS-Quell-Volume und dem NAS-Ziel-Volume schlägt fehl.
Ursache	Die Replikationsaufgabe schlägt fehl, da das System des Ziel-NAS-Volumes ausgefallen ist.
Problemumgehung	Der Administrator muss mithilfe des Überwachungsabschnitts im NAS-Manager überprüfen, ob das Dateisystem heruntergefahren ist. Wenn das Dateisystem der NAS-Cluster-Lösung nicht antwortet, muss der Administrator das System auf dem Ziel-Cluster starten. Die Replikation wird automatisch fortgesetzt, wenn das Dateisystem gestartet ist.

Replikationsziel nicht optimal

Beschreibung	Die Replikation zwischen dem NAS-Quell-Volume und dem NAS-Ziel-Volume schlägt fehl, da der Betriebszustand des Ziel-NAS-Volumes nicht optimal ist.
Ursache	Die Replikation schlägt fehl, da das Dateisystem des Ziel-NAS-Volumes nicht optimal ist.
Problemumgehung	Die Administratoren müssen den Systemstatus des Zielsystems mithilfe des Überwachungsabschnitts im NAS-Manager überprüfen, um herauszufinden, warum das Dateisystem nicht optimal ist. Die Replikation geht automatisch weiter, nachdem das Dateisystem wiederhergestellt ist.

Replikationsziel-Volume ist damit beschäftigt, Speicherplatz zurückzufordern

Beschreibung	Die Replikation zwischen dem NAS-Quell-Volume und dem NAS-Ziel-Volume schlägt fehl, da das Ziel-NAS-Volume damit beschäftigt ist, freien Speicherplatz zu organisieren.
Ursache	Die Replikationsaufgabe schlägt fehl, da das Ziel-NAS-Volume damit beschäftigt ist, freien Speicherplatz zu organisieren.
Problemumgehung	Die Replikation wird automatisch fortgesetzt, wenn der Speicherplatz verfügbar wird. Die Administratoren müssen überprüfen, dass die Replikation automatisch nach einem bestimmten Zeitraum (einer Stunde) fortgesetzt wird.

Ziel-Volume für die Replikation nicht verbunden

Beschreibung	Die Replikation zwischen dem NAS-Quell-Volume und dem NAS-Ziel-Volume schlägt fehl, da das NAS-Ziel-Volume vom NAS-Quell-Volume getrennt ist.
Ursache	Die Replikationsaufgabe schlägt fehl, da das Ziel-NAS-Volume zuvor vom Quell-NAS-Volume getrennt wurde.
Problemumgehung	Der Administrator muss den Trennvorgang auf dem NAS-Quell-Volume durchführen. Bei Bedarf verbinden Sie beide NAS-Volumes in einer Replikationsbeziehung neu.

Verbindung zur Replikation getrennt

Beschreibung	Die Replikation zwischen dem NAS-Quell-Volume und dem NAS-Ziel-Volume schlägt fehl, da die Verbindung zwischen den Quell- und Zielsystemen verloren gegangen ist.
Ursache	Die Verbindung der Netzwerkinfrastruktur zwischen Quelle und Ziel ist verloren gegangen.
Problemumgehung	Der Administrator muss überprüfen, ob die Replikation automatisch wiederhergestellt wird. Wenn sie nicht

	automatisch wiederhergestellt wird, überprüfen Sie die Netzwerkkommunikation zwischen dem Quell- und dem Ziel-Cluster. Die Netzwerkkommunikation kann mithilfe eines Drittsystems, das sowohl Quell- als auch Ziel-Cluster anpingen kann, im selben Subnetz überprüft werden.

Inkompatible Replikationsversionen

Beschreibung	Die Replikation zwischen dem NAS-Quell-Volume und dem NAS-Ziel-Volume schlägt fehl, da die Systemversion des NAS-Quell-Clusters höher ist als die Systemversion des Ziel-Clusters.
Ursache	Die Replikationsaufgabe schlägt fehl, da die Systemversion des NAS-Quell-Clusters höher ist als die des Ziel-Clusters.
Problemumgehung	Administratoren müssen die Systemversion des Ziel-Clusters so aktualisieren, dass sie mit der Systemversion des Quell-Clusters übereinstimmt.

Interner Replikationsfehler

Beschreibung	Die Replikation zwischen den Quell- und den Ziel-NAS-Volumes schlägt aufgrund eines internen Fehlers fehl.
Problemumgehung	Wenden Sie sich zur Lösung dieses Problems an Dell.

Replikation der Jumbo-Frames blockiert

Beschreibung	Die Replikation zwischen dem NAS-Quell-Volume und dem NAS-Ziel-Volume schlägt fehl, da die Jumbo-Frames auf dem Netzwerk geblockt werden.
Ursache	Die Replikationsaufgabe schlägt fehl, da die Jumbo-Frames auf dem Netzwerk blockiert werden.
Problemumgehung	Der Administrator muss sicherstellen, dass in der Netzwerkkonfiguration zwischen dem Quell-Cluster und dem Ziel-Cluster die Weiterleitung von Jumbo-Frames über Switche oder Router aktiviert ist.

Replikationsziel verfügt nicht über ausreichend Speicherplatz

Beschreibung	Die Replikation zwischen dem NAS-Quell- und dem NAS-Ziel-Volume schlägt fehl, da nicht ausreichend Speicherplatz auf dem Ziel-NAS-Volume vorhanden ist.
Ursache	Die Replikationsaufgabe schlägt fehl, da nicht ausreichend Speicherplatz auf dem Ziel-NAS-Volume vorhanden ist.
Problemumgehung	Erweitern Sie den Speicherplatz auf dem Ziel-NAS-Volume.

Replikationsquelle ist ausgelastet

Beschreibung	Die Replikation zwischen dem NAS-Quell- und dem NAS-Ziel-Volume schlägt fehl, da das Dateisystem des Quell-NAS-Volumes damit beschäftigt ist, andere NAS-Volumes zu replizieren.
Ursache	Die Replikationsaufgabe schlägt fehl, da das Dateisystem des Quell-NAS-Volumes damit beschäftigt ist, andere NAS-Volumes zu replizieren.
Problemumgehung	Die Replikation wird automatisch weitergeführt, wenn das Dateisystem einen Teil der Ressourcen freigibt. Administratoren müssen überprüfen, dass die Replikation automatisch nach einer bestimmten Frist weitergeht (eine Stunde).

Replikationsquelle ist ausgefallen

Beschreibung	Die Replikation zwischen dem NAS-Quell- und dem NAS-Ziel-Volume schlägt fehl, da das Dateisystem des Ziel-NAS-Volumes ausgefallen ist.
Ursache	Das Dateisystem des Quell-NAS-Volumes ist ausgefallen.
Problemumgehung	Administratoren müssen überprüfen, ob die NAS-Cluster-Lösung im Quellsystem ausgeschaltet ist, indem sie den Überwachungsabschnitt des NAS-Managers überprüfen. Wenn die NAS-Cluster-Lösung ausgeschaltet ist, müssen die Administratoren das Dateisystem auf dem Quell-Cluster starten. Die Replikation wird automatisch fortgesetzt, wenn das Dateisystem startet.

Replikationsquelle nicht optimal

Beschreibung	Die Replikation zwischen den Quell- und den Ziel-NAS-Volumes schlägt fehl, da das Dateisystem des Quell-NAS-Volumes nicht optimal ist.
Ursache	Die Replikation schlägt fehl, da das Dateisystem der Quelle nicht optimal ist.
Problemumgehung	Der Administrator muss den Dateisystemstatus des Quellsystems mithilfe des Überwachungsbereichs des NAS Manager überprüfen, um nachvollziehen zu können, warum das Dateisystem nicht optimal ist.

Replikationsziel-Volume ist damit beschäftigt, Speicherplatz zurückzufordern

Beschreibung	Die Replikation zwischen dem NAS-Quell- und dem NAS-Ziel-Volume schlägt fehl, da das Quell-NAS-Volume damit beschäftigt ist, freien Speicherplatz zurückzufordern.
Ursache	Die Replikationsaufgabe schlägt fehl, da das Quell-NAS-Volume damit beschäftigt ist, Speicherplatz zurückzufordern.
Problemumgehung	Die Replikation wird automatisch fortgesetzt, wenn der Speicherplatz verfügbar wird. Die Administratoren müssen überprüfen, dass die Replikation automatisch nach einem bestimmten Zeitraum (einer Stunde) fortgesetzt wird.

Fehlerbehebung – Active Directory-Fehler

Gruppenkontingent für einen Active Directory-Benutzer funktioniert nicht

Beschreibung	Das Gruppenkontingent wird für eine Active Directory-Gruppe definiert, wenn ein Gruppenmitglied jedoch Speicherplatz verbraucht, steigt der tatsächliche Verbrauch der Gruppe nicht an, und die Gruppenbeschränkung wird nicht erzwungen.
Ursache	Die Kontingenterzwingung der NAS-Cluster-Lösung wird auf der Basis der UID und der GID der Datei (UNIX) oder der SID und der GSID der primären Gruppe des Benutzers (NTFS) durchgeführt, falls definiert. Bei Benutzern von Active Directory sind die Einstellungen der Primary Group (Primären Gruppe) nicht verbindlich und wenn sie nicht definiert sind, wird der verwendete Speicherplatz keiner Gruppe zugerechnet. Damit ein Gruppenkontingent für Active Directory-Benutzer gilt, muss deren primäre Gruppe zugewiesen sein.
Problemumgehung	So richten Sie die primäre Gruppe für einen Active Directory-Benutzer ein: 1. Öffnen Sie die Active Directory-Verwaltung. 2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer. 3. Klicken Sie auf die Registerkarte **Mitglied von**. Die benötigte Gruppe muss angezeigt werden. 4. Klicken Sie auf die Gruppe und anschließend auf die Schaltfläche **Primäre Gruppe festlegen**. Nun gelten die Kontingente für die Gruppe des Benutzers.

Active Directory-Authentifizierung

Beschreibung	Ein gültiger Active Directory-Benutzer konnte nicht authentifiziert werden.
Ursache	Mögliche Ursachen: • Der Benutzer versucht, sich über ein falsches Kennwort zu authentifizieren. • Der Benutzer ist in Active Directory gesperrt oder deaktiviert. • Die Active Directory-Domain-Controller sind offline oder nicht erreichbar. • Die Systemuhr und die Active Directory-Uhr sind nicht synchron.
Problemumgehung	1. Prüfen Sie das Systemereignisprotokoll der NAS-Cluster-Lösung im NAS-Manager auf Fehler. 2. Stellen Sie sicher, dass der Benutzer in Active Directory nicht deaktiviert oder gesperrt ist. 3. Stellen Sie sicher, dass die Domain-Controller im Netzwerk online und erreichbar sind. 4. Kerberos erfordert, dass die Client-/Server-Uhren synchronisiert sind. Vergewissern Sie sich, dass die Systemuhrzeit mit der Uhrzeit des Domänencontrollers synchron ist und konfigurieren Sie bei Bedarf die NTP-Einstellungen des Systems.

Beheben von Fehlern in der Active Directory-Konfiguration

Beschreibung	Es können keine Active Directory-Benutzer oder -Gruppen zu den CIFS-Freigaben hinzugefügt werden.
Ursache	Mögliche Ursachen: • Domain konnte mithilfe von FQDM nicht angepingt werden. • DNS ist möglicherweise nicht konfiguriert. • NTP ist möglicherweise nicht konfiguriert.
Problemumgehung	Gehen Sie wie folgt vor, wenn Sie das System für die Verbindung mit einer Active Directory-Domain konfigurieren: 1. Stellen Sie sicher, dass Sie FQDM und nicht den NETBIOS-Namen der Domain oder die IP-Adresse des Domain-Controllers verwenden. 2. Stellen Sie sicher, dass der Benutzer über die entsprechenden Berechtigungen verfügt, um Systeme zur Domain hinzuzufügen. 3. Verwenden Sie das richtige Kennwort. 4. Weitere Informationen finden Sie auf der Registerkarte **DNS Configuration (DNS-Konfiguration)**, und geben Sie die entsprechenden Daten ein.

5. Konfigurieren Sie die NTP-Daten, und stellen Sie sicher, dass die Systemzeit mit der Domain-Zeit übereinstimmt.
6. Wenn mehrere NAS-System verwendet werden, stellen Sie sicher, dass Sie verschiedene NETBIOS-Namen eingerichtet haben. Das System stellt sich automatisch auf den CIFS-Speicher als Standardnamen ein.
7. Stellen Sie sicher, dass Sie die Option **Authenticate users' identity via Active Directory and local users database (Benutzeridentität über Active Directory und lokale Benutzerdatenbank authentifizieren)** auswählen.

Fehlerbehebung – NAS-Dateizugriffs- und Berechtigungsfehler

Eigentumsrecht einer Datei oder eines Ordners kann nicht geändert werden

Beschreibung	Jede Datei im NAS-System gehört entweder einem UNIX- oder einem NTFS-Benutzer. Kann das Eigentumsrecht nicht geändert werden, so muss danach gehandelt werden, ob der Zugriff nativ oder nicht nativ ist.
Ursache	Der Benutzer ist nicht berechtigt, eine Änderung am Eigentumsrecht vorzunehmen.
Problemumgehung	Dieser Vorgang muss von einem autorisierten Benutzer ausgeführt werden.

