Dell FluidFS NAS Solutions
管理者ガイド

メモ、注意、警告

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

2013 - 03

Rev. A01

目次

1

はじめに

Dell FluidFS network attached storage (NAS)（Dell FluidFS ネットワーク接続ストレージ（NAS））ソリューションは、複数の NAS コントローラを 1 つのクラスタに集約し、1 つの仮想ファイルサーバーとして UNIX、Linux 、および Microsoft Windows クライアントに表示する高可用性ストレージソリューションです。

本書で使用される用語

用語	説明
バックアップ電源装置（BPS）	電源が失われた際に、バックアップ用のバッテリ電源を提供します。
クライアントアクセス VIP	クライアントが FluidFS NAS ソリューションにホストされた CIFS 共有および NFS エクスポートへのアクセスに使用する仮想 IP アドレスです。FluidFS NAS ソリューションは、複数クライアントによる仮想 IP（VIP）へのアクセスをサポートします。
NAS アプライアンス	クラスタ化された FluidFS NAS システムでペアとして設定された 2 台の NAS コントローラです。キャッシュデータは、アプライアンス内でペアになる NAS コントローラの間でミラーリングされます。
コントローラ（NAS コントローラまたはノード）	NAS アプライアンスの 2 つのプライマリコンポーネントで、それぞれが FluidFS NAS クラスタの別のメンバーとして機能します。
データ管理アプリケーション（DMA）	バックアップアプリケーションサーバーとしても知られています。
Dell PowerVault Modular Disk Storage Manager（MDSM）	MD シリーズアレイに付属の管理ソフトウェアです。
Enterprise Manager	Storage Center を使用する FluidFS の管理に必要なマルチシステム管理ソフトウェアです。
Fluid File System（FluidFS）	NAS コントローラにインストールされている、高パフォーマンスで拡張可能なファイルシステムソフトウェアです。
ホストポート ID	ネットワークでホストを識別する固有の ID です。
LAN またはクライアントネットワーク（プライマリネットワーク）	クライアントが NAS 共有またはエクスポートにアクセスする際に経由するネットワークです。FluidFS NAS ソリューションは、カスタマーの IT 環境およびこのネットワークを使用する NAS クライアントに接続されています。NAS ソリューションを管理するストレージ管理者が使用するネットワークでもあります。
NAS ストレージプール	NAS ストレージプールは、仮想ディスクの上位の仮想ストレージ層です。NAS ストレージプールのサイズは、FluidFS NAS クラスタに利用されるすべての仮想ディスクの合計です。
NAS ボリューム（NAS コンテナまたは仮想ボリューム）	NAS ストレージプール内のストレージの容量を消費する仮想ボリュームです。システム管理者は、CIFS 共有および NFS エクスポートを NAS ボリューム上に作成することができ、それらを認証済みのユーザーと共有することができます。FluidFS NAS ソリューションは、複数の NAS ボリュームをサポートします。

用語	説明
NAS レプリケーション	2 つの FluidFS NAS ソリューション間または、2 つの NAS ボリューム間のレプリケーションです。
NAS レプリケーションパートナー	レプリケーションアクティビティに参加している FluidFS NAS ソリューションです。
ネットワークデータ管理プロトコル（NDMP）	バックアップおよび復元に使用されるネットワークデータ管理プロトコルです。
ピアコントローラ	FluidFS NAS ソリューション内で特定の NAS コントローラとペアになる、ピア NAS コントローラです。
PowerVault MD3*xx*0i	Dell PowerVault MD3200i、MD3220i、MD3600i、および MD3620i iSCSI の各ストレージソリューションを指します。
Storage Center	FluidFS 接続用に少なくとも 1 つのファイバーチャネル HBA を含む、Series 40（シリーズ 40）または SC8000 Compellent Storage center（SC8000 Compellent ストレージセンター）ソリューションです。
Dell NAS Initial Deployment Utility（IDU）	FluidFS NAS ソリューションを最初に検出して設定するのに使用するセットアップウィザードです。このユーティリティは、初期セットアップだけに使用されます。
NAS Manager	ウェブベースのユーザーインタフェースです。NAS cluster（NAS クラスタ）ソリューションソフトウェアの一部で FluidFS NAS ソリューションの管理に使用されます。
FluidFS NAS ソリューション	完全に設定済みの、高い可用性と拡張性を備えた NAS アプライアンスで、NAS コントローラのペア、ストレージサブシステム、および NAS Manager で構成される NAS（CIFS および / または NFS）サービスを提供します。
スタンバイコントローラ	FluidFS ソフトウェアでインストールされる NAS コントローラですが、クラスタの一部ではないものです。たとえば、デルの工場から出荷された新しいコントローラまたは交換のコントローラは、スタンバイコントローラと見なされます。
SAN ネットワーク	ブロックレベルのトラフィックを伝送し、ストレージサブシステムが接続されるネットワークです。 **メモ:** このネットワークは、LAN またはクライアントネットワークから分離するように設定してください。

Dell FluidFS NAS ソリューションのアーキテクチャ

ストレージアレイと併用した FluidFS NAS ソリューションは、統合されたストレージソリューションを提供します。このソリューションは、ブロックおよびファイルストレージの両方へのアクセスを提供します。

FluidFS のクラスタ化された NAS ソリューションは、コントローラのペアとストレージアレイの搭載された NAS アプライアンスで構成されています。さらに、それぞれの NAS コントローラは、BPS により保護されています。BPS は電源に障害が発生している間、データを保護するために使用します。

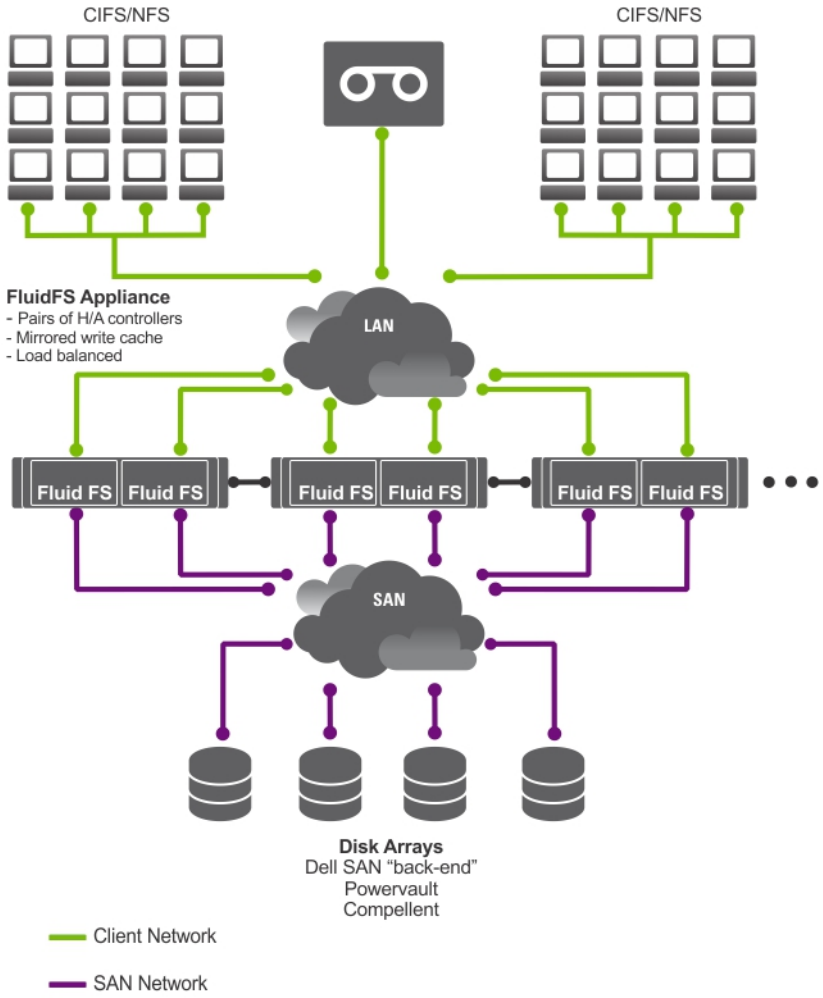

図 1. FluidFS NAS Cluster（FluidFS NAS クラスタ）ソリューションのアーキテクチャ

メモ: Dell Compellent FS8600 NAS ソリューションは、追加の内部ネットワークを使用していますが、この図には示されていません。

FluidFS でのポートラベル

イーサネットポートが接続を失うと、FluidFS はケーブルが外れどのポートの接続が解除されたかを示すイベントを生成します。ポートラベルは、常に **eth** の後に数字が続く形式、例えば、**eth0** のようになっています。次の図は、FluidFS イベントログのレポートとして、物理ポートが **eth** ラベルとどのように関連しているかを示しています。

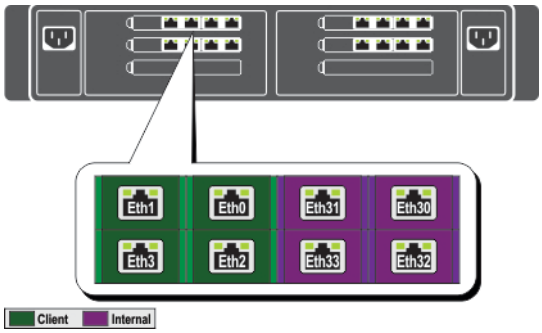

図 2. 1GbE システムのポートラベル

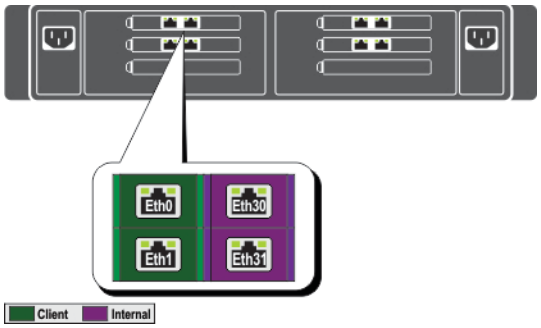

図 3. 10GbE システムのポートラベル

主な機能

NAS cluster（NAS クラスタ）ソリューション

- 管理者が、アプリケーションやユーザーに影響を及ぼすことなく、必要に応じて既存の容量を拡張し、パフォーマンスを改善するために役立ちます。
- システム運用およびストレージ管理を日々行うストレージ管理者のために、ストレージ管理機能を提供。
- データへの単一のインタフェースを作成する分散ファイルシステム。
- 単一のファイルシステムにテラバイト単位のデータを保存できます。
- 容量を動的に拡張できます。
- 一元化された使いやすいウェブベースの NAS 管理コンソール。
- オンデマンドの仮想ストレージプロビジョニング。
- ユーザーがアクセス可能なポイントインタイムのスナップショットを生成できます。
- Microsoft Windows、Linux、UNIX、および Mac ユーザーとのファイル共有が可能です。
- 柔軟で自動化されたオンラインレプリケーションおよび災害復旧機能を提供。
- パフォーマンス監視および容量計画機能を内蔵。

NAS cluster（NAS クラスタ）ソリューションのビュー

NAS cluster（NAS クラスタ）ソリューションには、ユーザーアクセス権限に応じてクライアントまたはシステム管理者としてアクセスできます。

メモ: CLI および NAS Manager の両方に同時にログオンしないことをお勧めします。

クライアントビュー

NAS cluster（NAS クラスタ）ソリューションは、1 つのファイルシステム、IP アドレス、および名前を持つ単一のファイルサーバーとしてクライアントに表示されます。NAS cluster（NAS クラスタ）ソリューションのグローバルファイルシステムは、パフォーマンスを制限することなく、すべてのユーザーに対して同時にサービスを提供します。エンドユーザーは各自のオペレーティングシステムの NAS プロトコルを使用して、NAS cluster（NAS クラスタ）ソリューションに接続できます。

- Linux および UNIX ユーザーは NFS プロトコルを使用します。
- Windows ユーザーは CIFS プロトコルを使用します。

管理者ビュー

管理者として CLI または NAS Manager のいずれかを使用すると、プロトコルの設定やユーザーの追加、パーミッションの設定といったシステム設定を指定または変更できます。

NAS Manager では、標準的なインターネットブラウザを使用してシステム機能にアクセスすることができます。

システムコンポーネント

NAS cluster（NAS クラスタ）ソリューションシステムは、次のコンポーネントで構成されます。

- ハードウェア
  - 1 つまたは複数の NAS アプライアンス
  - ストレージアレイ
- ネットワーク
  - SAN ネットワーク
  - 内部ネットワーク
  - LAN またはクライアントネットワーク

NAS アプライアンス

FluidFS NAS ソリューションは、クラスタとして構成された 1 つまたは複数の NAS アプライアンスで構成されます。各アプライアンスは、アクティブ-アクティブ設定の NAS コントローラのペアで構成されます。このような構成によって冗長性が確保されます。コントローラは、クライアント接続の負荷バランシング、読み取り / 書き込み操作の管理、およびキャッシングを行い、サーバーおよびワークステーションとのインタフェースを提供します。クラスタは、グローバルな名前空間を持つ単一のストレージプールです。クラスタへのアクセスには仮想 IP（VIP）が使用されます。

読み取り / 書き込み操作は、ミラーリングされた RAM を経由して処理されます。ペアになっている NAS コントローラ間でキャッシュデータをミラーリングすることで、データの整合性を完全に維持しながら、クライアントの要求に迅速に応答することができます。キャッシュから永続的ストレージへのデータ転送は、最適化されたデータ配置スキームを使用して非同期で実行されます。

ファイルシステムはキャッシュを効率的に使用して、高速かつ信頼性の高い書き込み / 読み取り処理を実行します。まず、キャッシュ内でファイルの書き込みまたは変更が実行されます。その後、ピアコントローラのキャッシュにデータがミラーリングされます。この機能により、すべてのトランザクションが確実に複製され、安全性が維持されます。

各コントローラには BPS が内蔵されており、電源障害が発生した場合は、コントローラに最低 5 分間連続して電力を供給します。コントローラは BPS のバッテリステータスを定期的に監視し、BPS が通常動作用に最小レベルの電力を維持していることを確認します。BPS には、コントローラが安全にシャットダウンできるだけの十分な電力が蓄電されています。

BPS によって、コントローラは NVRAM をキャッシュとして使用することができます。BPS を使用することで、コントローラの電源が停止しても、クラスタ化されたソリューションには、すべてのデータをキャッシュからディスクに書き込むだけの十分な時間があります。

ストレージアレイ

コントローラは、RAID サブシステムであるストレージアレイに接続しています。RAID ストレージサブシステムは、単一障害点を解消するように設計されています。ストレージサブシステムの各アクティブコンポーネントは、冗長でホットスワップ可能です。ソリューションは、RAID 1/10、RAID 5、および RAID 6 を含む標準の RAID 構成をサポートしています。

SAN ネットワーク

SAN ネットワークは、NAS cluster（NAS クラスタ）ソリューションに不可欠な要素です。コントローラペアは SAN ネットワークに常駐し、Dell PowerVault NX3500/NX3600/NX3610 の場合は iSCSI プロトコル、Dell Compellent FS8600 の場合はファイバチャネルプロトコルを使用してストレージサブシステムと通信します。

相互接続ネットワーク

相互接続ネットワークは、2 つの独立したネットワークで構成されます。相互接続ネットワークはハートビートメカニズムとして機能し、コントローラ間の内部データ転送を可能にします。2 台のコントローラを備えたシステムでは、スイッチは使用されません。3 台以上のコントローラを備えた構成の場合は、相互接続ネットワークに 2 つのスイッチが含まれます。すべての Dell Fluid File System（FluidFS）コントローラは、両方の相互接続スイッチに接続されています。これらのコントローラはデュアルリンクを採用し、冗長性と負荷バランシングを実現しています。

データを均等に分散し、高可用性を維持するには、Dell FluidFS クラスタシステムの各コントローラが、システム内にある他のすべてのコントローラにアクセスできなければなりません。相互接続ネットワークによってこの目的は達成できます。相互接続ネットワークでは、ハートビートモニタ、データ転送、コントローラのキャッシュ間における情報のミラーリング、システム内のすべての LUN での均等なデータ分散などの Dell FluidFS クラスタリングを可能にする接続が可能です。

LAN またはクライアントネットワーク

初期設定後、仮想 IP（VIP）アドレスで NAS cluster（NAS クラスタ）ソリューションとクライアントまたは LAN ネットワークを接続します。

VIP アドレスを使用すると、クライアントは単一のエンティティとして NAS cluster（NAS クラスタ）ソリューションにアクセスできるので、ファイルシステムへのアクセスが可能になります。VIP アドレスを使用して、NAS cluster（NAS クラスタ）ソリューションはコントローラ間の負荷バランシングを実行でき、コントローラの故障時にもサービスを継続させることができます。

LAN またはクライアントネットワークは、各コントローラにポートを備え、これによって LAN またはクライアントネットワークスイッチに接続されます。NAS cluster（NAS クラスタ）ソリューションは、NAS 管理 VIP 上の LAN またはクライアントネットワークを使用して管理されます。ルーティングされたネットワークの場合、システムで使用できる VIP の数は、ユーザーが使用できるクライアントポートの数によって決まります。たとえば、4 つのアプライアンスを備えた Dell Compellent FS8600（1 GbE）は 32 個のクライアント VIP を使用できます。フラットなネットワークの場合、クライアント VIP は 1 つだけで十分です。

その他の情報

警告: システムに付属のマニュアルで安全および認可機関に関する情報を参照してください。保証に関する情報は、この文書に含まれている場合と、別の文書として付属する場合とがあります。

- 『*Getting Started Guide*』（はじめに）では、お使いのシステムのセットアップ、および仕様の概要を説明しています。
- 『*Owner's Manual*』（オーナーズマニュアル）では、ソリューションの機能、システムのトラブルシューティング方法、およびシステムコンポーネントの取り付けまたは交換方法について説明しています。
- ラックソリューションに付属のマニュアルでは、システムをラックに取り付ける方法について説明しています（必要な場合）。
- 『*Deployment Guide*』（展開ガイド）では、ハードウェア展開、および NAS アプライアンスの初期展開についての情報を説明しています。
- 『*System Placemat*』（システム配置マット）では、お使いの NAS ソリューションのハードウェアのセットアップ方法およびソフトウェアのインストール方法についての情報を説明しています。
- 『*Online Help*』（オンラインヘルプ）では、ソフトウェアの設定および管理についての情報を説明しています。オンラインヘルプは、システムと統合されていて、NAS Manager ウェブインタフェースからアクセスできます。
- システムに付属のメディアには、OS、システム管理ソフトウェア、システムアップデート、およびシステムと同時に購入されたシステムコンポーネントに関するものを含め、システムの設定と管理用のマニュアルとツールが収録されています。
- 本書で使用されている略語や頭字語の正式名については、**dell.com/support/manuals** で『Glossary』（用語集）を参照してください。

メモ: アップデートには他の文書の内容を差し替える情報が含まれている場合がよくありますので、**www.dell.com/support/manuals** でアップデートがないかどうかを常に確認し、初めにお読みください。

2

FluidFS NAS ソリューションの監視

メモ: 本章の情報は NAS Manager を使用したファイル管理を指しています。以下を使用してブロックの管理と監視を行います。

- Dell PowerVault NX3500/NX3600/NX3610 NAS ソリューション用の **Dell PowerVault Modular Disk Storage Management**（MDSM）
- Dell Compellent FS8600 NAS ソリューション用の **Enterprise Manager**

NAS Manager の **Monitor**（モニタ）タブを使用して NAS ソリューションのステータスをモニタできます。ここでは、**Dashboard**（ダッシュボード）ページでシステムの全体のステータスを表示したり、クォータ使用レポートを参照したり、リモートのレプリケーションジョブのステータスレポートを受信したりすることができます。

それぞれの監視のページにアクセスするには、**Monitor**（モニタ）タブをクリックします。デフォルトで、**Dashboard**（ダッシュボード）ページが表示されます。

ダッシュボード

Dashboard（ダッシュボード）ページでは、システム全体のステータスが単一のビューに表示されます。**Dashboard**（ダッシュボード）ページには、リアルタイムおよび短期間のステータスを示す 5 つのセクションがあります。

- Status
- 容量
- Current Performance（現在のパフォーマンス）
- Recent Performance（最近のパフォーマンス）
- Load Balancing（負荷バランシング）

メモ: 画面の情報は、数秒間隔で自動更新されます。

メモ: 各セクションの詳細なステータスパラメータを表示するには、**Dashboard**（ダッシュボード）で各セクションをクリックします。

Status

Status（ステータス）セクションには、システムステータスと、ハードウェアコンポーネントのリストが表示されます。各ハードウェアコンポーネントタイプには、コンポーネントの合計数と問題のあるコンポーネント数が示されます。このリストには、コントローラとそれに関連付けられた NAS アプライアンスも含まれています。

容量

Capacity（容量）セクションには、Dell Fluid File System の総純容量を示す表と円グラフが表示されます。

現在のパフォーマンス

Current Performance（現在のパフォーマンス）セクションには、現在のネットワークスループットが表示されます。現在のネットワークスループットには、データの読み取り / 書き込みスループット（MBps）およびプロトコルごとの 1 秒あたりの読み取り / 書き込み動作の回数が含まれます。

最近のパフォーマンス

Recent Performance（最近のパフォーマンス）セクションには、過去 30 分間の読み取り / 書き込みスループットのグラフが表示されます。

負荷バランシング

Load Balancing（負荷バランシング）セクションには、コントローラのステータス、プロセッサ活用率、およびコントローラごとの接続数についてのリアルタイム情報を示した表が表示されます。

イベントビューアー

Events Viewer（イベントビューアー）では、システム内の情報イベントと主要イベントの両方を表示して、お使いの Fluid File System を監視することができます。

Events Viewer（イベントビューアー）ページにアクセスするには、**Monitoring**（監視）タブで **Events**（イベント）をクリックします。

Events Viewer（イベントビューアー）ページでは、次の操作を実行できます。

- イベントのフィルタリング
- イベントの並べ替え
- CSV ファイルへのイベントのエクスポート

イベントビューアでのイベントの表示

1. **Monitor → Overview → Events（モニタ > 概要 > イベント）**と選択します。
   Event Viewer（イベントビューア）ページが表示されます。
2. **Show**（表示）リスト、**events of**（イベントの種類）リスト、および **from**（イベント発生元）リストで適切なフィルタを選択し、**Show**（表示）をクリックします。
   選択したパラメータに応じて、イベントビューアの表にイベントが表示されます。
3. イベントを並べ替えるには、イベントビューアの表の列見出しをクリックします。
4. イベントの詳細について表示するには、イベントビューアの表で該当するイベントを選択します。
   選択したイベントの詳細が、**View Pane**（表示ペイン）に表示されます。
5. 表示されたイベントを CSV ファイルにエクスポートするには、**Export to CSV file**（CSV ファイルへエクスポート）をクリックします。
   新しいブラウザウィンドウが開き、イベントが CSV フォーマットで表示されます。
6. イベントを CSV ファイルにコピーして貼り付けるか、ウェブページを CSV ファイルとして保存します。

ネットワークパフォーマンス

Network Performance Over Time（経時ネットワークパフォーマンス）ページには、時間の経過に伴う Dell Fluid File System のパフォーマンスが表示されます。次の期間における FluidFS のネットワークパフォーマンスを表示できます。

- **過去 1 日**
- **過去 1 週間**
- **過去 1 か月**
- **過去 1 年間**

各タブをクリックして、該当する期間のネットワークパフォーマンスを表示します。ネットワークパフォーマンスについて、次の詳細情報を表示できます。

- **クライアントネットワークのスループット—読み取り**
- **クライアントネットワークのスループット—書き込み**
- **1 秒あたりの演算回数**
- **ネットワークの総スループット**

メモ: 経時ネットワークパフォーマンスの詳細については、『*Online Help*』（オンラインヘルプ）を参照してください。

負荷バランシング

負荷バランシングについて、次の詳細情報を表示できます。

- **経時**
- **クライアント接続**
- **CIFS 接続**

経時負荷バランシングの表示

1. **Monitor → Load Balancing → Over Time（モニタ > 負荷バランシング > 経時）** と選択します。
   Load Balancing Over Time（経時負荷バランシング）ページが表示されます。**Load Balancing Over Time**（経時負荷バランシング）には、**CPU Load**（CPU の負荷）、**CIFS Connections**（CIFS 接続）、**Read Throughput**（読み取りスループット）、および **Write Throughput**（書き込みスループット）が表示されます。
2. 適切なタブをクリックし、希望する期間の負荷バランシング情報を表示します。
   次の期間における負荷バランシング情報を表示できます。
   - **過去 1 日**
   - **過去 1 週間**
   - **過去 1 か月**
   - **過去 1 年間**
3. 負荷バランシング情報を表示したいコントローラを選択し、**Display**（表示）をクリックします。

   メモ: デフォルトでは、すべてのコントローラが選択されています。
4. 表示されたイベントを CSV ファイルへエクスポートするには、**Export to CSV file**（CSV ファイルへエクスポート）をクリックします。
   新しいブラウザウィンドウが開き、イベントが CSV フォーマットで表示されます。

5. イベントを CSV ファイルにコピーして貼り付けるか、ウェブページを CSV ファイルとして保存します。

クライアント接続

Client Connections（クライアント接続）ページでは、次の操作を実行できます。

- コントローラ間でのクライアントの分布状態を表示する。
- 特定のクライアントを 1 つのコントローラから別のコントローラへ手動で移行する。
- クライアントを自動的に移行するためのポリシーを設定する。

メモ: デフォルトでは、**Clients**（クライアント）タブにすべてのクライアント接続のリストが表示されます。

クライアント接続の表示

メモ: クライアント接続ページには、システムと同じサブネットに属するクライアント（ローカルクライアント）だけが表示されます。ルーター（またはレイヤ 3 スイッチ）経由でシステムにアクセスするクライアントはこのページに表示されず、代わりにそのルーターが表示されます。

1. **Monitor → Load Balancing → Client Connections（モニタ > 負荷バランシング > クライアント接続）** と選択します。
   Client Connections（クライアント接続）ページが表示されます。デフォルトでは、**Clients**（クライアント）タブにすべてのクライアント接続のリストが表示されます。
2. **Protocols**（プロトコル）および **Controller**（コントローラ）リストで適切なフィルタを選択します。
   クライアント接続テーブルに、選択したパラメータに応じたイベントが表示されます。
3. クライアント接続を並べ替えるには、クライアント接続テーブルの列見出しをクリックします。

別のコントローラへのクライアントの移行

ネットワーク負荷のバランスが適切でない場合、自動または手動操作によってコントローラ間でクライアントを移行することで、負荷のバランスを再調整できます。リスト内のクライアントまたはルーターを他のコントローラへ移行するかどうかを選択してください。

1. **Monitor**（モニタ）→**Load Balancing**（負荷バランシング）→**Client Connections**（クライアント接続）と選択します。
   Client Connections（クライアント接続）ページが表示されます。デフォルトでは、**Clients**（クライアント）タブにすべてのクライアント接続のリストが表示されます。
2. クライアント接続テーブルで、移行するクライアント接続を 1 つまたは複数選択し、**Assign Interface**（インタフェースの割り当て）をクリックします。
   Assign Interface（インタフェースの割り当て）ページが表示されます。
3. **Move to**（移行先）で特定のコントローラを移行先として選択するか、**Assigned Controller**（割り当て済みコントローラ）を選択します。
   - 選択したすべてのクライアントを特定のコントローラへ移行するには、リストからそのコントローラを選択します。
   - 故障したコントローラが復旧した後で、選択したすべてのクライアントを元のコントローラへ戻すには、Assigned Controller（割り当て済みコントローラ）を選択します。各クライアントに異なるコントローラを割り当てることができます。
4. **Interface**（インタフェース）で、適切なターゲットインタフェースを選択するか、システムがコントローラに自動的にターゲットインタフェースを割り当てるのを許可します。

   注意: クライアントが別のコントローラへ移行された場合、この操作によって CIFS 接続が切断されます。

5. **Automatic Rebalance**（自動再バランス）を有効にするには、**Allow these clients to migrate to other controllers when rebalancing the network load**（ネットワーク負荷の再バランス実行時に、これらのクライアントを別のコントローラへ移行させる）を選択します。
6. **Assign**（割り当て）をクリックします。

移行ポリシーの設定

コントローラのエラーの場合、システムはエラーの発生したコントローラから別のコントローラへ、それぞれの接続を自動的に移行します。これは、CIFS に対して **Migrate Manually**（手動で移行）ポリシーが選択されていない限り、CIFS クライアントの切断の原因になります。ただし、このオプションの選択は、クライアントの手動による移行が必要です。どのような場合でも CIFS クライアントの移行により、I/O は中断されます。Windows の **Cancel**（キャンセル）ボタンをクリックし、転送を再試行します。エラーの発生したコントローラを再起動する場合、クライアントを回復したコントローラに自動的に移行して戻すことによってシステムは負荷を再バランスします。この動作はフェイルバックと呼ばれます。

NFS を使用するクライアントは、ステートレスであり、フェイルバック中に影響を受けません。フェイルバック動作を最適化するために、システムはリカバリの移行に対して次のポリシーを提供しています。

- **Migrate Immediately**（ただちに移行） — 稼働時間中に CIFS クライアントが切り離される可能性があるものの、システムのバランスを常に良好に保ちます。
- **Migrate Automatically**（自動的に移行） — コントローラのエラーがごく短い期間の場合は、CIFS クライアントを切り離してシステムのバランスを常に良好に保ちます。このオプションは、エラーが長期間そのままであった場合、システムが数日間アンバランスな状態になる原因となります。

  このモードは、クライアントが短期エラーの間に新しいデータを作成しないため、短期のコントローラエラーに対処します。したがって、最良の方法はできる限り早急に再バランスすることです。エラーが 10 分よりも長い場合は、手動で再バランスされるまで、システムはアンバランスな状態のままです。
- **Migrate Manually**（手動で移行） — クライアントの移行は自動的に行われません。システムを再バランスするには、手動の操作が必要です。システムのフェイルオーバー後、再バランスするのに手動の操作が必要な場合、システムは適切な E メールメッセージをシステム管理者に送信します。

移行ポリシーを設定するには、次の手順を実行します。

1. **Monitor → Load Balancing → Client Connections（モニタ > 負荷バランシング > クライアント接続）** と選択します。

   Client Connections（クライアント接続）ページが表示されます。デフォルトでは、**Clients**（クライアント）タブにすべてのクライアント接続のリストが表示されます。
2. **Migration Policy**（移行ポリシー）をクリックします。

   Migration Policy（移行ポリシー）ページが表示されます。
3. それぞれの **Protocol**（プロトコル）で、**Client Network**（クライアントネットワーク）に対する適切な移行ポリシーを選択します。
4. **Save Changes**（変更の保存）をクリックします。

CIFS 接続の管理

現在の **CIFS 接続**を **CIFS Connections**（CIFS 接続）ページで表示できます。

CIFS 接続を管理するには、次の手順を実行します。

1. **Monitor → Load Balancing → CIFS Connections（モニタ > 負荷バランシング > CIFS 接続）** と選択します。

   CIFS Connection（CIFS 接続）ページが表示されます。
2. クライアントを CIFS プロトコルから切断するには、該当するクライアントを選択し、**Action**（操作）バーで **Disconnect**（切断）をクリックします。
3. 特定のコントローラ用の接続をすべて切断するには、該当するコントローラを選択し、**Action**（操作）バーで **Disconnect**（切断）をクリックします。

4. **Refresh**（更新）をクリックして、表示された情報を更新します。

ハードウェア

システム検証ステータスの表示

システムの検証を実行して、ハードウェアやネットワーク接続などのシステム構成を検証できます。

メモ: システムの検証は、CLI インタフェースを使用して実行することもできます。

システムの検証では、プロセッサ、監視の可否、NIC、IPMI、Ethernet 帯域幅、BPS の監視などについて情報を入手できます。

システム部品のステータスを更新するには、次の手順を実行します。

1. **Monitor → Hardware → System Validation（モニタ > ハードウェア > システムの検証）** と選択します。
   System Validation（システムの検証）ページが表示されます。
2. **Rerun**（再実行）をクリックして各システム部品でシステムの検証を再実行し、各システム部品のステータスを更新します。

詳細なコンポーネントステータスの表示

Component Status（コンポーネントのステータス）ページには、NAS cluster（NAS クラスタ）ソリューションの現在のステータスが表示されます。このページでは、各アプライアンスとそのコントローラについて、ステータス、内蔵ハードウェア、接続、および電源に関する情報を確認できます。

特定のコントローラまたはアプライアンスのステータスに関する詳細情報を表示するには、次の手順を実行します。

1. **Monitor → Hardware → Component Status（モニタ > ハードウェア > コンポーネントのステータス）**と選択します。
   Hardware Component Status（ハードウェアコンポーネントのステータス）ページが表示されます。
2. **Component**（コンポーネント）で該当するアプライアンスまたはコントローラを選択します。
   ウェブブラウザページが開き、選択したアプライアンスまたはコントローラの各コンポーネントのステータスが表示されます。
3. 新しいサンプル値が表示されるまで、**Sample Hardware Components**（サンプルハードウェアコンポーネント）をクリックして画面を更新します。

アプライアンスおよびコントローラの番号は 0 から始まります。Appliance0 には Controller0 と Controller1 が含まれ、Appliance1 には Controller2 と Controller3 が含まれ、以後同様に続きます。物理的なハードウェアを識別するには、**ApplianceX**（アプライアンス X）をクリックし、ポップアップウィンドウに表示されるサービスタグと、アプライアンス前面右の取っ手のステッカーに印字されたサービスタグを照合します。

容量

スペース使用率の表示

Space Utilization（スペース使用率）ページには、Dell Fluid File System のスペース使用率と、時間の経過に伴う Dell Fluid File System のスペース使用率が表示されます。

スペース使用率を表示するには、次の手順を実行します。

1. **Monitor → Capacity → Space Utilization（モニタ > 容量 > スペース使用率）** と選択します。

Space Utilization（スペース使用率）ページに、選択した期間におけるスペース使用率のテーブルが表示されます。デフォルトでは、**Current**（現在）のスペース使用率が表示されます。

2. 適切なタブをクリックして、希望する期間の負荷バランシングに関する情報を表示します。次の負荷バランシング情報を表示できます。
   - **過去 1 日**
   - **過去 1 週間**
   - **過去 1 か月**
   - **過去 1 年間**
3. スペース使用率を並べ替えるには、スペース使用率テーブルの列見出しをクリックします。

クォータ使用状況の表示

Quota Usage（クォータの使用状況）ページには、クォータが定義されていないユーザーも含めて、すべてのユーザーのクォータとその使用状況が表示されます。これには、システムから削除されたが使用量が残っているユーザーも含まれます。
クォータの使用状況を表示するには、次の手順を実行します。

1. **Monitor → Capacity → Quota Usage（モニタ > 容量 > クォータの使用状況）** と選択します。
   Quota Usage（クォータの使用状況）ページに、**すべての NAS ボリューム**のクォータ使用状況テーブルが表示されます。
2. **Show quota usage for NAS Volume**（NAS ボリュームのクォータ使用状況を表示）から適切な NAS ボリュームを選択するか、**All NAS Volumes**（すべての NAS ボリューム）を選択します。
   クォータ使用状況テーブルに、選択した NAS ボリュームの詳細なクォータ使用状況が表示されます。
3. クォータの使用状況を更新するには、**Refresh**（更新）をクリックします。

レプリケーション

NAS Replication（NAS レプリケーション）ページで NAS レプリケーションプロセスのステータスと進行状況を表示できます。
NAS レプリケーションポリシーのステータスと進行状況を表示するには次の手順を実行します。

1. **Monitor → Replication → NAS Replication（モニタ > レプリケーション > NAS レプリケーション）** と選択します。
   NAS Replication（NAS レプリケーション）ページに、複製元ボリューム、複製先ボリューム、または両方が Dell Fluid File System に存在するレプリケーションポリシーについて NAS レプリケーションの表が表示されます。
2. NAS レプリケーションを並べ替えるには、NAS レプリケーションの表の列見出しをクリックします。
3. レプリケーションポリシーの進行状況の履歴の詳細を表示するには、該当のレプリケーションポリシーのステータスをクリックします。