NAS-Dateien können nicht geändert werden

Beschreibung	Eine Datei kann nicht durch einen Benutzer oder eine Anwendung geändert werden.
Ursache	• Der Client kann eine Datei aufgrund von unzureichenden Berechtigungen für diese Datei nicht ändern. • Das NAS-Volume hat die maximale Kapazität erreicht, und das Dateisystem verweigert alle Schreibanfragen, einschließlich Überschreibungen. • Das NAS-Volume ist ein Ziel in einer Replikationsmitgliedschaft und ist schreibgeschützt.
Problemumgehung	• Wenn das Problem nur bei einigen Dateien auftritt, handelt es sich um ein Berechtigungsproblem. Vergewissern Sie sich, dass das Benutzerkonto über Berechtigungen zum Modifizieren verfügt, oder verwenden Sie ein anderes Benutzerkonto. • Wenn sich das Problem auf ein bestimmtes NAS-Volume bezieht: a. Überprüfen Sie, ob ausreichend Speicherplatz auf dem NAS-Volume

verfügbar ist. Ist dies nicht der Fall, erweitern Sie den Speicherplatz.

b. Überprüfen Sie, ob es sich bei dem NAS-Volume, auf das Sie zugreifen, um ein Ziel für eine Replikation handelt.

Gemischte Dateieigentumsrechte nicht zulässig

Beschreibung	Dateieigentümer und Gruppeneigentümer müssen vom gleichen Identitätstyp sein (entweder UNIX oder NTFS). Es wurde ein Versuch entdeckt, verschiedene Identitätstypen einzustellen.
Ursache	Es ist nicht möglich, nur die Besitzer-ID in UID zu ändern, wenn das Eigentumsrecht SID/GSID lautet.
Problemumgehung	Legen Sie zum Ändern des Dateieigentumsrechts in ein Eigentumsrecht der Art UNIX gleichzeitig die UID und die GID fest.

Problematischer SMB-Zugriff über einen Linux-Client

Beschreibung	Ein Linux/UNIX-Client versucht, eine NAS-Cluster-Lösung mithilfe von SMB zu mounten (mit dem Befehl /etc/fstab oder direkt mit dem Befehl smbmount). Ein Linux/UNIX-Client versucht, mit dem Befehl smbclient auf das Dateisystem zuzugreifen, z. B. : `smbclient //<nas>/<share> -U user %password -c ls`
Problemumgehung	Es wird empfohlen, dass Sie die NFS-Protokoll-Schnittstellen verwenden, um auf die FluidFS Systeme der NAS-Cluster-Lösung von Linux/UNIX-Clients aus zuzugreifen. So umgehen Sie dieses Problem: 1. Stellen Sie sicher, dass Ihr Administrator NFS-Exporte auf den gleichen Speicherorten erstellt, die Sie für den Zugriff mittels CIFS verwenden, und verbinden Sie sie mithilfe des Mount-Befehls über die Linux/UNIX-Clients. 2. Verwenden Sie NFS-basierte Schnittstellen, um auf die NAS-Cluster-Lösung zuzugreifen. Verwenden Sie zum Beispiel den Befehl `/check_disk` anstatt des Befehls `/check_disk_smb`.

Fremde UID- und GID-Nummern bei Dell NAS-Systemdateien

Beschreibung	Dateien, die über ubuntu 7.*x*-Clients neu erstellt wurden, werden die UID- und GID-Nummern 4294967294 (nfsnone) zugewiesen.
Ursache	Standardmäßig geben Ubuntu 7.*x* nfs-Clients keine rpc-Anmeldeinformationen bei ihren nfs-Abrufen an. Darum befinden sich Dateien, die von diesen Clients durch einen

	beliebigen Benutzer erstellt wurden, im Besitz von 4294967294 (nfsnone) UID und GID.
Problemumgehung	Fügen Sie zum Erzwingen von UNIX-Anmeldedaten auf nfs-Abrufen die Option **sec=sys** zu den NAS-Cluster-System-Mounts in der Ubuntu **fstab**-Datei hinzu.

Fehlerbehebung – Netzwerkfehler

Nameserver antwortet nicht

Beschreibung	Kein NIS-, LDAP- oder DNS-Server ist erreichbar oder antwortet.
Problemumgehung	Führen Sie auf jedem Server die folgenden Aktivitäten aus: 1. Pingen Sie den Server von einem Client auf der NAS-Cluster-Lösung an und überprüfen Sie, ob er antwortet. 2. Erstellen Sie über einen Client auf der NAS-Cluster-Lösung eine Anfrage beim Server, und stellen Sie fest, ob der Server antwortet. 3. Überprüfen Sie die Serverprotokolle, um zu ermitteln, warum der Server auf die Anfragen nicht reagiert.

Spezifische Subnetz-Clients können nicht auf die NAS-Cluster-Lösung zugreifen

Beschreibung	Benutzer (alte oder neue), die über bestimmte Netzwerke zugreifen oder keinen Zugriff auf die NAS-Cluster-Lösung haben.
Ursache	Dieses Problem wird durch einen Konflikt zwischen den Subnetz-Adressen des Benutzers und der internen Netzwerkadresse des NAS-Systems verursacht. Das NAS-System routet die Antwortpakete zum falschen Netzwerk.
Problemumgehung	1. Überprüfen Sie die internen Netzwerkadressen des NAS-Systems, und prüfen Sie, ob ein Konflikt mit den problematischen Client-Netzwerkadressen vorliegt. 2. Wenn ein Konflikt vorliegt, ändern Sie manuell die konfligierende interne NAS-Netzwerkadresse über den NAS Manager oder die Befehlszeilenschnittstelle.

Beheben von Fehlern in der DNS-Konfiguration

Beschreibung	Es konnte keine Verbindung zur NAS-Cluster-Lösung mithilfe des Systemnamens hergestellt werden und/oder die Hostnamen konnten nicht aufgelöst werden.
Ursache	Mögliche Ursachen: • Das System konnte mithilfe des Fully Qualified Domain Name (FQDM) nicht angepingt werden.

	• Es konnte keine Verbindung zum NAS Manager mithilfe des Systemnamens hergestellt werden.
Problemumgehung	1. Stellen Sie sicher, dass die IP-Adressinformationen des Clients korrekt sind. 2. Vergewissern Sie sich, dass der Controller der NAS-Cluster-Lösung für den korrekten DNS-Server konfiguriert ist. 3. Kontaktieren Sie den DNS-Serveradministrator, um die Erstellung des DNS-Datensatzes zu überprüfen.

IQN der Controller in der NAS-Cluster-Lösung mithilfe der CLI ermitteln

Beschreibung	Den IQN der Controller in der NAS-Cluster-Lösung mithilfe der CLI ermitteln.
Problemumgehung	Melden Sie sich mithilfe eines SSH-Clients und der VIP der NAS-Verwaltung bei der CLI der NAS-Cluster-Lösung als Administrator an. Geben Sie an der Befehlszeilenschnittstelle den folgenden Befehl ein: `system maintenance luns iscsi-configuration view`

Fehlerbehebung – Warnmeldungen der Art „RX/TX Pause“

Beschreibung	Die folgenden Warnmeldungen werden möglicherweise angezeigt, wenn der NAS Manager meldet, dass die Konnektivität nicht optimal ist:
	`Rx_pause for eth(x) on node 1 is off (Rx_pause for eth(x) auf Knoten 1 ist aus).`
	`Tx_pause for eth(x) on node 1 is off (Tx_pause for eth(x) auf Knoten 1 ist aus).`

Ursache	Die Flow Control ist auf dem/den Switch(es), die mit einem NAS-Cluster-System-Controller verbunden sind, nicht aktiviert.
Problemumgehung	Weitere Informationen zur Aktivierung der Flow Control auf Switches finden Sie in der Dokumentation des Switch-Anbieters.

Fehlerbehebung – NAS Manager-Fehler

NAS-Instrumententafel ist verzögert

Beschreibung	Die Metrik für die NAS-Instrumententafel ist verzögert und zeigt nach der Aktualisierung nicht sofort die aktualisierten Werte an.
Ursache	Die Ansicht in NAS Manager wird alle 40 Sekunden aktualisiert, die Daten in Bezug auf bestimmte Metriken werden jedoch in verschiedenen Intervallen gesammelt, daher gibt es keine Korrelation zwischen der Bildschirmaktualisierung und der Aktualisierung der tatsächlichen Metriken.
Problemumgehung	Verwenden Sie den Prozess in FluidFS, bei dem Daten zu verschiedenen Metriken im System gesammelt werden. • Statusfelder (Gesamtstatus, Service-Status, erverstatus) – Die Daten werden alle 40 Sekunden erfasst. • Kapazität – Die Daten werden alle 1.800 Sekunden erfasst. • Aktuelle Leistung (NFS, CIFS, Replikation, NDMP, Netzwerk) – Die Daten werden alle 40 Sekunden erfasst. • Kürzliche Leistung (das Diagramm) – Die Daten werden alle 60 Sekunden erfasst. • Lastenausgleich (CPU, Anzahl der Verbindungen) – Die Daten werden alle 40 Sekunden erfasst.

NAS-Systemzeit ist falsch

Beschreibung	Geplante Aufgaben werden zu falschen Zeiten ausgeführt. Datum/Uhrzeit von Ereignisprotokollnachrichten ist falsch.
Ursache	• Die Uhrzeit auf dem NAS-System ist falsch. • Es wurde kein NTP-Server für das NAS-System definiert. • Der NTP-Server, der die NAS-Cluster-Lösung bedient, ist entweder ausgefallen oder hat die Bereitstellung der NTP-Dienste unterbrochen. • Es liegen Probleme bei der Netzwerkkommunikation mit dem NTP-Server vor.
Problemumgehung	1. Identifizieren Sie den NAS-NTP-Server auf der Seite **Systemkonfiguration/Zeitkonfiguration**. Notieren Sie Hostnamen oder IP-Adressen für eine spätere Verwendung. 2. Wenn kein NTP-Server definiert ist, dann definieren Sie einen. Es wird empfohlen, die NAS-Systemuhr mit dem NTP-Server zu synchronisieren, der vom Active Directory Domain Controller (ADDC) verwendet wird. So werden Probleme mit

Zeitunterschieden und Authentifizierung vermieden. In jedem Fall ist der ADDC auch der NTP-Server.

3. Stellen Sie sicher, dass der NTP-Server betriebsbereit ist und den NTP-Dienst bereitstellt.
4. Überprüfen Sie den Netzwerkpfad zwischen dem NAS-System und dem NTP-Server, zum Beispiel durch Anpingen. Vergewissern Sie sich, dass die Antwortdauer im Bereich von Millisekunden liegt.

Verbindung mit NAS Manager nicht möglich

Beschreibung	Es konnte keine Verbindung mit dem NAS Manager hergestellt werden.
Ursache	Mögliche Ursachen: • Der Benutzer versucht, eine Verbindung über eine falsche IP-Adresse herzustellen oder verwendet einen falschen Systemnamen. • Die IP-Adressinformationen des Client-Computers wurden falsch konfiguriert. • Der Benutzer verwendet einen falschen Benutzernamen oder ein falsches Kennwort. • Die Browser-Eigenschaften des Benutzers verhindern den Verbindungsaufbau.
Problemumgehung	1. Stellen Sie sicher, dass die IP-Adressinformationen des Clients korrekt sind. 2. Stellen Sie sicher, dass die DNS-Informationen korrekt konfiguriert wurden. 3. Überprüfen Sie den Benutzernamen und das Kennwort. 4. Überprüfen Sie die Proxy-Informationen in den Browser-Einstellungen. 5. Wenn Sie Microsoft Windows Server 2008 verwenden, deaktivieren Sie IE ESC.

Leerer Anmeldebildschirm

Beschreibung	Es konnte keine Verbindung zum NAS Manager hergestellt werden, und der Anmeldebildschirm ist leer.
Ursache	Mögliche Ursachen: • Das Java-Skript wurde deaktiviert. • IE SEC ist aktiviert.
Problemumgehung	• Wenn Java Script deaktiviert ist, aktivieren Sie es. Informationen zum Aktivieren von Java Script finden Sie in der Hilfe Ihres Browsers. • Wenn IE SEC aktiviert wurde, deaktivieren Sie es.

Fehlerbehebung – Backup-Fehler

Beheben von Snapshot-Fehlern

Beschreibung	Beim Aufnehmen und Löschen von Snapshots treten Fehler auf.
Ursache	Mögliche Ursachen: • Es liegen viele Client-E/A-Anfragen zur Verarbeitung vor, einschließlich einer Anfrage zum Löschen eines großen Verzeichnisses. • Es liegen viele Anfragen zum Erstellen/Löschen von Snapshots vor, die derzeit bearbeitet werden. • Es wird derzeit eine andere Snapshot-Anfrage für dieses Volume ausgeführt. • Im System ist die maximale Anzahl von Snapshots erreicht. • In der Backup-Aufgabe wurde die falsche IP-Adresse angegeben.
Problemumgehung	• Wenn eine manuelle Anfrage fehlschlägt, versuchen Sie, den Snapshot nach Ablauf von wenigen Minuten erneut aufzunehmen oder zu löschen. • Wenn die Anfrage vom Snapshot-Zeitplaner stammt, warten Sie noch ein oder zwei Zyklen ab. Wenn der Fehler weiterhin besteht, versuchen Sie, den Snapshot auf demselben Volume manuell vorzunehmen oder zu löschen. • Überprüfen Sie das Dashboard daraufhin, ob das System unter hoher Arbeitsauslastung steht. Wenn das System unter hoher Arbeitsbelastung steht, warten Sie, bis die Arbeitsbelastung abnimmt und stellen Sie die Snapshot-Anfrage erneut. • Überprüfen Sie den Snapshot-Zeitplan. Ein sehr dichter Snapshot-Zeitplan hat einen negativen Einfluss auf die Gesamtleistung des Systems. Die kumulierte Snapshot-Rate darf 20 Snapshots pro Stunde pro System nicht übersteigen. • Überprüfen Sie die Gesamtzahl von Snapshots im System. Wenn die Zahl mehrere Tausend beträgt, löschen Sie einige Snapshots und versuchen Sie es erneut. • Vergewissern Sie sich, dass die virtuelle IP-Adresse des Clients in der Backup-Aufgabe angegeben ist.

Beheben von internen NDMP-Fehlern

Beschreibung	Backups oder Wiederherstellungen schlagen aufgrund eines internen Fehlers fehl.
Ursache	Die internen NDMP-Fehler sind ein Anzeichen dafür, dass ein Dateisystem nicht erreichbar oder ein NAS-Volume nicht verfügbar ist.
Problemumgehung	Die Backup-Anwendung war nicht in der Lage, eine Verbindung zu einer NAS-Appliance herzustellen:

1. Melden Sie sich beim NAS Manager an oder öffnen Sie ein Remote-Terminal zur Appliance.
2. Gehen Sie im NAS Manager auf die Seite **Datenschutz → NDMP → NDMP-Konfiguration** . Gehen Sie in der NAS-CLI in das Menü **Datenschutz NDMP Konfiguration**.
3. Überprüfen Sie, ob NDMP aktiviert ist. Wenn NDMP aktiviert ist, gehen Sie zu Schritt 5.
4. Im NAS Manager muss das Kontrollkästchen **Aktiviert** aktiviert sein.
5. Geben Sie in der NAS-Befehlszeilenschnittstelle den Befehl `Anzeigen` ein und stellen Sie sicher, dass **Status** auf **Aktiviert** gesetzt ist.
6. Sollte NDMP nicht aktiviert sein, aktivieren Sie es.
7. Stellen Sie sicher, dass die IP-Adresse für die Backup-Anwendung in NDMP aktiviert ist.
8. Im NAS Manager muss die DMA-Serverliste die IP-Adresse der Backup-Anwendung enthalten.
9. Geben Sie in der NAS-Befehlszeilenschnittstelle den Befehl `Anzeigen` ein und stellen Sie sicher, dass die Liste **DMA-Server** die IP-Adresse der DMA-Anwendung enthält, die versucht, auf die NAS-Appliance zuzugreifen.

Wenn die Backup-Appliance mit der NAS-Appliance verbunden werden kann, die Anmeldung jedoch scheitert, verwenden Sie backup_user als Benutzernamen für den NDMP-Client, und legen Sie das/die NDMP-Backup/Wiederherstellung in Ihrer Backup-Anwendung fest. Das Standardkennwort für NDMP-Client ist **Stor@ge!**

So ändern Sie das Kennwort:

1. Melden Sie sich beim NAS Manager an, oder öffnen Sie ein Remote-Terminal zur Appliance.
2. Gehen Sie im NAS Manager auf die Seite **Datenschutz → NDMP → NDMP-Konfiguration)** . Gehen Sie in der NAS-CLI in das Menü **Datenschutz → NDMP → Konfiguration**.
3. Klicken Sie im NAS Manager auf **Kennwort ändern**. Führen Sie in der NAS-CLI den Befehl aus:

   ```
   data-protection ndmp configuration
   set-Password <new_password>
   ```

Wenn sich die Backup-Anwendung bei der NAS-Appliance anmelden kann, jedoch keine Volumes für die

	Sicherung verfügbar sind, stellen Sie sicher, dass auf der NAS-Appliance NAS-Volumes verfügbar sind.

Fehlerbehebung – Systemfehler

Beheben von Fehlern beim Herunterfahren des Systems

Beschreibung	Während des Herunterfahrens des Systems mithilfe des NAS Manager konnte das System nicht angehalten werden, und die Controller wurden nach 20 Minuten nicht heruntergefahren.
Ursache	Das Herunterfahren des Systems besteht aus zwei separaten Prozessen: • Anhalten des Systems • Ausschalten von Controllern der NAS-Cluster-Lösung Aufgrund von Datenverlusten oder einer unterbrochenen Verbindung zum Speicher dauert es möglicherweise lange, bis das Dateisystem den Cache in den Speicher geleert hat. Während des Ausschaltens könnte dieses Problem dadurch verursacht werden, dass sich der Betriebssystem-Kernel auf dem Controller aufgehängt hat oder der Status nicht mit dem lokalen Laufwerk synchronisiert werden kann.
Problemumgehung	Wenn das Dateisystem angehalten wurde und einer der Controller weiterhin aktiv ist, können Sie den Controller über die Ein/Aus-Taste physikalisch ausschalten. Wenn das Dateisystem nicht angehalten wurde, müssen Sie es weiter arbeiten lassen. Das Dateisystem erreicht eine Zeitüberschreitung nach 10 Minuten, leert seinen Cache auf den lokalen Controllern und fährt mit dem Herunterfahren fort.

Verletzung der NAS-Containersicherheit

Beschreibung	Es liegt eine Verletzung der NAS-Containersicherheit vor.
Ursache	Das Auswählen eines Sicherheitstyps für einen NAS-Container gibt das vorherrschende Protokoll vor, das beim Einstellen von Berechtigungen auf Dateien in diesem Volume verwendet wird. NFS bei Volumes mit UNIX-Sicherheitstyp und CIFS bei Volumes mit NTFS-Sicherheitstyp. Daraus folgt, dass einige Vorgänge nicht ausgeführt werden können: • Festlegen von UNIX-Berechtigungen für eine Datei in einem NTFS-Sicherheitscontainer. • Festlegen des UID/GID-Eigentumsrechts für eine Datei in einem NTFS-Sicherheitscontainer.

- Festlegen der Zugriffskontrollliste für eine Datei in einem UNIX-Sicherheitscontainer.
- Ändern der Schreibschutzkennzeichnung für eine Datei in einem UNIX-Sicherheitscontainer.
- Festlegen des SID/GSID-Eigentumsrechts für eine Datei in einem UNIX-Sicherheitscontainer.

Die NAS-Containersicherheit muss das Hauptprotokoll widerspiegeln, das für den Zugriff auf die entsprechenden Dateien verwendet wird.

Problemumgehung

Wenn ein Benutzer häufig sicherheitsbezogene Aktivitäten über verschiedene Protokolle hinweg durchführen muss, teilen Sie die Daten auf der Basis des Hauptzugriffsprotokolls auf verschiedene NAS-Container auf.

Mehrere Fehler während der Formatierung des Dateisystems

Beschreibung

Während der Formatierung des Dateisystems sind mehrere Fehler aufgetreten.

Ursache

Mögliche Ursachen:

- Es werden falsche SAN-IPs im Dell NAS Initial Deployment Utility (IDU) verwendet.
- Bei der Definition von Hosts im MDSM wurden die falschen IQNs verwendet.
- Der Hostgruppe wurde eine ungerade Anzahl von LUNs zugeordnet.
- Die LUN-Größe ist unterhalb der erforderlichen Größe.
- Es ist weniger als die Mindestanzahl der benötigten LUNs verfügbar.

Problemumgehung

Gehen Sie wie folgt vor, wenn während der Ausführung des NAS IDU falsche SAN-IP-Adressen verwendet werden:

1. Stellen Sie sicher, dass sich die MD-Erkennungs-IP-Adresse, die im Rahmen der Ausführung des NAS IDU verwendet wird, auf dem gleichen Subnetz wie die beiden SAN-IP-Adressen befindet, die auf Ihren Controllern konfiguriert wurden.
2. Um die MD-Ermittlungs-IP zu überprüfen, melden Sie sich auf Ihrer NAS-Manager-IP mithilfe der CLI an und führen Sie den folgenden Befehl aus: `system maintenance luns configuration iscsi-view`

Dieser Befehl zeigt die MD-Erkennungs-IP-Adresse.

Wenn sich die IP-Adresse nicht auf dem gleichen Subnetz wie die für Ihren SAN konfigurierten IP-Adressen befindet, ändern Sie die MD-Erkennungs-IP-Adresse in eine der Subnetze um, die auf den SAN A und B Ihres Controllers definiert sind.

Wenn im Rahmen der Definition von Hosts im MDSM falsche IQNs verwendet werden, stellen Sie sicher, dass

die in MDSM angezeigten IQNs mit den Controller-IQNs übereinstimmen.

Zum Ändern der Ermittlungs-IP führen Sie den folgenden Befehl in der CLI aus:

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

Nachdem der Befehl abgeschlossen ist, aktualisieren Sie die Host-Port-Kennung. Nun können Sie den Konfigurationsassistenten vom NAS-Manager erneut ausführen.

1. Vergleichen Sie, ob die in MDSM angezeigten IQNs mit denen identisch sind, die auf der Registerkarte **Zuordnungen** im Host-Bereich des NAS Manager angezeigt werden.
2. Wenn es einen Unterschied gibt, korrigieren Sie die für die Hosts in MDSM verwendeten IQNs und versuchen Sie, das System zu formatieren. Die LUNs müssen ermittelt und formatiert werden.

Gehen Sie wie folgt vor, wenn das Problem aus einer ungeraden Anzahl von LUNs resultiert:

1. Wenn ein Fehler gefunden wird, stellen Sie sicher, dass eine gerade Anzahl an LUNs der Host-Gruppe zugeordnet ist. Eine ungerade Anzahl von LUNs wird nicht unterstützt. LUNs müssen in Paaren wachsen, beginnend von 2 bis 16.
2. Wenn eine ungerade LUN-Anzahl verwendet wird, korrigieren Sie die Anzahl, indem Sie LUNs entfernen oder hinzufügen.
3. Versuchen Sie, das System zu formatieren.

Gehen Sie wie folgt vor, wenn die LUN-Größe unterhalt der Mindestanforderungen liegt:

1. Stellen Sie sicher, dass die LUNs größer als die geforderte Mindestgröße von 125 GB sind.
2. Wenn die LUNs kleiner als 125 GB sind, ändern Sie die LUN-Größe, damit sie die erforderliche Mindestgröße erreicht oder überschreitet.
3. Versuchen Sie, das System zu formatieren.

Gehen Sie wie folgt vor, wenn die LUN-Anzahl unterhalb der Mindestanforderungen liegt:

1. Überprüfen Sie, dass der Host-Gruppe mehr als eine LUN zugeordnet ist. Es sind mindestens 2 LUNs erforderlich.
2. Wenn die LUN-Anzahl geringer als 2 ist, fügen Sie LUNs hinzu, um die Mindest-LUN-Anzahl von 2 zu erfüllen.
3. Versuchen Sie, das System zu formatieren.

Verknüpfen von LUN-Namen mit virtuellen Laufwerken

Beschreibung	Bestimmen, bei welchen LUNs im NAS-Manager es sich um virtuelle Festplatten im Modular Disk Storage Manager (MDSM) handelt.
Problemumgehung	Öffnen Sie die Web-Oberfläche des NAS-Managers und gehen Sie zu **Clusterverwaltung** → **Wartung** → **LUNs hinzufügen.** Diese Seite zeigt alle LUNs an, auf die die NAS-Cluster-Lösung zugreifen kann (die der Hostgruppe der NAS-Cluster-Lösung zugewiesen sind). Jede LUN kann über ihren World Wide Name identifiziert werden. Auf der Web-Oberfläche des NAS-Managers trägt der World Wide Name der LUN ein Präfix. Öffnen Sie MDSM, gehen Sie zur Registerkarte **Logisch** und klicken Sie auf **Virtuelles Laufwerk**. Die weltweite Kennung des virtuellen Laufwerks wird im Fensterbereich **Eigenschaften** angezeigt. Mit dieser Problemumgehung können Sie bestimmen, welche virtuellen Laufwerke dem NAS-Dateisystem zugeordnet sind.

NAS-IDU konnte keinen Controller finden

Beschreibung	NAS-IDU konnte keinen Controller finden
Ursache	IPV6 ist eventuell nicht auf Ihrer Workstation aktiviert.
Problemumgehung	Aktivieren Sie IPV6-Unterstützung auf Ihrer Verwaltungs-Workstation.