NDMP

NDMP Active Jobs（NDMP アクティブジョブ）ページに、NDMP のアクティブなジョブのステータスと進行状況を表示することができます。

3

ボリューム、共有、クォータの使用

User Access（ユーザーアクセス）タブでは、Dell Fluid File System をクライアントの視点で定義および管理することができます。

NAS ボリューム

NAS ボリュームはストレージプールのサブセットであり、容量の割り当て、データ保護、およびセキュリティ方式を管理する特定のポリシーを持っています。

NAS ボリュームは作成および設定することができます。管理者は、NAS プール全体を使用する 1 つの大規模な NAS ボリュームを作成するか、あるいは複数の NAS ボリュームを作成できます。いずれの場合も、これらの NAS ボリュームの作成、サイズ変更、または削除が可能です。

この項では、管理者が NAS ボリュームを使用して NAS cluster（NAS クラスタ）ソリューションストレージを割り当ておよび展開する方法について説明します。ユーザーが NAS ボリュームを使用できるようにするには、ユーザーがそれらのボリュームを個別に共有（エクスポート）する必要があります。ユーザーは各共有を明示的にマウントしなければなりません。

使用状況の考慮事項

複数の NAS ボリュームの定義を選択することによって、システム管理者はバックアップ、スナップショット、クォータ、およびセキュリティ方式などの異なる管理ポリシーをデータに適用できるようになります。使用するストラテジーに関係なく、ストレージは 1 つのストレージプールとして管理され、NAS ボリュームの割り当てられた容量を変更することによって、空き容量を NAS ボリューム間で容易に移行できます。

ストラテジーを選択する前に、次の要因を考慮してください。

- 一般的な要件
  - NAS ボリュームは論理的であり、システム容量に応じて容易に作成、削除、または増減による変更が可能です。
  - NAS ボリューム名は、230 文字以下にする必要があります。文字、数字、および下線（_）以外を含めることはできません。また文字か下線で始める必要があります。
  - NAS ボリュームはいくつでも作成可能ですが、合計容量がストレージの合計容量を超過することはできません。
  - ボリューム上で複数の共有を定義することにより、単一のボリュームにさまざまなタイプのデータを持たせることができます。
  - 仮想ボリュームは作成後にサイズを変更することができます。
  - NAS ボリューム 1 つの最小サイズは 20 MB です（ボリュームがすでに使用済みである場合、最小サイズは保存データとなります）。
  - NAS ボリュームの最大サイズは、未割り当て容量の残存量となります。
- ビジネス要件 — 分離または単一ボリュームの使用について会社またはアプリケーションの要件を考慮する必要があります。NAS ボリュームを使用して、要求に応じて部署にストレージを割り当てることができ、しきい値メカニズムを使用して、割り当てられた空き容量の終わりに近づくと部署に通知します。
- スナップショット — 各 NAS ボリュームには、保存されているデータタイプの保護に最も適した専用スナップショットスケジュールポリシーを使用することができます。
- セキュリティ方式 — 複数プロトコルの環境では、データを分けて、UNIX ベースのクライアントに対しては UNIX セキュリティ方式で、Windows ベースのクライアントに対しては NTFS で、NAS ボリュー

ムを定義することが有用な場合があります。これにより、システム管理者はセキュリティ方式をビジネス要件およびさまざまなデータアクセスパターンに合わせることができます。セキュリティ方式は、POSIX セキュリティおよび Windows ACL の両方を同じボリュームでサポートする混合に設定することもできます。

- クォータ — クォータは、NAS ボリュームごとにも定義されます。異なるクォータポリシーを異なる NAS ボリュームに適用することができ、それが適切である場合、システム管理者はクォータの管理に集中できるようになります。

使用例の一部は、コピー操作、リスト操作、および移動操作です。次の表に、さまざまな部署がある組織の例と NAS ボリュームの作成方法を示します。ボリュームは柔軟で、要求に応じて拡張や削減ができるため、正しいソリューションは、お客様の要件によって異なります。

表 1. NAS ボリュームの例

部署	優先アクセス管理コントロール	スナップショット	レプリケーション	バックアップ	CIFS または NFS クライアントおよび読み取り / 書き込み混合（一般的に 80/20）	既存データの毎時変化率（1% 以上は高）
ポストプロダクション	NFS	毎時	なし	毎週	20 – 20/80	1%
総務部および経理部	CIFS	なし	なし	毎週	10 – 50/50	なし
ブロードキャスト	混合	なし	なし	毎週	10 – 90/10	なし
報道	CIFS	日単位	なし	なし	5 – 10/90	およそ 5%
マーケティング	CIFS	日単位	あり	なし	5 – 50/50	なし

ソリューション 1

部署に基づいて NAS ボリュームを 5 つ作成します。システム管理者はストレージと管理を論理的に機能グループに分割します。このシナリオでは、部署の要件は全く異なり、部署の方針に沿って NAS ボリュームを論理的に作成するための設計をサポートします。

このソリューションには、次の利点があります。

- 論理的に NAS ボリュームを管理することが容易である。
- 部署ごとの要求にぴったりとマッチした NAS ボリュームを作成できる。

このオプションの欠点は、企業内の部署数が増えると NAS ボリュームの管理が難しくなる点です。

ソリューション 2

セキュリティ要件が似ている部署を NAS ボリュームでグループ化します。システム管理者は、NFS 用に 1 つ、CIFS 用に 1 つ、および混合用に 1 つの、3 つの NAS ボリュームを作成します。この利点は、NAS ボリュームが Windows と Linux の間で別々に動作することです。このソリューションには次の利点があります。

- NAS ボリューム内の全ファイルがバックアップされる。
- 不要なサービスが特定の部署に提供されている可能性があります。総務部および経理部のデータをバックアップするために、CIFS ボリュームが作成される場合、広報部および法務部でも必要がなくてもバックアップを取得します。

ソリューション 3

NAS ボリュームは機能に基づいて作成することもできます。このソリューションの欠点は、ユーザーマッピングが必要な点です。ユーザーは NTFS または UNIX のいずれかのセキュリティ方式を選択する必要があります。選択されたセキュリティ方式に基づいて、他のユーザー用に正しいマッピングが設定されます。

NAS ボリュームの管理

すべての NAS ボリュームでは、現在のステータスの表示、新規 NAS ボリュームの追加、既存 NAS ボリュームの削除または変更を行うことができます。

NAS ボリュームの追加

NAS ボリュームを追加するには、次の手順を実行します。

1. **User Access → NAS Volumes → Configuration（ユーザーアクセス > NAS ボリューム > 設定）**と選択します。
   NAS Volumes Configuration（NAS ボリュームの設定）ページに NAS ボリュームのリストが表示されます。
2. **追加** をクリックします。
   Add NAS Volume（NAS ボリュームの追加）ページが表示されます。
3. **NAS Volume**（NAS ボリューム）に NAS ボリューム名を入力します。
4. **NAS volume allocated space**（NAS ボリューム割り当て容量）に、この NAS ボリュームに割り当てられた容量を MB、GB、または TB 単位で入力します。

   メモ: NAS ボリュームの必要最小サイズは 20 MB で、最大サイズは使用可能な全容量に設定できます。
5. **Alert when used space reaches**（使用容量がこの値に達すると警告する）に、割り当てられた容量の割合を入力します。
6. **Send email alerts to administrator**（管理者に電子メールの警告を送信する）リストから、その電子メールアドレスにシステムが警告を送信する Dell Fluid File System 管理者を選択します。

   メモ: この機能は Dell Compellent FS8600 NAS ソリューションでは使用できません。詳細については、**Enterprise Manager** のマニュアルでこれらのソリューションにおける警告の処理方法を参照してください。
7. **Access time granularity**（アクセス時間の粒度）リストから、システムパフォーマンスの要件に基づいて、ファイルアクセスタイムスタンプの精度の解像度を選択します。
8. **File Access Security Style**（ファイルアクセスセキュリティ方式）リストから、NAS ボリュームのセキュリティ方式を選択します。
   NTFS、**MIXED**、または **UNIX** を選択できます。
9. **Default UNIX permissions of Windows files**（Windows ファイルのデフォルト UNIX パーミッション）で、Windows クライアントで作成される新規ファイルに対する UNIX パーミッションを定義します。
10. **Default UNIX permissions of Windows directories**（Windows ディレクトリのデフォルト UNIX パーミッション）で、Windows クライアントで作成される新規ディレクトリに対する UNIX パーミッションを定義します。
11. **Save Changes**（変更の保存）をクリックして NAS ボリュームを作成します。

NAS ボリュームの変更

特定の NAS ボリュームのパラメータを変更するには、次の手順を実行します。

1. **User Access → NAS Volumes → Configuration（ユーザーアクセス > NAS ボリューム > 設定）**と選択します。
   NAS Volumes Configuration（NAS ボリュームの設定）ページに NAS ボリュームのリストが表示されます。
2. 使用可能な NAS ボリュームのリストの **NAS Volume**（NAS ボリューム）列の下で該当の NAS ボリュームをクリックします。
   選択した NAS ボリューム用の **Edit NAS Volume**（NAS ボリュームの編集）ページが表示されます。
3. パラメータに必要な変更を行い、**Save Changes**（変更の保存）をクリックします。

   メモ: NAS ボリュームに割り当てられた容量を変更すると、新規割り当てはこのボリュームの使用済み容量（最小）と NAS cluster（NAS クラスタ）ソリューションの空き容量（最大）によって制限されます。

NAS ボリュームの削除

選択した NAS が削除されました。削除された NAS ボリュームの使用容量がバックグラウンドで再確保されます。

メモ: また、NAS ボリュームを正しく削除するには、NFS エクスポート、CIFS の共有、NAS レプリケーション、または削除されるその NAS ボリュームに対するすべてのリファレンスを先に削除しておく必要があります。

メモ: NAS ボリュームを削除すると、すべてのファイルとディレクトリだけでなく、共有、スナップショット定義などのプロパティも削除されます。 NAS ボリュームを削除すると、外部バックアップから再定義して復元しない限り、復元は不可能です。

NAS ボリュームを削除するには：

1. NAS ボリュームがマウントされていないことを確認し、関連するユーザーに切断されるとの通知を行います。
2. **User Access（ユーザーアクセス）→ NAS Volumes（NAS ボリューム）** → と選択します。
   NAS Volumes Configuration（NAS ボリュームの設定）ページに NAS ボリュームのリストが表示されます。
3. 使用可能な NAS ボリュームのリストから、関連する NAS ボリュームを選択し、**Delete（削除）**をクリックします。

共有およびエクスポート

ホストとユーザーに設定されたパーミッションに基づいて、ファイルシステム内のファイルへのアクセスパーミッションを定義できます。これは、NFS エクスポートと CIFS 共有を使用してディレクトリを共有することで実現されます。

NFS エクスポートの管理

NFS エクスポートは、UNIX/Linux ネットワーク間における効率的なファイルおよびデータ共有手段を提供します。

NFS エクスポートのリストを管理するには、**User Access**（ユーザーアクセス）タブの **Shares**（共有）の下で、**NFS Exports**（NFS エクスポート）を選択します。**NFS Exports**（NFS エクスポート）ページが表示され、現在定義されている NFS エクスポートのリストが表示されます。

NAS cluster（NAS クラスタ）ソリューションへの NFS エクスポートの追加

NFS エクスポートを追加するには、次の手順を実行します。

1. **User Access（ユーザーアクセス）→ Shares（共有）→ NFS Exports（NFS エクスポート）** と選択します。

   NFS Exports（NFS エクスポート）ページが表示されます。

2. **追加** をクリックします。

   Add NFS Export（NFS エクスポートの追加）ページが表示されます。このページは **General**（一般）および **Advanced**（詳細設定）の 2 つのタブで構成されています。デフォルトで、**General**（一般）タブが表示されます。

3. **NAS Volume**（NAS ボリューム）リストから、NFS エクスポートが配置される NAS ボリュームを選択します。

4. **Exported Directory**（エクスポートディレクトリ）に、エクスポートしたいディレクトリへのパスを入力するか、Browse（参照）アイコンをクリックして、適切なディレクトリへ移動します。

5. ディレクトリがない場合は、**Create the exported directory if it does not exist**（エクスポートディレクトリがなければ作成する）を選択します。

6. **Trust these users list**（信頼するユーザーのリスト）から、信頼済みのユーザーを選択します。

   メモ: 他のユーザーは guest として識別されます。

7. この NFS エクスポートへのアクセスを許可するクライアントマシンを定義します。次のオプションのいずれかを選択します。

   - **All Client Machines**（すべてのクライアントマシン）
   - **A Single Client Machine**（シングルクライアントマシン）— クライアントの **IP or Domain Name**（IP またはドメイン名）を入力する必要があります。
   - **All Client Machines in a Specific Network**（特定のネットワーク内のすべてのクライアントマシン）— クライアントの **IP Address and Netmask**（IP アドレスおよびネットマスク）を入力する必要があります。

     メモ: たとえば、ネットマスク `255.255.0.0` でサブネット `192.10.x.x/16` のすべてのメンバーに、アクセスを許可する場合、**IP address**（IP アドレス）フィールドに `192.10.0.0` を、**Subnet**（サブネット）フィールドに `255.255.0.0` を入力します。
   - **All Client Machines in a Specific Netgroup**（特定のネットグループ内のすべてのクライアントマシン）— クライアントの **Netgroup name**（ネットグループ名）を入力する必要があります。

8. **Allow access for**（アクセスの許可）で、共有に対する適切なアクセス権を選択します。**Read/Write**（読み書き）または **Read only**（読み取り専用）のどちらかを選択する必要があります。

   メモ: 共有に対するアクセス権が、特定のファイルに対して定義したものより厳密である場合、そのファイルのアクセス権は共有のアクセス権により優先されます。

9. **Advanced（詳細設定）** タブを選択します。

10. **Limit reported size**（レポートサイズの制限）で、NFS エクスポートのレポートサイズの制限を設定して、大きなファイルシステムを扱えないクライアントマシンによるアクセスを許可します。

    メモ: Limited reported size（レポートサイズの制限）を空白のままにした場合、レポートサイズは実際のサイズになります。

11. **Require secure port?**（セキュアポートの必要がある）で、**No**（いいえ）を選択して、非セキュアポート（1024 を超えるポート）経由のアクセスを有効にします。

12. **Comment**（コメント）に、NFS エクスポートに対するコメントまたは説明を追加します。

13. **変更の保存** をクリックします。

NFS エクスポートの変更

NFS エクスポートリスト内の特定の NFS エクスポートのパラメータを変更するには、次の手順を実行します。

1. **User Access（ユーザーアクセス）→ Shares（共有）→ NFS Exports（NFS エクスポート）** と選択します。

NFS Exports（NFS エクスポート）ページが表示されます。

2. 使用可能な NFS エクスポートリストの **Exported Directory（エクスポートされたディレクトリ）**列の下で、該当する NFS エクスポートをクリックします。
   選択した NFS エクスポート用の **Edit NFS Export（NAS エクスポートの編集）**ページが表示されます。
3. **General（一般）** and **Advanced（詳細設定）**タブで必要に応じてパラメータを変更し、**Save Changes（変更の保存）**をクリックします。

NFS エクスポートの削除

NFS エクスポートを削除するには、次の手順を実行します。

1. **User Access（ユーザーアクセス）** → **Shares（共有）** → **NFS Exports（NFS エクスポート）** と選択します。
   NFS Exports（NFS エクスポート）ページが表示されます。
2. 使用可能な NFS エクスポートのリストから、関連する NFS エクスポートを選択し、**Delete（削除）**をクリックします。

NFS を使用したアクセス

NAS ボリューム上の NFS エクスポートフォルダをマウントするには、クライアントシステムのシェルで、su コマンドを使用して root でログインし、次のコマンドを実行します。

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

ただし、UNIX や Linux の古いバージョンは、デフォルトで TCP を使用していません。次の mount コマンドでは正しい引数を指定しています。

NAS ボリューム上の NFS エクスポートフォルダをマウントするには、クライアントシステムのシェルで、su コマンドを使用して root でログインし、次のコマンドを実行します。

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

FluidFS バージョン 1 との下位互換性がある場合は、デフォルトの NAS ボリューム上の NFS エクスポートは次のコマンドでもマウントできます。

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

MAC から NAS ボリューム上の NFS エクスポートフォルダをマウントするには、次のコマンドを実行します。

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

メモ: 上記のパラメータは推奨パラメータです。詳細および他のオプションについては、マニュアルの mount コマンドのページを参照してください。

UDP または TCP 接続を許可するには、ファイアウォール設定を 2 つの方法で設定できます。

- ソース IP アドレスがクライアント VIP のものではなく、2 つのコントローラのどちらかからのものになるように、ファイアウォール設定を調整します。
- UDP 用のポート範囲を開放して、次のようにポートを許可します。

サービス名	FluidFS ポート
portmap	111
Statd	4000～4008
NFS	2049～2057

サービス名	FluidFS ポート
nlm（Lock Manager）	4050～4058
mount	5001～5009
Quota	5051～5059

CIFS 共有の管理

CIFS 共有は、Windows ネットワーク間における効率的なファイルおよびデータ共有手段となります。

CIFS 共有のプロパティおよびステータスの表示

既存の CIFS 共有の情報を表示するには、次の手順を実行します。

1. **User Access → Shares → CIFS Shares（ユーザーアクセス > 共有 > CIFS 共有）** と選択します。
   CIFS Share（CIFS 共有）ページが表示されます。
2. **Show CIFS Shares for NAS Volumes**（NAS ボリュームの CIFS 共有を表示）リストから特定の NAS ボリュームを選択するか、**All NAS Volumes**（すべての NAS ボリューム）を選択します。
   選択した NAS ボリュームに対応する CIFS エクスポートテーブルが表示されます。

CIFS 共有の追加

CIFS 共有を追加するには、次の手順を実行します。

1. **User Access（ユーザーアクセス） → Shares（共有） → CIFS Shares（CIFS 共有）** をクリックします。
   CIFS Share（CIFS 共有）ページが表示されます。
2. **CIFS Share**（CIFS 共有）ページで **Add**（追加）をクリックします。
   Add CIFS Share（CIFS 共有の追加）ページが表示されます。デフォルトでは、**General**（一般）タブが選択されています。
3. **NAS Volume**（NAS ボリューム）リストから適切な NAS ボリュームを選択します。
4. すべてのユーザーがアクセスできるディレクトリを設定するには、**General-access Share**（一般的なアクセス共有）を選択します。
   a) **Share name**（共有名）に CIFS 共有名を入力します。
   b) **Directory**（ディレクトリ）で、エクスポートするディレクトリのパスを入力するか、**Browse**（参照）ボタンをクリックし、該当するディレクトリに移動します。
   c) ディレクトリがない場合は、**Create the exported directory if it does not exist**（エクスポートディレクトリがなければ作成する）を選択します。
5. 各ユーザーが専用のディレクトリを持つユーザーベースのディレクトリを設定するには、**CIFS Share containing a user-based directory tree**（ユーザーベースのディレクトリツリーが含まれた CIFS 共有）を選択します。
   詳細については、「ホーム共有の作成」を参照してください。
   a) **Path template**（パステンプレート）に、CIFS 共有ボリュームのパステンプレート（ホームディレクトリの基準）を入力します。
   b) ホームディレクトリにユーザー名を追加する場合はユーザー、ホームディレクトリパスにプライマリグループおよびユーザーを追加する場合はグループ / ユーザーを選択します。
6. **Comment**（コメント）に、CIFS 共有に関する説明またはコメントを入力します。

注意: 外部のアンチウイルスサーバーを設定済みでなければ、Files should be checked for viruses（ファイルのウイルスチェックを行う）は選択しないでください。

7. **Files should be checked for viruses**（ファイルのウイルスチェックを行う）を選択し、アクセスを許可する前にファイルがウイルスに感染していないことを確認および検証するかどうか指定します。
8. **Advanced**（詳細設定）タブをクリックし、**Hide these files**（これらのファイルを非表示にする）に、共有が参照されている間は非表示にするファイルタイプを入力します。

   メモ: たとえば、.tmp 拡張子が付いたすべてのファイルを非表示にするには、*.tmp と入力します。
9. 未知のユーザーがゲストとして共有にアクセスするのを許可する場合は、**Allow guests**（ゲストを許可する）で **Yes**（はい）を選択します。

   メモ: General（一般）タブで **Files should be checked for viruses**（ファイルのウイルスチェックを行う）を選択した場合は、**Antivirus**（アンチウイルス）タブがアクティブになります。
10. **Antivirus**（アンチウイルス）タブをクリックし、**Select the policy for handling of virus-infected files:**（ウイルス感染したファイルの処理ポリシーを選択する）で次のいずれかを選択します。
    - **Do nothing**（何もしない）— クライアントへのアクセスを拒否しますが、ファイルは元の場所で維持します（アクセスは、ウイルスチェックを実行していない別の CIFS 共有を介してのみ許可されます）。
    - **Quarantine the file**（ファイルを検疫）— クライアントへのアクセスを拒否し、ファイルを NAS ボリュームのルートフォルダにある **.Quarantine** フォルダに移動します。
    - **Remove the file**（ファイルを削除）— クライアントへのアクセスを拒否し、ファイルを削除します。

    メモ: 指定されたオプションは、ウイルスに感染したファイルが特定され、アンチウイルスホストがそれを解決できない場合にシステムで適用されます。
11. **Specify which files should be checked for viruses**（ウイルスチェックを行うファイルを指定する）で次のいずれかを選択します。
    - **Scan all files except files with specific extensions（特定の拡張子を持つファイルを除き、すべてのファイルをスキャンする）**
    - **Scan files with specific extensions only（特定の拡張子を持つファイルだけをスキャンする）**

    メモ: 拡張子をカンマで区切ったリストを使用してください。たとえば、tmp, jpg, jpeg のように入力します。
12. **Exclude files in the following folders**（次のフォルダ内のファイルを除外する）に、アンチウイルスを行う必要がないフォルダ名を入力します。

    メモ: フォルダ名をカンマで区切ったリストを使用してください。フォルダ名にスペースまたはカンマが含まれる場合は、そのフォルダ名を二重引用符で囲みます。たとえば、/Marketing/temp*,/Secrets,"/All Finance" のように入力します。
13. **変更の保存** をクリックします。

    メモ: CIFS 共有の作成に Microsoft 管理コンソール（MMC）を使用しないでください。MMC は共有レベルパーミッション（SLP）の設定のみに使用します。

CIFS 共有の変更

CIFS 共有を一般的なアクセスディレクトリまたはユーザーベースのディレクトリのいずれかに設定すると、以後その設定を変更することはできません。特定の CIFS 共有のパラメータを変更するには、次の手順を実行します。

1. **User Access（ユーザーアクセス）** → **Shares（共有）** → **CIFS Shares（CIFS 共有）** をクリックします。
   CIFS Share（CIFS 共有）ページが表示されます。
2. 使用可能な CIFS 共有リストの **Share**（共有）列の下で、該当する CIFS 共有をクリックします。
   選択した CIFS 共有に対応する **Edit CIFS Share**（CIFS 共有の編集）ページが表示されます。デフォルトでは **General**（一般）タブが選択されています。

3. **General**（一般）タブで、一般的な CIFS 共有のパラメータを変更します。
4. **Advanced**（詳細設定）をクリックし、詳細な CIFS 共有パラメータを変更します。

   メモ: General（一般）タブで **Files should be checked for viruses**（ファイルのウイルスチェックを行う）を選択した場合は、**Antivirus**（アンチウイルス）タブがアクティブになります。
5. **Antivirus**（アンチウイルス）がアクティブな場合は、これをクリックしてアンチウイルスポリシーを変更します。
6. **変更の保存** をクリックします。

CIFS 共有の削除

CIFS 共有を削除するには、次の手順を実行します。

1. **User Access（ユーザーアクセス） → Shares（共有） → CIFS Shares（CIFS 共有）** をクリックします。**CIFS Share（CIFS 共有）**ページが表示されます。
2. 使用可能な CIFS 共有のリストから、関連する CIFS 共有を選択し、**Delete（削除）**をクリックします。

ホーム共有の作成

ユーザーベースのディレクトリ構造で CIFS 共有を作成（ホーム共有）する場合、最初はその共有にはアクセスできません。これは、各ユーザーのすべてのディレクトリはシステム管理者によって作成される必要があるためです。この作成はスクリプト（ユーザーが作成したスクリプト）、バッチファイル、またはストレージ管理者が書いた PowerShell の cmdlet によって行うことができます。または、システム管理者は手動でこれらのフォルダを作成することもできます。これにより、システム管理者はより強力なアクセス制御を利用できます。システム管理者は、ホーム共有を与えるアカウントを手動で確認するか、特定の Active Directory またはローカルユーザーデータベース内の一部またはすべてのユーザー用に、自動でフォルダを生成するスクリプトを書くことができます。

メモ: 次の手順は、NAS ストレージ管理者でもあるドメイン管理者が完了しなければなりません。

CIFS ホーム共有フォルダを手動で作成するには、次の手順を実行します。

1. **NAS Manager** で、システムがお使いの Active Directory に参加していることを確認します。
2. Active Directory を使用している場合は、**NAS Manager** で、**Cluster Management → CIFS Configuration（クラスタの管理 > CIFS 設定）**と選択し、**Authenticate users' identity via Active Directory and local users database**（Active Directory およびローカルユーザーデータベース経由でユーザー ID を認証）が選択されていることを確認します。
3. **NAS Manager** で、すべてのユーザーフォルダのルートである一般的なアクセス共有を作成します。

   たとえば、共有名が `users` である一般的なアクセス共有を `/users` ディレクトリで作成します。ディレクトリが存在しない場合はフォルダを作成するオプションを選択します。
4. **Windows エクスプローラ**を使用して、**users** という共有を CIFS のローカルのシステム管理者としてマウントします。
5. マウントした共有のセキュリティ設定で、**Advanced**（詳細設定）をクリックし、所有者を `Domain Admins`、または所有権を持とうとする特定のドメイン管理者かストレージ管理者のアカウントに変更します。

   これは、ホーム共有の各ユーザー用に（ユーザー作成スクリプトの使用または手動のどちらかで）フォルダを作成するアカウントです。
6. **user** という共有を切断またはアンマウントし、（Domain Admin、Storage Admin、または特定の所有権が設定されたアカウントとして）先に設定したように、所有権を持つアカウントとして再マウントします。
7. **NAS Manager** で、新しい CIFS 共有を作成し、**CIFS share containing a user-based directory tree**（ユーザーベースのディレクトリツリーが含まれた CIFS 共有）という共有タイプを選択します。

8. 先に、**users** という一般のアクセス共有がパス **/users** で作成されました。**Path template**（パスのテンプレート）で、**/users** を入力して、users の各フォルダに **/users/username** または **/users/domain/username** の形式を取らせるかどうかを選択します。
9. **Save Changes**（変更の保存）をクリックします。
10. **Windows エクスプローラ**を使用して、ホーム共有を与える各ユーザーに、前の手順で選択したパスのテンプレートに従うフォルダを作成します。
    これは、手動またはユーザー作成スクリプトによって行うことができます。

FluidFS でのアクセスコントロールリストおよび共有レベルパーミッションの設定

FluidFS CIFS 共有はアクセスコントロールリスト（ACL、Access Control List）および共有レベルパーミッション（SLP、Share Level Permissions）をサポートします。 Windows 管理者は Microsoft が定義しているベストプラクティスに従うことをお勧めします。SLP は完全な権限、すべてのユーザーまたはグループの変更と読み取り権限を、共有レベルで対処します。ACL はさらなる詳細をフォルダまたはファイルレベルで提供します。ACL では達成できないような特定の SLP 要件がある場合を除き、SLP のデフォルト設定（全員が完全な権限を持つ）をそのままにし、ACL を使って共有へのアクセスを制御することをお勧めします。

FluidFS ローカル管理者アカウント

組み込みの FluidFS ローカル管理者アカウントには、新規 CIFS 共有に対する初期設定の許可と所有権が与えられています。 このアカウントは NAS サービスが Active Directory ドメインに参加していない場合に、ACL の設定に使用されます。この組み込みアカウントには、セキュリティの目的でランダムに生成されたパスワードがあります。ACL または SLP を設定するためにこのアカウントを使用するには、このパスワードを変更してください。

CIFS フルアクセスユーザーアカウント（バックアップユーザー）

フルアクセスアカウント機能は、単一の **Active Directory**（AD）ユーザーに、すべての基本的な NAS データへの、完全なアクセスを付与するために使用されます。この機能は主に、FluidFS NAS デバイスでストレージ仮想化アプライアンスが使われる場合に使用されます。この種のアプライアンスは、1 つの AD アカウントを使ってすべての基本的な NAS システムにアクセスします。

この特権を AD アカウントに関連付けるためには、システムが AD のメンバーである必要があります。フルアクセスユーザー特権は、ファイル ACL の定義に関わらず AD アカウントにすべての共有とボリューム上の全データへの完全なアクセス権を与えます。ただし、**フルアクセスユーザー** 特権が付与された AD アカウントには、SLP 設定が適用されます。NAS システム管理者は、フルアクセスユーザーとして設定されたユーザーにすべての関連した SLP があることを検証する必要があります。

フルアクセスユーザーの管理

1. KVM による直接接続または管理 VIP への SSH 接続を使用して、CLI への接続を開始します。
2. **フルアクセスユーザー**アカウントを設定する、すなわち現在のエントリを上書きするには、CLI で次のコマンドを実行します。
   ```
   system authentication full-access-account set DOMAIN+username
   ```
3. **フルアクセスユーザー**アカウントが正しく設定されているかどうか確認するには、次のコマンドを実行します。
   ```
   system authentication full-access-account view
   ```
4. **フルアクセスユーザー**を削除するには、次のコマンドを実行します。
   ```
   system authentication full-access-account delete
   ```

Active Directory の設定

FluidFS は Active Directory ドメインに参加することができます。これには、NAS Manager で **Cluster Management（クラスタ管理）→ Authentication（認証）→ System Identity（システム ID）**と選択、または CLI を使用して行います。CLI を使用した Active Directory への参加に関する詳細は、**dell.com/support/manuals** で『*FluidFS Command Line Interface Guide*』（FluidFS コマンドラインインタフェースガイド）を参照してください。

FluidFS NAS アプライアンスが Active Directory ドメインに参加するには、ジョイン操作で資格情報を提供する必要があります。

メモ: 資格情報が必要となるのは、ジョイン操作の実行時のみです。FluidFS NAS アプライアンスが資格情報を保存したりキャッシュすることはありません。

FluidFS NAS アプランアンスを Active Directory に参加させるために使用する資格情報を決定する際、管理者には 3 つのオプションがあります。

- ドメイン管理者アカウントを使用して NAS クラスタに参加する。

  メモ: これが推奨される方法です。

- **コンピュータをドメインに参加させる** 特権 がすでに委任されていると共に、ドメイン内のすべてのコンピュータオブジェクト全体に完全制御権が委任されているアカウントを使用して、NAS クラスタと Active Directory ドメインに参加させます。
- ドメイン管理者アカウントまたは、ドメイン内のすべてのコンピュータオブジェクト全体に完全制御権が委任されているアカウントを使用できない場合、NAS アプランアンスを Active Directory ドメインに参加させるための最低要件は以下となります：
  - **コンピュータをドメインに参加させる** 特権 が委任されている部署（OU、Organizational Unit）管理者
  - OU 管理者は、コンピュータオブジェクトを含むその OU 内のオブジェクトに対する、完全制御権も委任されている必要があります。
  - ドメインにシステムを参加させる前に、 OU 管理者は管理用の OU 特権が提供されているシステムに、コンピュータオブジェクトを作成する必要があります。
  - 参加の時に使用された NAS アプライアンスのコンピュータオブジェクト名、および NetBIOS 名が一致する必要があります。
  - ドメインに参加させるために NAS アプライアンスのコンピュータオブジェクトを、許可の下の **User（ユーザー）**または **Group（グループ）**フィールドで作成する際に、OU 管理者アカウントを選択します。その後 NAS アプライアンスが OU 管理者資格情報を使用して参加することができます。

メモ: FluidFS NAS クラスタはすべてのユーザーに対して、 `tokenGroups` 属性の読み取りアクセスが必要です。すべてのドメインコンピュータに対する Active Directory のデフォルト設定では、`tokenGroups` 属性への読み取りアクセスが許可されています。許可が与えられていない場合、ネストされたグループまたは OU 内の Active Directory ドメインユーザーには、**Access Denied（アクセス拒否）**エラーが発生し、ネストされた OU またはグループ内にないユーザーには、アクセスが許可されます。

CIFS 共有での ACL または SLP の設定

FluidFS NAS ソリューションは、共有、ファイル、およびフォルダに対し、2 つのアクセス制御レベルをサポートします。

- アクセス制御リスト（ACL、Access Control Lists）— 特定のファイルおよびフォルダへのアクセスを統制します。管理者は、ユーザーおよびグループが実行できる広範囲な操作を制御できます。
- 共有レベル許可（SLP、Share Level Permissions）— 共有全体を統制します。管理者は、共有全体での読み取り、変更、または完全アクセスのみを制御します。

ACL は詳細なレベルでの制御を提供し、読み取り / 変更 / 完全アクセスのみならず、その他多くの操作を制御することができます。ACL では達成できないような特定の SLP 要件がある場合を除き、SLP のデフォルト設定（全員が完全な権限を持つ）をそのままにし、ACL を使って共有へのアクセスを制御することをお勧めします。

CIFS 共有を初めて作成した場合、ACL を設定する前、またはこの共有へのアクセスを試行する前に、共有の所有者を変更する必要があります。NAS cluster（NAS クラスタ）ソリューションが Active Directory ドメインに参加している場合は、次の方法で ACL を設定できます。

- ドメイン管理者グループとして設定されたプライマリグループが含まれている Active Directory ドメインのアカウントを使用する。
- FluidFS ローカル管理者アカウントを使用する（Active Directory に参加しない場合、またはドメイン管理者資格情報を使用できない場合に使用）。

ドメイン管理者グループのメンバーとして設定された Active Directory のアカウントの使用

ドメイン管理者グループとして設定されたプライマリグループが含まれている Active Directory ドメインのアカウントを使用するには、次の手順を実行します。

1. **Windows Explorer** を開き、アドレスバーに `\\<AccessVip>\C$` と入力します。
   指定された FluidFS システムで使用できるすべての NAS ボリュームが、フォルダとして表示されます。
2. 要求されたボリュームをダブルクリックします。
   この NAS ボリュームに対するすべての CIFS 共有が表示されます。
3. 希望の CIFS 共有（フォルダ）を右クリックして **Properties（プロパティ）** を選択します。
4. **Security（セキュリティ）** タブを選択して、**Advanced（詳細設定）** をクリックします。
5. **Owner（所有者）** タブを選択して、**Edit（編集）** タブを選択します。
6. **Other users or groups…**（その他のユーザーまたはグループ）ボタンをクリックして、この共有で ACL を設定するために使用されるドメイン管理者ユーザーアカウントを選択するか、Domain Admins（ドメイン管理者）グループを選択します。
7. **Replace owner on subcontainers and objects（サブコンテナおよびオブジェクトの所有者の差し替え）** にチェックが入っていることを確認して、**Apply（適用）** をクリックします。
8. **Ok** をクリックして、**Advanced Security Settings（セキュリティの詳細設定）** ウィンドウに戻ります。

Permissions（許可） タブを選択して、 Microsoft のベストプラクティスに従い、ACL 許可を CIFS 共有フォルダに割り当てます。

メモ: CIFS 共有と NFS 共有の両方が同じ NAS ボリュームで定義されている場合、そのボリュームに含まれる NFS と CIFS 両方の共有が見えます。必要な CIFS 共有のみを選択するように注意してください。

FluidFS ローカル管理者アカウントの使い方

1. **Map network drive（ネットワークドライブのマップ）** ウィザードを開始します。**Folder（フォルダ）** で、**\\<AccessVIP>\<share-name>** を入力します。

   メモ: クライアントアクセス VIP または DNS 名を使用して CIFS 共有に接続することができます。
2. **Connect using different credentials（別の資格情報を使用して接続する）** を選択します。
   次の資格情報を使用します：NetBIOS Name\Administrator
   デフォルトの NetBIOS 名は **CIFSStorage** です。

   メモ: System Management（システム管理） → Authentication（認証） → System Identity（システム ID） と移動して、NAS Manager の NetBIOS 名を変更することができます。
3. 新規にマップされた共有を右クリックして、**Properties（プロパティ）** を選択します。
4. **Security（セキュリティ）** タブを選択して、**Advanced（詳細設定）** をクリックします。
5. **Owner（所有者）** タブを選択して、**Edit（編集）** タブを選択します。