Fehler beim Hinzufügen

Beschreibung	Der Vorgang zum Hinzufügen des Controllers zum NAS-Cluster schlägt fehl.
Problemumgehung	• Schließen Sie eine Tastatur und einen Monitor an den Controller an, bei dem der Hinzufügevorgang fehlgeschlagen ist, und lesen Sie die Fehlermeldung, um zu ermitteln, warum das Hinzufügen fehlgeschlagen ist. • Überprüfen Sie folgende Punkte: – Während der Controller getrennt war, wurde die ihm im Client-Netzwerk zugewiesene IP-Adresse keinem anderen Host zugewiesen. Während der Controller getrennt ist, verliert er seine Identität, inkl. VIP-Adressen. Wenn er dann hinzugefügt wird, erhält der Controller seine Identität inkl. IP-Adressen zurück. – Stellen Sie mithilfe des NAS Managers sicher, dass das Standard-Gateway sich im **Primären** Subnetz befindet. Sehen Sie

sich das Standard-Gateway unter **Clusterverwaltung** → **Netzwerkkonfiguration** an und unter **Clusterverwaltung** → **Subnetze** finden Sie das **Primäre** Subnetz im Client-Netzwerk. Wenn sich das Standard-Gateway nicht im **Primären** Subnetz befindet, ändern Sie das Standard-Gateway. Damit das Hinzufügen erfolgreich ist, muss das Standard-Gateway **anzupingen** sein.

- Nachdem ein Hinzufügevorgang fehlgeschlagen ist, muss der Controller manuell in den Standby-Modus zurückgesetzt werden. Dies geschieht durch Anschließen einer Tastatur und eines Monitors an den Controller, der nicht hinzugefügt werden konnte, und Drücken auf die Systemidentifikationstaste , wie in den Anweisungen auf dem Bildschirm beschrieben.

Controller braucht sehr viel Zeit, um nach einer Service Pack-Aktualisierung zu starten.

Beschreibung	Der Controller braucht sehr lange, um nach der Service Pack-Aktualisierung der Controller-Firmware zu starten.
Problemumgehung	• Schließen Sie eine Tastatur und einen Monitor an den Controller an, der lange zum Starten braucht. • Wenn das System startet und sich in der Startphase befindet, lassen Sie die Aktualisierungen abschließen. Dies kann bis zu 60 Minuten dauern. • Starten Sie den Controller nicht manuell neu, wenn er sich in der Startphase beim **Ausführen von Systemaktualisierungen** befindet.

Fehlerbehebung bei Problemen des Dell NAS Initial Deployment Utility (IDU)

Fehler beim Ausführen des Dell NAS Initial Deployment Utility

Beschreibung	Beim Ausführen des Dell NAS Initial Deployment Utility (NAS IDU, Dienstprogramm zur ersten Bereitstellung von Dell NAS) ist ein Fehler aufgetreten.
Ursache	Der Fehler könnte entweder durch das Hardware-Setup, die Konfiguration des Netzwerk-Switches oder die Cluster-Systemkonfigurationen hervorgerufen werden.
Problemumgehung	Auf der Erkennungsseite wird ein Verbindungsfehler angezeigt: 1. Überprüfen Sie, dass die Management-Station, auf der **NAS IDU** ausgeführt wird, über eine Netzwerkverbindung zum Client-Switch des NAS-Clusters verfügt.

ANMERKUNG: Es ist zwingend erforderlich, dass die NAS-Controller und das System, das NAS IDU ausführt, nicht über einen Router verbunden sind.

2. Überprüfen Sie, ob IPv6 auf der Management-Station aktiviert ist, auf der das NAS IDU ausgeführt wird.
3. Schließen Sie an die NAS-Cluster-Controller eine USB-Tastatur und einen Monitor an und überprüfen Sie, dass wiederholt eine Nachricht mit der MAC-Adresse des Controllers und der Meldung **Press "i" - re-install standby node" (Drücken Sie „i" - Standby-Knoten neu installieren)** ausgegeben wird.

Wenn sich der Fehler auf der Konfigurations-NAS-Cluster-Seite befindet:

1. Erstellen Sie während der Cluster-Erstellung einen Screenshot der Fehlermeldung über das Fenster des NAS IDU
2. Erfassen Sie die Cluster-Konfigurationsdatei, die Protokolldatei des NAS IDU und die resultierende Datei aus dem Installationsverzeichnis, und zippen Sie den Konfigurationsordner aus dem Installationsverzeichnis.
3. Das NAS IDU soll Benutzer zum Wiederherstellungsfenster führen, in dem Knoten in den Standby-Modus wiederhergestellt werden.
4. Suchen Sie die Fehlermeldungen im aufgenommenen Screenshot und finden Sie die potentielle Ursache für den Fehler heraus. Korrigieren Sie diese Fehler und konfigurieren Sie das System mithilfe des NAS IDU neu.
5. Wenn der Fehler fortbesteht, stellen Sie alle Dateien in einem Bundle-Paket zusammen, und setzen Sie sich mit dem Support von Dell in Verbindung.

Dienstprogramm zur ersten Bereitstellung von Dell NAS kann nicht gestartet werden

Beschreibung	Dienstprogramm zur ersten Bereitstellung von Dell NAS kann nicht gestartet werden.
Ursache	Mögliche Ursachen: • Das Installationsprogramm für NAS Initial Deployment Utility konnte nicht installieren. • Die JAVA-Laufzeitumgebung wurde nicht ordnungsgemäß installiert.
Problemumgehung	Führen Sie folgende Schritte durch: • Überprüfen Sie, ob das Installationsprogramm für das NAS-Konfigurationsdienstprogramm erfolgreich abgeschlossen wurde. • Überprüfen Sie, ob die Mindestversion von JRE1.6x erfolgreich installiert wurde.

- Führen Sie unter Microsoft Windows den Befehl `java -version` über die Befehlskonsole aus, um eine gültige JRE-Version anzuzeigen.

7

Wartung der NAS-Cluster-Lösung

In diesem Kapitel finden Sie Informationen zum Aus- und Einschalten des Systems im Falle einer geplanten Stromausschaltung oder einer Verlegung des Systems an einen anderen Ort. In diesem Kapitel wird auch das Verfahren zum Aktualisieren der Software und Ausführen von Diagnoseprogrammen beschrieben.

ANMERKUNG: Weitere Informationen zur Wartung und Pflege der Hardware finden Sie im *Dell FluidFS NAS Solutions Owner's Manual* (Dell FluidFS NAS-System-Benutzerhandbuch) unter **dell.com/support**.

Ausschalten der NAS-Cluster-Lösung

VORSICHT: Halten Sie sich strikt an diese Anweisungen, um Dateninkonsistenzen zu vermeiden.

ANMERKUNG: Durch dieses Verfahren werden beide Controller heruntergefahren.

So fahren Sie das System herunter:

1. Öffnen Sie einen Browser, und stellen Sie eine Verbindung zur virtuellen IP-Adresse (VIP) von NAS Manager her, den Sie im Rahmen der Installation konfiguriert haben.
2. Wählen Sie im NAS-Manager **Clusterverwaltung** → **Wartung** → **Systemstopp/-start** aus.
   Die Seite **Systemstopp/-start** zeigt den Systemstatus an.
3. Wählen Sie aus der Liste **Durchzuführende Systemaktion Anhalten** aus.
4. Klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, mit dem Anhaltevorgang fortzufahren, klicken Sie auf **OK**.
   Dieser Vorgang kopiert den Cache des Dateisystems auf die Laufwerke und hält das Dateisystem an.
6. Drücken Sie kurz den eingelassenen Ein/Aus-Schalter ab der Rückseite eines jeden Controllers, um den Controller auszuschalten.

   ANMERKUNG: Wenn Sie den Ein/Aus-Schalter für mehrere Sekunden gedrückt halten, wird das System nicht ausgeschaltet.

Einschalten der NAS-Cluster-Lösung

Stellen Sie vor dem Einschalten des Systems sicher, dass alle Kabelverbindungen zwischen Controller und Rack ordnungsgemäß verbunden und die Komponenten an die Stromversorgung des Gebäudes angeschlossen sind.

Schalten Sie die Komponenten in der folgenden Reihenfolge ein:

1. Speicher-Arrays:
   - Schalten Sie alle Speicher-Arrays ein, indem Sie auf die EIN/AUS-Schalter an den zwei Stromversorgungen drücken, die sich auf der Rückseite der Einheiten befinden.
   - Warten Sie einen Augenblick, bis die Betriebs-LEDs für die Stromversorgung, die Controller und die Laufwerke dauerhaft leuchtet.
2. NAS-Cluster-Lösung:
   Um die Controller zu starten, schließen Sie alle NAS-Controller bzw. -Geräte an eine Stromquelle an.

3. Wählen Sie im NAS-Manager **Clusterverwaltung** → **Wartung** → **Systemstopp/-start** aus.
   Die Seite **Systemstopp/-start** zeigt den Systemstatus an.
4. Wählen Sie aus der Liste **Durchzuführende Systemaktionen Start** aus.
5. Klicken Sie auf **Weiter**.

Wiederherstellen der NAS-Volume-Konfiguration

Das Wiederherstellen der NAS-Volume-Konfiguration bietet dem Systemadministrator einen effektiven Weg, alle NAS-Volume-Einstellungen (Exporte, Freigaben, Snapshot-Zeitpläne, Kontingentregeln usw.) wiederherzustellen, ohne sie dabei manuell neu konfigurieren zu müssen. Dies ist nach dem Erstellen eines neuen NAS-Volumes, nach einer Neuinstallation des Systems oder nach einer Systemwiederherstellung nützlich.

Ein NAS-Volume kann wiederhergestellt werden, indem die Konfiguration eines NAS-Volumes (auch wenn es nur eine gespeicherte Konfiguration ist) auf ein anderes NAS-Volumes im selben oder in einem anderen System wiederhergestellt wird. Der Administrator muss die Konfiguration auf das NAS-Volume von dessen Backup oder von einem anderen NAS-Volume aus kopieren

Wann immer eine Änderung an der Volume-Konfiguration vorgenommen wird, so wird sie automatisch in einem Format gespeichert, durch das sie später wiederhergestellt werden kann. Die Konfiguration wird im Ordner **.clusterConfig** gespeichert, der sich im Stammordner des NAS-Volumes befindet.

Dieser Ordner kann gesichert werden, entweder individuell oder zusammen mit den Volume-Benutzerdaten, und später wiederhergestellt werden. Damit die im Ordner gespeicherte Konfiguration wirksam wird, muss der Administrator zuerst den Ordner **.clusterConfig** auf das wiederherzustellende NAS-Volume kopieren und dann die Seite **NAS-Volume-Konfiguration wiederherstellen** verwenden, um die Konfiguration auf das NAS-Volume anzuwenden.

ANMERKUNG: Wenn Sie ein NAS-Volume wiederherstellen, wird die vorhandene Konfiguration überschrieben und ersetzt. Benutzer, die derzeit mit dem System verbunden sind, werden getrennt.

Die folgenden Parameter können wiederhergestellt werden:

- NFS-Exporte
- CIFS-Freigaben
- Kontingentregeln
- Snapshot-Zeitplan
- NAS-Volume-Warnmeldungen, Sicherheitsstil und damit verbundene Parameter
- Name des NAS-Volumes
- Größe des NAS-Volumes

So stellen Sie eine NAS-Volume-Konfiguration wieder her:

ANMERKUNG: Wenn Sie ein Backup aus einem anderen System verwenden, funktioniert der Wiederherstellungsvorgang nur, wenn die gesicherte Konfiguration von einem System mit der gleichen Softwareversion genommen wurde.

1. Wählen Sie **Clusterverwaltung** → **Wartung** → **NAS-Volume-Konfiguration wiederherstellen** aus.
   Die Seite **NAS-Volume-Konfiguration wiederherstellen** wird angezeigt.
2. Wählen Sie aus der Liste **Konfiguration aktualisieren von** das System aus, dessen Konfiguration Sie aktualisieren möchten.
3. Wählen Sie aus der Liste **Konfiguration aus dem System nehmen** das Quell-Cluster für die Konfigurationsinformationen aus.
4. Wählen Sie eine oder mehrere Optionen aus der Liste der systemweiten Parameter aus, die wiederhergestellt werden können.
5. Klicken Sie auf **Anwenden**.

Wiederherstellen der Cluster-Konfiguration

Das Wiederherstellen der Systemkonfiguration ist eine effektive Methode, um die meisten Systemeinstellungen (wie Protokollkonfigurationen, lokale Benutzer und Gruppen) wiederherzustellen, ohne die Einstellungen manuell neu konfigurieren zu müssen. Dies kann sinnvoll sein nach einer Aktualisierung des Systems mit einer neuen Softwareversion, nach einer Neuinstallation des Systems oder nach der Wiederherstellung eines Systems.

Die Systemkonfiguration wird wiederhergestellt, indem die Konfiguration ausgewählt und auf dem betroffenen System wiederhergestellt wird, die auf dem aktuellsten NAS-Volume im Cluster gespeichert ist. Sie müssen die Konfiguration auf das NAS-Volume von seinem Backup oder von einem anderen System aus kopieren.

Wann immer eine Änderung an der Systemkonfiguration vorgenommen wird, so wird sie automatisch in einem Format gespeichert, durch das sie später wiederhergestellt werden kann. Die Konfiguration wird im Ordner **.clusterConfig** gespeichert, der sich im Stammordner eines jeden NAS-Volumes befindet.

Dieser Ordner kann gesichert werden, entweder alleine oder zusammen mit den Benutzerdaten des Volumes, und später wiederhergestellt werden. Damit die in dem Ordner gespeicherte Konfiguration wirksam wird, muss der Administrator zuerst den Ordner **.clusterConfig** auf eines der NAS-Volumes im System kopieren und dann die Konfiguration auf das System anwenden.

ANMERKUNG: Wenn Sie eine Systemkonfiguration wiederherstellen, wird die vorhandene Konfiguration überschrieben und ersetzt. Benutzer, die derzeit mit dem System verbunden sind, werden getrennt.

Die folgenden Parameter können wiederhergestellt werden:

- Protokollkonfigurationen
- Benutzer und Gruppen
- Benutzerzuordnungen
- Überwachungskonfiguration
- Time Configuration (Zeitkonfiguration)
- Antivirus-Hosts

1. Wählen Sie **Cluster Management (Clusterverwaltung)** → **Maintenance (Wartung)** → **Restore Cluster Configuration (Cluster-Konfiguration wiederherstellen).**

   Die Seite **Restore Cluster Configuration (Cluster-Konfiguration wiederherstellen)** wird angezeigt.
2. Wählen Sie aus der Liste **Configuration taken from system (Konfiguration aus System)** das System aus, dessen Konfiguration Sie aktualisieren möchten.
3. Wählen Sie eine oder mehrere Optionen aus der Liste der systemweiten Parameter aus, die wiederhergestellt werden können.
4. Klicken Sie auf **Apply (Anwenden)**.

Dateisystem formatieren

ANMERKUNG: Nur NX3600 und NX3610 unterstützen das Formatieren von Dateisystemen mithilfe des **NAS Manager**. Bei FS8600 wird **File System Format (Dateisystem formatieren)** vom **Enterprise Manager** durchgeführt, wenn FS8600 zum ersten Mal mit dem **Enterprise Manager** bereitgestellt wird.

Die Formatierung eines Dateisystems installiert das Dateisystem auf den LUNs, die dem NAS zugeordnet sind. Das Formatieren löscht alle auf den LUNs vorhandenen Daten. Damit ein NAS-Volume erstellt werden kann, muss eine Formatierung des Dateisystems durchgeführt werden. Normalerweise ist die Formatierung des Dateisystems ein einmaliges Ereignis, es sei denn, der NAS wird neu bereitgestellt und die vorhandenen Daten werden nicht länger benötigt.

Zum Formatieren des Dateisystems wählen Sie **Cluster Management (Clusterverwaltung)** → **Maintenance (Wartung)** → **File System Format (Dateisystem formatieren)** und klicken Sie auf **Format (Formatieren)**.

Installieren des Service Pack

Die NAS-Cluster-Lösung verwendet eine Service Pack-Methode, um die Software auf die jeweils aktuelle Version zu aktualisieren.

ANMERKUNG: Zur Aktualisierung Ihres Systems mit dem neuesten Service Pack siehe **dell.com/support**.

Aktualisieren des Service Packs mithilfe des NAS-Managers

Durch Service Packs ist Ihre Dell FluidFS NAS-Lösung immer auf dem neuesten Stand mit der aktuellsten Firmware und Software. Besuchen Sie **dell.com/support** und laden Sie die neuesten Service Packs herunter, damit Ihr System weiterhin sicher und effizient läuft.

VORSICHT: Wenn Sie die Software der NAS-Lösung von Version 1.x auf Version 2.x aktualisieren, verwenden Sie das Service Pack mit dem Dateinamenformat DellFS-2.0.xxxx-SP.sh. Wenn Sie die Software der NAS-Lösung von Version 2.0 und höher aktualisieren, verwenden Sie das Service Pack mit dem Dateinamenformat DellFluidFS-2.0.xxxx-SP.sh.

VORSICHT: Verändern Sie nicht den Dateinamen des Service Packs.

VORSICHT: Durch die Installation eines Service Packs starten die NAS-Controller während des Installationsvorgangs neu. Dies kann zu Unterbrechungen in den Client-Verbindungen führen. Es wird darum empfohlen, Service Packs während der eingeplanten Wartungszeitfenster zu installieren.

VORSICHT: Die Installation eines Service Packs ist nicht rückgängig zu machen. Ihr System kann nicht auf eine ältere Version zurückgesetzt werden, wenn es einmal aktualisiert ist.

So installieren Sie ein Service Pack:

1. Laden Sie das Service Pack über die folgende URL herunter: **dell.com/support/downloads**.
2. Wählen Sie im NAS-Manager **Clusterverwaltung** → **Wartung** → **Service Pack** aus.
   Die Seite **Service Pack** wird angezeigt.
3. Klicken Sie auf **Durchsuchen**.
4. Navigieren Sie zum neuesten Service Pack und klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Hochladen**.
6. Nachdem die Service Pack-Datei im System hochgeladen ist, klicken Sie auf **Installieren**.

Erweitern der NAS-Cluster-Speicherkapazitäten

Erweitern des NAS-Pools auf der Dell PowerVault NX3500/NX3600/NX3610 NAS-Lösung

Sie können die Speicherkapazitäten Ihres Systems erweitern, ohne die Dienste für die Clients zu beeinträchtigen. Der Prozess während eines Zeitraums, der von der Gesamtzahl der vorhandenen und hinzugefügten LUNs, der gesamten Speicherkapazität und der Arbeitsauslastung des Systems abhängt. Sie können zusätzliche LUNs aus der Speicherkapazität, die bereits auf Ihrem Speicher-Array verfügbar ist, zur NAS-Cluster-Lösung hinzufügen.

Das MD-Speicher-Array muss über zusätzliche Kapazitäten zum Zuweisen der NAS-Cluster-Lösung verfügen. Weitere Informationen zu Laufwerksgruppen und Erweiterungen von virtuellen Laufwerken finden Sie im Administrator's Guide (Administratorhandbuch) des Modular Disk Storage Manager unter **dell.com/support/manuals**.

So erweitern Sie die Speicherkapazitäten der NAS-Cluster-Lösung:

1. Starten Sie **NAS Manager** auf Ihrer Management-Station und melden Sie sich als **admin** an.

   ANMERKUNG: Standardmäßig ist das admin-Passwort **Stor@ge!**.

2. Wählen Sie **Clusterverwaltung → Wartung → LUNs erweitern** aus.
   Die Seite **(LUNs erweitern** wird angezeigt.
3. Klicken Sie auf **LUNs erweitern** unten rechts auf der Seite.
   Die Seite **Status** wird angezeigt und informiert über den Fortschritt der LUN-Erweiterung.
4. Klicken Sie auf **Fertigstellen**.

Erweitern des NAS-Pools in der FS8600 NAS-Lösung

1. Melden Sie sich auf dem **Enterprise Manager Client** an.
2. Klicken Sie auf **Storage (Speicher)** im linken Fensterbereich.
3. Klicken Sie auf **Expand NAS Pool (NAS-Pool erweitern)** im oberen Menü.
4. Geben Sie die Größe des NAS-Pools ein.

   ANMERKUNG: Die Obergrenze liegt bei 512 TB pro Storage Center. NAS-Pools können nur erweitert, nicht jedoch verkleinert werden.

ANMERKUNG: Der NAS-Pool kann auch durch Hinzufügen eines zweiten Storage Centers erweitert werden. Weitere Informationen zum Hinzufügen eines zweiten Storage Centers-Arrays zum FluidFS-Cluster finden Sie in *Enterprise Manager Administrator's Guide (Administratorhandbuch des Enterprise Managers)*.

Hinzufügen von LUNs zur PowerVault NX3500/NX3600/NX3610 NAS-Cluster-Lösung

Für diesen Vorgang ist es erforderlich, dass das MD-Speicher-Array über zusätzliche Kapazitäten verfügt, um die NAS-Cluster-Lösung aufzunehmen. Weitere Informationen zu Laufwerksgruppen und virtuellen Laufwerkserweiterungen im MD-Array finden Sie im MD Series Storage Array Administrator's Guide (Administratorhandbuch des MD Series Speicher-Array) unter **dell.com/support/manuals**.

WARNUNG: FluidFS unterstützt maximal 32 LUNs mit einer LUN-Maximalgröße von 32 TB; diese Grenzwerte können jedoch mithilfe von MDSM überschritten werden. Das Überschreiten der Höchstzahl an unterstützten LUNs kann zu Problemen bei Leistung und/oder Zugriff führen.

ANMERKUNG: Es wird empfohlen, weniger, aber dafür größere LUNs anstatt mehr, aber dafür kleinere LUNs zu verwenden. Erweitern Sie die vorhandenen LUNs, falls möglich, um die NAS-Poolgröße zu steigern.

1. Erstellen Sie in MDSM zusätzliche virtuelle Laufwerke in Paaren.

   ANMERKUNG: Weitere Informationen finden Sie im MD Series Storage Array Administrator's Guide (Administratorhandbuch des MD Series Speicher-Arrays) unter **dell.com/support/manuals**.

2. Fügen Sie die virtuellen Laufwerke, die Sie soeben erstellt haben, der **Hostgruppe** des Clusters hinzu.
3. Starten Sie den **NAS Manager** auf Ihrer Management-Station und melden Sie sich als **admin** an.

   ANMERKUNG: Standardmäßig ist das admin-Passwort **Stor@ge!**.

4. Wählen Sie **Clusterverwaltung → Wartung → LUNs hinzufügen.**
   Die Seite braucht eventuell einige Minuten, bis sie anzeigt. Die iSCSI-Ermittlung wird für alle in der NAS-Cluster-Lösung aufgenommenen virtuellen Laufwerke/LUNs vorgenommen.

Jede LUN kann mit ihrem World Wide Name identifiziert werden. Im NAS-Manager bekommt der World Wide Name einer LUN ein Präfix von Dell FluidFS. Die eindeutige Kombination aus Zahlen und Zeichen nach dem Präfix ist der World Wide Name.

Die Seite **LUNs hinzufügen** wird angezeigt.

5. Klicken Sie auf **LUNs hinzufügen**, um die neuen LUNs der NAS-Cluster-Lösung hinzuzufügen. Das System führt eine schrittweise Dateisystemformatierung auf den neuen LUNs durch.

   Dieser Prozess nimmt je nach Größe und Anzahl der LUNs einige Zeit in Anspruch.

   Nach Abschluss dieses Vorgangs kann der neue Bereich verwendet werden.
6. Klicken Sie auf **Fertigstellen**.

Diagnose ausführen

Über das Ausführen von Diagnoseprogrammen erhalten Sie Unterstützung bei der Fehlerermittlung, bevor Sie sich für weitere Unterstützung an Dell wenden.

Die folgenden Diagnoseoptionen sind für Ihre Lösung verfügbar:

- Onlinediagnose
- Offline-Diagnose

Onlinediagnose

Die Onlinediagnose kann ausgeführt werden, während das System noch online ist und Daten übermittelt. Die folgenden Diagnoseoptionen sind verfügbar:

- **Allgemein**
- **Dateisystem**
- **Netzwerkbetrieb**
- **Leistung**
- **Protokolle - Protokolle sammeln**
- **Protokolle - Einzelner Client**
- **Protokolle - Einzelne Datei**

So führen Sie diese Diagnosen aus:

1. Wählen Sie **Cluster Management** → **Maintenance (Wartung)** → **Diagnostics (Diagnose).**

   Die Seite **Diagnostics (Diagnose)** wird angezeigt.
2. Wählen Sie aus der Liste **Diagnostics type (Diagnosetyp)** die gewünschte Option aus und klicken Sie auf **Start**.

   Beim Abschluss der Diagnose werden Links zu dem komprimierten Archiv der Diagnosedateien angezeigt.
3. Klicken Sie auf den entsprechenden Link unter **Download diagnostics archive (Diagnosarchivdateien herunterladen)**.

   Eine Nachricht fordert Sie dazu auf, die ausgewählte Diagnosedatei entweder zu öffnen oder zu speichern.
4. Klicken Sie auf **Done (Fertig)**.

Offline-Diagnose

ANMERKUNG: Schließen Sie eine Tastatur und einen Monitor an, bevor Sie die folgenden Schritte ausführen:

Für die Offline-Diagnose ist es erforderlich, dass Ihre Lösung offline ist, d.h. dass sie nicht produziert und keine Daten übermittelt. Dies ist in der Regel hilfreich bei der Fehlerbehebung von Hardware-Problemen auf einer tiefen Ebene.

Für diese Diagnose werden die folgenden Dell-eigenen Tools verwendet:

- MP Memory
- Dell Diagnostics

MP Memory

MP Memory ein von Dell entwickeltes, auf MS DOS basierendes Tool zum Testen des Speichers. Dieses Tool ist bei großen Speicherkonfigurationen (über 4 GB) effizient. Es unterstützt sowohl Einzel- und Multiprozessorkonfigurationen als auch Prozessoren, die die Intel Hyper-Threading-Technologie verwenden.

MP Memory funktioniert nur auf Controllern, die auf einem Intel Prozessor basieren. Dieses Tool ergänzt die Dell 32-Bit-Diagnosetests und hilft bei der Bereitstellung von kompletten, umfassenden Diagnoseprogrammen auf dem Controller in einer Systemumgebung vor Inbetriebnahme.