6. **Other users or groups…（その他のユーザーまたはグループ）**ボタンをクリックして、この共有で ACL を設定するドメイン管理者ユーザーアカウントを選択するか、Domain Admins（ドメイン管理者）グループを選択します。また、CIFS ローカル管理者アカウントを使用することもできます。
7. **Replace owner on subcontainers and objects（サブコンテナおよびオブジェクトの所有者の差し替え）**にチェックが入っていることを確認して、**Apply（適用）**をクリックします。
8. **Ok** をクリックして、**Advanced Security Settings（セキュリティの詳細設定）**ウィンドウに戻ります。
9. 所有者を設定したら、ネットワークドライブのマッピングを解除します。
10. ネットワークドライブを、所有者またはいずれかのドメイン管理者として設定されている、ドメイン管理者アカウントとしてマップし直します。所有者がドメイン管理者グループに設定されている場合、Microsoft のベストプラクティスに従い、必要に応じてユーザーおよびグループに ACL 許可を割り当てます。

NAS サービスが Active Directory ドメインに参加していない場合、ACL の設定には CIFS 管理者のビルトインアカウント Administrator を使用する必要があります。SLP を定義するには、Microsoft Management Console（MMC）を使用します。

メモ: CIFS 共有の作成には、MMC を使用しないでください。

CIFS 共有へのネットワークドライブのマッピング

ACL を設定する予定の CIFS 共有にネットワークドライブをマッピングするには、次の手順を実行します。

1. **Connect using a different user name**（別のユーザー名を使用して接続）を選択します。
   プロンプトが表示されたら、次の資格情報を使用します。
   `<NetBios Name>\Administrator`
   デフォルトで、NetBios 名は **CIFSStorage** となっています。これが変更されていない場合、`CIFSStorage\Administrator` と入力します。

   メモ: Cluster Management → Authentication → System Identity（クラスタの管理 > 認証 > システム ID）と移動すると、NAS Manager の NetBios 名を変更できます。
2. 上記の手順に従って、CIFS 共有の所有者をドメイン管理者ユーザーアカウントまたはドメイン管理者グループのいずれかに設定します。
3. 所有者を設定したら、ネットワークドライブのマッピングを解除します。
4. すでに所有権が設定されたドメイン管理者ユーザーグループに属しているアカウントを使用して、ネットワークドライブを再マッピングします。Microsoft のベストプラクティスに従って、ユーザーとグループに ACL パーミッションを割り当てます。
   NAS サービスが Active Directory ドメインに参加していない場合、ACL の設定には CIFS 管理者のビルトインアカウント *Administrator* を使用する必要があります。SLP を定義するには、MMC を使用します。

   メモ: CIFS 共有の作成には、Microsoft Management Console（MMC）を使用しないでください。

CIFS を使用したアクセス

Microsoft Windows には、CIFS 共有に接続するための複数の方法が用意されています。
Windows からマッピングを行うには、次のオプションをいずれかひとつ選択してください。

Option 1（オプション 1）

コマンドプロンプトから **net use** コマンドを実行します。

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

オプション 2

1. **Start（スタート）**メニューで、**Run（ファイル名を指定して実行）**を選択します。
   Run（ファイル名を指定して実行） ウィンドウが表示されます。
2. 接続したい共有へのパスを入力します。
   `\\Client Access VIP >\<共有名>`。
3. **OK** をクリックします。
   Explorer ウィンドウが表示されます。

オプション 3

1. **Windows エクスプローラ**を開き、**Tools → Map Network Drive（ツール > ネットワークドライブのマッピング）**と選択します。
   Map Network Drive（ネットワークドライブのマッピング）ダイアログボックスが表示されます。
2. **Drive**（ドライブ）ドロップダウンリストから、使用可能なドライブを選択します。
3. **Folder**（フォルダ）フィールドにパスを入力するか、共有フォルダを参照します。
4. **Finish**（終了）をクリックします。

オプション 4

メモ: このオプションでは、共有に接続できますが、マッピングはできません。

1. Windows **デスクトップ**で、**ネットワークコンピュータ** をクリックして、NAS アプライアンスを見つけます。
2. NAS アプライアンスを選択し、選択した NAS アプライアンスをダブルクリックします。
3. **CIFS shares**（CIFS 共有）リストから、接続したい共有を選択します。

CIFS 共有レベルパーミッションの設定

CIFS Share Level Permissions（SLP）は、Microsoft Management Console（MMC）を使用しなければ設定することができません。
管理者は、あらかじめ定義された MMC ファイル（.msc）を Windows Server 2000/2003/2008 のスタートメニューから使用し、**共有フォルダ**のスナップインを追加して NAS クラスタに接続することができます。

MMC では、どのユーザーがリモートコンピュータに接続できるかを選択することはできません。デフォルトで、MMC はマシンにログオンしているユーザーを使って接続を確立します。

MMC 接続内の適切なユーザーを使用するには、次の手順を実行します。

- 管理しようとしている NAS アプライアンスが Active Directory に参加している場合、**<ドメイン>\Administrator** で管理ステーションにログインします。
- MMC を使用する前に、Windows Explorer のアドレスバーにクライアントアクセス仮想 IP アドレスを入力して、NAS クラスタソリューションに接続します。管理者アカウントでログインしてから MMC に接続します。

後者の手順を実行する場合は、ローカル管理者パスワードを先にリセットしておく必要があります。
事前定義した MMC ファイルがない場合は、次の手順を実行します。

1. **スタート → ファイル名を指定して実行** をクリックします。
2. `mmc` と入力して **OK** をクリックします。
   Console 1 - [Console Root]（コンソール 1 - [コンソールルート]） ウィンドウが表示されます。
3. **File（ファイル）→ Add/Remove Snap-in（スナップインの追加と削除）** をクリックします。
4. **Shared Folders（共有フォルダ）**を選択して **Add（追加）**をクリックします。

5. **Shared Folders（共有フォルダ）**ウィンドウで、**Another computer（別のコンピュータ）**を選択し、NAS クラスタソリューション名（DNS で設定されている）を入力します。また、クライアントアクセス VIP アドレスを使用することもできます。
6. **終了** をクリックします。
   新規共有ツリーが **Console Root（コンソールルート）**ウィンドウに表示されます。
7. 必要な共有を右クリックして **Properties（プロパティ）**を選択し、共有レベルパーミッションを設定します。
8. **Share Properties（共有のプロパティ）**ウィンドウで、**Share Permission（共有パーミッション）**タブを選択します。

アクセスベースの共有列挙

Dell Fluid File System の v2 リリースでは、SLP アクセスベースの共有列挙がデフォルトで有効になっています。したがって、共有レベルパーミッション（SLP）が与えられていない場合、ユーザーおよびグループにはその共有が表示されません。あるユーザーまたはグループが特定の共有に対する共有パーミッションを所持していない場合、**\\<client access VIP>** で NAS クラスタに直接アクセスすると、その共有は使用可能な共有のリストに一切表示されません。これまで Dell Fluid File System v1 ではアクセスベースの共有列挙が有効でなかったため、共有は表示されましたが、アクセスはできませんでした。

CIFS ローカル管理者パスワードのリセット

メモ: インストール中にランダムパスワードが生成されます。パスワードをリセットします。

これで管理者ユーザーとして MMC を参照できるようになります。これはローカル CIFS 管理者とも呼ばれます。

CIFS ローカル管理者のパスワードをリセットするには、次の手順を実行します。

1. NAS Manager にログインします。
2. **Cluster Management（クラスタの管理）** → **Authentication（認証）** → **Local Users（ローカルユーザー）** と選択します。
   Local Users（ローカルユーザー）ページが表示されます。
3. **Administrator（管理者）**ユーザーを選択します。
4. **Change password（パスワードの変更）**を選択します。

クォータ

ディスククォータは、ユーザーまたはグループが使用するディスク容量とファイル数を制限する一連のルールです。クォータでは、NAS ボリュームが使用する総容量、または NAS ボリューム内のユーザーおよびグループの使用量も制限できます。クォータ値は常に特定のボリュームと関連しており、MB 単位で指定されます。

メモ: 個々のクォータが定義されていないユーザーおよびグループは、デフォルトのユーザー / グループクォータを使用します。

クォータに関する考慮事項

- 混合タイプのボリュームを使用する際のクォータに関する考慮事項 — セキュリティスタイルが混合した NAS ボリュームの場合、Windows（Active Directory）ユーザーおよび UNIX ユーザー（LDAP または NIS）の両方に一意のクォータが設定されている必要があります。 Windows と UNIX のユーザーのクォータは、ユーザーがマップ（自動または手動）されていたとしても、相互に独立しています。
- CIFS および NFS の両方にアクセスする際のクォータに関する考慮事項 — NTFS または UNIX スタイルの許可を使用する NAS ボリュームでは、一意のクォータを 1 つだけ設定します。ユーザーのマッピン

グ機能によって、プロトコル間の相互運用性が解決されます。UNIX と Windows のユーザーは、マップされている Windows および UNIX アカウント両方で同じクォータを共有します。

デフォルトのクォータの管理

ボリュームのデフォルトのクォータを管理するには、次の手順を実行します。

メモ: デフォルトのクォータは、ユーザー固有またはグループ固有のクォータで上書きすることができます。

1. **User Access → Quota → Default（ユーザーアクセス > クォータ > デフォルト）** と選択します。
   Default Quota（デフォルトのクォータ）画面が表示されます。
2. **NAS Volume**（NAS ボリューム）リストから、クォータを追加または変更できる適切な NAS ボリュームを選択します。
3. **Default quota per user**（ユーザーごとのデフォルトのクォータ）で、希望のユーザークォータを MB 単位で選択および入力するか、**Unlimited**（無制限）を選択します。

   メモ: この制限を超過した場合、NAS ボリュームへの書き込みは許可されません。
4. **Alert administrator when quota reaches**（クォータが達した場合、システム管理者に警告する）で、希望のユーザークォータを MB 単位で選択および入力するか、**Disabled**（無効）を選択します。

   メモ: この制限を超過した場合、メール受信者のアドレスに警告メッセージが送信されます。このデフォルトは個別のクォータが定義されていないユーザーに使用されます。
5. **Default quota per group**（グループごとのデフォルトのクォータ）で、希望のユーザークォータを MB 単位で選択および入力するか、**Unlimited**（無制限）を選択します。

   メモ: この制限を超過した場合、NAS ボリュームへの書き込みは許可されません。
6. In **Alert administrator when quota reaches**（クォータが達した場合、システム管理者に警告する）で、希望のグループクォータを MB 単位で選択および入力するか、**Disabled**（無効）を選択します。

   メモ: この制限を超過した場合、システム管理者の電子メールアドレスに警告メッセージが送信されます。このデフォルトは個別のクォータが定義されていないユーザーに使用されます。
7. **Save Changes**（変更の保存）をクリックします。

ユーザーまたはグループ固有のクォータの管理

既存ユーザー / グループ固有のクォータの表示

特定のユーザークォータまたはグループクォータの詳細を表示するには、次の手順を実行します。

1. **User Access → Quota → User/Group（ユーザーアクセス > クォータ > ユーザー / グループ）** と選択します。
   User/Group Quota（ユーザー / グループクォータ）ページが表示されます。
2. **Show quotas for NAS Volume**（NAS ボリュームのクォータを表示）リストから該当する NAS ボリュームを選択するか、**All NAS Volumes**（すべての NAS ボリューム）を選択します。
   選択した NAS ボリュームに対して使用可能なユーザー / グループクォータのリストが表示されます。デフォルトでは、**すべての NAS ボリューム**のユーザー / グループクォータ情報が表示されます。

クォータの種類

次のクォータの種類が使用可能です。

- User — ユーザーごとのクォータ。
- All of group — グループ全体の合計のクォータ。
- Any user in group — グループに所属するユーザーのためのユーザーごとのクォータ。

ユーザー / グループ固有のクォータの追加

クォータを追加するには、次の手順を実行します。

1. **User Access（ユーザーアクセス）** → **Quota（クォータ）** → **User/Group（ユーザー / グループ）** と選択します。
   User/Group Quota（ユーザー / グループクォータ）ページが表示されます。
2. **Add（追加）**をクリックします。
   Create Quota（クォータの作成）ページが表示されます。
3. **NAS Volume（NAS ボリューム）**リストから、クォータを追加する適切な NAS ボリュームを選択します。
4. **Quota for（クォータ対象）**リストから、希望するクォータ制限のタイプを選択して適切なユーザーまたはグループ名を入力するか、または Browse（参照）ボタンをクリックして適切なユーザーまたはグループを選択します。

   メモ: ユーザーのリスト作成には、Active Directory ドメインにいるユーザー数によって時間がかかる場合があります。 この間、不定期に認証エラーが発生する場合があります。 ユーザー名がわかっている場合、すべてのユーザーがリストされるのを待つのではなく、その名前を入力することができます。
5. **Quota（クォータ）**で、MB を選択してクォータ入力するか、または **Unlimited（制限なし）**をクリックします。

   メモ: ユーザーまたはグループがすでにこのデータ量を使用している場合、新しい書き込みは拒否されます。
6. **Alert administrator when quota reaches（クォータが達した場合、システム管理者に警告する）**で、MB を選択して希望のグループクォータを入力するか、**Disabled（無効）**を選択します。

   メモ: この制限を超過した場合、システム管理者の電子メールアドレスに警告メッセージが送信されます。

   メモ: このデフォルトは個別のクォータが定義されていないユーザーに使用されます。
7. **Save Changes（変更の保存）**をクリックします。

ユーザー / グループ固有のクォータの変更

既存のクォータを変更するには、次の手順を実行します。

1. **User Access → Quota → User/Group（ユーザーアクセス > クォータ > ユーザー / グループ）**と選択します。
   User/Group Quota（ユーザー / グループクォータ）ページが表示されます。
2. **NAS Volume**（NAS ボリューム）リストから適切な NAS ボリュームを選択します。
   User/Group Quota（ユーザー / グループクォータ）の表に、選択した NAS ボリューム用の使用可能な**ユーザー / グループクォータ**のリストが表示されます。
3. **Name/ID**（名前 /ID）列の下の使用可能なユーザー / グループクォータのリストから、該当のユーザー / グループクォータをクリックします。
   Edit Quota（クォータの編集）ページが表示されます。
4. 必要に応じてクォータルールを変更して、**Save Changes**（変更の保存）をクリックします。

クォータの削除

クォータルールを削除するには、次の手順を実行します。

1. **User Access → Quota → User/Group（ユーザーアクセス > クォータ > ユーザー / グループ）**と選択します。
   User/Group Quota（ユーザー / グループクォータ）ページが表示されます。
2. **NAS Volume**（NAS ボリューム）リストから適切な NAS ボリュームを選択します。

User/Group Quota（ユーザー / グループクォータ）の表に、選択した NAS ボリューム用の使用可能な**ユーザー / グループクォータ**のリストが表示されます。

3. 使用可能なユーザー / グループクォータのリストから、適切なクォータルールを選択して、**Delete**（削除）をクリックします。

4

FluidFS NAS cluster（FluidFS NAS クラスタ）ソリューションでのデータ保護

データ保護は、すべてのストレージインフラストラクチャにおいて重要かつ不可欠な要素です。Dell Fluid File System では、次のようなさまざまなデータ保護の方法を設定できます。

- スナップショット
- レプリケーション
- バックアップからのシステムの復元
- バックアップエージェントの設定

スナップショット

スナップショットテクノロジは、ボリューム内にあるデータのポイントインタイムのバックアップを作成します。スナップショットの作成には、さまざまなポリシーを設定することができます。これには、スナップショットを取得する時刻、保存するスナップショットの数、スナップショットを削除するまでに使用できる NAS ボリュームの容量などが含まれます。スナップショットは変更セットをベースにしています。NAS ボリュームの最初のスナップショットが作成されると、基本となるこのスナップショットよりも後に作成されたすべてのスナップショットは、前のスナップショットとの差分になります。

スナップショットの詳細については、『*Online Help*』（オンラインヘルプ）を参照してください。

スナップショットポリシーの追加または変更

1. **Data Protection → Snapshots → Policies**（データ保護 > スナップショット > ポリシー）と選択します。
   Snapshot Policies（スナップショットポリシー）ページが表示されます。
2. **NAS Volume**（NAS ボリューム）リストから適切な NAS ボリュームを選択します。
3. **Alert the administrator when snapshot space is % of total volume**（スナップショットの容量がボリューム全体の % になったら管理者に警告する）で、NAS ボリューム容量全体に対する割合を入力します。
   この制限を超えると、スナップショットは自動的に削除されます。

   メモ: スナップショット容量のイベントを無効にするには、このフィールドを空にしておきます。

   メモ: スケジュールされたスナップショットとユーザーが作成したスナップショットはどちらも削除されます。レプリケーションスナップショットは削除されません。
4. 1 時間以内のスナップショットを取得するには、**Periodic**（周期）をクリックします。
   a) **Every Minutes**（分単位）リストから分単位の周期を選択します。
   b) **Number of snapshots to keep**（保存するスナップショット数）を入力します。
5. 時間単位でスナップショットを取得するには、**Hourly**（毎時）を選択します。
   a) **Every hour**（1 時間ごと）を選択するか、**At**（時刻）を選択してスナップショットを取得する具体的な時間と分を指定します。
   b) **Number of snapshots to keep**（保存するスナップショット数）を入力します。
6. 日付に基づいてスナップショットを取得するには、**Daily**（日単位）を選択します。
   a) **Every day**（毎日）を選択するか、**On**（日付）を選択して特定の日付を指定します。

b) **At**（時刻）でスナップショットを生成する時刻を選択します。
c) **Number of snapshots to keep**（保存するスナップショット数）を入力します。

7. 週単位でスナップショットを取得するには、**Weekly**（毎週）を選択します。
   a) **On**（曜日）リストで、スナップショットを生成する曜日と時刻を選択します。
   b) **Number of snapshots to keep**（保存するスナップショット数）を入力します。
8. **Save Changes**（変更の保存）をクリックします。

スナップショットの作成（ポリシーなし）

1. **Data Protection → Snapshots → List（データ保護 > スナップショット > リスト）** と選択します。
   Snapshots List（スナップショットリスト）ページに既存のスナップショットのリストが表示されます。
   デフォルトで、すべての NAS ボリュームのスナップショットが表示されます。
2. **作成** をクリックします
   Create Snapshot（スナップショットの作成）ページが表示されます。
3. **NAS Volume**（NAS ボリューム）リストから適切な NAS ボリュームを選択します。
4. **Snapshot name**（スナップショット名）で、新しいスナップショットの名前を入力します。
5. **作成** をクリックします
   新しいスナップショットが作成され、**Snapshots List**（スナップショットリスト）ページのスナップショットのリストに追加されます。

スナップショットへのアクセス

スナップショットを作成すると、エクスポートまたは共有から特別フォルダにアクセスすることができます。

UNIX の場合は、各 NFS エクスポートの **.snapshots** というディレクトリから特別フォルダにアクセスします。

Microsoft Windows の場合は、各共有の **.snapshots** というディレクトリから特別フォルダにアクセスします（これはシャドウコピーに統合され、旧バージョンを有効化します）。

スナップショットでは、アクティブなファイルシステムと同じセキュリティ方式が維持されます。したがって、スナップショットを使用している場合でも、ユーザーがアクセスできるのは、現在のパーミッションに基づいた自身のファイルだけです。特定のスナップショットにアクセスするときに使用できるデータは、特定の共有およびそのサブディレクトリのレベルにあるため、ユーザーはファイルシステムの他の部分にはアクセスできません。

スナップショットの変更

メモ: スナップショット名は変更することができます。

1. **Data Protection → Snapshots → List（データ保護 > スナップショット > リスト）** と選択します。
   Snapshots List（スナップショットリスト）ページに既存のスナップショットのリストが表示されます。
   デフォルトで、すべての NAS ボリュームのスナップショットが表示されます。
2. **Show Snapshots for NAS Volume**（NAS ボリュームのスナップショットを表示）リストから適切な NAS ボリュームを選択するか、**All NAS volumes**（すべての NAS ボリューム）を選択します。
   選択された NAS ボリュームに対応する既存のスナップショットが表示されます。
3. 使用可能なスナップショットリストの **Name**（名前）列で、該当するスナップショットをクリックします。
   Edit Snapshot（スナップショットの編集）画面が表示されます。
4. **Snapshot name**（スナップショット名）で既存の名前を変更します。

5. **Calculate Snapshot Delta**（スナップショットデルタの計算）をクリックし、スナップショットの削除によってできる実際の空き容量を計算します。
6. **Save Changes**（変更の保存）をクリックします。

データの復元

データの復元には次の 2 つの方法があります。

- コピーアンドペースト：個別ファイルの復元
  誤ってファイルを削除または変更してしまったためそれを復元したい場合、現在の NFS エクスポートまたは共有にあるスナップショットディレクトリ（作成時刻による）にアクセスして、ファイルを元の場所にコピーしてください。 この方法は、各ファイルの毎日の復元に便利です。
- スナップショットからの NAS ボリュームの復元
  ボリューム全体のデータを復元する必要がある場合（アプリケーションエラーまたはウィルス攻撃による場合）、大量のデータをコピーアンドペーストすると処理時間がかかるため、NAS ボリューム全体を復元することができます。

スナップショットの削除

1. **Data Protection（データ保護）** → **Snapshots（スナップショット）** → **List（リスト）** と選択します。
   Snapshots List（スナップショットリスト）ページに既存のスナップショットのリストが表示されます。
   デフォルトで、すべての NAS ボリュームのスナップショットが表示されます。
2. **Show Snapshots for NAS Volume（NAS ボリュームのスナップショットを表示）**リストから適切な NAS ボリュームを選択するか、**All NAS volumes（すべての NAS ボリューム）**を選択します。
   選択された NAS ボリュームに対応する既存のスナップショットが表示されます。
3. 使用可能なスナップショットのリストから、関連するスナップショットを選択し、**Delete（削除）**をクリックします。

スナップショットからの NAS ボリュームの復元

1. **Data Protection（データ保護）** → **Snapshots（スナップショット）** → **Restore（復元）** と選択します。
   Snapshot Restore（スナップショットの復元）ページが表示されます。
2. **Choose the volume to be reverted（復元するボリュームの選択）**で、適切な NAS ボリュームを選択します。
   Choose a snapshot for revision（改訂するスナップショットの選択）リストに、選択した NAS ボリュームのスナップショットが表示されます。
3. **Choose a snapshot for revision（改訂するスナップショットの選択）**で、ボリュームを復元するスナップショットを選択します。
4. **Next（次へ）**をクリックします。
   復元プロセスを開始する前に実行する手順を示すメッセージが表示されます。
5. NAS ボリュームを選択したスナップショットに復元するには、**Yes（はい）**をクリックします。
   NAS ボリュームがスナップショットに復元されます。

   注意: Restore（復元）操作は元に戻すことができません。 スナップショットの時刻と復元操作が完了した時刻の間に作成または変更されたデータはすべて消去されます。

レプリケーション

Dell FluidFS NAS ソリューションにおけるレプリケーションは、ブロックベースかつ非同期です。

- ブロックベース—ファイル全体ではなく、変更のあるブロックのみが複製されます
- 非同期—データが複製されているときでもクライアントとの通信が継続します

レプリケーションは、異なるレベルのデータ保護を実現するために、さまざまなシナリオで使用されます。その中には次のシナリオが含まれます。

迅速なバックアップおよび復元	データロス、破損、またはユーザーの間違いに対する保護のためデータのフルコピーを維持します。
災害復旧	フェイルオーバー用にリモートロケーションにデータをミラーリングします。
リモートデータアクセス	アプリケーションはミラーリングしたデータに読み取り専用または読み取り / 書き込みモードでアクセスできます。
オンラインデータ移行	データ移行に関連するダウンタイムを最小化します。

レプリケーションは、NAS cluster（NAS クラスタ）ソリューションファイルシステムのスナップショットテクノロジを活用しています。最初のレプリケーションの後は、差分だけが複製されます。これにより、より迅速なレプリケーションおよびプロセッササイクルの効率的な使用を可能にします。データの整合性を保ちながら、ストレージの容量の節約もできます。

レプリケーションは、ボリュームベースであり、同じ NAS アプライアンス上のボリュームまたは別の NAS アプライアンス上のボリュームを複製するのに使用できます。ボリュームを別の NAS アプライアンスに複製する場合、他の NAS アプライアンスをレプリケーションパートナーとしてセットアップする必要があります。

Replication Partners（レプリケーションパートナー）

パートナー関係が構築されると、レプリケーションは双方向で実行されます。一方のシステムが、相手システムにレプリケーションする複製元ボリュームだけでなく、相手システムの複製先ボリュームも保持できるようになります。レプリケーションデータは、セキュアな ssh トンネルを介して、クライアントネットワーク上でシステムからシステムへ送信されます。

レプリケーションポリシーは、オンデマンドその他のさまざまなスケジュールに従って実行されるように設定できます。すべてのシステム設定（ユーザークォータ、スナップショットポリシーなど）は、各ボリュームに保存されます。ボリュームがレプリケーションされると、複製先ボリュームでも同じ情報が保持されます。レプリケーションポリシーを削除する場合は、ボリューム設定を転送するためのオプションが表示されます。

メモ: レプリケーションパートナーのコントローラカウントは同じでなければなりません。たとえば、4 つのコントローラアプライアンスを 2 つのコントローラアプライアンスにレプリケーションすることは避けてください。

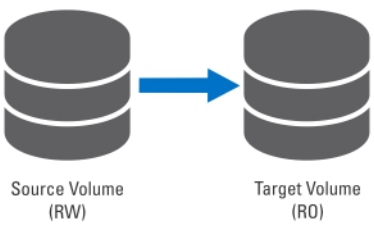

図 4. ローカルレプリケーション

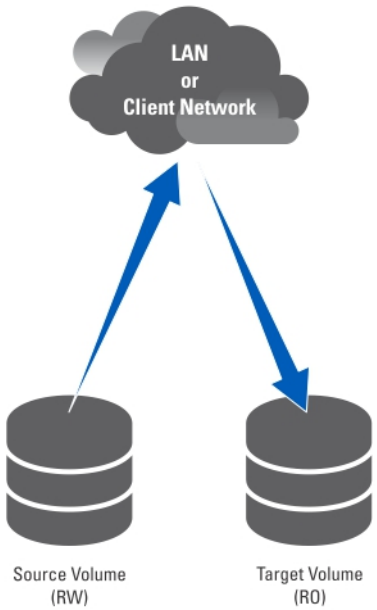

図 5. パートナーレプリケーション

既存のレプリケーションパートナーの表示

レプリケーションパートナーのリストを表示することができます。選択したシステムで信頼されているレプリケーションパートナーを表示するには、**Data Protection → Replication → Replication Partners（データ保護 > レプリケーション > レプリケーションパートナー）**と選択します。**Replication Partners**（レプリケーションパートナー）画面に、既存のレプリケーションパートナー名のリストが表示されます。

レプリケーションパートナーのセットアップ

リモートシステムでも、複製元システムがパートナーになります。これで双方向レプリケーションの信頼関係が構築されます。複製元ボリュームと複製先ボリュームは、どちらのシステムにでも配置することができます。

レプリケーションパートナーを追加するには、次の手順を実行します。

1. **Data Protection → Replication → Replication Partners（データ保護 > レプリケーション > レプリケーションパートナー）**と選択します。

   Replication Partners（レプリケーションパートナー）画面が表示されます。
2. **追加**をクリックします。

   Add Replication Partner（レプリケーションパートナーの追加）画面が表示されます。
3. **Remote NAS management VIP**（リモート NAS 管理 VIP）に、リモートシステム NAS Manager の VIP アドレスを入力します。
4. **User name**（ユーザー名）と **Password**（パスワード）に、リモートシステムの管理者アカウントのユーザー名とパスワードを入力します。

   メモ: これらの値は Dell Fluid File System には保存されません。
5. **Save Changes**（変更の保存）をクリックします。

レプリケーションパートナーの設定変更

レプリケーションパートナーの設定は、パラメータを変更することで変更できます。

レプリケーションパートナーのパラメータを変更するには、次の手順を実行します。

1. **Data Protection → Replication → Replication Partners（データ保護 > レプリケーション > レプリケーションパートナー）**と選択します。

   Replication Partners（レプリケーションパートナー）画面に、既存のレプリケーションパートナー名のリストが表示されます。

2. **Replication Partner Name**（レプリケーションパートナー名）で、該当するレプリケーションパートナーを選択します。

   Edit Replication Partner（レプリケーションパートナーの編集）ページが表示されます。

3. 必要に応じて、**Remote NAS management VIP**（リモート NAS 管理 VIP）で VIP アドレスを変更します。

4. 必要に応じて、**User name**（ユーザー名）と **Password**（パスワード）で管理者の資格情報を変更します。

5. **Save Changes**（変更の保存）をクリックします。

レプリケーションパートナーの削除

システムのレプリケーションパートナーは、レプリケーションパートナーリストから削除することによって、削除することができます。レプリケーションパートナーを削除する場合は、両方のシステムがアップ状態で実行中であることを確認します。システムの一方がダウン状態か、またはアクセスできない場合、警告メッセージが表示されます。

レプリケーションパートナーの設定を削除するには、次の手順を実行します。

1. **Data Protection → Replication → Replication Partners（データ保護 > レプリケーション > レプリケーションパートナー）**と選択します。

   Replication Partners（レプリケーションパートナー）画面に、既存のレプリケーションパートナー名のリストが表示されます。

2. 既存のレプリケーションパートナーのリストから、適切なレプリケーションパートナーを選択して、**Delete（削除）**をクリックします。

NAS レプリケーションポリシー

ボリューム間のレプリケーションは、ポリシーを介して管理されます。次の手順を実行することにより NAS Manager を介して、接続ボリュームとしても知られる NAS のレプリケーションポリシーを作成することができます。

1. 複製元と複製先のシステム間の信頼の作成。

   これには、リモートシステムの IP アドレスの入力およびシステム管理者のユーザー名とパスワードの指定が必要です。

2. レプリケーションポリシーを追加します。

   これには、複製元ボリューム、複製先ボリュームの選択、およびレプリケーションの定期的なスケジュールの指定が必要です。

   複製先システムに複製元システムで使用できないデータがある場合、警告が発行され、このデータを失うことを認めるか尋ねられます。

3. レプリケーションの進行状況をモニタします。

   レプリケーションが順調に実行されていることを確認します。

   レプリケーションポリシーは削除することができ、複製先システムを書き込み可能にします。NAS レプリケーションポリシーの詳細については、『*Online Help*』（オンラインヘルプ）を参照してください。

   メモ: レプリケーションポリシーに関連付けられた場合、複製先ボリュームのレプリケーションは、**読み取り専用**です。

レプリケーションポリシーの追加

1. **Data Protection → Replication → Replication Partners（データ保護 > レプリケーション > NAS レプリケーション）** と選択します。

   NAS Replication（NAS レプリケーション）ページに、既存の NAS レプリケーションポリシーのリストが表示されます。
2. **追加** をクリックします。

   Add NAS Replication Policy（NAS レプリケーションポリシーの追加）ページが表示されます。
3. **Source NAS volume**（複製元 NAS ボリューム）に複製元 NAS ボリュームを入力するか、**Browse**（参照）ボタンをクリックして適切な NAS ボリュームを選択します。
4. **Destination cluster**（複製先クラスタ）リストから次のいずれかを選択します。

   – このシステムに複製元ボリュームをレプリケーションする場合は **localhost**（ローカルホスト）。
   – 使用可能な他の Dell Fluid File System レプリケーションパートナー。
5. **Destination NAS volume**（複製先 NAS ボリューム）に複製先 NAS ボリュームを入力するか、**Browse**（参照）ボタンをクリックして適切な NAS ボリュームを選択します。
6. 次のリカバリポイントスケジュールオプションからいずれか 1 つを選択します。

   – **Replicate every hour after（1 時間ごとにレプリケーション）**
   – **Replicate every day at（毎日定時にレプリケーション）**
   – **Replicate every week on（毎週決まった曜日にレプリケーション）**
   – **Replicate on demand (not scheduled)（オンデマンドでレプリケーション）（スケジュールなし）**
7. **Save Changes**（変更の保存）をクリックします。

レプリケーションポリシーの変更

1. **Data Protection → Replication → Replication Partners（データ保護 > レプリケーション > NAS レプリケーション）** と選択します。

   NAS Replication（NAS レプリケーション）ページに、既存の NAS レプリケーションポリシーのリストが表示されます。
2. **Source NAS Volume**（複製元 NAS ボリューム）列で適切な NAS ボリュームを選択します。

   Edit NAS Replication Policy（NAS レプリケーションポリシーの編集）ページが表示されます。
3. **Source NAS volume**（複製元 NAS ボリューム）に複製元 NAS ボリュームを入力するか、**Browse**（参照）ボタンをクリックして適切な NAS ボリュームを選択します。
4. **Destination cluster**（複製先クラスタ）リストから次のいずれかを選択します。

   – このシステムに複製元ボリュームをレプリケーションする場合は **localhost**（ローカルホスト）。
   – 使用可能な他の Dell Fluid File System レプリケーションパートナー。
5. **Destination NAS volume**（複製先 NAS ボリューム）に複製先 NAS ボリュームを入力するか、**Browse**（参照）ボタンをクリックして適切な NAS ボリュームを選択します。
6. 次のリカバリポイントスケジュールオプションからいずれか 1 つを選択します。

   – **Replicate every hour after（1 時間ごとにレプリケーション）**
   – **Replicate every day at（毎日定時にレプリケーション）**
   – **Replicate every week on（毎週決まった曜日にレプリケーション）**
   – **Replicate on demand (not scheduled)（オンデマンドでレプリケーション）（スケジュールなし）**
7. **Save Changes**（変更の保存）をクリックします。

NAS レプリケーションの一時停止、復帰、および実行

選択された NAS ボリュームのステータスに応じて、NAS レプリケーションをオンデマンドで一時停止、復帰、または実行することができます。

1. **Data Protection → Replication → Replication Partners（データ保護 > レプリケーション > NAS レプリケーション）** と選択します。

   NAS Replication（NAS レプリケーション）ページに、既存の NAS レプリケーションポリシーのリストが表示されます。
2. 既存の NAS ボリュームのリストから、該当する NAS ボリュームを選択します。
3. 選択した NAS レプリケーションを保留にするには、**Pause**（一時停止）をクリックします。
4. 選択した NAS レプリケーションの NAS レプリケーションを続行するには、**Resume**（復帰）をクリックします。
5. 選択した NAS ボリュームのレプリケーションをただちに開始するには、**Replicate Now**（今すぐレプリケーション）をクリックします。

レプリケーションポリシーの削除

レプリケーションポリシーを削除する際、両方のボリュームにソースシステムのシステム構成が含まれます。 ソースシステム構成をターゲットシステムボリュームに転送するのは任意です。 この構成には、ユーザー、クォータ、スナップショットポリシー、セキュリティスタイルおよびその他のプロパティが含まれます。 このオプションは災害復旧時に便利です。

メモ: レプリケーションポリシーをターゲットボリュームのシステムから削除すると警告メッセージが表示され、ソースシステムからもポリシーを削除する必要があります。

レプリケーションポリシーを削除するには、次の手順に従います。

1. **Data Protection（データ保護）→ Replication（レプリケーション）→ NAS Replication（NAS レプリケーション）** と選択します。

   NAS Replication（NAS レプリケーション）ページに、既存の NAS レプリケーションポリシーのリストが表示されます。
2. 既存の NAS ボリュームのリストから、適切な NAS ボリュームを選択し、**Delete（削除）**をクリックします。

レプリケーションを使用した災害復旧

レプリケーション機能を使用して、ソースクラスタ（クラスタ A） をそのバックアップクラスタ（クラスタ B）から再構築することができます。

メモ:

- **クラスタ A** — バックアップする必要のあるデータが含まれた複製元クラスタである。
- **クラスタ B** — バックアップクラスタであり、構成は完了しているがボリュームは作成されておらず、複製元クラスタ A からデータをバックアップする。

レプリケーションを使用した災害復旧を設定する前に、次の条件を満たしていることを確認してください。

- クラスタ A と クラスタ B は両方とも同じタイプと構成である。

  メモ: たとえば、クラスタ A が 4 基のクアッドコアプロセッサを搭載した NX3600 の場合、クラスタ B も 4 基のクアッドコアプロセッサを搭載した NX3600 でなければなりません。
- クラスタ B のレプリケーションバージョンは、クラスタ A と同じである。
- クラスタ B には、クラスタ A のすべてのデータをレプリケーションできるだけの十分な容量がある。
- クラスタ B のネットワーク設定（クライアント、SAN、など）はクラスタ A の設定とは異なりますが、両方のクラスタはレプリケーションプロセスを実行できるよう、相互に通信できなければなりません。

レプリケーションを使用した災害復旧の設定は、3 つのフェーズで構成されます。

- フェーズ 1 — クラスタ A と クラスタ B 間にレプリケーションの構造が構築される
- フェーズ 2 — クラスタ A が停止し、クライアント要求がバックアップクラスタ B にフェイルオーバーされる
- フェーズ 3 — クラスタ A のフェイルバックをクラスタ B からクラスタ A に復元する

単一ボリュームフェールオーバー用 DNS 設定

単一ボリュームフェールオーバーでは、フェールオーバーする NAS ボリュームのユーザーが、フェールオーバーしない他の NAS ボリュームのユーザーに影響することなく、正しく移行できるように環境を設定することが重要です。

NAS ボリュームが、ある NAS クラスタから別のクラスタにフェールオーバーした場合、アクセス用に使用されていた IP アドレスは、クラスタ A の IP アドレスからクラスタ B の IP アドレスに変わります。この変化を容易にするために DNS を使用するようお勧めします。単一ボリュームフェールオーバーが必要な場合、DNS エントリを各 NAS ボリュームと関連するように設定し、フェールオーバーが生じたら単一ボリュームの DNS エントリを変更するようお勧めします。

例えば、マーケティングとセールスがそれぞれ独自の NAS ボリュームを持ち、*marketing_share* と *sales_share* という名前の CIFS 共有が NAS ボリュームにあるとします。*FluidFSmarketing* という名前の DNS エントリがマーケティング用に作成され、セールス用には別の DNS エントリが *FluidFSsales* という名前で作成されます。両方のボリュームはソースクラスタ A の同じクライアントアクセス VIP のセットをポイントしています。マーケティングは **\\FluidFSmarketing\marketing** を使用してマーケティングのボリュームまたは共有にアクセスでき、セールスは **\\FluidFSsales\sales** を使用してセールスのボリュームまたは共有にアクセスできます。

当初、両方の DNS エントリ *FluidFSmarketing* と *FluidFSsales* は同じクライアントアクセス VIP のセットをポイントしていました。この時点で、*marketing* と *sales* 両方の共有に *FluidFSmarketing* または *FluidFSsales* のいずれかの DNS 名でアクセスが可能です。単一ボリュームをフェールオーバーさせたい場合（例えば *Marketing*）、*FluidFSmarketing* の DNS エントリを変更してクラスタ B 上のクライアントアクセス VIP を解決します。

各 NAS ボリュームに対してどちらの DNS エントリが使用されたかを追跡するために、表を維持することをお勧めします。これはフェールオーバーの実行とグループポリシーの設定の際に便利です。

メモ: 単一の FluidFS NAS クラスタに、2 セットのホーム共有を含めることはできません。クラスタ A とクラスタ B の両方が別々のサイト用に、またはユーザーベースでホーム共有を持っているとします。クラスタ A と クラスタ B は、ホーム共有を含むお互いの NAS ボリュームのレプリケーション先として使用されます。管理者がホーム共有を含むクラスタ A の NAS ボリュームをクラスタ B にフェールオーバーしようとすると、クラスタ B にはすでのホーム共有が定義されているため、この操作は拒否されます。

フェーズ 1 — 複製元クラスタ A とバックアップクラスタ B 間のレプリケーションパートナーシップの構築

1. クラスタ A にログオンします。
2. 複製元クラスタ A とバックアップクラスタ B 間にレプリケーションパートナーシップを設定します。
   レプリケーションパートナーの詳細に関しては、「レプリケーションパートナーのセットアップ」を参照してください。
3. クラスタ A のソースボリュームからクラスタ B のターゲットボリュームへのレプリケーションポリシーを作成します。
   レプリケーションポリシーの詳細に関しては、「レプリケーションポリシーの追加」を参照してください。

メモ: レプリケーションポリシーとは、ボリュームベースに一致するものです。次の例を参照してください。

ソースボリューム A1（クラスタ A）からターゲットボリューム B1（クラスタ B）

ソースボリューム A2（クラスタ A）からターゲットボリューム B2（クラスタ B）

.....