Ausführen der integrierten Systemdiagnose

VORSICHT: Verwenden Sie die integrierte Systemdiagnose ausschließlich zum Testen des Systems. Der Einsatz dieses Programms auf anderen Systemen kann zu ungültigen Ergebnissen oder Fehlermeldungen führen.

1. Schließen Sie eine Tastatur, einen Monitor und eine Maus an den VGA-Port und die USB-Ports des Controllers an.
2. Drücken Sie zum Neustarten des Controllers kurz den Ein/Aus-Schalter (auf der Rückseite des Controllers), um den Controller auszuschalten. Drücken Sie den Ein/Aus-Schalter (auf der Rückseite des Controllers) erneut, um den Controller wieder einzuschalten.
3. Drücken Sie beim Hochfahren des Systems <F10>.
4. Verwenden Sie die Pfeiltasten, um **System Utilities (Systemprogramme) → Launch Dell Diagnostics (Dell-Diagnose starten)** auszuwählen.

   Das Fenster **ePSA Pre-boot System Assessment** (ePSA-Systemüberprüfung vor dem Start) wird angezeigt und listet alle Geräte auf, die im System erkannt wurden. Die Diagnose beginnt mit der Ausführung der Tests an allen erkannten Geräten.
5. Wenn der Vorgang abgeschlossen ist, entfernen Sie die Tastatur, den Monitor und die Maus vom Controller, und starten Sie den Controller neu.

Neuinstallieren der NAS-Cluster-Lösung

VORSICHT: Durch die Neuinstallation Ihrer NAS-Cluster-Software wird Ihr System zurück auf die Werkseinstellungen gesetzt. Alle Daten in der NAS-Lösung sind nach Durchführen dieses Vorgangs gelöscht.

ANMERKUNG: Installieren Sie die neuesten Service Pack-Aktualisierungen, nachdem Sie die Software der NAS-Lösung neu installiert haben.

ANMERKUNG: Schließen Sie eine Tastatur und einen Monitor an, bevor Sie die folgenden Schritte ausführen.

ANMERKUNG: Die Software der NAS-Cluster-Lösung kann nur auf unterstützter Hardware installiert werden.

So installieren Sie die Software der NAS-Cluster-Lösung neu:

1. Schalten Sie den Controller mithilfe des eingelassenen Ein/Aus-Schalters an der Rückseite des Systems AUS.
2. Schalten Sie den Controller mithilfe des eingelassenen Ein/Aus-Schalters an der Rückseite des Systems EIN.
3. Wenn das BIOS startet, drücken Sie <F11> um auf das Pop-up-Menü zuzugreifen.
4. Wählen Sie **Allgemeines Speichergerät**.
5. Wählen Sie aus dem Pop-up-Menü **FluidFS neu installieren** aus.
6. Geben Sie `resetmysystem` in die Eingabeaufforderung ein.

   Die Software startet die Installation automatisch.

7. Wenn die Softwareinstallation abgeschlossen ist, startet der Controller neu in den Standby-Modus.

Erweitern des NAS-Clusters

Sie können die Anzahl der Geräte in einem NAS-Cluster erweitern. Durch das Erweitern der Geräteanzahl in dem bestehenden Cluster wird die Gesamtleistung des NAS-Clusters gesteigert, da zusätzliche Client-Verbindungen zugelassen werden und der Datenfluss zwischen allen Controllern und Back-End-Speichern gleichmäßig verteilt wird. Das ursprüngliche Gerätepaar widmet nicht mehr länger seine gesamten Systemressourcen den NAS-Cluster-Vorgängen, sondern verringert die Verwendung seiner Systemressourcen, da andere Gerätepaare nun mit ihren Ressourcen ihren Teil beitragen.

Ein NAS-Gerät besteht aus zwei NAS-Controllern in einem Gehäuse. Sie können immer nur ein Gerät gleichzeitig hinzufügen. Je nach Version der Dell NAS-Lösung beträgt die Höchstzahl der Geräte in einer Cluster-Lösung vier (insgesamt acht Controller).

- Bei Dell PowerVault NX3600 ist die Höchstzahl der unterstützten Geräte 1 (2 Controller).
- Bei Dell PowerVault NX3610 ist die Höchstzahl der unterstützten Geräte 2 (4 Controller).
- Bei Dell Compellent FS8600 ist die Höchstzahl der unterstützten Geräte 4 (8 Controller).

Das Hinzufügen eines NAS-Gerätes ist ein problemloser Vorgang, der die aktuellen NAS-Cluster-Vorgänge nicht unterbricht. Nachdem das Gerät/die Geräte erfolgreich hinzugefügt wurden, werden die neuen Client-Verbindungen automatisch auf alle Controller verteilt, sodass ein effizienter Lastenausgleich zwischen allen Controllern gewährleistet wird.

Hinzufügen eines zusätzlichen NAS-Gerätes zum NAS-Cluster

Vor dem Hinzufügen eines zusätzlichen NAS-Gerätes stellen Sie sicher, dass:

- das zusätzliche NAS-Gerät im Rack eingebaut, verkabelt und EIN-geschaltet ist,
- die Service-Tags des Gerätes aufgenommen werden und
- neue IP-Adressen verfügbar sind (um sie dem zusätzlichen Gerät hinzuzufügen).

So fügen Sie ein zusätzliches NAS-Gerät hinzu:

1. Wählen Sie **Clusterverwaltung** → **Hardware** → **Assistent zum Hinzufügen von NAS-Geräten** aus.
   Der **Assistent zum Hinzufügen von NAS-Geräten** wird angezeigt.
2. Klicken Sie auf **Weiter**.
   Die Seite **Assistent zum Hinzufügen von NAS-Geräten (Netzwerk nach NAS-Geräten durchsuchen)** wird angezeigt.
3. Wählen Sie aus der Liste **Gehäusenummer** das NAS-Gerät aus, das Sie dem NAS-Cluster hinzufügen möchten und klicken Sie auf **Weiter**.
   Die Seite **Assistent zum Hinzufügen von NAS-Geräten (Subnetze)** wird angezeigt.
4. Verwenden Sie entweder die vorgeschlagenen IP-Adressen oder geben Sie neue für das zusätzliche Controllerpaar in allen erforderlichen Subnetzen an und klicken Sie auf **Weiter**.

   ANMERKUNG: Durch Klicken auf **Weiter** wird das nächste Subnetz angezeigt, bis die IP-Adressen für alle Subnetze angegeben sind.

   Nachdem die IP-Adressen für alle Subnetzbereiche eingegeben sind, werden Sie von einer Meldung darüber informiert, dass das System die eingegebenen IP-Adressen speichert.
5. Klicken Sie auf **Weiter**.
   Die Seite **Assistent zum Hinzufügen von NAS-Geräten (Controller zum Hinzufügen eines Gerätes vorbereiten)** wird angezeigt.

6. Um die erforderlichen Hardware-Bedingungen für die Erweiterung zu validieren, klicken Sie auf **Weiter**.

   Die Seite **Assistent zum Hinzufügen von NAS-Geräten (Systemvalidierung)** wird angezeigt. Verschiedene Komponenten und Parameter sind markiert und der Status jeder Komponente und jedes Parameters des neuen NAS-Gerätes wird angezeigt.
7. Um die Validierung zu überspringen, klicken Sie auf **Überspringen**.
8. Nachdem die Validierung abgeschlossen ist, klicken Sie auf **Erneut durchführen**, um die Validierung erneut zu starten, oder auf **Weiter**.

   Wenn Sie auf **Erneut durchführen** klicken, startet der Validierungsprozess erneut. Wenn Sie auf **Weiter** klicken, wird die Seite **Assistent zum Hinzufügen von NAS-Geräten (neues Mitglied anfügen)** angezeigt.
9. Klicken Sie auf **Weiter**.

   Die Seite **Assistent zum Hinzufügen von NAS-Geräten (Controllerverwaltung)** wird angezeigt. Die Controller auf dem neu hinzugefügten NAS-Gerät werden an das NAS-Cluster angefügt. Nachdem das NAS-Gerät erfolgreich dem Cluster angefügt wurde, wird die Seite **Assistent zum Hinzufügen von NAS-Geräten (LUN-Konfiguration)** angezeigt.

   - Für die PowerVault NX3500/NX3600/NX3610 Lösungen werden die neuen IQNs angezeigt. Erstellen Sie vom **Modulare Datenspeicherverwaltung** (MDSM) zwei neue virtuelle Hosts in der vorhandenen Host-Gruppe und verbinden Sie die neuen IQNs mit den virtuellen Hosts. Weitere Informationen finden Sie unter Erstellen eines Hosts in PowerVault NX3500/NX3600/NX3610.

     ANMERKUNG: Weitere Informationen zum Erstellen von virtuellen Hosts und IGN-Verbindungen finden Sie in Administrator's Guide (Administratorhandbuch) des Modular Disk Storage Manager unter **dell.com/support/manuals**.
   - Für die Dell Compellent FS8600 NAS-Lösung können Sie sich neben der **LUN-Konfiguration** auch die **Konfiguration der Fibre Channel-WWNs** ansehen.
10. Für die Dell Compellent FS8600 NAS-Lösung werden die WWN-Informationen für die neu hinzugefügten Controller in der obigen Tabelle unter FC WWNs aufgelistet.

    ANMERKUNG: Die neuen WWNs und definieren Sie vor dem Fortfahren die erforderlichen FC-Zonen-Bedingungen auf dem Fibre Channel-Switch.

    ANMERKUNG: Überspringen Sie den nächsten Schritt, wenn Sie der Dell PowerVault NX3610 NAS-Lösung ein zusätzliches Gerät hinzufügen.
11. Für die Dell Compellent FS8600 NAS-Lösung klicken Sie auf **Erneut prüfen**.

    Vergewissern Sie sich, dass die zusätzlichen Controller nun in der unteren Tabelle unter **Erreichbare Controller** aufgelistet sind. Wenn die Controller nicht aufgelistet sind, überprüfen Sie Ihre Speicherverbindungen durch Klicken auf die Schaltfläche **Speicherverbindung überprüfen** im **Enterprise Manager**.
12. Klicken Sie auf **Weiter**.

    Die Seite **Assistent zum Hinzufügen von NAS-Geräten (NAS-Gerät hinzufügen)** wird angezeigt.
13. Klicken Sie auf **Weiter**.

    Eine Meldung informiert Sie darüber, dass die Systemerweiterung abgeschlossen ist und zeigt die Anzahl der Geräte im NAS-Cluster an.

Erstellen eines Hosts in PowerVault NX3500/NX3600/NX3610

Bei PowerVault NX3500/NX3600/NX3610 NAS-Lösungen können Sie Hosts manuell mithilfe des Modular Disk Storage Manager (MDSM) erstellen.

So erstellen Sie einen Host in der Host-Gruppe, die Sie erstellt haben:

1. Klicken Sie mit der rechten Maustaste aud die von Ihnen erstellte Host-Gruppe.
2. Klicken Sie auf **Definieren → Host**.

   Das Fenster **Hostnamen angeben (Host definieren)** wird angezeigt.

3. Geben Sie den Namen des neuen Hosts unter **Hostname** ein.
4. Klicken Sie auf **Weiter**.
   Der Bildschirm **Host-Port-Kennungen angeben (Host definieren)** wird angezeigt.
5. Wählen Sie die Host-Port-Kennung aus der Liste **Hinzufügen durch Auswahl einer bekannten, nicht zugewiesenen Host-Port-Kennung**.
6. Geben Sie den Hostnamen in **Benutzerkennzeichnung** ein und fügen Sie an den Hostnamen die Erweiterung IQN an.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **Weiter**.
   Der Bildschirm **Host definieren** wird angezeigt.
9. Wählen Sie **Linux** aus der Liste **Hosttyp (Betriebssystem)** aus.
10. Klicken Sie auf **Weiter**.
    Der Bidlschirm **Vorschau (Host definieren)** wird angezeigt.
11. Klicken Sie auf **Fertigstellen**.
    Das Fenster **Erstellung erfolgreich (Host definieren)** wird angezeigt.
12. Klicken Sie auf **Ja**, um einen weiteren Host zu definieren.
    Wiederholen Sie Schritt 2 bis 10, um einen weiteren Host zu erstellen.

Austauschen eines Controllers in der NAS-Cluster-Lösung

Im Falle eines schweren Fehlers müssen Sie den Controller austauschen, wenn der Controller nicht wieder online geschaltet werden kann.

Voraussetzungen

Bevor Sie den Controller austauschen, stellen Sie Folgendes sicher:

- Sie können physisch auf die Controller zugreifen.
- Der Controller wurde als fehlerhaft diagnostiziert (wenn er durch einen neuen Controller ersetzt wird).

Schritte beim Austauschen eines Controllers:

- Trennen des Controllers
- Herausnehmen und Austauschen des Controllers
- Einsetzen eines neuen Controllers

Trennen des Controllers der FluidFS NAS-Cluster-Lösung

Um das Cluster in den Journal-Modus zu bringen, trennen Sie einen Controller, während Hardware ausgetauscht wird. So wird sichergestellt, dass das System ohne Ausfallzeit zurück in die Dienstfunktion gebracht werden kann.