ソースボリューム A*n*（クラスタ A）からターゲットボリューム B*n*（クラスタ B）

メモ: FluidFS v2 は、レプリケーションポリシーの追加時にターゲットボリュームの自動生成をサポートします。FluidFS 1.0 では、クラスタ B にターゲットボリュームを作成して、ボリュームサイズがクラスタ A 内の対応するソースボリュームデータを格納するのに十分な大きさであることを確認する必要があります。

4. クラスタ A のソースボリュームすべてに対して少なくとも 1 つのレプリケーションが成功するよう、レプリケーションスケジューラを開始します。

   レプリケーションが失敗したら、発生した問題を解決してレプリケーション処理を再スタートします。これにより、クラスタ A 内のすべてのソースボリュームの正しいレプリケーションコピーが、クラスタ B に少なくとも 1 つ作成されることが確実となります。規則的なレプリケーションをスケジュールして、クラスタ B 内のターゲットボリュームには常に、クラスタ A の最新のレプリケーションコピーがあるようにします。

注意: レプリケーションによる復元は完全な BMR 復元ではなく、ネットワーク構成（クライアント、SAN、および IC）のような設定は、レプリケーションの方法ではバックアップして復元することはできません。将来のために、ネットワーク構成を含むすべてのクラスタ A の設定（クラスタ A の復元時に使用）、ボリューム名、アラート設定、およびその他のクラスタ全般の設定をメモしておきます。 システムの復元操作でこれらの設定を復元できなかった場合、手動でクラスタ A の設定を元の値に戻すことができます。

フェーズ 2 — クラスタ A が停止し、クライアント要求がバックアップクラスタ B にフェイルオーバーされる

予期しないエラー（ハードウェア、ディスクなど）によりソースクラスタ A が停止した場合、次の手順を実行してください。

1. バックアップクラスタ A にログオンします。
2. すべてのレプリケーションターゲットボリュームの既存レプリケーションポリシーをすべて削除します。
   - 宛先クラスタ B からレプリケーションポリシーを削除する場合 — FluidFS レプリケーションマネージャがソースクラスタ A と通信しようとしますが失敗します。宛先クラスタ B のボリュームには、**Cluster Management（クラスタ管理）→ Restore NAS Volume Configuration（NAS ボリューム設定の復元）**を使用して、設定が復元されている必要があります。
   - ソースクラスタ B からレプリケーションポリシーを削除する場合 — ソースボリュームの設定を宛先ボリュームに適用するかどうかのオプションが与えられます。このオプションを選択し忘れたり失敗した場合、**Cluster Management（クラスタ管理）→ Restore NAS Volume Configuration（NAS ボリューム設定の復元）**を使用して、クラスタ A からのソースボリュームの設定をクラスタ B の宛先ボリュームに復元することができます。
3. バックアップクラスタ B でのレプリケーションポリシーの削除と、クラスタ A からのソースボリューム設定の適用を承認します。

   現時点で復元できるボリューム設定は次のとおりです。
   - NFS エクスポート
   - CIFS 共有
   - クォータルール
   - スナップショットスケジュール
   - NAS ボリュームアラート、セキュリティ方式、および関連パラメータ

- NAS ボリューム名
- NAS ボリュームサイズ

これによって、ターゲットボリューム（B1、B2、.. B*n*）がスタンドアロンボリュームに変換されます。この手順を繰り返して、クラスタ B のすべてのターゲットボリュームを、クラスタ A からのボリューム設定が適用されたスタンドアロンボリュームにします。

4. NAS Manager web インターフェースで、クラスタ A からの NAS システム構成を復元します。

   NAS システム構成の詳細に関しては、「クラスタ設定の復元」を参照してください。

   これにより、クラスタ B の設定がクラスタ A の設定に復元されます。現在、次のクラスタシステム設定が復元可能です：

   - プロトコル設定
   - ユーザーおよびグループ
   - ユーザーマッピング
   - 監視設定
   - 時刻設定
   - アンチウイルスホスト

5. フェイルオーバータイム中は、クライアントの要求に応えるのに一時的にクラスタ B が使用されるようにします。

   管理者は、次の手順を実行して DNS と認証を設定する必要があります。

   a) DNS サーバーから、クラスタ A ではなくクラスタ B へ DNS 名をポイントします。

      クラスタ B の DNS サーバーが、クラスタ A の DNS サーバーと同じまたは、同じ DNS ファーム内にあることを確認します。既存のクライアント接続は切断されるため、再確立する必要があります。クライアントの NFS エクスポートをアンマウントしてから再度マウントする必要もあります。

      メモ: 単一ボリュームのフェールオーバーには、手順 b、c、および d のみを完了します。

   b) DNS では、ファールオーバーした NAS ボリューム用の DNS エントリを手動でアップデートします。

      この手順は、このボリュームにクラスタ A からアクセスしていたエンドユーザーを、引き続き同じ DNS 名を使用してアクセスしている間に、クラスタ B に再ポイントさせるためです。

      メモ: クライアントシステムでは、DNS キャッシュを更新する必要があります。

   c) CIFS と NFS クライアントをクラスタ B に強制するには、クラスタ A の CIFS 共有と NFS エクスポートも削除する必要があります。

      これにより、 CIFS と NFS クライアントをクラスタ B に接続されていた時のように、強制的に再接続させます。クラスタ B のソースボリューム設定が復元された後、すべての共有とエクスポートは宛先ボリューム（クラスタ B 上）に存在するため、共有 / エクスポートの設定情報が紛失することはありません。

   d) フェールオーバーしたボリュームは、クラスタ B でホストされていることだけを除いて、クラスタ A でホストされていたものと全く同じ DNS 名と共有名を使用してアクセス可能となります。

      メモ: NFS マウントはアンマウントしてから再度マウントする必要があります。アクティブな CIFS の転送はこの処理中に失敗しますが、CIFS 共有がローカルドライブとしてマップされていれば、レプリケーションが削除され、DNS がアップデートされてクラスタ A の NFS/CIFS 共有が削除されると、自動的に再接続されます。

   e) AD サーバーまたは LDAP/NIS に参加します。

      AD と LDAP が同じ AD/LDAP ファームまたは同じサーバーにあるようにします。

フェーズ 3 — クラスタ A のフェイルバックをクラスタ B からクラスタ A に復元

1. クラスタ A が失敗（ハードウェアの交換、ディスクの交換など）した理由を是正し、必要に応じて FluidFS を再インストールします。
2. クラスタ（前に保存しておいたクラスタ A の設定を使用）をリビルドし、NAS リザーブをフォーマットし、前と同様にネットワーク（クライアント、SAN および IC）を設定します。
3. クラスタ B にログオンして、クラスタ B とクラスタ A のレプリケーションパートナーシップを設定します。

   レプリケーションパートナーの詳細に関しては、「レプリケーションパートナーのセットアップ」を参照してください。
4. クラスタ B のソースボリュームからクラスタ A のターゲットボリュームへのレプリケーションポリシーを作成します。

   レプリケーションポリシーの詳細に関しては、「レプリケーションポリシーの追加」を参照してください。

   メモ: レプリケーションポリシーとは、ボリュームベースに一致するものです。次の例を参照してください。

   ソースボリューム B1（クラスタ B）からターゲットボリューム A1（クラスタ A）

   ソースボリューム B2（クラスタ B）からターゲットボリューム A2（クラスタ A）

   .....

   ソースボリューム B*n*（クラスタ B）からターゲットボリューム A*n*（クラスタ A）

   メモ: FluidFS v2 は、レプリケーションポリシーの追加時にターゲットボリュームの自動生成をサポートします。FluidFS 1.0 では、クラスタ B にターゲットボリュームを作成し、ボリュームサイズがクラスタ A 内の対応するソースボリュームデータを格納するのに十分な大きさであることを確認する必要があります。
5. NAS Manager ウェブインターフェースで、**Data Protection（データ保護）→ Replication（レプリケーション）→ NAS Replication（NAS レプリケーション）**を選択して、クラスタ B の全ボリューム（B1、B2、.., B*n*）に対して **Replicate Now（今すぐレプリケーションを行う）**をクリックします。

   レプリケーションが失敗したら、発生した問題を解決してレプリケーション処理を再スタートします。すべてのボリュームがクラスタ A に正しくレプリケートされていることを確認します。
6. すべてのボリューム（B1、B2、.. B*n*）のレプリケーションポリシーを削除し、クラスタ B からクラスタ A へのソースボリューム構成を適用します。

   この手順を繰り返してすべてのレプリケーションポリシーを削除し、クラスタ A の全ターゲットをスタンドアロンボリュームに持ち込みます。

   - 宛先クラスタ B からレプリケーションポリシーを削除する場合 — FluidFS レプリケーションマネージャがソースクラスタ A と通信しようとしますが失敗します。宛先クラスタ B のボリュームには、**Cluster Management（クラスタ管理）→ Restore NAS Volume Configuration（NAS ボリューム設定の復元）**を使用して、設定が復元されている必要があります。
   - ソースクラスタ B からレプリケーションポリシーを削除する場合 — ソースボリュームの設定を宛先ボリュームに適用するかどうかのオプションが与えられます。このオプションを選択し忘れたり失敗した場合、**Cluster Management（クラスタ管理）→ Restore NAS Volume Configuration（NAS ボリューム設定の復元）**を使用して、クラスタ A からのソースボリュームの設定をクラスタ B の宛先ボリュームに復元することができます。
7. クラスタ A にログオンします。
8. NAS Manager ウェブインターフェースで、クラスタ B からの NAS システム構成を復元します。

   NAS システム構成の詳細に関しては、「クラスタ設定の復元」を参照してください。

   これにより、プロトコル設定、時間設定、認証パラメータなどのグローバル構成設定がクラスタ B 設定に変更されます。

メモ: システム構成の復元に失敗した場合、手動で元の設定に戻します（前に保存しておいたクラスタ A の設定を使用）。

クラスタ A が元の設定に復元されます。

9. クラスタ A の使用を開始して、クライアント要求に応えます。

   管理者は、次の手順を実行して DNS と認証を設定する必要があります。

   a) DNS サーバーから、クラスタ B ではなくクラスタ A へ DNS 名をポイントします。

      クラスタ A の DNS サーバーが、クラスタ B の DNS サーバーと同じまたは、同じ DNS ファーム内にあることを確認します。既存のクライアント接続は切断されるため、この処理中に再確立する必要があります。

      メモ: 単一ボリュームのフェールオーバーには、手順 b、c、および d のみを完了します。

   b) DNS では、ファールオーバーした NAS ボリューム用の DNS エントリを手動でアップデートします。

      この手順は、このボリュームにクラスタ B からアクセスしていたエンドユーザーを、引き続き同じ DNS 名を使用してアクセスしている間に、クラスタ A に再ポイントさせます。

      メモ: クライアントシステムでは、DNS キャッシュを更新する必要があります。

   c) CIFS と NFS クライアントをクラスタ A に強制するには、クラスタ B の CIFS 共有と NFS エクスポートも削除する必要があります。

      これにより、 CIFS と NFS クライアントを、クラスタ A に接続されていた時のように強制的に再接続させます。クラスタ A のソースボリューム設定が復元された後、すべての共有とエクスポートは宛先ボリューム（クラスタ A 上）に存在するため、共有 / エクスポートの設定情報が紛失することはありません。

   d) フェールオーバーしたボリュームは、クラスタ A でホストされていることを除いて、クラスタ B でホストされていたものと全く同じ DNS 名と共有名を使用してアクセス可能となります。

      メモ: NFS マウントはアンマウントしてから再度マウントする必要があります。アクティブな CIFS の転送はこの処理中に失敗しますが、CIFS 共有がローカルドライブとしてマップされていれば、レプリケーションが削除され、DNS がアップデートされてクラスタ B の NFS/CIFS 共有が削除されると、自動的に再接続されます。

   e) AD サーバーまたは LDAP/NIS に参加します。

      AD と LDAP が同じ AD/LDAP ファームまたは同じサーバーにあるようにします。

10. ソースクラスタ A とバックアップクラスタ B 間のレプリケーション構造を構築して、クラスタ A とクラスタ B のレプリケーションポリシーを設定し、クラスタ B をレプリケーションターゲットボリュームとして使用し、次の災害復旧に備えます。

データのバックアップと復元

メモ: 一定期間ごとにデータをバックアップすることをお勧めします。

NAS cluster（NAS クラスタ）ソリューションは、Network Data Management Protocol（NDMP）を使用したデータのバックアップおよび復元をサポートしています。NAS cluster（NAS クラスタ）ソリューションにインストールされた NDMP エージェントにより、NDMP プロトコルに対応している業界標準のデータ管理アプリケーション（DMA）を使用して、保存されたデータをバックアップおよび復元できます。ベンダー固有のエージェントを NAS アプライアンスにインストールする必要はありません。

バックアップおよび復元操作を実行するには、DMA が LAN またはクライアントネットワークを使用して NAS アプライアンスにアクセスできるよう設定しておく必要があります。NAS cluster（NAS クラスタ）ソリューションでは、バックアップ操作に専用アドレスは使用しません。バックアップおよび復元操作には、設定済みの任意の LAN またはクライアントネットワークアドレスを使用できます。

NAS cluster（NAS クラスタ）ソリューションでの NDMP バックアップは、LAN またはクライアントネットワークを使用して実行されます。DMA は NAS cluster（NAS クラスタ）ソリューションのクライアント VIP（または DNS 名）のいずれかにアクセスできるよう設定されていなければなりません。

NAS cluster（NAS クラスタ）ソリューションは、LAN またはクライアントネットワークに設定されている専用のバックアップ IP アドレスをサポートしません。LAN またはクライアントネットワークに設定されたすべての仮想 IP は、バックアップソフトウェアでのバックアップおよび復元に使用できます。

NAS cluster（NAS クラスタ）ソリューションは、NDMP エージェントを有効にする一般的なユーザーインタフェースを提供するほか、インストールされている NDMP エージェントから独立して動作するようプログラムされています。

レプリケーションターゲットの NAS ボリュームのバックアップ

レプリケーションターゲットボリュームのバックアップを実行する際、FluidFS は専用の NDMP スナップショットを作成しません。 FluidFS は代わりに、前回成功したレプリケーションからベースレプリカスナップショットを使用します。

レプリケーションと NDMP バックアップのスケジュールが重なる場合、ターゲットボリュームの NDMP バックアップ実行中に、新しいレプリケーション操作が実行されて完了する可能性もあります。 この場合、レプリケーション操作により前のベースレプリカスナップショットが削除されて、新しいベースレプリカが作成されます。

注意: これにより、NDMP バックアップは終了します。 このシナリオを回避するためには、NDMP バックアップがレプリケーション開始前に完了するようレプリケーションとバックアップ操作をスケジュールしてください。

NDMP 設計の考慮事項

- DMA でバックアップを設定する場合は、NDMP サーバー用に DNS 名を使用してください。これにより負荷バランシングが使用されます。
- 同時バックアップジョブ数はコントローラ 1 台につき 1 つに制限してください。データ転送が速くなります。
- お使いのソリューションは、3-way バックアップのみをサポートしています。3-way バックアップでは、DMA サーバーが NAS アプライアンスとストレージデバイス間のデータ転送を調整します。DMA サーバーに十分な帯域幅があることを確認してください。

サポートされているアプリケーション

NAS cluster（NAS クラスタ）ソリューションは次の DMA で動作することが確認されています。

- Symantec BackupExec 2010 R3 および Symantec BackupExec 2012
- Symantec NetBackup 7.0 以降
- CommVault Simpana 9.0 以降
- IBM Tivoli 6.3

NDMP サポートの有効化

NDMP バックアップはクライアントネットワークを使用して実行されます。DMA は、NAS クラスタのクライアント VIP（または DNS 名）のいずれかにアクセスするように設定する必要があります。

メモ: NDMP サポートを有効化する前に、システムでクライアント VIP が設定されていなければなりません。クライアント VIP が設定されているかどうかを確認するには、**System Management → Network → Subnets（システム管理 > ネットワーク > サブネット）**と選択し、**Primary**（プライマリ）サブネットが設定されていることを確認します。

NDMP サポートを有効にするには、次の手順を行います。

1. **Data Protection → NDMP → NDMP Configuration（データ保護 > NDMP > NDMP の設定）** と選択します。
   NDMP Configuration（NDMP の設定）ページが表示されます。
2. **Enable NDMP**（NDMP の有効化）を選択します。

   メモ: 初めは **backup_user** パスワードは設定されていません。ユーザー名を変更するかデフォルトを使用した後で、パスワードも設定する必要があります。

   メモ: デフォルトの NDMP クライアントポートは 10000 です。
3. **DMA server**（DMA サーバー）で、承認済み DMA サーバーの IP アドレスを入力します。

   メモ: DNS 名はサポートされていません。
4. **変更の保存** をクリックします。

NDMP パスワードとバックアップユーザー名の変更

DMA で NDMP サーバーを設定する際、ユーザー名とパスワードが必要です。デフォルトのユーザー名は **backup_user** です。デフォルトパスワードはランダムに抽出されており、NDMP を使用する前に変更する必要があります。
NDMP パスワードを変更するには、次の手順を実行します。

1. **Data Protection → NDMP → NDMP Configuration（データ保護 > NDMP > NDMP の設定）** と選択します。
   NDMP Configuration（NDMP の設定）ページが表示されます。
2. 必要に応じて、**Backup username**（バックアップユーザー名）で現在のバックアップユーザー名を変更し、**Save Changes**（変更の保存）をクリックします。
   バックアップユーザー名が変更されます。
3. **Change Backup User Password**（バックアップユーザーパスワードの変更）をクリックします。
   Change Password（パスワードの変更）ウィンドウに現在のバックアップユーザー名が表示されます。
4. **admin password**（管理者パスワード）に既存の管理者パスワードを入力します。
5. Backup username（バックアップユーザー名）の下の **New password**（新しいパスワード）に、新しいパスワードを入力します。
6. **Retype password**（パスワードの再入力）に、**New password**（新しいパスワード）フィールドで入力したパスワードを正確に入力します。
7. **Save Changes**（変更の保存）をクリックします。

DMA サーバーリストの変更

NAS cluster（NAS クラスタ）ソリューションの NDMP のバックアップを取得するには、DMA サーバーのホワイトリストにバックアップアプリケーションサーバーが含まれている必要があります。

DMA サーバーの追加

DMA サーバーをリストに追加するには、次の手順を実行します。

1. **Data Protection → NDMP → NDMP Configuration（データ保護 > NDMP > NDMP の設定）** と選択します。
   NDMP Configuration（NDMP の設定）ページが表示されます。
2. 空の **DMA server**（DMA サーバー）フィールドがない場合は、**Add DMA server**（DMA サーバーの追加）をクリックします。
   別の **DMA server**（DMA サーバー）フィールドが追加されます。
3. 空の **DMA server**（DMA サーバー）に、DMA サーバーの IP アドレスを入力します。

メモ: DNS 名はサポートされていません。

4. **Save Changes**（変更の保存）をクリックします。

DMA サーバーの削除

DMA サーバーをリストから削除するには、次の手順を実行します。

1. **Data Protection → NDMP → NDMP Configuration（データ保護 > NDMP > NDMP の設定）** と選択します。
   NDMP Configuration（NDMP の設定）ページが表示されます。
2. 適切な DMA サーバーを選択して、**Remove DMA Server**（DMA サーバーの削除）をクリックします。

   メモ: ホワイトリストから DMA サーバーを削除しても、この DMA サーバーが関連している進行中のバックアップ復元動作は中断されません。

バックアップ用 NAS ボリュームの指定

ほとんどのバックアップアプリケーションでは、バックアップに使用できるボリュームが自動的にリストされます。Symantec NetBackup 7.0 では、ボリュームパスを手動で入力できます。

NAS クラスタソリューションでは、次のパスにバックアップボリュームが表示されます。

/<NASVolumeName>

ここで **<NASVolumeName>** は、ユーザーインタフェースに表示されるのと同じ名前です。

アクティブな NDMP ジョブの表示

NAS cluster（NAS クラスタ）ソリューションによって実行されるすべてのバックアップまたは復元操作は、**NDMP Active Jobs（NDMP アクティブジョブ）**ページで表示できます。アクティブな NDMP ジョブを表示するには、**Data Protection → NDMP → NDMP Active Jobs（データ保護 > NDMP > NDMP アクティブジョブ）** または **Monitor → NDMP Active Jobs（モニタ > NDMP アクティブジョブ）** と選択します。

アクティブな NDMP ジョブの終了

アクティブな NDMP ジョブを終了することができます。アクティブな NDMP ジョブを終了するには、次の手順を実行します。

1. **Data Protection → NDMP → NDMP Active Jobs（データ保護 > NDMP > NDMP アクティブジョブ）** と選択します。
   NDMP Active Jobs（NDMP アクティブジョブ）ページにアクティブな NDMP ジョブがすべて表示されます。
2. 終了するセッションを選択します。
3. **Kill Active NDMP Job**（アクティブな NDMP ジョブの終了）をクリックします。

   メモ: 一度に複数のセッションを選択することができます。

アンチウイルスアプリケーションの使用

NAS cluster（NAS クラスタ）ソリューションは、業界標準の ICAP 対応アンチウイルスソフトウェアと機能を統合することで、CIFS クライアントから書き込まれるファイルにウイルスが含まれるのを阻止します。アンチウイルスホストでは、ICAP 対応の Symantec ScanEngine 5.2 または Symantec Protection Engine for Cloud Services 7.0 を実行する必要があります。

既存のアンチウイルスホストの表示

システムに定義されているアンチウイルスホストを表示するには、**Data Protection → Antivirus → Antivirus Hosts（データ保護 > アンチウイルス > アンチウイルスホスト）**と選択します。**Antivirus Hosts**（アンチウイルスホスト）ページに、定義済みのアンチウイルスホスト、その IP アドレス（または名前）、および ICAP ポートが表示されます。

アンチウイルスホストの追加

ウイルススキャンの可用性を高め、ファイルアクセスの待ち時間を減らすために、複数のアンチウイルスホストを定義しておくことをお勧めします。使用できるアンチウイルスホストがない場合、ファイルアクセスが拒否されてサービスに不備が生じる可能性があります。
アンチウイルスオプションを有効にするには、次の手順を行います。

1. **Data Protection → Antivirus → Antivirus Hosts（データ保護 > アンチウイルス > アンチウイルスホスト）**と選択します。
   Antivirus Hosts（アンチウイルスホスト）ページに、既存のアンチウイルスホストが表示されます。
2. 空の **Antivirus host**（アンチウイルスホスト）フィールドがない場合は、**Add**（追加）をクリックします。
   別の **Antivirus host**（アンチウイルスホスト）フィールドが追加されます。
3. **Antivirus host**（アンチウイルスホスト）に、アンチウイルスホストの IP アドレス（または名前）を入力します。
4. **Port**（ポート）に、ホスト ICAP プロトコルがリッスンしているポートを入力します。
   デフォルトの ICAP ポートは 1344 です。
5. **Save Changes**（変更の保存）をクリックします。

アンチウイルスホストの削除

アンチウイルスホストのリストからホストを削除するには、次の手順を実行します。

1. **Data Protection → Antivirus → Antivirus Hosts（データ保護 > アンチウイルス > アンチウイルスホスト）**と選択します。
   Antivirus Hosts（アンチウイルスホスト）ページに、既存のアンチウイルスホストが表示されます。
2. 使用可能なアンチウイルスホストのリストから、適切なアンチウイルスホストを選択し、**Delete**（削除）をクリックします。

CIFS 共有ごとのアンチウイルスサポートの有効化

アンチウィルスサポートは、CIFS 共有ごとに利用できます。
CIFS 共有ごとのアンチウイルスサポートを有効にするには：

1. **User Access（ユーザーアクセス） → Shares（共有） → CIFS Shares（CIFS 共有）**をクリックします。
2. アンチウイルスサポートを有効にしたい CIFS 共有をクリックします。
3. ページ下側にある **Files should be checked for viruses**（ファイルのウイルスチェックを行う）チェックボックスにチェックを入れます。
4. ページ上部、**General**（一般）および **Advanced**（詳細設定）の隣に表示される **Antivirus**（アンチウイルス）リンクをクリックします。
5. ウイルス感染したファイルに対する処理動作を設定します（オプション）。

6. ウイルスチェックを行うファイルを設定します（オプション）。
7. 除外リストを設定します（オプション）。
8. **変更の保存** をクリックします。

5

FluidFS NAS ソリューションの管理

Cluster Management（クラスタの管理）タブから、一般システム情報の表示と設定、ファイルシステムパラメータとネットワークパラメータの設定、および必要なプロトコルの設定ができます。さらに、認証設定も設定することができます。
Cluster Management（クラスタの管理）オプションにアクセスするには、NAS Manager を始動します。**Cluster Management**（クラスタの管理）タブをクリックします。**General Information**（一般情報）ページが表示されます。

システムの管理

NAS Manager を使用して、クラスタで管理操作を行うことができます。
NAS Manager にアクセスするには、NAS 管理の仮想 IP アドレスが必要です。 この IP アドレスを使用すると、クラスタを単一のエンティティとして管理できます。
システム内の個別コントローラとシステムの両方に対してその他の IP アドレスも必要となります。クライアント はこれらの IP アドレスに直接アクセスできません。

クライアントアクセスの管理

Subnets（サブネット）ページでは、クライアントがシステムの共有およびエクスポートへのアクセスに使用する仮想 IP アドレスを 1 つまたは複数設定できます。お使いのネットワークがルーティングされている場合は、複数の仮想 IP アドレスを定義しておくことをお勧めします。
複数のサブネットを定義すると、クライアントはルータを経由せずに直接 NAS cluster（NAS クラスタ）ソリューションにアクセスできるようになります。IP アドレス間の負荷バランシングを有効にするには、お使いの DNS サーバー上で、各サブネットに対して単一の名前を設定します。

メモ: すべての仮想 IP アドレスは、現場のシステム管理者が割り当てたネットワーク上で有効な IP アドレスでなければなりません。

Subnets（サブネット）ページでは、管理および相互接続のためにシステム内部で使用する IP アドレスの範囲をアップデートすることもできます。
システムサブネットについては、現在の設定の表示、新しいサブネット情報の追加、既存サブネットの削除または変更が可能です。IP アドレス間の負荷バランシングを有効にするには、お使いの DNS サーバー上で、各サブネットに対して単一の名前を設定します。

定義済みサブネットの表示

定義済みサブネットを表示するには、**Cluster Management → Network → Subnets（クラスタの管理 > ネットワーク > サブネット）** と選択して、**Subnets**（サブネット）ページに既存のサブネットのリストを表示します。

サブネットの追加

1. **Cluster Management → Network → Subnets（クラスタの管理 > ネットワーク > サブネット）** と選択します。

Subnets（サブネット）ページに、既存のサブネットのリストが表示されます。

2. **追加** をクリックします。
   Add/Edit Subnet（サブネットの追加 / 編集）ページが表示されます。
3. **Subnet name**（サブネット名）に、サブネットに適した名前を入力します。
4. **Physical network**（物理ネットワーク）リストから適切なネットワークを選択します。
5. **Subnet mask**（サブネットマスク）リストにサブネットマスクアドレスを入力します。
6. 該当する場合は、サブネットの VLAN ID を指定します。

   メモ: VLAN ID は、VLAN が複数のスイッチにまたがっている場合に、どのポートとインタフェースがブロードキャストパケットを送信するかを指定するために使用されます。
7. **Management console VIP**（管理コンソール VIP）に、システム管理コンソールの IP アドレスを入力します。
8. **Private IP**（プライベート IP）に、各コントローラに対応する個々のシステムコントローラの IP アドレスを入力します。

   メモ: これらの IP アドレスは、テクニカルサポートによってコントローラの管理に使用されます。
9. **VIP address**（VIP アドレス）に、1 つまたは複数のクライアントの仮想 IP アドレスを入力します。

   メモ: これらの VIP は、システム上のファイルへのアクセスに使用されます。

   メモ: VIP の数はネットワークの構成によって異なります。詳細については、オンラインヘルプを参照してください。
10. **変更の保存** をクリックします。

サブネットの変更

メモ: プライマリサブネット、または内部サブネット（相互接続および管理）の名前の変更はできません。内部サブネットの IP アドレスをアップデートする必要がある場合は、希望の IP アドレスを編集する前にファイルシステムを停止する必要があります。

メモ: 初期展開の後は、相互接続または管理用サブネットを変更しないでください。初期展開で設定されるこれらのサブネットは、最適な機能性のために重要です。

1. **Cluster Management（クラスタの管理）** → **Network（ネットワーク）** → **Subnets（サブネット）** と選択します。
   Subnets（サブネット）ページに、既存のサブネットのリストが表示されます。
2. 表示されたサブネットのリストから、**Subnet Name（サブネット名）** 列の下の適切なサブネットを選択します。
   選択したサブネットに対する **Add/Edit Subnet**（サブネットの追加 / 編集）ページが表示されます。
3. 必要に応じてパラメータの変更を行います。
4. **変更の保存** をクリックします。

サブネットの削除

メモ: プライマリサブネット、または内部サブネット（相互接続および管理）を削除することはできません。

1. **Cluster Management（クラスタの管理）** → **Network（ネットワーク）** → **Subnets（サブネット）** と選択します。
   Subnets（サブネット）ページに、既存のサブネットのリストが表示されます。
2. 表示されたサブネットのリストから該当するサブネットを選択し、**Delete（削除）** をクリックします。

管理者ユーザーの管理

管理者は、Dell Fluid File System CLI またはウェブインタフェースを使用して Dell Fluid File System を管理することができます。

管理者ユーザーの表示

既存の管理者ユーザーを表示するには、**Cluster Management → General → Administrators（クラスタの管理 > 一般 > 管理者）**を選択します。**Administrators**（管理者）ページに、現在定義されている管理者のリストが表示されます。

システム管理者の追加

システム管理者の定義時、システム管理者のパーミッションレベルを指定します。パーミッションレベルはシステムであらかじめ定義されています。
定義済みのパーミッションレベルは次のとおりです。

- システム管理者
- 表示のみ

パーミッションレベルは、このレベルのユーザーに許可されているアクション一式を定義します。
システム管理者を追加するには、次の手順を実行します。

1. NAS Manager で、**Cluster Management → General → Administrators（クラスタの管理 > 一般 > システム管理者）** と選択します。
   Administrators（システム管理者）ページが表示されます。
2. **追加** をクリックします。
   Add Administrator（システム管理者の追加）ページが表示されます。デフォルトで、**Properties**（プロパティ）タブが表示されます。
3. **User name**（ユーザー名）に、システム管理者用の名前を入力します。
4. **Password**（パスワード）に、6 文字以上のパスワードを入力します。
5. **Retype password**（パスワードの再入力）に、password（パスワード）フィールドに入力したパスワードを正確に入力します。

   メモ: パスワードが簡単すぎる場合、より複雑なパスワードを入力するように求められます。
6. **User ID**（ユーザー ID）に、UID を入力するか、システムが提供するデフォルトの UID を使用します。
7. **Level**（レベル）リストから、システム管理者用のパーミッションレベルを選択します。**3-Administrator**（3-システム管理者）または **4-View only**（4-表示のみ）を選択できます。

   メモ: 自分より階層的に低いパーミッションレベルを持つ他のシステム管理者しか定義することはできません。
8. **E-mail address**（電子メールアドレス）で、それぞれの使用可能な **E-mail address**（電子メールアドレス）フィールドにシステム管理者の電子メールアドレスを入力します。
   システムは、この電子メールアドレスを使用して警告をシステム管理者に送信します。**Add Email address**（電子メールアドレスの追加）をクリックして、追加の電子メールアドレスを追加することができます。
   Filters（フィルタ）タブを使用して、システム管理者に送信する電子メール警告のタイプを設定することができます。
9. **Filters**（フィルタ）タブを選択して、SNMP トラップに対するフィルタルールを定義します。
10. トラップの各カテゴリ用に送信される、トラップの最低重要度を定義します。

メモ: デフォルトオプションでは、すべてのカテゴリについて **Major**（主要）トラップが送信されます。

11. **変更の保存** をクリックします。

システム管理者の変更

1. **Cluster Management → General → Administrators（クラスタの管理 > 一般 > 管理者）** と選択します。
   Administrators（管理者）ページが開き、現在定義されているシステム管理者が表示されます。
2. 使用可能な管理者リストの **User Name**（ユーザー名）列で、該当する管理者をクリックします。
   Edit Administrator（管理者の編集）ページが表示されます。デフォルトでは、**Properties**（プロパティ）タブが選択されています。
3. 選択した管理者の **Level**（レベル）と **Email address**（電子メール アドレス）を変更できます。
4. **Filters**（フィルタ）タブでは、項目ごとに SNMP トラップのフィルタルールを変更できます。
5. **Save Changes**（変更の保存）をクリックします。

管理者パスワードの変更

注意: Dell Compellent FS8600 では、管理者パスワードを変更すると、Enterprise Manager とクラスタ間の接続ができなくなります。Enterprise Manager とクラスタ間の接続を再度確立するには、admin password（管理者パスワード）を変更した後、Enterprise Manager で Reconnect to FluidFS Cluster（FluidFS クラスタに再接続）をクリックします。

1. **Cluster Management（クラスタの管理）→ General（一般）→ Administrators（管理者）** と選択します。
   Administrators（管理者）ページが開き、現在定義されているシステム管理者が表示されます。
2. 使用可能な管理者リストの **User Name**（ユーザー名）列で、該当する管理者をクリックします。
   Edit Administrator（管理者の編集）ページが表示されます。デフォルトでは、**Properties**（プロパティ）タブが選択されています。
3. **Change Password**（パスワードを変更）をクリックします。
   Change Password（パスワードの変更）ウィンドウが表示されます。
4. **admin password**（管理者パスワード）に、選択した管理者の現在のパスワードを入力します。
5. **New password**（新しいパスワード）の **admin**（管理者）に新しいパスワードを入力します。
6. **Retype password**（パスワードの再入力）に、**New password**（新しいパスワード）フィールドで入力したパスワードを正確に入力します。
7. **Change Password**（パスワードの変更）ウィンドウで **Save Changes**（変更の保存）をクリックします。
   Edit Quota（クォータの編集）ページが表示されます。
8. **変更の保存** をクリックします。

管理者の削除

1. **Cluster Management（クラスタの管理）→ General（一般）→ Administrators（管理者）** と選択します。
   Administrators（管理者）ページが開き、現在定義されているシステム管理者が表示されます。
2. 使用可能な管理者のリストから、関連する管理者を選択し、**Delete（削除）**をクリックします。

ローカルユーザーの CIFS および NFS アクセスの管理

メモ: 現場で外部 NIS/LDAP データベースが設定されている場合は、この項を省略してください。

ローカルユーザーを設定すると、それらのユーザーは外部 NIS、LDAP、または Active Directory が導入されてもクラスタに接続することができます。

ローカルユーザーの場合、ファイルシステムへのアクセスはボリューム、共有、およびエクスポートによって決定されます。

NAS cluster（NAS クラスタ）ソリューションでローカルユーザーの定義を使用できるようにするには、次の手順を実行します。

1. **Cluster Management → Authentication → Identity Management Database（クラスタの管理 > 認証 > ID 管理データベース）**と選択します。

   Identity Management Database（ID 管理データベース）ページが表示されます。
2. **Users are not defined in an external user database**（ユーザーは外部ユーザーデータベースで定義されていない）を選択します。
3. CIFS ユーザーの場合は、**Cluster Management → Protocols → CIFS Configuration（クラスタの管理 > プロトコル > CIFS 設定）**と選択します。

   CIFS Protocol Configuration（CIFS プロトコルの設定）ページが表示されます。
4. ユーザーの ID の認証に使用するモードを選択します。次のいずれかを選択できます。

   - **Authenticate users' identity via Active Directory and local user database（Active Directory およびローカルユーザーデータベース経由でユーザー ID を認証する）**
   - **Authenticate users' identity via local users database（ローカルユーザーデータベースを経由してユーザー ID を認証する）**
5. **Local Users**（ローカルユーザー）リストを管理するには、**Cluster Management → Authentication → Local Users（クラスタの管理 > 認証 > ローカルユーザー）**と選択します。

ローカルユーザーの表示

既存のユーザーのリストを表示するには、**Cluster Management → Authentication → Local Users（クラスタの管理 > 認証 > ローカルユーザー）**と選択して、**Local User**（ローカルユーザー）ページに既存のユーザーのリストを表示します。

ローカルユーザーの追加

1. **Cluster Management（クラスタの管理）→ Authentication（認証）→ Local Users（ローカルユーザー）**と選択します。

   Local Groups（ローカルグループ）ページが表示されます。
2. **Add（追加）**をクリックします。

   Add User（ユーザーの追加）ページが表示されます。デフォルトで、**ユーザーの追加**の **Properties**（プロパティ）タブが表示されます。
3. **User name（ユーザー名）**に、ローカルのユーザー名を入力します。
4. **Password（パスワード）**で、ローカルユーザーに割り当てるパスワード（6 文字以上）を入力します。
5. **Retype password（パスワードの再入力）**の **password（パスワード）**フィールドに入力したパスワードを正確に入力します。
6. **User ID（ユーザー ID）**に、固有の UNIX UID を入力するか、システムが提供するデフォルトの UID を使用します。
7. **Primary group（プライマリグループ）**で次のいずれかを実行します。

   - ローカルユーザーのプライマリグループの名前を入力する。
   - **Browse**（参照）ボタンをクリックし、プライマリグループのリストを参照する。
   - システムに設定されているデフォルトグループを使用する。

8. **Additional groups（追加グループ）**に、ローカルユーザーが属する別のグループの名前を入力するか、**Browse**（参照）ボタンをクリックしてグループのリストから探します（オプション）。

   メモ: 複数のグループを追加できます。
9. 追加のフィールドやオプションのフィールドを表示するには **Advanced（詳細設定）**タブを選択します。
10. **Real name（実名）**にユーザーの実名を入力します。
11. **Remarks（備考）**にユーザーに関するコメントを入力します（オプション）。
12. **Save Changes（変更の保存）**をクリックします。

ローカルユーザーの変更

1. **Cluster Management → Authentication → Local Users（クラスタの管理 > 認証 > ローカルユーザー）**と選択します。

   Local User（ローカルユーザー）ページに、既存のローカルユーザーのリストが表示されます。
2. 既存ユーザーリストの **User Name**（ユーザー名）で、該当する**ユーザー名**をクリックします。

   Edit User（ユーザーの編集）ページが表示されます。デフォルトでは、**General**（一般）タブが選択されています。

   メモ: General（一般）タブで選択したユーザーのグループ情報のみを変更できます。
3. **Primary group**（プライマリグループ）で次のいずれかを実行します。
   - ローカルユーザーのプライマリグループの名前を入力する。
   - **Browse**（参照）ボタンをクリックし、プライマリグループのリストを参照する。
   - システムに設定されているデフォルトグループを使用する。
4. **Additional groups**（追加グループ）に、ローカルユーザーが属する別のグループの名前を入力するか、**Browse**（参照）ボタンをクリックし、グループのリストから選択します（オプション）。
5. 追加のフィールドやオプションのフィールドを表示するには **Advanced**（詳細設定）タブを選択します。
6. **Real name**（実名）にユーザーの実名を入力します。
7. **Remarks**（備考）にユーザーに関するコメントを入力します（オプション）。
8. **Save Changes**（変更の保存）をクリックします。

ローカルユーザーの削除

1. **Cluster Management（クラスタの管理）→ Authentication（認証）→ Local Users（ローカルユーザー）**と選択します。

   Local User（ローカルユーザー）ページに、既存のローカルユーザーのリストが表示されます。
2. 既存管理者のリストから、ユーザー名を選択して **Delete（削除）**をクリックします。

パスワードの変更

ローカルユーザーのパスワードは、**Edit User**（ユーザーの編集）ページで変更することができます。

ローカルストレージユーザーのパスワードを変更するには、次の手順を実行します。

1. **Cluster Management → Authentication → Local Users（クラスタの管理 > 認証 > ローカルユーザー）**と選択します。

   Local User（ローカルユーザー）ページに、既存のローカルユーザーのリストが表示されます。
2. 既存ユーザーリストの **User Name**（ユーザー名）で、該当するユーザー名をクリックします。

   Edit User（ユーザーの編集）ページが表示されます。デフォルトでは、**General**（一般）タブが選択されています。

3. **admin password**（管理者パスワード）に、選択した管理者の現在のパスワードを入力します。
4. **New password**（新しいパスワード）の **admin**（管理者）に新しいパスワードを入力します。
5. **Retype password**（パスワードの再入力）に、**New password**（新しいパスワード）フィールドで入力したパスワードを正確に入力します。
6. **Change Password**（パスワードの変更）ウィンドウで **Save Changes**（変更の保存）をクリックします。
   Edit Quota（クォータの編集）ページが表示されます。
7. **Save Changes**（変更の保存）をクリックします。

ローカルグループの管理

設置場所が外部 NIS データベースで設定されている場合、本項は省略できます。

NFS を使った NAS クラスタソリューションへのアクセス権が必要となる Linux/UNIX エンドユーザーがあまりいない場合に備えて、ローカルグループのみを定義します。この場合も、外部 NIS データベースがない場合にのみ行います。

NAS クラスタソリューショングループは、ユーザーの組織と管理を支援します。 ユーザーを定義する際、ローカルストレージユーザーを 1 つ、または複数のグループに割り当てることができます。 NAS クラスタソリューションには、UNIX システムで定義したグループなど、外部で定義しグループまたはユーザーが含まれる場合もあります。

ローカルグループの表示

既存の **Local Groups（ローカルグループ）** を表示するには、**Cluster Management → Authentication → Local Groups（クラスタの管理 > 認証 > ローカルグループ）** と選択します。**Local Groups**（ローカルグループ）ページに、既存のローカルグループのリストが表示されます。

ローカルグループの追加

1. **Cluster Management → Authentication → Local Groups（クラスタの管理 > 認証 > ローカルグループ）** と選択します。
   Local Groups（ローカルグループ）ページが表示されます。
2. **Add**（追加）をクリックします。
   Add Group（グループの追加）ページが表示されます。
3. **Group Name**（グループ名）にグループの名前を入力します。
4. **Group ID**（グループ ID）にグループの識別番号を入力します。

   メモ: Dell Fluid File System グループは、200 より上の識別番号を使用します。

   メモ: グループには、使用可能な次の識別番号が自動的に割り当てられます。識別番号は必要に応じて変更できます。
5. **Save Changes**（変更の保存）をクリックします。

ローカルグループの削除

1. **Cluster Management → Authentication → Local Groups（クラスタの管理 > 認証 > ローカルグループ）** と選択します。
   Local Groups（ローカルグループ）ページに、既存のローカルグループのリストが表示されます。
2. 既存のローカルグループのリストから該当するローカルグループを選択し、**Delete**（削除）をクリックします。

認証

Authentication（認証）エントリでは、Network Information Services（NIS）、Active Directory（AD）、Light-weight Directory Access Protocol（LDAP）などの認証権限を設定できます。また、ローカルユーザーおよびグループの管理や、Windows SID から UNIX UID へのユーザー名のマッピングも可能です。

NAS cluster（NAS クラスタ）ソリューションは、次の設定モードをサポートしています。

- Active Directory 認証混合モードおよびネイティブモード
- NIS 認証のみ
- LDAP 認証のみ
- ローカル内部ユーザーのみ
- NIS または LDAP および Active Directory

ID 管理データベースの設定

ID 管理データベースを使用して、システムでユーザーレベルのアクセスコントロールを認証および管理できます。このデータベースは、ユーザーとそのパスワード、グループ、およびユーザーとグループの関係を管理します。

Active Directory ドメインに参加しているシステムは、ID 管理データベースとしても機能します。必要に応じて、追加の UNIX データベースを定義することができます。

UNIX ID 管理データベースには NIS および LDAP が含まれ、これらはクライアントが NFS プロトコル（UNIX/Linux クライアント）を使用してシステムにアクセスする場合のみ機能します。

お使いのネットワーク環境に応じて、次のオプションをいずれか 1 つ選択できます。

- NIS データベース経由でユーザー認証を有効にする
- LDAP データベース経由でユーザー認証を有効にする
- 外部 UNIX ID 管理データベースの使用を無効にする

NIS データベース経由でユーザー認証を有効にする

1. **Cluster Management → Authentication → Identity Management Database（クラスタの管理 > 認証 > ID 管理データベース）**と選択します。

   Identity Management Database（ID 管理データベース）ページが表示されます。

2. **Users and groups are defined in a NIS database**（ユーザーとグループは NIS データベースで定義）を選択します。
3. **Domain name**（ドメイン名）に、NIS データベースのドメイン名を入力します。
4. 任意の空白の **NIS server**（NIS サーバー）に、NIS サーバーの名前または IP アドレスを入力します。
5. 冗長性を実現するために NIS サーバーを追加するには、**Add NIS server**（NIS サーバーの追加）をクリックします。

   追加の **NIS サーバー**が NIS サーバーのリストに表示されます。

6. リストから NIS サーバーを削除するには、削除したい NIS サーバーを選択して、**Delete NIS server（s）**（NIS サーバーの削除）をクリックします。
7. 変更の承諾を求められたら、**OK** をクリックします。
8. **変更の保存** をクリックします。

LDAP データベース経由でユーザー認証を有効にする

1. **Cluster Management → Authentication → Identity Management Database（クラスタの管理 > 認証 > ID 管理データベース）** と選択します。

   Identity Management Database（ID 管理データベース）ページが表示されます。

2. **Users and groups are defined in an LDAP database**（ユーザーとグループは LDAP データベースで定義）を選択します。
3. **LDAP server**（LDAP サーバー）に LDAP サーバーの IP アドレスを入力します。
4. **Base DN**（ベース DN）に、認証目的で使用するベース DN（識別可能な名前）を入力します。

   ベース DN（識別可能な名前）は、認証に使用するドメインを表す一意の LDAP 文字列です。通常は次のフォーマットで表されます。

   `dc=domain`

   `dc=com`
5. **変更の保存** をクリックします。

外部 UNIX ID 管理データベースの使用を無効にする

1. **Cluster Management → Authentication → Identity Management Database（クラスタの管理 > 認証 > ID 管理データベース）** と選択します。

   Identity Management Database（ID 管理データベース）ページが表示されます。

2. **Users are not defined in an external user database**（ユーザーは外部ユーザーデータベースで定義されていない）を選択します。
3. **Save Changes**（変更の保存）をクリックします。

Active Directory

Active Directory サービスは、コンピュータネットワーク上のすべてのオブジェクトに関する情報を保存し、管理者とユーザーがこれらの情報を検索して適用できるようにします。Active Directory を使用して、ユーザーはネットワーク上の任意の場所にあるリソースに 1 回のログオン操作でアクセスできます。

同じく管理者は、ネットワーク上のすべてのオブジェクトをシングルポイントで管理できます。これらのオブジェクトは階層構造で表示できます。Active Directory エントリでは、Active Directory の設定を指定し、ユーザー認証のオプションを設定することができます。さらに、Active Directory ドメインへの参加も可能です。

NAS cluster（NAS クラスタ）ソリューションと Active Directory サーバーの同期化

現場で Active Directory を使用しており、NAS cluster（NAS クラスタ）ソリューションが Windows ネットワークに属している場合は、タイムクロックを Active Directory サーバーに同期させます。タイムクロックを Active Directory サーバーに同期させるには、**Cluster Management → General → Time Configuration（クラスタの管理 > 一般 > 時刻設定）** と選択します。

Active Directory サービスの設定

1. **Cluster Management → Authentication → System Identity（クラスタの管理 > 認証 > システム ID）** と選択します。

System Identity（システム ID）ページが表示されます。このページには、現在の設定と、NAS cluster（NAS クラスタ）ソリューションがすでに Active Directory ドメインに参加しているかどうかが表示されます。

2. **System name**（システム名）にシステム名を入力します。
   この名前によって、システムが送信するアラートで Dell Fluid File System が識別されます。この名前は、Active Directory を設定する際の Dell Fluid File System のデフォルト名でもあります。
3. Dell Fluid File System を Active Directory ドメインに参加させる場合は、**The system is a member of a Microsoft Windows Network**（このシステムは Microsoft Windows ネットワークのメンバーです）を選択し、次の手順に進みます。それ以外の場合は **Save Changes**（変更の保存）をクリックします。
4. **System NetBIOS name**（システムの NetBIOS 名）に、近隣のネットワークで表示される Dell Fluid File System の NetBIOS 名を入力します。
   この名前は 15 文字までに制限されています。特に指示がない限り、システム名を使用してください。
5. **Domain**（ドメイン）に、Dell Fluid File System が属するドメインを入力します。
   NetBIOS ドメイン名ではなく、mydomain.company.com などの完全修飾ドメイン名（FQDN）を使用してください。
6. **User name**（ユーザー名）に、Active Directory ドメインへの参加に使用する管理者ユーザー名を入力します。

   メモ: このユーザー名は Dell Fluid File System には保存されません。
7. **Password**（パスワード）に管理者パスワードを入力します。

   メモ: このパスワードは Dell Fluid File System には保存されません。

   注意: デルサポートから特に指示がない限り、Advanced Configuration（詳細設定）の選択は解除してください。このフィールドでは、Active Directory との関連性が高いパラメータを設定できます。

   Advanced Configuration（詳細設定）オプションを使用すると、システムが選択したデフォルトのコントローラを上書きするように、ドメインコントローラを設定することができます。
8. **変更の保存** をクリックします。

ネットワーク構成の概要

システムにアクセスするには、クライアントがアクセスできる IP アドレスを定義します。この IP アドレスを DNS サーバーに追加して、クライアントが IP アドレスに加えて名前でシステムにアクセスできるようにすることをお勧めします。

メモ: ドメインへの参加後、ユーザーを認証するために CIFS を設定する必要があります。ユーザーを認証するには、**Cluster Management → Protocols → CIFS Configuration（クラスタの管理 > プロトコル > CIFS 設定）**と選択します。**Authenticate users' identity using Active Directory and local user database**（Active Directory およびローカルユーザーデータベース経由でユーザー ID を認証する）を選択します。

メモ: クライアントアクセス VIP は、初期設定時に **Dell NAS Initial Deployment Utility** を使用して設定されます。設定したアドレスは、NAS Manager で **Cluster Management → Network → Subnets（クラスタの管理 > ネットワーク > サブネット）**に移動すると確認できます。ページ下部の **Primary**（プライマリ）をクリックすると、**VIP address**（VIP アドレス）のラベルが付いたクライアントアクセス VIP が表示されます。

システムのアーキテクチャは複数のコントローラから成るクラスタであるため、この IP アドレスは VIP であり、クラスタ内のすべてのコントローラに対応します。したがって、クライアントは単一のユニットとしてシステムにアクセスでき、システムはコントローラ間の負荷バランシングを実行できます。さらに、コントローラの故障時にサービスを継続させることも可能です。クライアントは、システムの高可用性と高パフォーマンスの利点を活用できます。

クライアントユーザーは、さまざまなネットワークトポロジを使用してシステムにアクセスします。ネットワークインフラストラクチャの物理的機能に応じて、NAS cluster（NAS クラスタ）ソリューションを次のように構成します。

- すべての LAN またはクライアントサブネットに属する。パフォーマンスの面ではこれが最適な構成です。このようなネットワーク構成では、各サブネットに対してクライアントアクセス用の VIP を 1 つ定義するだけで十分です。
- いずれの LAN またはクライアントサブネットにも属さず、すべてのクライアントはルーティングされていると見なされる。この場合、クライアントはルーターまたはレイヤ 3 スイッチを経由してデータにアクセスします。このようなネットワーク構成では、単一のサブネット内でクライアントアクセス用の VIP を複数定義し、クライアントがそのリストから IP アドレスを選択できるようにしておくことが推奨されます。
- いずれかの LAN またはクライアントサブネットに属し、フラットなクライアントとルーティングされたクライアントがある。このようなネットワーク構成では、上記に示した両方の方法を使用し、クライアントがフラットかルーティングされているかに応じて、使用する必要がある VIP をユーザーに通知することが推奨されます。

システムが属する各サブネットに対し、DNS でエントリを定義しておくことをお勧めします。これにより、クライアントは VIP を記憶していなくてもデータにアクセスすることができます。サブネット内に複数の VIP がある場合は、DNS サーバーで単一の名前を定義して、そのリストからラウンドロビン方式で IP アドレスが発行され、すべてのクライアントがシステムにアクセスできるようにします。

メモ: 異なるサブネットにある VIP を 1 つの DNS 名に混在させないでください。

パフォーマンスおよび静的ルート

ルーティングされたネットワークでは、静的ルートと呼ばれる機能を通じてパフォーマンスを向上させる機会が提供されます。この機能によって、ルーティングされたネットワーク上で、システムがさまざまなクライアントと通信する正確なパスを設定できるようになります。

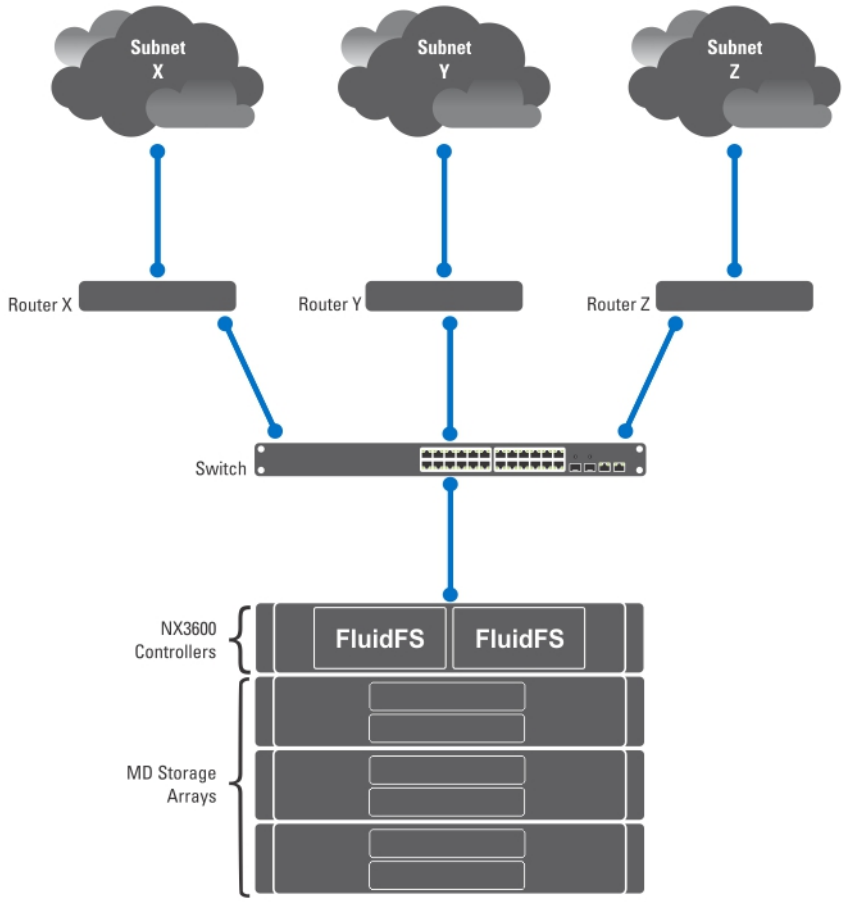

図 6. ネットワークの構成

上部のネットワークで、システムのデフォルトゲートウェイになれるのは 1 つだけです。*ルーター X* を選択すると仮定します。

サブネット Y のクライアントに送信されるパケットは、ルーター X にルーティングされ、（スイッチを経由して）ルーター Y に戻されます。これらのパケットは、ルーター X 経由で不必要に伝送され、ネットワーク内のすべてのサブネットのスループットが下がります。

ソリューションは、デフォルトゲートウェイに加えて、特定のサブネット用の固有のゲートウェイ、つまり静的ルートの設定を定義することです。これを実行するために、ネットワーク内の各サブネットを特徴づけ、そのサブネットにアクセスするのに最適なゲートウェイを識別する必要があります。

ネットワーク全体について同じことをする必要はありません。パフォーマンスに問題がない場合、デフォルトゲートウェイは最適です。パフォーマンスのニーズに最適な静的ルートを使用する時間と場所を選択することができます。

DNS の設定

ドメインネームシステム（DNS）は、ドメイン名を使用することによって、ユーザーがネットワーク上またはインターネット（TCP/IP ネットワーク）上でコンピュータを探せるようになる名前解決サービスです。DNS サーバーは、ドメイン名（ホスト名）と対応する IP アドレスのデータベースを維持し、名前対アドレスおよびアドレス対名前の解決サービスを IP ネットワーク上で提供します。1 つ、または複数の外部 DNS サーバー（NAS cluster（NAS クラスタ）ソリューションの外部ですがサイトの内部）を設定して、名前解決に使用することができます。

DNS サーバーの表示

既存の DNS サーバーとそのパラメータのリストを表示するには、 **Cluster Management → Network → DNS Configuration（クラスタの管理 > ネットワーク > DNS 設定）**と選択し、**DNS Configuration**（DNS 設定）ページに既存の DNS サーバーとそのパラメータのリストを表示します。

DNS サーバーと DNS サフィックスの追加

1. **Cluster Management → Network → DNS Configuration（クラスタの管理 > ネットワーク > DNS の設定）**と選択します。
   DNS Configuration（DNS の設定）ページが表示されます。
2. DNS サーバーを追加するには、**Add DNS Server**（DNS サーバーの追加）をクリックします。
   DNS サーバーのリストに新しい空の列が追加されます。
3. クライアント環境のプライマリ DNS の IP アドレスを設定します。
4. DNS サフィックスを追加するには、**Add DNS Suffix**（DNS サフィックスの追加）をクリックします。
   DNS サフィックスのリストに新しい空の列が追加されます。
5. DNS サフィックスを優先順位の高い順に入力します。
6. **Save Changes**（変更の保存）をクリックします。

DNS サーバーと DNS サフィックスの削除

1. **Cluster Management（クラスタの管理） → Network（ネットワーク） → DNS Configuration（DNS の設定）**と選択します。
   DNS Configuration（DNS の設定）ページに、既存の DNS サーバーとそのパラメータのリストが表示されます。
2. 適切な DNS サーバーおよび/または DNS サフィックスを選択して、**Remove（削除）**をクリックします。
   削除された DNS サーバーがすべての変更内容を保存しているというメッセージが表示されます。
3. **OK** をクリックします。

静的ルートの管理

ルーター間のホップを最低限に抑えるため、NAS クラスタソリューションからさまざまなルーターに対する複数のダイレクトパスがある場合、ルーテッドネットワークでの静的ルートの使用が推奨されます。

静的ルートの表示

Cluster Management → Network Management → Static Routes（クラスの管理 > ネットワーク管理 > 静的ルート）と選択します。**Static Routes**（静的ルート）ページに、現在定義されている静的ルートが表示されます。

静的ルートの追加

静的ルートを定義する際、サブネットのプロパティと、このサブネットにアクセスするためのゲートウェイを指定する必要があります。

1. **Cluster Management → Network Management → Static Routes（クラスタの管理 > ネットワーク管理 > 静的ルート）**と選択します。

Static Routes（静的ルート）ページが表示されます。

2. **追加** をクリックします。
   Add Static Routes（静的ルートの追加）ページが表示されます。
3. **Network**（ネットワーク）リストから、サブネットにアクセス可能なネットワークを選択します。
4. **Gateway IP**（ゲートウェイ IP）に、サブネットへのゲートウェイの IP アドレスを入力します。これは宛先サブネットへのアクセスに最も適した IP アドレスです。
5. **Destination Subnet**（宛先サブネット）に、静的ルートを経由してアクセスする宛て先のサブネットを入力します。
6. **Netmask**（ネットマスク）に、このサブネットを他のサブネットから分離するネットマスクを入力します。
7. **Save Changes**（変更の保存）をクリックします。

静的ルートの変更

1. **Cluster Management（クラスタの管理）→ Network Management（ネットワーク管理）→ Static Routes（静的ルート）** と選択します。
   Static Routes（静的ルート）ページに現在定義されている静的ルートのリストが表示されます。
2. 既存の静的ルートのリストから、適切な静的ルートを選択して **Edit（編集）** をクリックします。
   選択された静的ルートのプロパティが表示されます。
3. 必要に応じてプロパティを変更します。

静的ルートの削除

1. **Cluster Management → Network Management → Static Routes（クラスタの管理 > ネットワーク管理 > 静的ルート）** と選択します。
   Static Routes（静的ルート）ページに現在定義されている静的ルートのリストが表示されます。
2. 既存の静的ルートのリストから、適切な静的ルートを選択して **Delete**（削除）をクリックします。

ファイルシステムプロトコルの定義

ファイルシステムプロトコルは、ファイルシステム共有サービスを提供するネットワーキングプロトコルです。次のプロトコルに準拠することで、NAS cluster（NAS クラスタ）ソリューションはファイルシステムサーバーとして機能します。

- CIFS：Common Internet File System は、Microsoft Windows ユーザーまたはその他の CIFS クライアント用で、CIFS 共有を使用してディレクトリが共有されます。
- NFS：Network File System プロトコルは、UNIX クライアントまたはサービス用で、NFS レイヤで動作します。ディレクトリは NFS エクスポートを使用して共有されます。

Protocol（プロトコル）エントリでは、CIFS および NFS プロトコルをシステムレベルで管理できます。

CIFS パラメータの設定

CIFS Protocol Configuration（CIFS プロトコルの設定）では、Windows ユーザーが NAS cluster（NAS クラスタ）ソリューションシステムに接続できるよう設定できます。Linux ユーザーが CIFS プロトコルを使用してシステムにアクセスできるよう設定し、それらのユーザーを NIS、LDAP、または NAS cluster（NAS クラスタ）ソリューションのローカルユーザーを介して認証することもできます。

General（一般）タブでは、Active Directory ドメインまたは内部ユーザーデータベースのどちらを使用してユーザーを認証するかを選択できます。CIFS プロトコルの使用の有効化または無効化も可能です。

CIFS 一般パラメータの設定

1. **Cluster Management（クラスタの管理）** → **Protocols（プロトコル）** → **CIFS Configuration（CIFS 設定）** と選択します。
   CIFS Protocol Configuration（CIFS プロトコルの設定）ページが表示されます。デフォルトでは、**General**（一般）タブが選択されています。
2. **Allow clients to access files via the CIFS protocol**（クライアントの CIFS プロトコル経由のアクセスを許可する）チェックボックスを選択して、CIFS のファイル共有プロトコルを有効にします。
3. **System description**（システムの説明）に、サーバーについての簡単な説明を入力します。
   この説明は、Windows エクスプローラのタイトルバーに表示されます。
4. システムがユーザー ID を認証する方法を選択します。次のいずれかの方法を選択することができます。
   - システムが参加している Active Directory ドメインを使用してユーザーを認証するには、**Authenticate users' identity via Active Directory and local user database**（Active Directory およびローカルユーザーデータベース経由でユーザー ID を認証）を選択します。
   - 内部ユーザーデータベースを使用してユーザーを認証するには、**Authenticate users' identity via local users database**（ローカルユーザーデータベースを経由してユーザー ID を認証する）を選択します。
5. **変更の保存** をクリックします。
   これですべてのユーザー接続が再起動されます。

CIFS プロトコルを使用したユーザーのファイルアクセスを拒否する

1. **Cluster Management → Protocols → CIFS Configuration（クラスタの管理 > プロトコル > CIFS 設定）** と選択します。
   CIFS Protocol Configuration（CIFS プロトコルの設定）ページが表示されます。デフォルトでは、**General**（一般）タブが選択されています。
2. **Allow clients to access files via the CIFS protocol**（クライアントの CIFS プロトコル経由のアクセスを許可する）の選択を解除します。
3. **Save Changes**（変更の保存）をクリックします。
   これですべてのユーザー接続が再起動されます。

CIFS 詳細パラメータの設定

Advanced（詳細設定）タブで、次の各項目を設定できます。

- DOS コードページで使用される文字セット。
- NAS クラスタソリューションで使用される UTF8 文字セット。

CIFS 詳細パラメータを設定するには、次の手順を実行します。

1. **Cluster Management（クラスタの管理）** → **Protocols（プロトコル）** → **CIFS Configuration（CIFS 設定）** と選択します。
   CIFS Protocol Configuration（CIFS プロトコルの設定）ページが表示されます。デフォルトでは、**General（一般）**タブが選択されています。
2. **Advanced（詳細設定）**タブを選択します。

3. **DOS Code Page（DOS コードページ）**リストから、UNICODE に対応していないクライアントが使用する文字セットを選択します。
4. **Unix Charset**（Unix 文字セット）リストから、システムで使用されている UTF8 文字セットのバージョンを選択します。これにより、接続されているクライアントの文字セットにテキストが正しく変換されるようになります。
5. **変更の保存** をクリックします。

   メモ: これですべてのユーザー接続が再起動されます。

システムの時間パラメータの設定

このページでは、システムのタイムクロックを設定し、NTP サーバーを使用して時刻を自動アップデートする方法を定義し、システムのタイムゾーンを設定することができます。システムが正しく動作するには、タイムクロックの同期が不可欠です。

同期によって以下が可能になります。

- Windows クライアントでシステムをマウントする。
- スナップショットやレプリケーションといったスケジュールされたタスクを、正しい時刻に実行する。
- 正しい時刻をシステムログに記録する。

タイムゾーンの変更

1. **Cluster Management → General → Time Configuration（クラスタの管理 > 一般 > 時刻設定）** と選択します。

   Time Configuration（時刻設定）ページが表示されます。
2. **Time zone**（タイムゾーン）リストから、クラスタが配置されている地域に適したタイムゾーンを選択します。
3. **Save Changes**（変更の保存）をクリックします。

現在の日付と時刻の手動設定

お使いの環境に時刻同期サーバーがない場合、現在の日付と時刻を手動で設定します。

現在の日付と時刻を手動で設定するには、次の手順を実行します。

1. **Cluster Management（クラスタの管理）→ General（一般）→ Time Configuration（時刻設定）** と選択します。

   Time Configuration（時刻設定）ページが表示されます。
2. **There is no NTP server to synchronize time with（時刻を同期する NTP サーバーがない）**を選択します。
3. **Date（日付）**に、現在の日付を入力します。

   メモ: DD/MM/YYYY フォーマット（DD は日付、MM は月、YYYY は年を示します）を使用します。たとえば、*30/05/2012* のように入力します。
4. **Time （時刻）**に、現在の時刻を入力します。

   メモ: HH:MM:SS フォーマット（HH は 24 時間形式）を使用します。たとえば、*17:38:23* のように入力します。
5. **変更の保存** をクリックします。

NTP サーバーの削除

LAN またはクライアントネットワーク内に NTP サーバーがなくなった場合、その NTP サーバーを削除します。
NTP サーバーを削除するには、次の手順を実行します。

1. **Cluster Management（クラスタの管理）** → **General（一般）** → **Time Configuration（時刻設定）** とクリックします。
   Time Configuration（時刻の設定）ページに、使用可能な NTP サーバーのリストが表示されます。
2. 適切な NTP サーバーを選択して、**Delete NTP server(s)（NTP サーバーの削除）**をクリックします。
3. **Save Changes（変更の保存）**をクリックします。

NAS cluster（NAS クラスタ）ソリューションとローカル NTP サーバーの同期化

Network Time Protocol（NTP）を使用して、時間分布を同期および調整することができます。NTP サーバーはネットワーク上で時計を同期させる際に役立ちます。
システムが Windows ネットワークに属していない場合は、ローカル NTP サーバー（存在する場合）またはインターネット上の NTP サーバーと同期するようにシステムを設定します。ただし、システムが Windows ネットワークに属している場合は、AD が NTP サーバーとして動作します。

NAS cluster（NAS クラスタ）ソリューションをローカル NTP サーバーまたはインターネット上の NTP サーバーと同期するよう設定するには、次の手順を実行します。

1. **Cluster Management（クラスタの管理）** → **General（一般）** → **Time Configuration（時刻設定）** と選択します。
   Time Configuration（時刻設定）ページが表示されます。
2. **Time should be synchronized with an NTP server**（時刻を NTP サーバーと同期させる）を選択します。
3. **NTP Server**（NTP サーバー）を選択します。
4. **NTP server**（NTP サーバー）に、ローカル NTP サーバーまたはインターネット上の NTP サーバーの名前を入力します。
5. 冗長 NTP サーバーを追加するには、**Add NTP Server**（NTP サーバーの追加）をクリックし、**NTP server**（NTP サーバー）フィールドに冗長 NTP サーバーの名前を入力します。
6. **変更の保存** をクリックします。

ライセンスの管理

NAS 管理ソフトウェアで、インストールしたライセンスを表示したり、管理したりすることができます。

ライセンスの表示

インストールされたライセンスを表示するには、**Cluster Management → General → Licensing（クラスタの管理 > 一般 > ライセンス）**と選択します。**Licensed Features**（ライセンス付き機能）ページに、インストールされたライセンスのリストが表示されます。