Es kann erforderlich sein, den Controller unter den folgenden Umständen zu trennen:

- Ein Controller muss durch einen neuen Standby-Controller ausgetauscht werden.
- Der Administrator möchte einen betriebsbereiten Controller mit einem anderen (kritischeren) Cluster verbinden.

Trennen eines Controllers mithilfe des NAS Managers

1. Wählen Sie **Cluster Management (Clusterverwaltung) → Hardware → Controllers Management (Controllerverwaltung).**

Die Seite **Controllers Management (Controllerverwaltung)** wird angezeigt.

2. Wählen Sie aus der Liste der verfügbaren Controller den gewünschten Controller aus und klicken Sie auf **Detach (Abtrennen)**.

   Der ausgewählte Controller wird aus dem Cluster getrennt und ausgeschaltet. Dieser Vorgang dauert ca. 10 bis 15 Minuten.

Entfernen und Austauschen des Controllers der NAS-Cluster-Lösung

So entfernen Sie den Controller der NAS-Cluster-Lösung und tauschen ihn aus:

1. Kennzeichnen Sie alle Kabel korrekt, bevor Sie ihre Verbindung trennen.
2. Trennen Sie alle Kabelverbindungen auf der Rückseite des Controllers.
3. Entfernen Sie den fehlerhaften Controller aus dem Gerätegehäuse.
4. Setzen Sie den neuen Controller in das Gerätegehäuse ein.
5. Verbinden Sie alle Kabel mit dem neuen System.

   ANMERKUNG: Weitere Informationen zum Entfernen und Einsetzen von Controllern finden Sie in *Dell FluidFS NAS Solution Owner's Manual (Dell FluidFS NAS-System-Benutzerhandbuch)* unter **dell.com/support/manuals**.
6. Stellen Sie beim Einsetzen des Controllers sicher, dass die Kabel mit denselben Anschlüssen wie vorher verbunden werden.
7. Schalten Sie das neue System durch Einstecken des Stromversorgungskabels ein.

Anfügen des Controllers der NAS-Cluster-Lösung

Bevor Sie dieses Verfahren durchführen, stellen Sie sicher, dass der anzufügende Controller sich im Standby-Modus befindet und eigeschaltet ist. Sie können erkennen, dass der Controller eingeschaltet ist und sich im Standby-Modus befindet, wenn die Betriebsanzeige-LED ca. zweimal pro Sekunde grün aufblinkt.

Hinzufügen eines Controllers mithilfe des NAS Managers

1. Wählen Sie **Cluster Management (Clusterverwaltung)** → **Hardware** → **Controllers Management (Controllerverwaltung).**

   Die Seite **Controllers Management (Controllerverwaltung)** wird angezeigt.
2. Wählen Sie aus der Liste der verfügbaren Controller den gewünschten Controller aus und klicken Sie auf **Attach (Verbinden)**.

   ANMERKUNG: Die folgenden zusätzlichen Schritte sind bei Dell Compellent FS8600 NAS-Lösungen erforderlich.

   ANMERKUNG: Das Fabric-Zonen muss manuell auf dem Lichtwellenleiter-Switch aktualisiert werden.
3. Nach Abschluss des Hinzufügevorgangs zeigt der NAS Manager WWNs für den neu hinzugefügten Controller zum Fibre Channel-Switch-Zonen an.

   ANMERKUNG: Um die WWNs jederzeit mithilfe der CLI anzuzeigen, führen Sie den folgenden Befehl aus:
   ```
   system maintenance Luns configuration Fc-view
   ```

NAS Manager-Funktionen im heruntergestuften Modus

Wenn sich das NAS-Gerät im heruntergestuften Modus befindet, werden die folgenden Funktionen im NAS Manager entweder mit dem Status **View only (Nur Anzeige)** oder **Fail (Fehlgeschlagen)** angezeigt.

Lasche	Funktion	Status in degraded mode (Status im heruntergestuften Modus)
access (Zugriff)	Delete NAS volume (NAS-Volume Löschen)	Fehlgeschlagen
	NFS Exports (NFS-Exporte)	View only (Nur Anzeige)
	CIFS Shares (CIFS-Freigaben)	View only (Nur Anzeige)
Data Protection (Datenschutz)	Snapshot restore (Snapshot wiederherstellen)	Fehlgeschlagen
	Replication Partners (Replikationspartner)	View only (Nur Anzeige)
System Management (Systemverwaltung)	Time Configuration (Zeitkonfiguration)	View only (Nur Anzeige)
	Network Configuration (Netzwerkkonfiguration)	View only (Nur Anzeige)
	Subnets (Subnetze)	View only (Nur Anzeige)
	Local hosts (Lokale Hosts)	View only (Nur Anzeige)
	Static Routes (Statische Routen)	View only (Nur Anzeige)
	CIFS Configuration (CIFS-Konfiguration)	View only (Nur Anzeige)
	NIS/LDAP	View only (Nur Anzeige)
	Local users/groups (Lokale Benutzer/ Hosts)	View only (Nur Anzeige)
	Mapping (Zuweisung)	Zuweisung
	SNMP	View only (Nur Anzeige)
	Restore Cluster Config (Cluster-Konfiguration wiederherstellen)	Fehlgeschlagen
	Format (Formatieren)	Fehlgeschlagen
	Expand LUNS (LUNs erweitern)	Fehlgeschlagen
	Add LUNs (LUNs hinzufügen)	Fehlgeschlagen
	Add nodes (Knoten hinzufügen)	Fehlgeschlagen

8

Internationalisierung

Übersicht

Die NAS-Cluster-Lösung bietet volle Unicode-Unterstützung und ermöglicht so die Unterstützung mehrerer Sprachen gleichzeitig. Verzeichnisse und Dateinamen werden intern im Unicode-Format (UTF-8) gewartet und verwaltet.

Ungeachtet des Codierungstyps, den der Benutzer beim Erstellen einer Datei verwendet, speichert die NAS-Cluster-Lösung den Dateinamen bzw. Verzeichnisnamen im Unicode-Format. Wenn ein Nicht-Unicode-Client eine Datei in einer Freigabe, einer Bereitstellung oder einem Volume erstellt, wird die Datei von der NAS-Cluster-Lösung sofort in die angemessene Unicode-Darstellung umgewandelt.

Unicode-Unterstützung für Clients – Übersicht

Unicode-Clients können nativ auf Unicode-Verzeichnisse und -Dateien zugreifen, während andere, Nicht-Unicode-Clients (z. B. Windows 98-, Windows ME-, Mac OS 9.x-Clients) den Zugriff auf das Dateisystem durch die Fähigkeit der NAS-Cluster-Lösung erhalten, Codepage-Umwandlungen für Dateinamen, Verzeichnisse, Freigaben und Volumes gemäß der durch den Client verwendeten Codepage bereitzustellen.

Zu den nativen Unicode-Clients gehören:

- Microsoft Windows 7/Server 2008 R2
- Microsoft Windows Vista/Server 2008
- Microsoft Windows XP
- Microsoft Windows 2000/2003
- Microsoft Windows NT
- UNIX-basierte Clients

NFS-Clients

NFS-Clients können eine abweichende Codepage für verschiedene Freigaben konfigurieren und gleichzeitig Nicht-Unicode-Clients unterstützen, die verschiedene Sprachen verwenden.

CIFS-Clients

CIFS-Benutzer können eine Codepage für die Verwendung für alle Nicht-Unicode-Windows- und DOS-Clients konfigurieren.

ANMERKUNG: Die Web-Oberfläche bietet volle Unicode-Unterstützung. Um Unicode-Daten mithilfe der CLI anzuzeigen und zu verwenden, muss UTF-8 XTERM verwendet werden.

Unicode-Konfigurationsparameter

Die folgenden Konfigurationsparameter können Unicode-Zeichen enthalten.

Parameter	Unicode-Zeichen
CIFS	Server-Beschreibung
Basisfreigaben	Verzeichnisname
SNMP	Kontakt Standort
NFS Exports (NFS-Exporte)	Verzeichnisname
CIFS Shares (CIFS-Freigaben)	Name Verzeichnis Beschreibung Benutzergruppen

Unicode-Konfigurationsbeschränkungen

Im Folgenden erhalten Sie einen Überblick über die Unicode-Konfigurationsbeschränkungen:

- Dateigröße und Verzeichnisname
- Client-Kompatibilitätsprobleme
- Kompatibilitätsprobleme mit der japanischen Sprache

Dateigröße und Verzeichnisname

Die Größe der Datei und die Verzeichnisnamen sind auf 255 Bytes beschränkt. Bei der Verwendung von Unicode sind möglicherweise weniger als 255 Zeichen möglich, da jedes UTF-8-Zeichen zwischen 1 und 6 Bytes beansprucht.

Client-Kompatibilitätsprobleme

In manchen Fällen verwenden verschiedene Hersteller verschiedene UTF-8-Kodierungen für die gleichen Codepage-Einträge. Als Ergebnis werden diese Zeichen entweder nicht angezeigt oder durch andere Zeichen mit ähnlicher Form ersetzt.

Kompatibilitätsprobleme mit der japanischen Sprache

Administratoren, die die Befehlszeilenschnittstelle verwenden, können in den Konfigurationsparametern nur über die Webschnittstelle japanische Zeichen eingeben, da XTERM-Anwendungen, wie z.B. KTERM, die Verwendung von UTF-8-Zeichen nicht unterstützen.

In der folgenden Tabelle werden die Zeichen beschrieben, die mit dem japanischen Zeichensatz nicht kompatibel sind.

Zeichen	UNIX	Windows	Macintosh
Tilde (~)	U+301C (TILDE)	U+FF5E (TILDE VOLLER LÄNGE)	U+301C (TILDE)
DOPPELTE VERTIKALE LINIE (||)	U+2016 (DOPPELTE VERTIKALE LINIE)	U+2225 (PARALLEL ZU)	U+2016 (DOPPELTE VERTIKALE LINIE)
MINUS-ZEICHEN (-)	U+2212 (MINUS-ZEICHEN)	U+FF0D (BINDESTRICH VOLLER LÄNGE, MINUS-ZEICHEN)	U+2212 (MINUS-ZEICHEN)

Zeichen	UNIX	Windows	Macintosh
ÜBERSTRICH (¯)	U+FFE3 (MICRON VOLLER LÄNGE)	U+FFE3 (MICRON VOLLER LÄNGE)	U+203E (ÜBERSTRICH)
CENT-ZEICHEN (¢)	U+00A2 (CENT-ZEICHEN)	U+FFE0 (CENT-ZEICHEN VOLLER LÄNGE)	U+00A2 (CENT-ZEICHEN)
POUND-ZEICHEN (#)	U+00A3 (POUND-ZEICHEN)	U+FFE1 (POUND-ZEICHEN VOLLER LÄNGE)	U+00A3 (POUND-ZEICHEN)
NICHT-ZEICHEN (¬)	U+00AC (NICHT-ZEICHEN)	U+FFE2 (NICHT-ZEICHEN VOLLER LÄNGE)	U+00AC (NICHT-ZEICHEN)

Die NAS-Cluster-Lösung bietet eine besondere Codepage für den CIFS-Dienst, um die Übertragbarkeit zwischen Protokollen zu unterstützen. Die Verwendung dieser Option wird empfohlen, wenn Sie in einer Umgebung mit mehreren Protokollen arbeiten und Dateien und Verzeichnisse zwischen den Protokollen freigeben möchten.

Wenn der CIFS-Dienst so konfiguriert ist, dass er UTF-8-JP für die interne Codierung verwendet (UNIX-Codepage), so wird die nicht mit Windows kompatible Codierung der angemessenen UNIX/Mac OS-Codierung in der NAS-Cluster-Lösung zugeordnet. Dadurch wird sichergestellt, dass in jedem Fall korrekte und nicht korrekte Zeichen richtig zugeordnet werden.

9

Häufig gestellte Fragen (FAQs)

NDMP

1. Ist NDMP ein High Availability (HA)-Protokoll (ein Protokoll mit Hochverfügbarkeit? Was passiert, wenn eine Backup-Sitzung wegen eines Verbindungsfehlers unterbrochen wird?

   NDMP ist nicht HA. Eine Sitzung, die unterbrochen wird, ist beendet.

2. Wie funktioniert NDMP?

   Zu Beginn der NDMP-Sitzung wird ein Fluid File System (FluidFS)-Snapshot auf dem NAS-Zieldateisystem gemacht. Dieser Snapshot wird dann zur Datenverwaltungsanwendung (DMA) übertragen. Am Ende der Sitzung wird der Snapshot gelöscht.

3. Gibt es besondere Anweisungen für NDMP-Snapshots?

   Nein, es handelt sich dabei um reguläre, einmalige FluidFS-Snapshots.

4. Wer ist für die Bereitstellung des Lastenausgleichs zuständig?

   NDMP verfügt über keinen eingebauten Lastenausgleich. Eine DMA-Sicherung von 10 Volumes aus einer Client-VIP erzwingt alle 10 Sitzungen auf demselben Knoten. Verwenden Sie DNS-Roundrobin, um einen Lastenausgleich herzustellen, indem Sie einen DNS-Namen Ihres NAS-Gerätes in der DMA angeben.