ライセンスの追加

ライセンスファイルの機能は、システムでそのファイルが検証され、画面が更新された後、ライセンス画面に表示されます。

ライセンスを追加するには、次の手順を実行します。

1. **Cluster Management → General → Licensing（クラスタの管理 > 一般 > ライセンス）** と選択します。
   Licensed Features（ライセンス付き機能）ページが表示されます。
2. **Upload the license XML file**（ライセンス XML ファイルのアップロード）にライセンス XML ファイルのパスを入力するか、**Browse**（参照）ボタンをクリックしてライセンス XML ファイルの場所を参照します。
3. **Upload**（アップロード）をクリックしてライセンスファイルをアップロードします。
   システムでファイルが検証され、画面が更新されると、ライセンスファイルの機能がライセンス画面に表示されます。

ライセンスの削除

注意: ライセンスの削除は、デルテクニカルサポートの指示によってのみ行ってください。

ライセンスファイルの機能は、システムでそのファイルが検証され、画面が更新された後、ライセンス画面に表示されます。

1. **Cluster Management → General → Licensing（クラスタの管理 > 一般 > ライセンス）** と選択します。
   Licensed Features（ライセンス機能）ページに、インストールされたライセンスのリストが表示されます。
2. インストールされたライセンスのリストから該当する機能を選択し、**Delete License for feature**（機能のライセンスを削除する）をクリックします。

PowerVault NX3500/NX3600/NX3610 NAS ソリューションでの電子メールパラメータの設定

メモ: この機能は Dell Compellent FS8600 NAS ソリューションではサポートされていません。Dell Compellent FS8600 では、すべての電子メールアラートに Enterprise Manager を使用します。詳細については、『*Enterprise Manager Users Guide*』（Enterprise Manager ユーザーズガイド）を参照してください。

Dell Fluid File System では、電子メールをアラートおよびリモートサポートの基盤として使用します。Dell Fluid File System から送信される次のタイプのメッセージのいずれか 1 つ、またはすべてについて、その受信者を指定できます。

- ハートビート — ハートビートは 5 分ごとに電子メール受信者に送信されます。これによって、リモートサポートチームはシステム障害に対応することができます。
- システムログ — システムログは定期的に電子メール受信者に送信されます。これにより、リモートサポートチームは中程度のシステムエラーを特定し、必要に応じて修正することができます。
- アラート — アラートは、システムサービスについて報告する電子メールメッセージです。

受信者は必要に応じて追加できます。管理者を受信者として追加する場合は、システムアラートのみを管理者に送信するよう設定することをお勧めします。

必要に応じて、システム情報レポートを送信するよう手動でシステムに要求することもできます。

SMTP サーバーの表示

設定されている SMTP サーバーのリストを表示するには、**Cluster Management → Monitoring Configuration → Email Configuration（クラスタの管理 > 監視設定 > 電子メールの設定）**と選択します。**Email Configuration**（電子メールの設定）ページに設定済み SMTP サーバーのリストが表示されます。

SMTP サーバーの設定

SMTP サーバーにより、同じドメインでないユーザーに電子メールを送信することができます。SMTP サーバーにより、カスタマーのドメインからリモートのサポートメールボックスへトラップメッセージを転送することができます。
SMTP サーバーを追加するには、次の手順を実行します。

1. **Cluster Management → Monitoring Configuration → Email Configuration（クラスタの管理 > 監視設定 > 電子メールの設定）**と選択します。
   Email Configuration（電子メールの設定）ページが表示されます。デフォルトで、**General**（一般）タブが選択されます。
2. **Add SMTP server**（SMTP サーバーの追加）をクリックします。
   Add SMTP server（SMTP サーバーの追加）ページが表示されます。
3. **SMTP server**（SMTP サーバー）に、電子メールサーバーの IP アドレスまたは名前を入力します。
4. **Description**（説明）に、サーバーの説明を入力します。
5. **The SMTP server requires authentication**（SMTP サーバーで認証を要求する）を選択し、**User name**（ユーザー名）および **Password**（パスワード）で入力したユーザー名とパスワードを使用して、SMTP サーバー上のすべての電子メールを認証します。
6. **Save Changes（変更の保存）**をクリックします。

SMTP サーバーの設定変更

1. **Cluster Management → Monitoring Configuration → Email Configuration（クラスタの管理 > 監視設定 > 電子メールの設定）**と選択します。
   Email Configuration（電子メールの設定）ページに、既存の SMTP サーバーのリストが表示されます。
2. 既存 SMTP サーバーリストの **SMTP server**（SMTP サーバー）で該当する SMTP サーバーをクリックします。
   Edit SMTP server（SMTP サーバーの編集）ページが表示されます。
3. **SMTP server**（SMTP サーバー）に、電子メールサーバーのアップデートされた IP アドレスまたは名前を入力します。
4. **Description**（説明）に、サーバーのアップデートされた説明を入力します。
5. **User name**（ユーザー名）と **Password**（パスワード）で入力したユーザー名とパスワードを使用して、SMTP サーバーですべての電子メールを認証するには、**The SMTP server requires authentication**（SMTP サーバーで認証を要求する）を選択します。
6. **Save Changes**（変更の保存）をクリックします。

電子メール送信者の削除

1. **Cluster Management → Monitoring Configuration → Email Configuration（クラスタの管理 > 監視設定 > 電子メールの設定）**と選択します。
   Email Configuration（電子メールの設定）ページに、既存の SMTP サーバーのリストが表示されます。
2. 既存の SMTP サーバーのリストで **Delete SMTP Server(s)**（SMTP サーバーの削除）を選択します。

電子メール送信者の設定

一部の電子メールシステムでは、送信者が特定のドメインに属していないと、その電子メールメッセージの送信が阻止される場合があります。必要なドメイン内の特定のユーザーからの電子メールメッセージをすべて送信するように、システムを設定することができます。

電子メールメッセージを送信するときに **From**（送信者）フィールドに表示する電子メールアドレスを指定するには、**Send E-mails From**（この送信者からの電子メールを送信する）に、必要なドメインに属している電子メールアドレスを入力します。

詳細設定オプションの設定

1. **Cluster Management → Monitoring Configuration → Email Configuration（クラスタの管理 > 監視設定 > 電子メールの設定）**と選択します。

   Email Configuration（電子メールの設定）ページが表示されます。デフォルトで、**General**（一般）タブが選択されます。
2. **Advanced**（詳細設定）タブをクリックします。

   Add SMTP server（SMTP サーバーの追加）ページが表示されます。
3. **Maximum mail size (kB)**（最大メールサイズ（kB））に、各電子メールメッセージの最大サイズを入力します。
4. **Messages sent in intervals of (seconds)**（メッセージの送信間隔（秒））に、警告が送信される前に待機できる最長時間を入力します。
5. **Save Changes**（変更の保存）をクリックします。

SNMP の設定

Dell Fluid File System は、通常使用されるネットワーク管理プロトコルである Simple Network Management Protocol（SNMP）をサポートしています。これにより、デバイス検出、監視、およびイベント生成などの SNMP 互換の管理機能が使用できます。

SNMP ページにより、SNMP 互換の管理機能を設定できます。

SNMP のプロパティを設定するには次の手順を実行します。

1. **Cluster Management → Monitoring Configuration → SNMP Configuration（クラスタの管理 > 監視設定 > SNMP の設定）**と選択します。

   SNMP Configuration（SNMP の設定）ページが表示されます。デフォルトで、**Properties**（プロパティ）タブが選択されます。
2. **System contact**（システムの連絡先）に、必要な担当者名を入力します。
3. **System location**（システムの設置場所）に、システムの設置場所の説明を入力します。
4. **Read community**（読み取りコミュニティ）に、Dell Fluid File System から SNMP 値を読み取るデバイス用の SNMP コミュニティを入力するか、またはデフォルト値を使用します。
5. **Trap recipient**（トラップ受信者）に、ネットワーク管理サーバーまたは Dell Fluid File System が生成した SNMP トラップを受信する別のホストの IP アドレスまたはホスト名を入力します。
6. 追加のトラップ受信者を追加するには、**Add**（追加）をクリックします。

   トラップ受信者がリストに追加されます。
7. ネットワーク管理サーバーの IP アドレスまたはホスト名を入力します。
8. リストからトラップ受信者を削除するには、適切なトラップ受信者を選択して **Delete**（削除）をクリックします。

   トラップ受信者がリストから削除されます。

9. **Filter**（フィルタ）タブを選択して、さまざまなカテゴリのトラップについて送信する必要のある、最低のトラップ重大度を選択します。

   メモ: デフォルトでは、すべてのカテゴリのすべてのトラップを送信することになります。

10. **変更の保存** をクリックします。

6

トラブルシューティング

CIFS の問題のトラブルシューティング

AV ホストの設定が間違っているため、CIFS ファイルへのアクセスが拒否される

説明	Dell NAS cluster（Dell NAS クラスタ）ソリューションは、CIFS 共有ベースでのアンチウイルススキャンをサポートしています。共有上のファイルがクライアントアプリケーションによって開かれると、NAS cluster（NAS クラスタ）ソリューションはスキャンを実行するために、そのファイルをアンチウイルスホストに送信します。 アンチウイルスホストがない場合、ファイルおよび共有全体へのアクセスが禁止されます。
原因	NAS cluster（NAS クラスタ）ソリューションでアンチウイルスホストが使用できないため、アンチウイルスが有効な CIFS 共有でファイルを開くことができません。
対策	アンチウイルスが有効になっている共有でのみこの問題が発生しており、他の共有にアクセスしているクライアントには同じ問題が生じていないことを確認します。 アンチウイルスホストのステータス、および NAS cluster（NAS クラスタ）ソリューションとアンチウイルスホスト間のネットワークパスを確認します。

CIFS アクセスの拒否

説明	CIFS によるファイルまたはフォルダへのアクセスが拒否されます。
原因	十分なパーミッションを持たないクライアントがファイルまたはフォルダで操作を実行しています。
対策	ファイルまたはフォルダのパーミッションを確認し、必要なパーミッションを設定します。

CIFS ACL の破損

説明	CIFS ACL の破損です。
原因	• ユーザーまたはスクリプトによって ACL が誤って変更されました。 • アンチウイルスアプリケーションが誤って関連するファイルを検疫した後に、ACL が破損しました。

- バックアップアプリケーションによるデータの復元後、互換性の問題が原因で ACL が破損しました。
- *RoboCopy* などのサードパーティアプリケーションを使用してデータを別の場所から移行した後に、ACL が破損しました。

対策

Windows クライアントの現在の ACL 設定を確認します。Windows クライアントの最初に定義した方法と同じ方法を使用して、ファイルの ACL を再定義します。ファイル、ディレクトリ、および共有の所有者として ACL が設定されていることを確認します。現在パーミッションがないために ACL を再定義できない場合は、次の手順を実行します。

1. スナップショットまたはバックアップからファイルを復元します。
2. **RoboCopy** アプリケーションを使用してデータを別の場所から移行させた場合、データ全体を再コピーする代りに ACL のメタデータのみをコピーすることで、ACL を復元できる可能性が十分あります。
3. ファイルシステムのすべての ACL が破損している場合は、NAS レプリケーションパートナーからすべてのデータを復元できます。

CIFS クライアントのクロックスキュー

説明

CIFS クライアントの時刻がずれています。

原因

クライアントの時計は、Active Directory である Kerberos サーバーの時計との誤差が 5 分以内でなければなりません。

対策

クライアントの時計を （NTP サーバーとして動作する）Active Directory と同期するように設定し、時計のずれが生じないようにします。

ファイル読み取り時の CIFS クライアント切断

説明

ファイル読み取り時に CIFS クライアントが切断されます。

原因

コントローラのフェイルオーバー時に CIFS に過剰な負荷がかかっています。

対策

クライアントを再接続してファイルを再度開く必要があります。

CIFS クライアントの一般的な切断

説明

CIFS クライアントが切断されます。

原因

システムが CIFS サービスで一般的な問題を識別した場合、問題は自動的に回復されますが、その障害によってすべてのユーザーが切断され、上記のイベントがトリガされます。

対策	この問題が頻繁に繰り返される場合は、デルにお問い合わせください。

CIFS クライアントログインの失敗

説明	CIFS クライアントがログインできません。
原因	ユーザーが接続時に誤ったパスワードを入力しました。
対策	インタラクティブユーザーは、正しいパスワードを使用してログインを再試行できます。アプリケーションとサーバーでは、通常はスクリプトまたは設定ファイルで設定されるユーザーまたはパスワードの期限が切れている可能性があるため、特別な注意を要する場合があります。

CIFS 接続失敗

説明	CIFS クライアントの共有アクセスが拒否されています。
原因	ユーザーは Active Directory サーバーで不明で、NAS システムはこのユーザーを guest ユーザーにマップしました。共有が guest のアクセスを許可していない場合、ユーザーはアクセス拒否の警告を受信します。
対策	NAS が使用している Active Directory サーバーで、ユーザーがリストされていることを確認します。または、共有に対する guest の制限を外すことができます。ユーザーが guest として共有にアクセスできるようになった場合は、新しく作成されたファイルは nobody/guest ユーザーの所有になります。

CIFS Delete-On-Close の拒否

説明	ファイルが使用中に削除されます。
原因	ファイルが開いている時に削除されると、削除のマークが付きそのファイルが閉じた時に削除されます。それまでは、ファイルは元の場所に表示されたままですが、開こうとする要求はすべて拒否されます。
対策	ファイルを開こうとしているユーザーに、ファイルが削除 されたことを伝えます。

CIFS ファイルアクセスの拒否

説明	CIFS によるファイルアクセスが拒否されます。
原因	ファイルで要求された操作を実行するための十分な権限がクライアントにありません。
対策	これは情報イベントです。ユーザーは、アクセスが許可されるようにファイルの ACL を変更するよう要求することができます。

CIFS ファイル共有の拮抗

説明	CIFS ファイル共有が拮抗しています。
原因	CIFS プロトコルを使用してファイルが開かれると、ファイルを開くアプリケーションによって、このファイルが開いている間に使用すべき共有モードが通知されます。 共有モードには、このファイルが開かれている間に、他のユーザーのどのアクティビティが許可されるかが記述されています。 この定義はアプリケーションによって送信され、ユーザーがこれを制御または設定することはできません。 共有定義に違反があると、ユーザーはアクセス拒否エラーを受信し、このイベントが発行されます。
対策	これは情報イベントで、管理者はロックしているユーザーに問い合わせて、このファイルを参照しているアプリケーションを閉じるように要求することができます。 ファイルを開いたアプリケーションは、正しくシャットダウンされない場合があります。可能であればクライアントを再起動することをお勧めします。

CIFS ゲストアカウントが無効

説明	CIFS サービスを開始できません。
原因	CIFS を機能させるには有効な CIFS ゲストアカウントが必要です。
対策	有効なアカウントでシステムにゲストアカウントを設定します。

CIFS ロックの不整合

説明	CIFS インターロックの問題で CIFS サービスが中断されています。
原因	CIFS クライアントのインターロックシナリオです。
対策	システムは自動的に復元し、復元時に上記のイベントを発行します。

CIFS 最大接続数に到達

説明	NAS コントローラ 1 台あたりの最大 CIFS 接続数に到達しています。
原因	NX3600 アプライアンスでは、1 台あたりの CIFS 同時接続数は 200 までに制限されており、NX3610 および FS8600 では 1500 までに制限されています。 • システムは最適な状態にあり、いずれかのコントローラにアクセスする CIFS クライアント数が最大値に達しています。このようなシ

ナリオでは、別の NAS アプライアンスを追加することを検討してください。

- システムは最適な状態ですが、NAS コントローラ間でクライアントが著しくバランスを欠いています。この場合は、NAS Manager を使用してクライアントのバランスを再調整してください。
- システムは劣化した（1 台または複数の NAS コントローラが故障している）状態で、CIFS クライアントは残りのコントローラ上で待機しています。この場合は、システムが最適な状態に戻るまで待つか、システム内の CIFS クライアントの数を減らします。

対策

すべての NAS コントローラが最適モードにある場合、接続は両方のコントローラ間で分割されます。

CIFS 共有が存在しない

説明

クライアントが存在しない共有に接続を試みています。

原因

- クライアント側の綴りが間違っています。
- 間違ったサーバーにアクセスする

対策

利用可能な NAS 共有をリストし、すべての共有が表示されており、誤って変更が行われていないことを確認します。

Windows クライアントを使用し、次の手順を実行して問題のある共有にアクセスできることを確認します。

1. **実行** をクリックします。
2. 次のようにクライアントアクセス VIP および共有名を入力します。**\\<Client_VIP>\<CIFS_share_name>**

CIFS パスの共有が見つからない

説明

クライアントが、NAS コンテナ内に存在しないディレクトリを参照している共有にアクセスしました。

原因

- NAS システムは、バックアップまたはリモートレプリケーションから復元されます。復元中はディレクトリの構造が完全ではなく、いくつかのディレクトリは存在していない可能性があります。
  ステータスを通知し、復元プロセスが完了するのを待ちます。
- 認証が必要なクライアントでは、他のクライアントによってマウントされたディレクトリを削除または変更します。
  複数のユーザーが同じデータセットにアクセスしている場合は、このような拮抗を避けるため、厳密なパーミッションスキームを適用することをお勧めします。

対策

NAS で使用可能なすべての共有をリストし、問題のある共有を特定します。問題のある共有には、その共有へのアクセスができないことが示されています。

1. 問題のあるパスをバックアップから復元します。
2. 欠落しているディレクトリを手動で作成します。必要に応じて、アクセスを制御するためのパーミッションを設定します。
3. 共有を削除し、クライアントに通知します。

CIFS による読み取り専用ボリュームへの書き込み

説明

クライアントが読み取り専用ボリュームでファイルの変更を試みています。

原因

NAS ボリュームが、レプリケーションのターゲットであるのにもかかわらず読み取り専用に設定されています。

このイベントの最もよくある原因は次のいずれかです。

- ユーザーは読み取り目的でターゲットシステムにアクセスしたつもりだが、誤ってファイルの変更も試みた。
- 名前 /IP が似ていたため、ユーザーが誤ったシステムにアクセスした。
- ユーザーが、知らないうちにレプリケーションターゲットにされていた NAS コンテナにアクセスしようとしている。

対策

このボリュームに書き込むために、レプリケーションを最初に分離する必要があります。ユーザーを正しい場所に差し向けてください。

NFS の問題のトラブルシューティング

NFS エクスポートをマウントできない

説明

NFS エクスポートをマウントしようとすると、次のような理由でマウントコマンドがエラーになります。

- パーミッションが拒否されました。
- ポートマッパーエラーのため、アプライアンスが応答しない — RPC タイムアウトまたは入力 / 出力エラーです。
- プログラムが登録されていないため、アプライアンスが応答しません。
- アクセスが拒否されました。
- ディレクトリではありません。

原因

- クライアントが NFS/UDP を使用して接続されており、接続経路中にファイアウォールがあります。
- クライアントはエクスポートリストに入っておらず、サーバーが NIS 経由でクライアント

システムを認識できなかったか、またはアプライアンスが提供された ID を承諾しません。

- NAS クラスタソリューションがダウンしているか、または内部ファイルシステムに問題があります。
- マウントコマンドはポートマッパーに到達していますが、**rpc.mountd** NFS のマウントデーモンが登録されていません。
- クライアントシステムの IP アドレス、IP 範囲、ドメイン名または netgroup が、NAS アプライアンスからのマウントを試みているボリューム用のエクスポートリストにありません。
- リモートパスまたはローカルパスのいずれかがディレクトリではありません。
- クライアントにルート権限がないかシステムグループのメンバーではありません。NFS のマウントとマウント解除は、ルートユーザーとシステムグループのメンバーにのみ許可されています。

対策

問題の原因が NFS/UDP およびファイアウォールである場合、クライアントがマウントに UDP（通常これがデフォルト）を使用しているか、パスにファイアウォールがあるかどうかをチェックします。ファイアウォールがある場合はそのファイアウォールに適切な例外を追加します。

問題の原因がパーミッションである場合：

- 提供したパスが正しいことを確認します。
- ルートとしてマウントを試みていることを確認します。
- システムの IP アドレス、IP 範囲、ドメイン名または netgroup がエクスポートリストにあることを確認します。

ポートマッパーの障害が原因でアプライアンスが応答しない場合：

- NAS クラスタソリューションのステータスを確認します。
- NFS のマウントを別のシステムから試して、ネットワーク接続を確認します。
- ほかのユーザーにも同じ問題が生じているかどうか確認します。

登録されていないプログラムが原因でアプライアンスが応答しない場合は、クライアントのポートマッパーが起動しているかどうかをチェックします。

問題の原因がアクセス拒否である場合：

- 次のコマンドを使用して、アプライアンスがエクスポートしたファイルシステムのリストを取得します。

  ```
  showmount -e <FluidFS hostname>
  ```

- システム名またはネットグループ名がファイルシステムのユーザーリストにないことを確認します。
- NAS クラスタソリューションユーザーインタフェース経由で NFS に関連付けられているファイルシステムを確認します。

問題の原因がディレクトリの場合は、コマンドのスペルをチェックし、両方のディレクトリでマウントコマンドの実行を試行します。

NFS エクスポートが存在しない

説明

存在しないエクスポートをマウントしようとしました。

原因

この障害は通常、クライアントシステムでのスペル間違い、または誤ったサーバーへのアクセスによって発生します。

対策

1. NAS で使用可能なエクスポートをチェックし、必要なエクスポートがすべて存在していることを確認します。
2. 問題のあるクライアントで、当該のエクスポートがこのクライアントで使用可能であることを次のように確認します。
3. `% showmount -e <Server name/IP>`
4. `Export list for <Server name/IP>:`
5. `/abc 10.10.10.0`
6. `/xyz 10.10.10.0`
7. エクスポートが使用可能な場合は、クライアント上で該当するマウントコマンドのエクスポート名のスペルを確認します。エクスポート名は、showmount の出力からマウントコマンドにコピーペーストすることをお勧めします。

NFS ファイルへのアクセス拒否

説明

このイベントは NFS ユーザーが NAS コンテナのファイルに対して十分なパーミッションを持たない時に発行されます。

原因

ファイル所有権が UID/UNIX でユーザーがこのファイルにアクセスする権限を持たない、または所有権が SID/ACL で UID/UNIX への変換後、ファイルへのアクセスが許可されなくなっています。

対策

ネイティブアクセス（CIFS ユーザーが SID/ACL ファイルへ、または NFS ユーザーが UID/UNIX ファイルへアクセス）に関しては、欠落している権限を把握することが基本です。

アクセスがネイティブでない場合、変換ルールがかかわってくるため、デルテクニカルサポートにお問い合わせいただくことをお勧めします。

セキュアなエクスポートへの NFS の非セキュアアクセス

説明

ユーザーがセキュアでないポートからセキュアなエクスポートにアクセスを試行しています。

原因

セキュアなエクスポートの要件とは、アクセスしているクライアントが well-known ポート（1024 以下）を使用する必要があり、通常これはクライアントに

おいて root（uid=0）である必要があることを意味します。

対策

- 該当のエクスポートを特定し、セキュアに設定されていることを確認します（セキュアなクライアントポートが必要）。
- セキュアなエクスポートを維持する必要のある場合は、well-known ポート（1024 以下）からマウントリクエストを発行するために、NFS クライアントのマニュアルを参照してください。
- セキュアなエクスポートが必要ではない場合（たとえばネットワークがパブリックではない場合）、エクスポートがセキュアでないことを確認してからアクセスを再試行します。

エクスポートオプションによる NFS のマウントの失敗

説明

このイベントは、NFS のマウントがエクスポートオプションのために失敗する時に発行されます。

原因

エクスポートリストはクライアントのアクセスを IP、ネットワーク、またはネットグループでフィルタし、アクセスしているクライアントをスクリーニングします。

対策

1. 該当のエクスポートの詳細を確認します。すべての既存のオプションを戻せるように、書き留めます。
2. エクスポートの IP/ クライアントの制限を外して、マウントを再試行します。
3. マウントが正しく行われた場合、IP またはドメインが明確に指定されているか、または定義済みのネットワークやネットグループの一部であることを確認します。ネットワークのネットマスクは直観的でなく、陥りやすい過ちに注意してください。たとえば、192.175.255.254 は、192.168.0.0/12 の一部ですが、192.168.0.0/16 の一部ではありません。
4. マウントが正しく行われたら、オリジナルのオプションを適宜調整します。

ネットグループ障害による NFS マウントの失敗

説明

このイベントは、必要なネットグループ情報が取得できないためにクライアントが NFS エクスポートのマウントに失敗した場合に発行されます。

原因

このエラーは通常、NAS システムと NIS/LDAP サーバー間の通信エラーによって発生します。ネットワークの問題、ディレクトリサーバーのオーバーロード、ソフトウェアの誤作動が原因となる場合もあります。

対策

設定済みの各 NIS サーバーに対して次の処理を繰り返します。処理ごとに単一の NIS のみを使用します。問題のある NIS サーバーから始めてください。

1. NIS/LDAP サーバーのログを調べて、エラーの原因がログにレポートされているか確認します。

2. ネットワークのテストを完了するために、NIS/LDAP サーバーと同じサブネットにあるクライアントから NAS に ping を送信します。
3. NAS と同じサブネットにあるクライアントから、NIS/LDAP サーバーに ping を送信します。
4. 上記のいずれかでパケットの損失が認められた場合は、環境内のネットワークの問題を解決してください。
5. NAS と同じサブネットにあり、同じディレクトリサーバーを使用するように設定されている Linux クライアントから、適切なコマンドを使用して NIS/LDAP サーバーにネットグループ詳細のクエリーを実行します。適切な時間内（最大 3 秒）に応答が返されることを確認します。

エクスポートでのネットグループの制限を削除するか、代替ディレクトリサーバーを定義することによって、この問題を一時的に回避できます。

ネットグループの定義に注意しながら、関連するエクスポートとそれに定義されたオプションを特定します。使用されたネットグループを記録し、問題が解決されたらそのネットグループを復元し、ネットグループの制限を削除できるようにしておきます。

NFS マウントパスが存在しない

説明

クライアントが存在しないマウントパスを NAS コンテナでマウントしようとしています。

原因

このエラーは通常、次のシナリオのいずれかによって発生します。

- バックアップまたはリモートレプリケーションから復元中のシステムにアクセスしている場合。完全なディレクトリ構造は、復元が完了してはじめて使用できるようになります。
- 同じパス内の上位ディレクトリへのアクセス権限を持つクライアントが、他のクライアントがマウントしているディレクトリを削除または変更した場合。
- 複数のユーザーが同じデータセットにアクセスしている場合は、このようなシナリオを避けるため、厳密なパーミッションスキームを適用することをお勧めします。

対策

1. NAS システムが復元中の場合、現在のステータスをクライアントに通知し、復元プロセスが完了するまで待機するように指示します。
2. その他のケースでは、次の 3 つのオプションがあります。
   - 問題のあるパスをバックアップから復元します。
   - 欠落しているディレクトリを手動で作成し、マウントができるようにします。削除されたパスにある既存データにアクセスしようとすると、クライアントにエラーが返されます。
   - エクスポートを削除し、これをクライアントに通知します。
3. NAS で使用可能なすべてのエクスポートをリストし、問題のあるエクスポートを特定します。

問題のあるエクスポートには、そのエクスポートへのアクセスができないことが示されています。

4. エクスポートを削除するか、エクスポートが指定する場所にディレクトリを作成します。

NFS 所有者の操作の制限

説明	NFS クライアントに、要求されたアクションを特定のファイルに対して実行する許可が与えられていません。
原因	NFS ユーザーが、所有していないファイルに対して chmod または chgrp 操作を試みました。
対策	これは重要性の低い、ユーザーレベルの問題です。このタイプのイベントが頻繁に発生する場合は、制限されているデータへの悪意あるアクセスを示している場合があります。

NFS による読み取り専用エクスポートへの書き込み

説明	NFS クライアントが、読み取り専用エクスポート上で変更の実行を試みています。
原因	NFS エクスポートが読み取り専用エクスポートとして定義されている可能性があります。読み取り専用エクスポートにアクセスしているクライアントは、含まれているファイルに対する書き込み操作や変更を実行できません。
対策	このイベント自体では、システム管理者による作業は必要としません。

NFS による読み取り専用ボリュームへの書き込み

説明	NFS ユーザーが、読み取り専用ボリューム上のファイルへの変更を試みています。
原因	NAS ボリュームは、レプリケーション関係でターゲットとして設定される際に読み取り専用になっています。レプリケーション関係が削除されるか、ボリュームがシンプルな正常状態に戻るまで、読み取り専用ボリュームの変更は禁止されます。
対策	ユーザーに対し、NAS ボリュームの状態を通知します。

NFS によるスナップショットへの書き込み

説明	NFS ユーザーがスナップショットにあるファイルを変更しようとしています。
原因	NAS ボリュームのスナップショットは、設計上変更することができません。

対策	スナップショットデータは変更できません。スナップショットは、作成時の NAS ボリュームデータを正確に表したものです。

NFS ファイルまたはディレクトリへのアクセス拒否

説明	ユーザーが NFS オブジェクトを所有するグループに属しており、グループメンバーは操作を実行することが許可されているにも関わらず、ユーザーは NFS ファイルまたはディレクトリにアクセスできません。
原因	NFS サーバー（バージョン 2 および 3）は、NFS クライアントの認証にリモートプロシージャコール（RPC）プロトコルを使用します。ほとんどの RPC クライアントには、最大で 16 のグループが NFS サーバーに渡されるという制限があります。一部の UNIX フレーバでサポートされるように、ユーザーが 16 を超える UNIX グループに所属する場合、グループの一部は渡されず、NFS サーバーでチェックされないため、ユーザーのアクセスが拒否される可能性があります。
対策	この問題を検証し得る方法として、newgrp を使用して一時的にユーザーのプライマリグループを変更することで、サーバーに確実に渡されるようにする方法があります。 簡単な回避策としては、ユーザーを不要なグループから削除して、グループを 16 以下にする方法がありますが、常に実行可能ではありません。

レプリケーションのトラブルシューティング

レプリケーション設定エラー

説明	複製元と複製先のシステムのトポロジに互換性がないため、複製元と複製先 NAS ボリューム間のレプリケーションが失敗します。
原因	複製元と複製先のシステムに、レプリケーションのための互換性がありません。
対策	ダウンしている NAS クラスタソリューションをアップグレードします。複製元と複製先の NAS コントローラの数が同じであることを確認します。 **メモ:** 4 ノード NAS クラスタと 2 ノード NAS クラスタ間では、レプリケーションできません。

ビジー状態の複製先クラスタ

説明	複製先クラスタを必要なレプリケーションのために使用できないため、複製元の NAS ボリュームと複製先の NAS ボリューム間のレプリケーションに失敗しています。
原因	複製先クラスタを必要なレプリケーションに使用できないため、レプリケーションタスクに失敗します。

対策	システム管理者は、複製先システムのレプリケーションステータスを確認する必要があります。

複製先 FS がビジー状態

説明	複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションが失敗します。
原因	必要なレプリケーションの処理で複製先クラスタが一時使用不能になっているため、レプリケーションタスクを実行できません。
対策	ファイルシステムがリソースの一部を開放すると、レプリケーションは自動的に再開されます。管理者は、一定時間（1 時間）後にレプリケーションが自動的に再開されていることを確認する必要があります。

ダウン状態の複製先

説明	複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションが失敗します。
原因	送信先 NAS ボリュームのファイルシステムがダウンしているため、レプリケーションタスクに失敗します。
対策	システム管理者は、NAS Manager の Monitoring（監視）セクションを使用して、複製先システムでファイルシステムがダウン状態かどうかを確認する必要があります。NAS cluster（NAS クラスタ）ソリューションファイルシステムが応答しない場合、システム管理者は複製先クラスタ上のシステムを開始する必要があります。ファイルシステム開始後、レプリケーションは自動的に続行します。

非最適状態の複製先

説明	複製先 NAS ボリュームが最適状態でないため、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗しています。
原因	複製先 NAS ボリュームのファイルシステムが最適ではないため、レプリケーションに失敗しています。
対策	システム管理者はファイルシステムが最適ではない理由を把握するため、NAS Manager の Monitoring（監視）セクションを使用して、複製先システムのシステムステータスを確認する必要があります。ファイルシステムの回復後、レプリケーションは自動的に続行します。

容量の再確保のためビジー状態のレプリケーションの複製先ボリューム

説明	複製先 NAS ボリュームが容量の解放に費やされていることから、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗しています。
原因	複製先 NAS ボリュームが容量の解放のためにビジー状態にあり、レプリケーションタスクに失敗しています。
対策	容量が使用可能になると、レプリケーションは自動的に続行します。システム管理者は、一定時間（1 時間）後、レプリケーションが自動的に続行することを確認する必要があります。

分離したレプリケーションの複製先ボリューム

説明	複製先 NAS ボリュームが複製元 NAS ボリュームから分離しているため、複製元 NAS ボリュームと複製先 NAS ボリューム間でのレプリケーションに失敗しています。
原因	複製先 NAS ボリュームが複製元 NAS ボリュームから以前分離されていたため、レプリケーションタスクに失敗します。
対策	システム管理者は、複製元 NAS ボリュームで分離アクションを実行する必要があります。必要に応じて、両方の NAS ボリュームをレプリケーション関係に再度接続します。

レプリケーションの接続切断

説明	複製元と複製先のシステム間の接続が失われているために、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションができません。
原因	複製元と複製先間のネットワークインフラストラクチャの接続が切断しています。
対策	管理者はレプリケーションが自動的に回復するかどうかを確認する必要があります。レプリケーションが自動的に回復しない場合は、複製元クラスタと複製先クラスタ間のネットワーク通信を確認します。ネットワーク通信の確認は、同じサブネット内にあり、複製元クラスタと複製先クラスタの両方に ping できるサードパーティ製システムを使用して行うことができます。

互換性のないバージョンのレプリケーション

説明	複製元の NAS クラスタのシステムのバージョンが複製先クラスタのシステムのバージョンよりも上位であるため、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗しています。
原因	複製元 NAS クラスタのシステムのバージョンが複製先クラスタのシステムのバージョンよりも上位であるために、レプリケーションタスクに失敗します。
対策	システム管理者は、複製元クラスタのシステムのバージョンに合わせて、複製先クラスタのシステムのバージョンをアップグレードする必要があります。

レプリケーション内部エラー

説明	内部エラーのために、複製元と複製先の NAS ボリューム間のレプリケーションに失敗します。
対策	この問題を解決するには、デルにお問い合わせください。

ブロックされたレプリケーションジャンボフレーム

説明	ネットワークでジャンボフレームがブロックされているため、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗します。
原因	ネットワークでジャンボフレームがブロックされているため、レプリケーションタスクに失敗します。
対策	ネットワーク管理者は、複製元クラスタと複製先クラスタ間において、スイッチまたはルーター間のジャンボフレームの転送が有効化されていることを確認してください。

容量が十分でないレプリケーションの複製先

説明	複製先 NAS ボリュームに十分な容量がないため、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗しています。
原因	複製先 NAS ボリュームに十分な容量がないために、レプリケーションタスクに失敗します。
対策	複製先 NAS ボリュームの容量を増やします。

ビジー状態のレプリケーション複製元

説明	複製元 NAS ボリュームのファイルシステムが別の NAS ボリュームのレプリケーションでビジー状態であるため、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗しています。
原因	複製元 NAS ボリュームのファイルシステムが別の NAS ボリュームのレプリケーションでビジー状態であるため、レプリケーションタスクに失敗します。
対策	ファイルシステムがリソースの一部をリリースすると、レプリケーションは自動的に続行します。システム管理者は、一定時間（1 時間）後、レプリケーションが自動的に続行することを確認する必要があります。

ダウン状態のレプリケーション複製元

説明	複製元 NAS ボリュームのファイルシステムがダウンしているため、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗しています。
原因	複製元 NAS ボリュームのファイルシステムがダウンしています。
対策	システム管理者は、NAS Manager の Monitoring（監視）セクションを確認して、複製元システムで NAS cluster（NAS クラスタ）ソリューションがダウン状態かどうかを確認する必要があります。NAS cluster（NAS クラスタ）ソリューションがダウン状態の場合は、システム管理者は複製元システムのファイルシステムを開始する必要があります。ファイルシステムが開始すると、レプリケーションは自動的に続行します。