5. Warum wird ein **ndmp_backup_xxxx_nodeX**-Snapshot auf meinem Volume angezeigt?

   Dies ist der Snapshot, den NDMP gemacht hat. Nach einer erfolgreichen Backup-Sitzung wird dieser Snapshot gelöscht. Wenn die Backup-Sitzung mit einem Fehler beendet wird, bleibt der Snapshot eventuell bestehen und kann manuell sicher gelöscht werden.

6. Wie viele DMAs können gleichzeitig ein Backup ausführen?

   In einer NAS-Cluster-Lösung können bis zu 16 DMAs eingerichtet werden. Es gibt keine Beschränkung bei der Anzahl der DMAs, die gleichzeitig ein Backup ausführen können.

7. Kann ich eine einzelne Datei wiederherstellen?

   Ja.

8. Kann ich ein altes Backup auf einem anderen NAS-Gerät wiederherstellen?

   Ja.

9. Kann ich ein Backup auf einem anderen NDMP-Gerät wiederherstellen?

   Die Daten von NDMP werden unformatiert gesendet, so dass sie durch das Zielgerät unterstützt werden.

10. Ist erkennbar, welche aktiver Backups derzeit verarbeitet werden?

    Ja. Über die NAS-Befehlszeilenschnittstelle sind die aktiven Backups erkennbar, die derzeit verarbeitet werden. Um die aktiven Backups anzuzeigen, die derzeit verarbeitet werden, führen Sie zum Auflisten den Befehl `data-protection ndmp active-jobs` aus.

11. Ist es möglich, NDMP zum Sichern eines Netzlaufwerks zu verwenden, das ich mit meinem Client verknüpft habe?

    Nein, NDMP kann nicht zum Sichern eines Netzlaufwerks verwendet werden.

Replikation

1. Wie funktioniert Replikation?

Die Replikation verwendet die FluidFS-Snapshot-Technologie und andere Berechnungen, um sicherzustellen, dass die replizierten Daten des virtuellen Volumes den Quelldaten des virtuellen Volumes zu dem Zeitpunkt entsprechen, an dem eine Replikation gestartet wurde. Nur die Blöcke, die seit der letzten Replikation geändert wurden, werden über das Client-Netzwerk übertragen.

2. Wie lange dauert die Replikationsaufgabe?

   Das ist abhängig von der Datenmenge auf dem virtuellen Volume und der Datenmenge, die seit dem letzten Replikationszyklus geändert wurde. Replikation ist jedoch eine Aufgabe auf einer tieferen Ebene und hat gegenüber Datenübermittlung Priorität. Der Administrator kann den Fortschritt der Replikation durch Klicken auf **Aktualisieren** überwachen. Das Fenster zeigt an, wie viel Prozent ungefähr des Vorgangs bereits abgeschlossen sind.

3. Ist es möglich, ein virtuelles Volume auf mehrere virtuelle Ziel-Volumes zu replizieren?

   Nein, nachdem ein Quell-Volume über eine Replikationsrichtlinie mit einem virtuellen Ziel-Volume verfügt, können weder das virtuelle Quell- noch das virtuelle Ziel-Volume für die Replikation verwendet werden.

4. Warum ist es nicht möglich, mit NFS oder CIFS auf das virtuelle Ziel-Volume zu schreiben?

   Nachdem eine Replikationsrichtlinie festgelegt wurde, ist das virtuelle Ziel-Volume schreibgeschützt. Wenn die Replikationsrichtlinie aufgelöst wird, ist das virtuelle Ziel-Volume nicht mehr schreibgeschützt.

5. Ich befinde mich auf dem Zielsystem, ich kann jedoch keine Replikation für mein virtuelles Ziel-Volume auslösen.

   Replikationen müssen auf dem virtuellen Ziel-Volume ausgeführt werden.

6. Ist es möglich, eine Replikation auf das gleiche System durchzuführen?

   Ja. Sie können eine Replikation von einem virtuellen Quell-Volume auf ein virtuelles Ziel-Volume auf dem gleichen System ausführen.

7. Wird die bi-direktionale Replikation zwischen beiden Systemen unterstützt?

   Ja. Sie können über eine Kombination aus Ziel- und Quell-Volumes auf Replikationspartnern verfügen.

8. Kann ich über mehrere Replikationspartnersysteme verfügen?

   Ja. mehrere Replikationspartner sind zulässig, Sie können jedoch nur ein virtuelles Quell-Volume auf mehrere Ziel-Volumes replizieren.

9. Wenn ich die Replikationsrichtlinie lösche, werde ich gefragt, ob ich die Konfiguration des Quell-Volumes auf die Konfiguration des Ziel-Volumes anwenden möchte. Was bedeutet das?

   Das bedeutet, dass Sie die Option haben, alle Ebeneneigenschaften des virtuellen Volumes (Sicherheitsstil, Kontingente, NFS-Exporte, CIFS-Freigaben usw.) auf das Ziel-Volume zu übertagen. Dies könnte von Ihnen gewünscht werden, wenn dieses virtuelle Volume die Stelle des virtuellen Quell-Volumes einnehmen soll, oder auch in anderen IT-Szenarien.

10. Mein Client-Netzwerk wird langsamer während der Replikation. Kann ich die Prioritäten von Replikationen gegenüber der Bedienung von Clients ändern?

    Dies ist so festgelegt. Replikation ist ein Prozess auf einer tieferen Ebene und hat Priorität vor der Bedienung von Clients. Der Administrator kann den Fortschritt der Replikation durch Klicken auf **Aktualisieren** überwachen. Das Fenster zeigt an, wie viel Prozent ungefähr des Vorgangs bereits abgeschlossen sind.

11. Warum kann ich die Replikationsrichtlinie auf dem virtuellen Ziel-Volume nicht ändern?

    Dies ist so festgelegt. Alle Konfigurationsänderungen müssen auf dem virtuellen Quell-Volume durchgeführt werden. Wenn das System, in dem sich das Quell-Volume befindet, nicht erreicht werden kann (wenn es ausgeschaltet ist, fehlt usw.), dann können Sie die Replikationsrichtlinie auf dem Ziel löschen.

10

Gesicherte Verwaltung

Wenn die gesicherte Verwaltung aktiviert ist, verschiebt sie den ganzen Verwaltungsdatenverkehr auf ein Subnetz, wodurch alle anderen Subnetze nur für den Clientzugriff (CIFS/NFS), die Replikation und den NDMP-Datenverkehr verfügbar sind. Dies hindert Benutzer auf Client (Daten-)-Zugriffssubnetzen daran, auf alle Verwaltungsfunktionen zuzugreifen. In FluidFS nehmen die unten erwähnten Anschlüsse nicht an der NFS/CIFS-Kommunikation teil, sind auf dem Clientnetzwerk aber sichtbar. Standardmäßig sind alle Verwaltungsanschlüsse auf allen Subnetzen offen, zusammen mit den anderen Anschlüssen, die für den Clientzugriff, die Replikation und NDMP nötig sind.

Für einige Benutzer muss der Verwaltungsdatenverkehr als privilegiert behandelt werden und darf nur auf einem Subnetz sichtbar sein. Das Subnetz, auf dem die gesicherte Verwaltung aktiviert ist, hat auch die nötigen offenen Anschlüsse für den Clientzugriff (CIFS/NFS), die Replikation und den NDMP-Datenverkehr.

Dienstleistung	Schnittstelle
Webdienste	80
Webdienste	443
FTP	44421
FTP	44422
SSH	22
SOAP	35451

Die Funktion der gesicherten Verwaltung ermöglicht die Aktivierung der **gesicherten Verwaltung** auf einen spezifischen Subnetz. Dadurch wird der ganze Verwaltungsdatenverkehr auf dieses spezifische Subnetz beschränkt. Die Ports dieser Gruppen hören nicht auf anderen Subnetzen ab. Wenn die gesicherte Verwaltung aktiviert ist, muss mit sicherem HTTP, **https://<managementVIP>/**, anstatt nur **http**. auf FluidFS NAS Manager (Web GUI) zugegriffen werden. Wenn die gesicherte Verwaltung aktiviert ist, ist Port 80 auf allen Subnetzen deaktiviert. Die gesicherte Verwaltung kann erst nach vollständiger Implementierung des Systems aktiviert werden.

- Die Funktion **gesicherte Verwaltung** wird über die FluidFS-Befehlszeilenschnittstelle verwaltet.
- So sichern Sie ein Subnetz:
  - Es muss vor dem Sicherungsvorgang bereits vorhanden sein
  - Es muss sich auf dem physischen Clientnetzwerk befinden.
  - Sie müssen sich von diesem Subnetz aus bei CLI anmelden.

Weitere Informationen über den CLI-Befehl für gesicherte Verwaltung finden Sie im *Dell FluidFS NAS Solutions CLI-Referenzhandbuch* unter **dell.com/support/manuals**.

ANMERKUNG: Die Aktivierung der gesicherten Verwaltung auf einem Subnetz unterbricht die Verbindung vorhandener Verwaltungssitzungen auf anderen Netzwerken nicht. Sie werden gewarnt, wenn solche Sitzungen vorhanden sind. Um sicherzustellen, dass es keine vorhandenen Sitzungen gibt, unterbrechen Sie die Verbindung der gemeldeten Sitzungen, deaktivieren die gesicherte Verwaltung und aktivieren dann die gesicherte Verwaltung. Überprüfen Sie, dass keine weiteren Verwaltungssitzungen gemeldet wurden.

Verwendete FluidFS NAS-Ports

Tabelle 2. Erforderliche Ports

FluidFS Portnummer	Protokoll	Dienstname
445	TCP und UDP	CIFS/SMB
427	TCP und UDP	SLP
2049 - 2049+(Domain-Nummer - 1)	TCP und UDP	NFS
5001 - 5001+(Domain-Nummer - 1)	TCP und UDP	mount (Einbinden)
5051 - 5051+(Domain-Nummer - 1)	TCP und UDP	Quota (Kontingent)
4050 - 4050+(Domain-Nummer - 1)	TCP und UDP	nlm (lock manager)
4000 - 4000+(Domain-Nummer - 1)	TCP und UDP	statd
111	TCP und UDP	portmap
44421	TCP	FTP
22	TCP	SSH
80	TCP	HTTP
443	TCP	Web-Verwaltung HTTPS
53	UDP	DNS

Tabelle 3. Verwendete Ports, basierend auf Erforderung

FluidFS Portnummer	Protokoll	Dienstname
138	UDP	NetBIOS
139	TCP	NetBIOS
88	TCP und UDP	Kerberos
464	TCP und UDP	Kerberos v5
543	TCP	Kerberos-Anmeldung
544	TCP	Kerberos-Remote-Shell
749	TCP und UDP	Kerberos-Verwaltung
135	TCP	AD - RPC
711	UDP	NIS
714	TCP	NIS
389	TCP und UDP	LDAP
3268	TCP	Globaler LDAP-Katalog
3269	TCP	Globaler LDAP-Katalog über TLS/SSL
636	TCP	LDAP über TLS/SSL

FluidFS Portnummer	Protokoll	Dienstname
123	UDP	NTP
161	UDP	SNMP-Agent
162	TCP	SNMP-Trap
10000	TCP	NDMP
10560-10568	TCP	Replikation
1344	TCP	Antivirus - ICAP
8004	TCP	ScanEngine Server WebUI (AV-Host)

11

Wie Sie Hilfe bekommen

Kontaktaufnahme mit Dell

ANMERKUNG: Dell bietet verschiedene Optionen für Online- und Telefonsupport an. Wenn Sie über keine aktive Internetverbindung verfügen, so finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Dell Produktkatalog. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar.

So erreichen Sie den Verkauf, den technischen Support und den Kundendienst von Dell:

1. Rufen Sie die Website dell.com/contactdell auf.
2. Wählen Sie auf der interaktiven Karte Ihr Land oder Ihre Region aus.
   Wenn Sie eine Region auswählen, werden die Länder der ausgewählten Region angezeigt.
3. Wählen Sie unter dem von Ihnen ausgewählten Land eine Sprache aus.
4. Wählen Sie Ihr Geschäftsfeld aus.
   Die Hauptsupportseite für das ausgewählte Geschäftsfeld wird angezeigt.
5. Wählen Sie gemäß Ihrem Anliegen die entsprechende Option aus.

Ausfindig machen der Service-Tag-Nummer

Ihr System wird durch einen eindeutigen Express-Servicecode und eine eindeutige Service-Tag-Nummer identifiziert. Der Express-Servicecode und die Service-Tag-Nummer befinden sich an der Rückseite des Systems; ziehen Sie das Informations-Tag aus. Mithilfe dieser Informationen kann Dell Support Anrufe an den richtigen Mitarbeiter weiterleiten.

Feedback zur Dokumentation

Wenn Sie uns Ihre Meinung zu diesem Dokument mitteilen möchten, schreiben Sie an documentation_feedback@dell.com. Alternativ können Sie auf den Link **Feedback** klicken, der sich auf allen Seiten der Dell-Dokumentation befindet, das Formular ausfüllen und auf **Submit** (Senden) klicken, um uns Ihre Rückmeldung zukommen zu lassen.