複製元が非最適状態

説明	複製元 NAS ボリュームのファイルシステムが最適な状態ではないため、複製元と複製先の NAS ボリューム間のレプリケーションができません。
原因	複製元のファイルシステムが最適な状態ではないため、レプリケーションができません。
対策	管理者は NAS Manager の Monitoring（監視）セクションを使用して、複製元システムのシステムステータスを確認し、ファイルシステムが最適ではない理由を特定してください。

容量の再確保のためビジー状態のレプリケーションの複製元ボリューム

説明	複製元 NAS ボリュームが容量の再確保に費やされていることから、複製元 NAS ボリュームと複製先 NAS ボリューム間のレプリケーションに失敗しています。
原因	複製元 NAS ボリュームが容量の再確保でビジーのため、レプリケーションタスクに失敗します。
対策	容量が使用可能になると、レプリケーションは自動的に続行します。システム管理者は、一定時間（1 時間）後、レプリケーションが自動的に続行することを確認する必要があります。

Active Directory の問題のトラブルシューティング

Active Directory ユーザーのためのグループクォータが機能しない

説明	グループクォータは Active Directory グループに定義されています。ただし、グループのメンバーが容量を消費すると、グループの実際の使用率は上昇せずグループの制限が強制されません。
原因	NAS cluster（NAS クラスタ）ソリューションクォータの強制はファイル（UNIX）の UID および GID または、定義されている場合はユーザー（NTFS）のプライマリグループの SID および GSID に基づいて実行されます。 Active Directory ユーザーのために、プライマリグループの設定は必須ではありません。定義されていない場合、使用済み容量はどのグループにも報告されません。グループクォータが Active Directory ユーザーで有効であるためには、プライマリグループは割り当てられている必要があります。
対策	Active Directory ユーザーのためにプライマリグループをセットアップするには、次の手順を実行します。 1. Active Directory の管理画面を開きます。 2. 希望のユーザーを右クリックします。 3. **Member Of**（所属するグループ） タブをクリックします。 必要なグループがリストされます。 4. グループをクリックして、**Set Primary Group**（プライマリグループの設定）ボタンをクリックします。 これでユーザーのグループ用のクォータが有効になります。

Active Directory 認証

説明	有効な Active Directory ユーザーが認証に失敗します。
原因	次の原因が考えられます。 • ユーザーが誤ったパスワードを使用して認証を試みている。 • ユーザーが Active Directory 内でロックまたは無効にされている。 • Active Directory のドメインコントローラがオフラインまたはアクセスできない。 • システムのクロックと Active Directory のクロックが同期していない。
対策	1. NAS Manager の NAS クラスタソリューションシステムのイベントログにエラーがないかどうか確認します。 2. ユーザーが Active Directory で無効またはロックされていないことを確認します。 3. ドメインコントローラがオンラインで、ネットワークを使用したアクセスが可能であることを確認します。 4. Kerberos にはクライアントとサーバーの時計が同期している必要があります。システムの時間とドメインコントローラの時間が同じであることを確認し、必要であればシステムの NTP 設定を行います。

Active Directory 設定のトラブルシューティング

説明	Active Directory のユーザーとグループを CIFS 共有に追加できません。
原因	次の原因が考えられます。 • FQDN を使用してドメインに ping 送信できない。 • DNS が設定されていない可能性がある。 • NTP が設定されていない可能性がある。
対策	Active Directory ドメインへの接続のためにシステムを設定する時に、次の手順を実行します。 1. ドメインの NETBIOS 名、またはドメインコントローラの IP アドレスを使用しないで、FQDN を使用するようにする。 2. ユーザーが、ドメインにシステムを追加するパーミッションを所有しているようにする。 3. 正しいパスワードを使用する。 4. **DNS Configuration**（DNS 設定）タブを参照して正しい情報を入力する。 5. NTP の情報を設定し、システムの時刻とドメインの時刻が一致していることを確認する。 6. 複数の NAS システムを使用している場合は、異なる NETBIOS 名を設定していることを確認す

る。システムは、デフォルトで CIFS Storage を名前にします。

7. **Authenticate users' identity via Active Directory and local user database** (Active Directory およびローカルユーザーデータベース経由でユーザー ID を認証）が選択されていることを確認します。

NAS ファイルアクセスおよびパーミッションのトラブルシューティング

ファイルまたはフォルダの所有権を変更できない

説明	NAS システム上のすべてのファイルは UNIX ユーザーまたは NTFS ユーザーが所有しています。所有権を変更できない場合の対応は、アクセスがネイティブか非ネイティブかによって異なります。
原因	ユーザーは所有権の変更を許可されていません。
対策	このアクションは認証済みのユーザーが実行する必要があります。

NAS ファイルを変更できない

説明	ユーザーまたはアプリケーションがファイルを変更できません。
原因	• ファイルへのパーミッションがないため、クライアントがファイルを変更できません。 • NAS ボリュームが最大容量に達し、ファイルシステムが上書きを含む書き込みリクエストを拒否しています。 • NAS ボリュームはレプリケーション関係におけるターゲットで、読み取り専用になっています。
対策	• 問題が一部のファイルでのみ発生する場合は許可に問題があります。ユーザーアカウントにそのファイルの変更許可があることを確認するか、別のユーザーアカウントを使用します。 • 問題が特定の NAS ボリュームに関係する場合： a. NAS ボリュームに十分な空き容量があることを確認するか、拡張します。 b. アクセスしている NAS がレプリケーションのターゲットではないことを確認します。

ファイル所有権の混在が拒否された

説明	ファイル所有者とグループ所有者は、同じ ID タイプ（UNIX または NTFS のいずれか）に属していなけれ

	ばなりません。違う ID タイプを設定しようとする操作が検出されました。
原因	元のファイル所有権が SID/GSID の場合、ファイル所有者 ID だけを UID に変更することはできません。
対策	ファイルの所有権を UNIX スタイルの所有権に変更するには、UID と GID を同時に設定します。

Linux クライアントからの問題のある SMB アクセス

説明	Linux/UNIX クライアントが SMB（/etc/fstab を使用、または直接 smbmount を使用）を使用して NAS cluster（NAS クラスタ）ソリューション共有をマウントしようとしています。 Linux/UNIX クライアントが、次のような smbclient コマンドを使用して、ファイルシステムにアクセスしようとしています。 `smbclient //<nas>/<share> -U user %password -c ls`
対策	Linux/UNIX クライアントから NAS cluster（NAS クラスタ）ソリューション FluidFS システムにアクセスする場合は、NFS プロトコルインタフェースを使用することが推奨されます。この問題の対処方法は次のとおりです。 1. ユーザーが CIFS でアクセスするために使用する場所と同じ場所に管理者が NFS エクスポートを作成するようにし、Linux/UNIX クライアントからマウントコマンドを使用してその場所に接続します。 2. NFS ベースのインタフェースを使用して NAS cluster（NAS クラスタ）ソリューションにアクセスします。たとえば NAGIOS Linux 管理システムから、`/check_disk_smb` コマンドではなく `/check_disk` コマンドを使用します。

Dell NAS システムファイルにある不明な UID および GID 番号

説明	ubuntu 7.*x* クライアントから作成された新規ファイルが 4294967294 の UID および GID （nfsnone）を取得します。
原因	デフォルトでは、Ubuntu 7.*x* nfs クライアントは nfs の呼び出しで rpc 資格情報を指定しません。 その結果、これらのクライアントから作成されたファイル（ユーザーを問わない）は、4294967294 (nfsnone) UID と GID の所有となります。
対策	nfs の呼び出しで UNIX 証明書を強制するには、ubuntu **fstab** ファイルで NAS クラスタソリューションのマウントに **sec=sys** オプションを追加します。

ネットワーク接続のトラブルシューティング

ネームサーバーが応答しない

説明

NIS、LDAP、または DNS サーバーのすべてにアクセスできないか応答しません。

対策

各サーバーについて、次を実行してください。

1. NAS cluster（NAS クラスタ）ソリューションサブネット上のクライアントからサーバーに ping 送信して、応答があるか確認します。
2. NAS cluster（NAS クラスタ）ソリューションサブネット上のクライアントからサーバーにリクエストを発行し、応答があるか確認します。
3. サーバーのログをチェックして、なぜサーバーが要求への応答に失敗するかを調べます。

特定のサブネットクライアントが NAS cluster（NAS クラスタ）ソリューションにアクセスできない

説明

ユーザー（新規または既存）が特定のネットワークからアクセスしているか NAS cluster（NAS クラスタ）ソリューションにアクセスできません。

原因

この問題は、ユーザーのサブネットアドレスと NAS システムの内部ネットワークのアドレスが拮抗していることによって発生します。NAS システムは、応答パケットを間違ったネットワークにルーティングします。

対策

1. NAS システムの内部ネットワークアドレスを確認し、問題のあるクライアントネットワークアドレスと拮抗しているかどうかを確認します。
2. 拮抗している場合は、NAS Manager または CLI を使用して、拮抗している NAS 内部ネットワークアドレスを手動で変更します。

DNS 設定のトラブルシューティング

説明

システム名を使用して NAS クラスタソリューションに接続することができません。または、ホスト名の名前解決ができません。

原因

次の原因が考えられます。

- 完全修飾ドメイン名（FQDN）を使用してシステムに ping できない。
- システム名を使用して NAS Manager に接続できない。

対策

1. クライアントの IP 情報が正しく設定されていることを確認します。

2. NAS クラスタソリューションコントローラが正しい DNS サーバーに設定されていることを確認します。
3. DNS サーバーの管理者に問い合せて DNS の記録の作成を確認します。

CLI を使用した NAS cluster（NAS クラスタ）ソリューションコントローラの IQN の特定

説明

CLI を使用して、NAS cluster（NAS クラスタ）ソリューションコントローラの IQN を特定します。

対策

ssh クライアントおよび NAS 管理 VIP を使用して、管理者として NAS cluster（NAS クラスタ）ソリューション CLI にログインします。

コマンドラインで次のように入力します。

```
system maintenance luns iscsi-configuration view
```

RX および TX 一時停止警告メッセージのトラブルシューティング

説明

NAS Manager が接続性に関して Not Optimal（非最適）状態を報告した場合、次の警告メッセージが表示される場合があります。

`Rx_pause for on node 1 is off.`（ノード 1 の `eth（x）の Rx_pause` がオフです。）

`Tx_pause for on node 1 is off.`（ノード 1 の `eth（x）の Tx_pause` がオフです。）

原因

NAS cluster（NAS クラスタ）ソリューションコントローラに接続されたスイッチで、フロー制御が有効になっていません。

対策

スイッチベンダーのマニュアルを参照して、スイッチのフロー制御を有効にしてください。

NAS Manager の問題のトラブルシューティング

NAS ダッシュボードが遅延状態

説明

NAS ダッシュボードメトリクスが遅延し、アップデートされた値がアップデート後すぐに表示されません。

原因

NAS Manager のビューは 40 秒ごとに更新されますが、特定のメトリクスに関する情報は異なる間隔で収集されます。これは、画面の更新と実際のメトリクスの更新の間に相関関係がないからです。

対策

システム内のさまざまなマトリックスに関して情報を収集する、FluidFS のプロセスを使用します。

- Status（ステータス）フィールド（全体の状態、サービスステータス、サーバーステータス）— 情報は 40 秒間隔で収集されます。
- Capacity（容量）— 情報は 1,800 秒間隔で収集されます。
- Current performance（現在のパフォーマンス）（NFS、CIFS、レプリケーション、NDMP、ネットワーク）— 情報は 40 秒間隔で収集されます。
- Recent performance（最近のパフォーマンス）（グラフ）— 情報は 60 秒間隔で収集されます。
- Load balancing（負荷バランシング）（CPU、接続数）— 情報は 40 秒間隔で収集されます。

NAS システム時間が間違っている

説明

スケジュールされたタスクが間違った時刻に実行されています。イベントログメッセージの日付または時間が正しくありません。

原因

- NAS システムの時刻が正しくありません。
- NAS システムに NTP サーバーが定義されていません。
- NAS cluster（NAS クラスタ）ソリューションにサービスを提供している NTP サーバーがダウンしているか、NTP サービスの提供を停止しました。
- NTP サーバーとの通信にネットワーク上の問題があります。

対策

1. **System Configuration/ Time Configuration**（システム設定 / 時刻設定）ページで NAS NTP サーバーを特定します。今後の参照用に、ホスト名または IP アドレスを記録しておきます。
2. NTP サーバーが定義されていない場合は定義してください。NAS システムクロックを Active Directory Domain Controller（ADDC）で使用される NTP サーバーと同期させることをお勧めします。これにより、時差や認証に関する問題を回避できます。多くの場合、ADDC は NTP サーバーでもあります。
3. NTP サーバーが起動し、NTP サービスを提供していることを確認します。
4. ping などを使用して NAS システムと NTP サーバー間のネットワークパスを確認します。応答時間がミリ秒の範囲内であることを確認してください。

NAS Manager に接続できない

説明	NAS Manager に接続できません。
原因	次の原因が考えられます。 • ユーザーが正しくない IP アドレスを使用して接続しようとしているか、誤ったシステム名を使用している。 • クライアントコンピュータの IP 情報が正し設定されていない。 • ユーザーが正しくないユーザー名またはパスワードを使用している。 • ユーザーのブラウザのプロパティが接続を妨げている。
対策	1. クライアントの IP 情報が正しく設定されていることを確認します。 2. DNS 情報が正しく設定されていることを確認します。 3. ユーザー名とパスワードを確認します。 4. ブラウザの設定でプロキシ情報を確認します。 5. Microsoft Windows Server 2008 を使用している場合は、IE ESC を無効にします。

空白のログイン画面

説明	NAS Manager に接続できず、ログイン画面が空白です。
原因	次の原因が考えられます。 • Java スクリプトが無効になっている。 • IE SEC が有効になっている。
対策	• Java スクリプトが無効になっている場合は、有効にします。Java スクリプトの有効化の詳細については、ブラウザのヘルプを参照してください。 • IE SEC が有効になっている場合は、無効にします。

バックアップの問題のトラブルシューティング

スナップショットのトラブルシューティング

説明	スナップショットの取得および削除ができません。
原因	次の原因が考えられます。 • 容量の大きいディレクトリの削除など、待機中の I/O リクエストが多数ある。

- 現在処理中のスナップショット作成 / 削除リクエストが多数ある。
- このボリュームに対して別のスナップショットリクエストが現在実行されている。
- スナップショットの合計数がシステムの上限に達した。
- バックアップジョブで間違った IP アドレスが指定された。

対策

- 手動リクエストエラーの場合は、1～2 分後にスナップショットの取得または削除を再試行します。
- スナップショットスケジューラからのリクエストの場合は、1～2 サイクル待ちます。エラーが解消されない場合は、同じボリュームでスナップショットの取得または削除を手動で実行します。
- システムに高い負荷がかかっていないかどうか、ダッシュボードを確認します。システムに高い負荷がかかっている場合は、負荷が低下するまで待ち、スナップショットリクエストを再発行します。
- スナップショットのスケジュールを確認します。過密なスナップショットスケジュールは、システムの全体的なパフォーマンスに悪影響を与えます。1 台のシステムで、スナップショットの累積回数が 1 時間あたり 20 スナップショットを超えてはいけません。
- システムのスナップショットの合計数を確認します。合計数が数千単位になる場合は、いくつかのスナップショットを削除し、再試行します。
- バックアップジョブで、クライアントの仮想 IP アドレスを正確に指定します。

NDMP 内部エラーのトラブルシューティング

説明

内部エラーが発生してバックアップまたは復元が失敗します。

原因

NDMP 内部エラーは、ファイルシステムへのアクセスができなくなっているか、NAS ボリュームが使用できなくなっていることを示します。

対策

バックアップアプリケーションを NAS アプライアンスに接続できない場合は、次の手順を実行します。

1. NAS Manager にログインするか、アプライアンスへのリモートターミナルを開きます。
2. NAS Manager では、**Data Protection → NDMP → NDMP Configuration（データ保護 > NDMP > NDMP の設定）**ページに移動します。NAS CLI では、**Data Protection NDMP Configuration**（データ保護 > NDMP > 設定）メニューに移動します。
3. NDMP が有効になっていることを確認します。NDMP が有効になっている場合は手順 5 に進みます。
4. NAS Manager では、**Enabled**（有効）チェックボックスにチェックを入れます。

5. NAS CLI では、`view` と入力し、**State**（状態）が **Enabled**（有効）に設定されていることを確認します。
6. NDMP が有効になっていない場合、有効にします。
7. NDMP でバックアップアプリケーションの IP アドレスが 設定されていることを確認します。
8. NAS Manager では、DMA サーバーリストにバックアップアプリケーションの IP アドレスが含まれていなければなりません。
9. NAS CLI では、`view` と入力し、NAS アプライアンスにアクセスしようとしている DMA アプリケーションの IP アドレスが **DMA Servers**（DMA サーバー）リストに含まれていることを確認します。

バックアップアプライアンスが NAS アプライアンスに接続できるものの、ログインができない場合は、お使いのバックアップアプリケーションで NDMP バックアップ / 復元をセットアップする際、NDMP クライアント用のユーザー名に backup_user を使用します。NDMP クライアントのデフォルトパスワードは **Stor@ge!** です。

パスワードを変更するには、次の手順を実行します。

1. NAS Manager にログインするか、アプライアンスへのリモートターミナルを開きます。
2. NAS Manager では、**Data Protection → NDMP → NDMP Configuration（データ保護 > NDMP > NDMP の設定）**ページに移動します。NAS CLI では、**Data Protection → NDMP → Configuration（データ保護 > NDMP > 設定）**メニューに移動します。
3. NAS Manager では、**Change Password**（パスワードの変更）をクリックします。NAS CLI では、コマンドを実行します：

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

バックアップアプリケーションが NAS アプライアンスにログインできるものの、バックアップに使用できるボリュームがない場合、NAS アプライアンスで NAS ボリュームが作成されているかを確認します。

システムのトラブルシューティング

システムシャットダウンのトラブルシューティング

説明	NAS Manager を使用してシステムをシャットダウン中、20 分経過してもシステムが停止せず、コントローラがシャットダウンしません。
原因	システムのシャットダウン手順は、次に示す 2 つの異なるプロセスで構成されています。 • ファイルシステムの停止 • NAS cluster（NAS クラスタ）ソリューションコントローラの電源オフ データ量が多い、またはストレージへの接続が断続的であるために、ファイルシステムがストレージの

キャッシュをクリアするのに長時間を要する場合があります。

電源がオフの段階では、OS カーネルがコントローラでハングしている、または、ローカルドライブへの状態の同期でエラーが発生していることが原因として考えられます。

対策

ファイルシステムが停止し、いずれかのコントローラがまだ電源オンの状態であれば、電源ボタンを押して物理的に電源をオフにすることができます。

ファイルシステムが停止していない場合は、その動作を継続させる必要があります。ファイルシステムは、10 分のタイムアウトに達するとキャッシュをローカルコントローラにフラッシュし、シャットダウンプロセスを続行します。

NAS コンテナのセキュリティ違反

説明

NAS コンテナがセキュリティに違反しています。

原因

NAS コンテナのセキュリティ方式を選択すると、このボリューム内のファイルでパーミッションを設定する際に使用する主要プロトコルが指定されます。UNIX セキュリティ方式のボリュームには NFS、NTFS セキュリティ方式のボリュームには CIFS が使用されます。

その結果、以下に示す一部の操作が無効になります。

- NTFS セキュリティ方式のコンテナ内にあるファイルへの UNIX パーミッションの設定。
- NTFS セキュリティ方式のコンテナ内にあるファイルへの UID/GID 所有権の設定。
- UNIX セキュリティ方式のコンテナ内にあるファイルへの ACL の設定。
- UNIX セキュリティ方式コンテナ内にあるファイルの読み取り専用フラグの変更。
- UNIX セキュリティ方式のコンテナ内にあるファイルへの SID/GSID 所有権の設定。

NAS コンテナのセキュリティ方式は、そのファイルへのアクセスに使用する主要プロトコルを反映していなければなりません。

対策

ユーザーがプロトコルをまたいでセキュリティ関連のアクティビティを頻繁に実行しなければならない場合は、主要アクセスプロトコルに基づいてデータを別々の NAS コンテナに分割します。

ファイルシステムのフォーマット中における複数エラーの受信

説明

ファイルシステムのフォーマット中に、複数のエラーを受信します。

原因

次の原因が考えられます。

- Dell NAS Initial Deployment Utility（IDU）で誤った SAN IP が使用されている。
- MDSM でのホストの定義中に誤った IQN が使用された。

- ホストグループに奇数の LUN がマップされた。
- LUN のサイズが最小要求サイズに満たない。
- LUN の数が最小必要数より少ない。

対策

NAS IDU の実行中に誤った SAN IP が使用された場合は、次の手順を実行します。

1. NAS IDU の実行中に使用した MD 検出 IP が、お使いのコントローラに設定されている 2 つの SAN IP のうちいずれか一方と同じサブネット上にあることを確認します。
2. MD 検出 IP を確認するには、CLI を使用して NAS Manger IP にログインし、次のコマンドを実行します。`system maintenance luns configuration iscsi-view`

このコマンドによって MD 検出 IP が表示されます。

お使いの SAN に設定された IP と同じサブネットに IP がない場合は、MD 検出 IP を、お使いのコントローラの SAN A および B で定義されたいずれかのサブネットに変更します。

MDSM でのホスト定義中に誤った IQN が使用された場合、MDSM に表示されている IQN がコントローラの IQN に一致することを確認します。

CLI で検出 IP を変更するには、次のコマンドを実行します。

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

コマンドが完了したら、ホストポート ID を更新します。これで NAS Manager から再び設定ウィザードを実行できます。

1. MDSM に表示された IQN が、NAS Manager の hosts（ホスト）セクションにある **Mappings**（マッピング）タブ下に表示されたものと同じかどうかを確認します。
2. 同じでない場合は、MDSM のホストで使用される IQN を修正し、システムのフォーマットを試行します。LUN が検出され、フォーマットされていなければなりません。

LUN の数が奇数であるために問題が生じている場合は、次の手順を実行します。

1. エラーが発生した場合は、偶数の LUN がホストグループにマッピングされていることを確認します。奇数の LUN はサポートされません。LUN は 2 から始まり、16 までペアで増分されます。
2. 奇数の LUN が使用されている場合は、LUN を追加または削除して数を修正します。
3. システムのフォーマットを試行します。

LUN のサイズが最小要件より小さい場合は、次の手順を実行します。

1. LUN が最小要件の 125 GB よりも大きいことを確認します。

2. LUN が 125 GB 未満の場合、最小要求サイズ以上になるように LUN のサイズを変更します。
3. システムのフォーマットを試行します。

LUN の数が最小要件よりも少ない場合は、次の手順を実行します。

1. 複数の LUN がホストグループにマッピングされていることを確認します。LUN の最小必要数は 2 です。
2. LUN の数が 2 未満の場合、LUN を追加して最小必要数の 2 を満たします。
3. システムのフォーマットを試行します。

LUN 名の仮想ディスクへの関連付け

説明	NAS Manager 内のどの LUN が Modular Disk Storage Manager（MDSM）の仮想ディスクであるかを特定します。
対策	NAS Manager ウェブインタフェースを開き、**Cluster Management → Maintenance → Add Luns（クラスタの管理 > メンテナンス > LUN の追加）**へ移動します。このページに、NAS cluster（NAS クラスタ）ソリューションがアクセスする（NAS cluster（NAS クラスタ）ソリューションのホストグループに割り当てられた）すべての LUN が表示されます。各 LUN はワールドワイド名で識別できます。NAS Manager ウェブインタフェースでは、LUN のワールドワイド名の前にプレフィックスが付いています。 MDSM を開いて **Logical**（論理）タブへ移動し、**Virtual Disk**（仮想ディスク）をクリックします。仮想ディスクのワールドワイド ID が **Properties**（プロパティ）ペインに表示されます。この方法により、どの仮想ディスクが NAS ファイルシステムに割り当てられているかを特定できます。

NAS IDU がコントローラを検出できない

説明	NAS IDU がコントローラを検出できません。
原因	IPV6 がワークステーションで有効化されていない可能性があります。
対策	お使いの管理ワークステーションで IPV6 を有効にしてください。

接続操作の失敗

説明	コントローラを NAS クラスタに接続できません。
対策	• 接続操作に失敗したコントローラにキーボードとモニタを接続し、エラーメッセージを確認して操作が失敗した原因を特定します。 • 次の点を確認します。

- コントローラが接続されていないとき、クライアントネットワーク上でそのコントローラに割り当てられている IP は他のホストに割り当てられなかった。コントローラが接続されていない間、IP アドレスを含むコントローラの ID は失われる。コントローラが接続されると、IP アドレスを含む ID が再びコントローラに適用される。
- NAS Manager を使用して、デフォルトゲートウェイが **プライマリ** サブネット内にあることを確認します。**Cluster Management → Network Configuration（クラスタの管理 > ネットワークの設定）**でデフォルトゲートウェイを表示します。**Cluster Management → Subnets（クラスタの管理 > サブネット）**でクライアントネットワークの **プライマリ** サブネットを表示します。デフォルトゲートウェイが **プライマリ** サブネットにない場合は、デフォルトゲートウェイを変更します。接続が正しく行われるには、デフォルトゲートウェイへの **ping が可能** でなければなりません。

- 接続操作が失敗した場合は、コントローラを手動でスタンバイモードにリセットする必要があります。接続に失敗したコントローラにキーボードとモニタを接続し、画面の指示に従ってシステム識別ボタンキー を押してください。

サービスパックのアップグレード後、コントローラの起動に時間がかかる

説明

コントローラファームウェアのサービスパックをアップグレードした後、コントローラの起動に時間がかかります。

対策

- 起動に時間がかかっているコントローラにキーボードとモニタを接続します。
- システムが起動し、起動フェーズの状態にある場合は、そのままアップグレードを完了させてください。これには最大で 60 分かかることがあります。
- コントローラが起動フェーズの **Executing System Upgrades**（システムアップグレードの実行中）の状態にある間は、コントローラを手動で再起動しないでください。

Dell NAS Initial Deployment Utility（IDU）のトラブルシューティング

Dell NAS Initial Deployment Utility の実行中におけるエラーの受信

説明	Dell NAS Initial Deployment Utility（IDU）を実行中にエラーが発生しました。
原因	エラーは、ハードウェアのセットアップ、ネットワークスイッチの設定、クラスタシステムの設定のいずれかが原因で発生する可能性があります。
対策	検出ページに接続失敗と表示されている場合は、次を実行します。 1. **NAS IDU** が実行されている管理ステーションに NAS クラスタのクライアントスイッチへのネットワーク接続があることを確認します。 **メモ:** NAS コントローラおよび NAS IDU が実行されているシステムにルーターを決して接続しないでください。 2. NAS IDU が実行されている管理ステーションで IPv6 が有効になっているかをチェックします。 3. USB キーボードおよびモニタを NAS クラスタコントローラに接続し、**Press "i" -re-install standby node"**（「i」を押してスタンバイノードを再インストールします）というメッセージとともにコントローラの MAC アドレスを表示するメッセージが繰り返されるかどうかを確認します。 NAS クラスタの設定ページにエラーがある場合は、次を実行します。 1. クラスタ化中、NAS IDU のウィンドウからエラーメッセージのスクリーンショットを取得します。 2. クラスタ設定ファイル、NAS IDU ログファイル、およびインストールディレクトリの結果ファイルを収集し、インストールディレクトリから config フォルダを Zip 形式で圧縮します。 3. NAS IDU でウィンドウの復元を求められ、ノードがスタンバイモードに復元されます。 4. 取得したスクリーンショットでエラーメッセージを探し、エラーの潜在的原因を見つけます。それらのエラーを修正し、NAS IDU を使用してシステムを再設定します。 5. 引き続き障害が残る場合は、バンドルパッケージ内のすべてのファイルを収集して、デルサポートにお問い合わせください。

Dell NAS Initial Deployment Utility（IDU）を起動できない

説明	Dell NAS Initial Deployment Utility（IDU）を起動できません。
原因	次の原因が考えられます。 • NAS Initial Deployment Utility のインストーラがインストールを実行できない。 • JAVA ランタイム環境が正しくインストールされていない。
対策	次の手順を実行します。 • NAS ID Utility のインストーラが正しく完了していることを検証します。 • 最低 JRE1.6x が正しくインストールされていることを検証します。 • Microsoft Windows でコマンドコンソールから `java -version` を実行し、有効な JRE バージョンを表示します。

7

NAS クラスタソリューションのメンテナンス

本章では、計画的な機能停止またはシステムを別の場所に移動するといったイベントの際の、システムのシャットダウンと電源投入に関する情報を提供します。

メモ: ハードウェアのサービスおよびメンテナンスについては、**dell.com/support** にある『*Dell FluidFS NAS Solutions Owner's Manual*』（Dell FluidFS NAS ソリューションハードウェアオーナーズマニュアル）を参照してください。

NAS cluster（NAS クラスタ）ソリューションのシャットダウン

注意: データの整合性を維持するため、次の手順に確実に従ってください。

メモ: この手順により、両方のコントローラがシャットダウンします。

システムをシャットダウンするには、次の手順を実行します。

1. ウェブブラウザを開き、インストール処理で設定した NAS 管理仮想 IP（VIP）アドレスに接続します。
2. NAS Manager で **Cluster Management → Maintenance → System Stop/Start（クラスタの管理 > メンテナンス > システムの停止 / 起動）**と選択します。

   System Stop/Start（システムの停止 / 起動）ページにシステムステータスが表示されます。
3. **System action to perform**（実行するシステムアクション）リストから **Stop**（停止）を選択します。
4. **次へ** をクリックします。
5. 停止処理を続行するよう求めるプロンプトが表示されたら、**OK** をクリックします。

   この操作により、ファイルシステムキャッシュがディスクにコピーされ、ファイルシステムが停止します。
6. 各コントローラの背面に埋め込まれた電源ボタンを押して放すと、コントローラがシャットダウンされます。

   メモ: 電源ボタンを数秒間押し続けると、システムの電源はオフになりません。

NAS cluster（NAS クラスタ）ソリューションの電源投入

システムに電源を投入する前に、ラック内のコントローラ間のすべてのケーブルが接続されていること、およびコンポーネントが施設の電源に接続されていることを確認します。

次の順序でコンポーネントに電源を入れます。

1. ストレージアレイ：
   - ユニットの後方にある 2 台の電源装置のオン / オフスイッチを押して、すべてのストレージアレイの電源を入れます。
   - 電源装置、コントローラ、およびディスク LED が確実に点灯するまで待ちます。
2. NAS cluster（NAS クラスタ）ソリューション：

   コントローラを起動するには、NAS コントローラまたはアプライアンスをそれぞれ電源に接続します。

3. NAS Manager で **Cluster Management → Maintenance → System Stop/Start（クラスタの管理 > メンテナンス > システムの停止 / 起動）**と選択します。

   System Stop/Start（システムの停止 / 起動）ページにシステムステータスが表示されます。

4. **System action to perform**（実行するシステムアクション）リストから **Start**（開始）を選択します。

5. **次へ** をクリックします。

NAS ボリューム設定の復元

NAS ボリューム設定の復元は、システム管理者がすべての NAS ボリュームの設定（エクスポート、共有、スナップショットのスケジュール、クォータルールなど）を、手動で再設定しなくても復元できる効果的な方法です。この方法は、新規 NAS ボリュームの作成後、システムのインストール直後、またはシステムの回復後に利用すると便利です。

NAS ボリュームの復元は、1 つの NAS ボリュームの設定を（それが保存された唯一の設定であっても）同じシステムまたは違うシステム上の別の NAS ボリュームに復元することで実行できます。管理者は対象とする NAS ボリュームに、バックアップまたは別の NAS ボリュームから設定をコピーする必要があります。

ボリュームの設定が変更されると、その変更はユーザーが後から復元できるフォーマットで自動的に保存されます。設定は、NAS ボリュームのルートフォルダにある **.clusterConfig** フォルダに保存されます。

このフォルダは個別に、またはボリュームのユーザーデータと一緒にバックアップしておき、後で復元することができます。フォルダに保存された設定を有効にするには、管理者はまず **.clusterConfig** フォルダを復元対象の NAS ボリュームにコピーし、その後 **Restore NAS Volume Configuration**（NAS ボリューム設定の復元）画面を使用してその NAS ボリュームに設定を適用する必要があります。

メモ: NAS ボリュームを復元すると、既存の設定は上書きおよび置換されます。そのときにシステムに接続しているユーザーは切断されます。

復元できるパラメータは次のとおりです。

- NFS エクスポート
- CIFS 共有
- クォータルール
- スナップショットスケジュール
- NAS ボリュームアラート、セキュリティ方式、および関連パラメータ
- NAS ボリューム名
- NAS ボリュームサイズ

NAS ボリュームの設定を復元するには、次の手順を実行します。

メモ: 他のシステムのバックアップを使用している場合は、同じソフトウェアリリースを使用するシステムから保存済みの設定が取得された場合のみ、復元操作を実行できます。

1. **Cluster Management → Maintenance → Restore NAS Volume Configuration（クラスタの管理 > メンテナンス > NAS ボリューム設定の復元）**と選択します。

   Restore NAS Volume Configuration（NAS ボリューム設定の復元）ページが表示されます。

2. **Update the configuration of**（設定をアップデートする）リストから、設定をアップデートするシステムを選択します。

3. **Configuration taken from system**（システムから設定を取得）リストから、設定情報のソースクラスタを選択します。

4. 復元可能なシステム全体のパラメータのリストから、1 つまたは複数のオプションを選択します。

5. **適用** をクリックします。

クラスタ設定の復元

システム設定の復元は、手動で再設定をしなくても、システム設定（プロトコルの設定、ローカルユーザー、グループなど）の大部分を復元できる効果的な方法です。この方法は、新しいソフトウェアリリースでシステムをアップグレードした後、システムのインストール直後、またはシステムの回復後に利用すると便利です。

システム設定の復元は、クラスタ内で最新の NAS ボリュームに保存された設定を取得し、それを現在のシステム上で復元することで実行できます。設定はバックアップまたは他のシステムから NAS ボリュームにコピーする必要があります。

システムの設定が変更されると、その変更はユーザーが後から復元できるフォーマットで自動的に保存されます。設定は、NAS ボリュームのルートフォルダにある **.clusterConfig** フォルダに保存されます。

このフォルダは個別に、またはボリュームのユーザーデータと一緒にバックアップしておき、後で復元することができます。フォルダに保存された設定を有効にするには、管理者はまず **.clusterConfig** フォルダをシステム上のいずれかの NAS ボリュームにコピーし、その後システムに設定を適用する必要があります。

メモ: システム設定を復元すると、既存の設定は上書きおよび置換されます。そのときにシステムに接続しているユーザーは切断されます。

復元できるパラメータは次のとおりです。

- プロトコルの設定
- ユーザーおよびグループ
- ユーザーマッピング
- 監視設定
- 時刻設定
- アンチウイルスホスト

1. **Cluster Management → Maintenance → Restore Cluster Configuration（クラスタの管理 > メンテナンス > クラスタ設定の復元）** と選択します。

   Restore Cluster Configuration（クラスタ設定の復元）ページが表示されます。

2. **Configuration taken from system**（システムから設定を取得）リストから、設定をアップデートするシステムを選択します。
3. 復元可能なシステム全体のパラメータのリストから、1 つまたは複数のオプションを選択します。
4. **適用** をクリックします。

ファイルシステムのフォーマット

メモ: NAS Manager を使用したファイルシステムのフォーマットは NX3600 および NX3610 のみでサポートされます。FS8600 では、**Enterprise Manager** を使用して FS8600 を初めて導入するときに、**Enterprise Manager** によって**ファイルシステムフォーマット**が実行されます。

ファイルシステムフォーマットを実行すると、NAS にマッピングされた LUN にファイルシステムがインストールされます。ファイルシステムフォーマットによって、LUN に格納されている既存のデータはすべて消去されます。NAS ボリュームを作成するには、その前にファイルシステムフォーマットを実行する必要があります。通常は、NAS が再配置されて既存のデータが必要でなくなった場合を除き、ファイルシステムフォーマットは 1 回限りのイベントです。

ファイルシステムをフォーマットするには、**Cluster Management → Maintenance → File System Format（クラスタの管理 > メンテナンス > ファイルシステムフォーマット）** を選択し、**Format**（フォーマット）をクリックします。

サービスパックのインストール

NAS クラスタソリューションでは、ソフトウェアを最新バージョンにアップデートするためにサービスパック方式を使用します。

メモ: お使いのシステムを最新サービスパックでアップデートするには、**dell.com/support** を参照してください。

NAS Manager を使用したサービスパックのアップグレード

サービスパックは、最新のファームウェアとソフトウェアを使用して、お使いの Dell FluidFS NAS ソリューションを最新の状態に保ちます。システムが安全かつ効率的な動作を維持できるよう、**dell.com/support** で最新のサービスパックをダウンロードしてください。

注意: NAS ソリューションソフトウェアをバージョン 1.x からバージョン 2.x へアップグレードする場合は、ファイル名フォーマットが DellFS-2.0.xxxx-SP.sh のサービスパックを使用してください。バージョン 2.0 以降の NAS ソリューションソフトウェアをアップグレードする場合は、ファイル名フォーマットが DellFluidFS-2.0.xxxx-SP.sh のサービスパックを使用してください。

注意: サービスパックのファイル名は変更しないでください。

注意: サービスパックをインストールすると、インストール処理中に NAS コントローラが再起動されます。これによってクライアントの接続は中断されます。したがって、サービスパックのインストールは、スケジュールされたメンテナンスウィンドウで行うことをお勧めします。

注意: サービスパックのインストール処理は元に戻すことができません。システムを一度アップデートすると、以前のバージョンに戻すことはできません。

サービスパックをインストールするには、次の手順を実行します。

1. **dell.com/support/downloads** からサービスパックをダウンロードします。
2. NAS Manager で、**Cluster Management → Maintenance → Service Pack（クラスタの管理 > メンテナンス > サービスパック）**と選択します。

   Service Pack（サービスパック）ページが表示されます。
3. **Browse**（参照）をクリックします。
4. 最新のサービスパックへ移動し、**Open**（開く）をクリックします。
5. **Upload**（アップロード）をクリックします。
6. サービスパックファイルがシステムにアップロードされたら、**Install**（インストール）をクリックします。

NAS クラスタのストレージ容量の拡張

Dell PowerVault NX3500/NX3600/NX3610 NAS ソリューションでの NAS プールの拡張

クライアントへのサービスに支障なく、お使いのシステムのストレージ容量を拡張することができます。ただし、期間中に発生する処理は、既存と追加された LUN の合計数、ストレージの合計容量、およびシステムの作業負荷によります。ストレージアレイですでに使用可能となっているストレージ容量からの LUN を、NAS クラスタソリューションに追加することができます。

MD Storage Array には、NAS クラスタソリューションへの割り当て用の追加の容量が必要です。ディスクグループおよび仮想ディスクの拡張に関する詳細は、**dell.com/support/manuals** にある『Modular Disk Storage Manager Administrator's Guide』（Modular Disk Storage Manager 管理者ガイド）を参照してください。

NAS クラスタソリューションのストレージ容量を拡張するには、次の手順を実行します。

1. 管理ステーションで **NAS Manager** を起動し、**管理者**としてログオンします。

   メモ: デフォルトの管理者パスワードは **Stor@ge!** です。

2. **Cluster Management（クラスタの管理）** → **Maintenance（メンテナンス）** → **Add LUNs（LUN の追加）** と選択します。
   Expand Luns（LUN の拡張）ページが表示されます。
3. ページの左下にある **Expand Luns（LUN の拡張）**をクリックします。
   Status（ステータス）ページが表示され、LUN 拡張の進捗状況が示されます。
4. **終了** をクリックします。

FS8600 NAS ソリューション上の NAS プールの拡張

1. **Enterprise Manager クライアント**にログオンします。
2. 左側ペインで **Storage**（ストレージ）をクリックします。
3. トップメニューで **Expand NAS Pool**（NAS プールの拡張）をクリックします。
4. NAS プールサイズを入力します。

   メモ: Storage Center ごとの最大限度は、512 TB です。NAS プールは拡張だけが可能であり、NAS プールの縮小は許可されません。

メモ: NAS プールは、2 つ目の Storage Center を追加することによっても拡張できます。FluidFS クラスタへの 2 つ目の Storage Center アレイの追加方法の詳細については、『*Enterprise Manager Administrator's Guide*』（Enterprise Manager 管理者ガイド）を参照してください。

PowerVault NX3500/NX3600/NX3610 NAS Cluster（PowerVault NX3500/NX3600/NX3610 NAS クラスタ）ソリューションへの LUN の追加

この手順では、NAS cluster（NAS クラスタ）ソリューションに割り当てるための追加容量が MD ストレージアレイで必要になります。MD アレイのディスクグループおよび仮想ディスク拡張の詳細については、**dell.com/support/manuals** の『MD Series Storage Array Administrator's Guide』（MD シリーズストレージアレイ管理者ガイド）を参照してください。

警告: FluidFS は、最大 32 個の LUN と最大 32 TB の LUN サイズをサポートしています。ただし、MDSM を使用するとこの制限を上回ることができます。サポートされる LUN の最大数を超えると、パフォーマンスまたはアクセスに問題が生じることがあります。

メモ: 小さいサイズの LUN を多数使用するよりも、少数の大きい LUN を使用することをお勧めします。可能な場合は既存の LUN を拡張し、NAS プールサイズを拡大します。

1. MDSM では、追加の仮想ディスクをペアで作成します。

   メモ: 詳細については、**dell.com/support/manuals** で『MD Series Storage Array Administrator's Guide』（MD シリーズストレージアレイ管理者ガイド）を参照してください。

2. 作成した仮想ディスクをクラスタの**ホストグループ**に追加します。
3. 管理ステーションで **NAS Manager** を起動し、**管理者** としてログオンします。

   メモ: デフォルトの管理者パスワードは **Stor@ge!** です。

4. **Cluster Management** → **Maintenance** → **Add LUNs（クラスタの管理 > メンテナンス > LUN の追加）** と選択します。

このページは表示されるまでに数分かかる場合があります。このページでは、NAS cluster（NAS クラスタ）ソリューションに割り当てられたすべての仮想ディスク / LUN について iSCSI 検索が実行されます。

各 LUN はそれぞれのワールドワイド名を使用して識別できます。NAS Manager では、LUN のワールドワイド名に Dell FluidFS というプレフィックスが付けられます。このプレフィックスに続く、数値と文字から成る一意のセットがワールドワイド名です。

Add LUN（LUN の追加）ページが表示されます。

5. **Add LUNs**（LUN の追加）をクリックし、新しい LUN を NAS cluster（NAS クラスタ）ソリューションに追加します。システムで、新しい LUN の増分ファイルシステムフォーマットが実行されます。

   この処理は、LUN のサイズと数に応じて若干時間がかかります。

   完了すると、新規容量が使用可能になります。

6. **終了** をクリックします。

診断プログラムの実行

診断を実行することで、デルへお問い合わせの前に問題をトラブルシューティングする手助けになります。お使いのソリューションでは、次の診断オプションが使用可能です。

- オンラインの Diagnostics（診断）
- オフラインの Diagnostis（診断）

オンラインの Diagnostics（診断）

オンラインの Diagnostics（診断）は、システムがまだオンラインの状態でデータを供給している間に実行することができます。次の Diagnostics（診断）オプションが使用可能です。

- **一般**
- **File System**
- **ネットワーク**
- **パフォーマンス**
- **プロトコル - ログの収集**
- **プロトコル - 単一クライアント**
- **プロトコル - 単一ファイル**

上記いずれかの Diagnostics（診断）を実行するには、次の手順を行います。

1. **Cluster Management → Maintenance → Diagnostics（クラスタの管理 > メンテナンス > 診断）** と選択します。

   Diagnostics（診断）ページが表示されます。

2. **Diagnostics type**（診断タイプ）リストから、適切なオプションを選択して **Start**（開始）をクリックします。

   Diagnostics（診断）の完了時に、Diagnostics（診断）ファイルの圧縮されたアーカイブへのリンクが表示されます。

3. **Download diagnostics archive**（診断アーカイブのダウンロード）ファイルで適切なリンクをクリックします。

   選択した Diagnostics（診断）ファイルを開くか保存するように求めるメッセージプロンプトが表示されます。

4. **Done**（完了）をクリックします。

オフラインの Diagnostis（診断）

メモ: 次の手順を実行する前に、キーボードとモニタを接続してください。

オフラインの診断を行うには、ソリューションがオフライン、つまり稼動を中止し、データを処理していない状態でなければなりません。オフラインの診断は、主に低レベルのハードウェア問題のトラブルシューティングに役立ちます。

オフラインの診断には、次のデルのネイティブツールが使用されます。

- MP Memory
- Dell Diagnostics（診断）プログラム

MP Memory

MP Memory はデルが開発した MS DOS ベースのメモリテストツールです。このツールは大きな（4 GB より大きい）メモリ構成に効果的です。ツールは単一のプロセッサまたはマルチプロセッサ構成の他に、Intel ハイパースレッディングテクノロジを使用するプロセッサもサポートします。

MP Memory は、Intel プロセッサベースのコントローラ上でのみ動作します。 このツールは、Dell 32 ビット診断テストを補足し、オペレーティングシステム前の環境でコントローラに完全で総合的な診断を提供します。

内蔵されたシステム診断プログラムの実行

注意: 内蔵されたシステム診断プログラムは、お使いのシステムをテストする場合にのみ使用してください。このプログラムを他のシステムで使用すると、無効な結果やエラーメッセージが発生する場合があります。

1. キーボード、モニタ、およびマウスをコントローラの VGA ポートおよび USB ポートに接続します。
2. コントローラを再起動するには、コントローラの背面にある電源ボタンを押して離し、コントローラをシャットダウンした後、コントローラの背面にある電源ボタンを再度押して離し、コントローラを再度オンにします。
3. システム起動中に <F10> を押します。
4. 上下矢印キーを使用して、**System Utilities（システムユーティリティ） → Launch Dell Diagnostics（Dell 診断の起動）** の順に選択します。

   ePSA Pre-boot System Assessment（ePSA 起動前システムアセスメント）ウィンドウが表示され、システム内に検知された全デバイスがリストアップされます。Diagnostics（診断）が検知された全デバイスのテストを開始します。
5. 完了したら、キーボード、モニタ、およびマウスをコントローラから取り外し、コントローラを再起動します。

NAS クラスタソリューションの再インストール

注意: NAS クラスタソフトウェアの再インストールは、お使いのシステムを工場出荷時のデフォルトに戻します。この手順を実行すると、NAS ソリューション上のすべてのデータは削除されます。

メモ: NAS ソリューションソフトウェアの再インストール後、最新サービスパックをインストールしてください。

メモ: 次の手順を実行する前に、キーボードとモニタを接続してください。

メモ: NAS クラスタソリューションソフトウェアは、サポートされていないハードウェアにインストールできません。

NAS クラスタソリューションソフトウェアを再インストールするには、次の手順を実行します。

1. システムの背面に埋め込まれた電源ボタンを使って、コントローラの電源をオフにします。
2. システムの背面に埋め込まれた電源ボタンを使って、コントローラの電源をオンにします。
3. BIOS が起動したら、<F11> を押してポップアップメニューにアクセスします。
4. **Generic Storage Device（汎用ストレージデバイス）**を選択します。
5. ポップアップメニューから、**FluidFS Reinstall（FluidFS の再インストール）**を選択します。
6. プロンプトに `resetmysystem` と入力します。
   ソフトウェアによってインストールが自動で開始されます。
7. ソフトウェアインストールが完了したら、コントローラがスタンバイモードで再起動します。

NAS クラスタの拡張

NAS クラスタ内のアプライアンスの数は増やすことができます。既存クラスタ内のアプライアンス数を増やすと、クライアント接続の追加が可能になるため NAS クラスタ全体のパフォーマンスが向上します。また、データフローはすべてのコントローラおよびバックエンドストレージに均等に分散されます。元のアプライアンスペアは、すべてのシステムリソースを NAS クラスタ操作専用に使用することはなくなりますが、他のアプライアンスペアからリソースが提供されるので、元のアプライアンスペアのシステムリソース使用率は減少します。

NAS アプライアンスは、単一のシャーシ内にある 2 台の NAS コントローラで構成されます。一度に追加できるアプライアンスは 1 つです。Dell NAS ソリューションのバージョンによっては、クラスタソリューション内の最大アプライアンス数は 4 つ（コントローラは合計 8 台）になります。

- Dell PowerVault NX3600 の場合、サポートされるアプライアンスの最大数は 1（コントローラ 2 台）です。
- Dell PowerVault NX3610 の場合、サポートされるアプライアンスの最大数は 2（コントローラ 4 台）です。
- Dell FS8600 FS8600 の場合、サポートされるアプライアンスの最大数は 4（コントローラ 8 台）です。

NAS アプライアンスの追加はシームレスな操作であり、現在の NAS クラスタ操作に割り込むことはありません。アプライアンスが正常に追加されると、新しいクライアント接続が自動的にすべてのコントローラに分散され、すべてのコントローラ間で効率的な負荷バランシングが行われます。

NAS クラスタへの NAS アプライアンスの追加

他の NAS アプライアンスを追加する前に、以下のことを確認します。

- 追加の NAS アプライアンスがラックに設置され、ケーブルが接続され、電源がオンになっている。
- アプライアンスのサービスタグが記録されている。
- 新しい IP アドレスが使用可能である（アドオンアプライアンスに追加するため）。

他のアプライアンスを追加するには、次の手順を実行します。

1. **Cluster Management → Hardware → Add NAS Appliance Wizard（クラスタの管理 > ハードウェア > NAS アプライアンス追加ウィザード）**と選択します。
   NAS アプライアンス追加ウィザードが表示されます。
2. **次へ** をクリックします。
   Add NAS Appliance Wizard (Scan Network for NAS Appliances)（NAS アプライアンス追加ウィザード（NAS アプライアンス用スキャンネットワーク））ページが表示されます。
3. **Chassis number**（シャーシ番号）リストから、NAS クラスタに追加する NAS アプライアンスを選択し、**Next**（次へ）をクリックします。
   Add NAS Appliance Wizard (Subnets)（NAS アプライアンス追加ウィザード（サブネット））ページが表示されます。

4. すべての必要なサブネットに対し、追加ペア用の推奨 IP アドレスを使用するか、新しい IP アドレスを入力し、**Next**（次へ）をクリックします。

   メモ: Next（次へ）をクリックすると次のサブネットが表示され、すべてのサブネットの IP アドレスが入力されるまで続きます。

   すべてのサブネットの IP アドレスが入力されると、システムが入力された IP アドレスの保存中であることを示すメッセージが表示されます。

5. **次へ** をクリックします。

   Add NAS Appliance Wizard (Prepare Controllers To Add Appliance)（NAS アプライアンス追加ウィザード（コントローラのアプライアンス追加準備））ページが表示されます。

6. 拡張プロセスに必要なハードウェア条件を検証するには、**Next**（次へ）をクリックします。

   Add NAS Appliance Wizard (System Validation)（NAS アプライアンス追加ウィザード（システムの検証））ページが表示されます。さまざまなコンポーネントとパラメータが確認され、各コンポーネントのステータスと新しい NAS アプライアンスのパラメータが表示されます。

7. 検証を省略するには、**Skip**（スキップ）をクリックします。

8. 検証が終了したら、**Rerun**（再実行）をクリックして検証を再開するか、**Next**（次へ）をクリックします。

   Rerun（再実行）をクリックすると、検証プロセスが再開されます。**Next**（次へ）をクリックすると、**Add NAS Appliance Wizard (Attach New Member)**（NAS アプライアンス追加ウィザード（新規メンバーの接続））ページが表示されます。

9. **次へ** をクリックします。

   Add NAS Appliance Wizard (Controller Management)（NAS アプライアンス追加ウィザード（コントローラの管理））ページが表示されます。新しく追加された NAS アプライアンス上のコントローラは NAS クラスタに接続されます。NAS アプライアンスが NAS クラスタに正しく接続されると、**Add NAS Appliance Wizard (LUNs Configuration)**（NAS アプライアンス追加ウィザード（LUN の設定））ページが表示されます。

   - PowerVault NX3500/NX3600/NX3610 ソリューションでは、新しい IQN が表示されます。**Modular Data Storage Manager**（MDSM）で、既存のホストグループに新しい仮想ホストを 2 つ作成し、新しい IQN をそれらの仮想ホストに関連付けます。詳細については、「PowerVault NX3500/NX3600/NX3610 でのホストの作成」を参照してください。

     メモ: 仮想ホストの作成および IQN の関連付けの詳細については、**dell.com/support/manuals** の『Modular Disk Storage Manager Administrator's Guide』（Modular Disk Storage Manager 管理者ガイド）を参照してください。

   - Dell Compellent FS8600 NAS ソリューションでは、**LUN configuration**（LUN の設定）のほか、**Fibre Channel WWNs Configuration**（ファイバチャネル WWN の設定）も表示できます。

10. Dell Compellent FS8600 NAS ソリューションでは、新しく追加されたコントローラの WWN 情報が FC WWN 下の上側の表にリストされます。

    メモ: さらに先に進むには、ファイバチャネルスイッチに必要な FC ゾーン状態を新しい WWN に定義します。

    メモ: アプライアンスを Dell PowerVault NX3610 NAS ソリューションに追加している場合は、次の手順を省略してください。

11. Dell Compellent FS8600 NAS ソリューションでは、**Rescan**（再スキャン）をクリックします。

    追加のコントローラが **Accessible Controllers**（アクセス可能なコントローラ）の下側のテーブルにリストされていることを確認します。すべてのコントローラがリストされていない場合は、**Enterprise Manager** で **Verify Storage Connection**（ストレージ接続を検証）ボタンをクリックしてストレージ接続を確認します。

12. **次へ** をクリックします。

    Add NAS Appliance Wizard (Add NAS Appliance)（NAS アプライアンス追加ウィザード（NAS アプライアンスの追加））ページが表示されます。

13. **次へ** をクリックします。
    システムの拡張が完了したことを示すメッセージが表示され、NAS クラスタ内のアプライアンスの数が表示されます。

PowerVault NX3500/NX3600/NX3610 でのホストの作成

PowerVault NX3500/NX3600/NX3610 NAS ソリューションでは、Modular Disk Storage Manager（MDSM）を使用してホストを手動で作成できます。

作成したホストグループ内でホストを作成するには、次の手順を実行します。

1. 作成するホストグループを右クリックします。
2. **定義 → ホスト** をクリックします。
   ホスト名の指定（ホストの定義）画面が表示されます。
3. **ホスト名** で新規ホストの名前を入力します。
4. **次へ** をクリックします。
   ホストポート識別子の指定（ホストの定義）画面が表示されます。
5. **既知の未関連なホストポート識別子を選択して追加**のリストからホストポート識別子を選択します。
6. **ユーザーラベル** にホスト名を入力し、ホスト名の末尾に IQN と加えます。
7. **追加** をクリックします。
8. **次へ** をクリックします。
   ホストタイプの指定（ホストの定義） 画面が表示されます。
9. **ホストタイプ（オペレーティングシステム）**のリストから **Linux** を選択します。
10. **次へ** をクリックします。
    プレビュー（ホストの定義） 画面が表示されます。
11. **終了** をクリックします。
    正常に作成されました（ホストの定義） 画面が表示されます。
12. **はい** をクリックして別のホストを定義します。
    手順 2 から手順 10 を繰り返して別のホストを作成します。

NAS クラスタソリューションコントローラの交換

既存のコントローラがオンラインに回復しない致命的なエラーが発生した場合、コントローラを交換する必要があります。

作業を開始する前に

コントローラを交換する前に、次のことを確認します。

- コントローラへの物理的なアクセスが可能。
- コントローラの故障が確認されている（新品と交換する場合）。

コントローラの交換手順は次のとおりです。

- コントローラの切り離し。
- コントローラの取り外しと取り付け。
- 新規コントローラの接続。

FluidFS NAS クラスタソリューションコントローラの取り外し

クラスタをジャーナリングモードにするには、ハードウェアの交換中はコントローラを取り外します。これにより、ダウンタイムなしでシステムが稼働状態に戻るようになります。

次の状況では、コントローラを切り離す必要がある場合があります。

- コントローラを新品のスタンバイコントローラと交換する必要がある。
- システム管理者が、稼働しているコントローラを別の（より重要な）クラスタに取り付けることを希望している。

NAS Manager を使用したコントローラの取り外し

1. **Cluster Management → Hardware → Controllers Management（クラスタの管理 > ハードウェア > コントローラの管理）** と選択します。

   Controllers Management（コントローラの管理）ページが表示されます。
2. 使用可能なコントローラのリストから該当するコントローラを選択し、**Detach**（取り外し）をクリックします。

   選択されたコントローラがクラスタから分離され、電源がオフになります。この動作には約 10～15 分かかります。

NAS クラスタソリューションコントローラの削除と交換

NAS クラスタソリューションコントローラを削除して交換するには、次の手順を実行します。

1. ケーブルを取り外す前に、すべてのケーブルにラベルをつけます。
2. コントローラ背面からすべてのケーブルを取り外します。
3. アプライアンスシャーシから故障したコントローラを取り外します。
4. アプライアンスシャーシにコントローラをインストールします。
5. すべてのケーブルを新規コントローラに接続します。

   メモ: コントローラを削除してインストールする方法については、**dell.com/support/manuals** で『*Dell FluidFS NAS Solution Owner's Manual*』（Dell FluidFS NAS ソリューションオーナーズマニュアル）を参照してください。
6. コントローラを再インストールする際、各ケーブルを同じポートに接続してください。
7. 電源ケーブルを差し込んで新しいシステムの電源をオンにします。

NAS cluster（NAS クラスタ）ソリューションコントローラの接続

この手順を実行する前に、接続するコントローラがスタンバイモードであり、電源が入っていることを確認します。新しいコントローラの電源 LED が 1 秒間に約 2 回緑色に点滅していれば、コントローラは電源が入ってスタンバイモードになっています。

NAS Manager を使用したコントローラの接続

1. **Cluster Management → Hardware → Controllers Management（クラスタの管理 > ハードウェア > コントローラの管理）** と選択します。

   Controllers Management（コントローラの管理）ページが表示されます。
2. 使用可能なコントローラのリストから該当するコントローラを選択し、**Attach**（接続）をクリックします。

メモ: Dell Compellent FS8600 NAS ソリューションでは、次の追加手順が必要です。

メモ: 光ファイバスイッチで、ファブリックゾーニングを手動でアップデートする必要があります。

3. 接続操作が完了すると、ファイバチャネルスイッチのゾーニングに使用する、新しく接続されたコントローラの WWN が NAS Manager に表示されます。

   メモ: CLI を使用して次のコマンドを実行すると、WWN をいつでも表示できます。

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

劣化モードでの NAS Manager の機能

NAS アプライアンスが劣化モードである場合、NAS Manager における次の機能のステータスは、**View only**（表示のみ）または **Fail**（失敗）のどちらかになります。

Tab	機能	劣化モードのステータス
Access（アクセス）	Delete NAS volume（NAS ボリュームの削除）	Fails（失敗）
	NFS exports（NFS エクスポート）	View only（表示のみ）
	CIFS shares（CIFS 共有）	View only（表示のみ）
Data Protection（データ保護）	Snapshot restore（スナップショットの復元）	Fails（失敗）
	Replication Partners（レプリケーションパートナー）	View only（表示のみ）
System Management（システム管理）	Time configuration（時刻設定）	View only（表示のみ）
	Network configuration（ネットワークの設定）	View only（表示のみ）
	Subnets（サブネット）	View only（表示のみ）
	Local hosts（ローカルホスト）	View only（表示のみ）
	Static routes（静的ルート）	View only（表示のみ）
	CIFS configuration（CIFS 設定）	View only（表示のみ）
	NIS/LDAP	View only（表示のみ）
	Local users/groups（ローカルユーザー / グループ）	View only（表示のみ）
	Mapping（マッピング）	Mapping（マッピング）
	snmp	View only（表示のみ）
	Restore Cluster Config（Cluster Config の復元）	Fails（失敗）
	Format（フォーマット）	Fails（失敗）
	Expand LUNS（LUNS の拡張）	Fails（失敗）
	Add LUNs（LUN の追加）	Fails（失敗）

Tab	機能	劣化モードのステータス
	Add nodes（ノードの追加）	Fails（失敗）

8

国際化

概要

NAS cluster（NAS クラスタ）ソリューションはユニコードを完全サポートしており、同時にさまざまな言語に対応できます。ディレクトリ名とファイル名は、ユニコードフォーマット（UTF-8）で内部的に維持および管理されます。

ファイルを作成するクライアントで使用されるエンコードタイプに関係なく、NAS cluster（NAS クラスタ）ソリューションはファイル名およびディレクトリ名をユニコードフォーマットで保存します。ユニコード非対応のクライアントが共有、マウント、またはボリューム上にファイルを作成した場合、そのファイルは NAS cluster（NAS クラスタ）ソリューションによってただちに適切なユニコード表示に変換されます。

ユニコードクライアントサポートの概要

ユニコードクライアントがユニコードディレクトリおよびファイルにネイティブにアクセスできることに対し、ユニコード以外のクライアント（Windows 98、Windows ME、Mac OS 9.x クライアント）は、ファイル名、ディレクトリ、共有および、ボリュームをクライアントが使用するコードページに応じて変換する NAS クラスタソリューションのコードページ変換提供機能によって、ファイルシステムへアクセスすることが可能になります。

ネイティブのユニコードクライアントは、次のとおりです。

- Microsoft Windows 7/Server 2008 R2
- Microsoft Windows Vista/Server 2008
- Microsoft Windows XP
- Microsoft Windows 2000/2003
- Microsoft Windows NT
- UNIX ベースのクライアント

NFS クライアント

NFS クライアントは、異なる言語を使用する非ユニコードクライアントを同時にサポートしながら、異なる共有に対して異なるコードページを設定することが可能です。

CIFS クライアント

CIFS ユーザーは、ユニコード非対応のすべての Windows および DOS クライアント用に使用するコードページを設定することができます。

メモ: ウェブインタフェースはユニコードを完全サポートします。CLI を使用してユニコードデータを表示および使用するには、UTF-8 XTERM を使用する必要があります。

ユニコード設定パラメータ

次の設定パラメータにユニコード文字を含めることができます。

パラメータ	ユニコード文字
CIFS	サーバーの説明
ホーム共有	ディレクトリ名
snmp	連絡先 場所
NFS Exports（NFS エクスポート）	ディレクトリ名
CIFS Shares（CIFS 共有）	名前 ディレクトリ 説明 ユーザーグループ

ユニコード設定の制限

ユニコード設定の制限は、次のとおりです。

- ファイルサイズとディレクトリ名
- クライアントの互換性問題
- 日本語の互換性問題

ファイルサイズとディレクトリ名

ファイルのサイズとディレクトリ名は 255 バイトに制限されており、UTF-8 文字それぞれは 1〜6 バイトを占めるため、Unicode を使用すると 255 文字未満になる場合があります。

クライアントの互換性問題

同じコードページのエントリに対し、異なるベンダーが別々の UTF-8 エンコードを使用する場合があります。その結果、それらの文字は表示されないか、形の似ている別の文字に置き換えられます。

日本語の互換性問題

KTERM 等の XTERM アプリケーションでは UTF-8 文字を使用できないため、CLI を使用しているシステム管理者は、ウェブインタフェースを経由した場合に限り、設定パラメータに日本語文字を入力することができます。
次の表に、日本語に互換性のない文字の詳細について説明します。

文字	UNIX	Windows	Macintosh
波ダッシュ（~）	U+301C（波ダッシュ）	U+FF5E （全角チルダ）	U+301C（波ダッシュ）
二重縦線（‖）	U+2016（二重縦線）	U+2225（並行）	U+2016（二重縦線）
マイナス記号（-）	U+2212 （マイナス記号）	U+FF0D（全角ハイフンマイナス記号）	U+2212 （マイナス記号）
上線（￣）	U+FFE3（全角ミクロン）	U+FFE3（全角ミクロン）	U+203E（上線）
セント記号（¢）	U+00A2（セント記号）	U+FFE0（全角セント記号）	U+00A2（セント記号）

文字	UNIX	Windows	Macintosh
ポンド記号（#）	U+00A3（ポンド記号）	U+FFE1（全角ポンド記号）	U+00A3（ポンド記号）
否定記号（¬）	U+00AC（否定記号）	U+FFE2（全角否定記号）	U+00AC（否定記号）

NAS クラスタソリューションは CIFS サービスに特別コードページを提供して、プロトコル間のポータブル性をサポートします。 複数プロトコル環境で作業していて、プロトコル間でファイルとディレクトリを共有したい場合、このオプションが推奨されます。

CIFS サービスが内部エンコーディング（UNIX コードページ）に UTF-8-JP を使用するよう設定されている場合、NAS クラスタソリューションでは Windows と互換性のないエンコーディングが適切な UNIX/ Mac O/S エンコーディングにマッピングされます。 これにより、正しくない文字でも正しくマッピングされます。

9

よくあるお問い合わせ

NDMP

1. NDMP は高可用性（HA）プロトコルですか? 接続が切れたためにバックアップセッションが中断された場合は、どうなりますか?

   NDMP は HA ではありません。中断されたセッションは終了します。

2. NDMP はどのように動作しますか?

   NDMP セッションの最初に、Fluid File System（FluidFS）のスナップショットが、ターゲットの NAS ファイルシステムで取得されます。このスナップショットは、データ管理アプリケーション（DMA）に転送されます。セッションの最後に、スナップショットは削除されます。

3. NDMP スナップショットは特別なものですか?

   いいえ。通常のワンタイム FluidFS スナップショットです。

4. 負荷バランシングは提供されていますか?

   NDMP にはビルトインの負荷バランシングはありません。単一クライアント VIP からの単一 DMA による 10 ボリュームのバックアップは、同じノードで 10 セッションすべてを強制します。負荷バランシングを提供するには、DMA 内で NAS アプライアンスの DNS 名を指定することによって、DNS ラウンドロビンを使用します。

5. 使用中のボリュームに **ndmp_backup_xxxx_nodeX** というスナップショットがあるのはなぜですか?

   これは NDMP によって取得されたスナップショットです。バックアップセッションが正常に終了すると、このスナップショットは削除されます。バックアップセッションがエラー状態で終了すると、スナップショットはそのまま残る場合がありますが、手動で安全に削除することができます。

6. 1 度にバックアップを実行できる DMA の数はいくつですか?

   最大 16 まで DMA を NAS cluster（NAS クラスタ）ソリューションでセットアップできます。ある時点でバックアップを取得する DMA の数に制限はありません。

7. 単一ファイルを復元できますか?

   はい。

8. 古いバックアップを別の NAS アプライアンスに復元できますか?

   はい。

9. バックアップを別の NDMP アプライアンスに復元できますか?

   はい。NDMP からのデータは RAW 形式で送信されるため、対象のアプライアンスはこの形式をサポートしています。

10. 現在進行中のアクティブなバックアップを確認することはできますか?

    はい。NAS CLI を使用すると、現在進行中のアクティブなバックアップを確認することができます。現在進行中のアクティブなバックアップを確認するには、`data-protection ndmp active-jobs` リストを実行します。

11. すでにクライアントにマップ済みのネットワークドライブをバックアップするために NDMP を使用できますか?

    いいえ。ネットワークドライブをバックアップするために NDMP を使用することはできません。

レプリケーション

1. レプリケーションはどのように動作しますか?

   レプリケーションは FluidFS スナップショットテクノロジおよびその他の計算方法を使用して、レプリケーションされた仮想ボリュームのデータが、レプリケーションタスクが開始された日時における、ソース仮想ボリュームのデータと一致することを確実にします。 最後のレプリケーションタスク後に変更されたブロックのみが、クライアントネットワークに転送されます。

2. レプリケーションの所要時間はどれくらいですか?

   仮想ボリューム上のデータの量と、最後のレプリケーションサイクル以降に変更されたデータの量によります。ただし、レプリケーションはレベルの低いタスクですがデータの提供よりも優先されます。管理者は **Refresh**（更新）をクリックして、レプリケーションの進行状況を監視できます。画面には大体の完了率が表示されます。

3. 1 つの仮想ボリュームを複数のターゲット仮想ボリュームにレプリケーションできますか?

   いいえ。ソースボリュームにターゲット仮想ボリュームとのレプリケーションポリシーが作成されると、どちらの仮想ボリュームもレプリケーション（複製元または複製先）に使用できなくなります。

4. NFS または CIFS でターゲット仮想ボリュームに書き込みできないのはなぜですか?

   レプリケーションポリシーが設定されると、ターゲット仮想ボリュームは読み取り専用となります。レプリケーションポリシーが切り離されると、ターゲット仮想ボリュームは読み取り専用ではなくなります。

5. ターゲットシステム上で、複製先仮想ボリュームに対するレプリケーションを開始できません。

   レプリケーション動作はソース仮想ボリューム上で実行される必要があります。

6. 同一のシステムに対してレプリケーションを実行できますか?

   はい。 1 つのソース仮想ボリュームから同一のシステム上の複製先仮想ボリュームにレプリケーションを行うことができます。

7. 2 つのシステム間で双方向レプリケーションはサポートされていますか?

   はい。レプリケーションパートナー上にターゲットボリュームとソースボリュームを混在させることが可能です。

8. 複数のレプリケーションパートナーシステムを使用できますか?

   はい。複数のレプリケーションパートナーが使用できます。ただし、1 つの仮想ソースボリュームから複数のターゲットボリュームにレプリケーションを行うことはできません。

9. レプリケーションポリシーを削除しようとすると、ソースボリューム設定をターゲットボリューム設定に適用するかどうか尋ねられます。どういうことですか？

   これは、すべての仮想ボリュームレベルのプロパティ（セキュリティスタイル、クォータ、NFS エクスポート、CIFS 共有、およびその他）をターゲットボリュームに転送するオプションがあるということです。仮想ボリュームがソース仮想ボリュームの代わりとなる場合およびその他の IT のシナリオ用にこれを行うようにします。

10. レプリケーション中、クライアントネットワークが遅くなります。クライアント供給に対してレプリケーションの優先度を変更できますか？

    これは設計によるものです。レプリケーションは低レベルの処理ですが、クライアントへの対応よりも優先されます。管理者は **Refresh**（更新）をクリックして、レプリケーションの進行状況を監視できます。画面には大体の完了率が表示されます。

11. ターゲット仮想ボリュームからレプリケーションポリシーを削除できないのはなぜですか?

    これは設計によるものです。すべての設定の変更はソース仮想ボリューム上で行われる必要があります。ソースボリュームが存在するシステムと通信ができない場合（ダウン、欠落、その他）は、レプリケーションポリシーをターゲットから削除できます。

10

セキュアな管理

セキュアな管理が有効の場合、すべての管理トラフィックが 1 つのサブセットに移され、その他すべてのサブネットはクライアントアクセス（CIFS/NFS）、レプリケーション、および NDMP トラフィック用に使用されます。 これにより、クライアント（データ）アクセスサブネット上のユーザーが管理機能にアクセスすることを防ぎます。FluidFS では、以下にあるポートが NFS/CIFS の通信に参加することはありませんが、クライアントネットワークには表示されます。デフォルトで、すべてのサブネット上のすべての管理ポートが、クライアントアクセス、レプリケーション、および NDMP 用に必要なその他のポートと共にオープンとなります。

ユーザーによっては、管理トラフィックが特権として処理される必要があり、1 つのサブネットのみに表示される必要があります。セキュアな管理が有効となっているサブネットでも、クライアントアクセス（CIFS/NFS）、レプリケーション、および NDMP トラフィック用に必要なポートはオープンとなります。

サービス	ポート
ウェブサービス	80
ウェブサービス	443
FTP	44421
FTP	44422
SSH	22
SOAP	35451

セキュアな管理機能は、1 つの特定サブネット上で **セキュアな管理** を有効にします。そうすることで、すべての管理トラフィックがその特定のサブネットのみに限定されます。その他のサブネットでは、それらのグループのポートが管理トラフィックをリッスンすることはありません。セキュアな管理が有効の場合、FluidFS NAS Manager（Web GUI）には単なる **http** ではなく、セキュア HTTP **https://<managementVIP>/** を使用してアクセスする必要があります。セキュアな管理が有効の場合、すべてのサブネットでポート 80 が無効となります。セキュアな管理は、システムが完全に展開された後でのみ有効にすることができます。

- **セキュアな管理** 機能は、FluidFS コマンドラインインタフェースによって管理されます。
- サブネットをセキュアにするには：
  - セキュア操作の前にサブネットが存在する必要があります。
  - サブネットがクライアントの物理ネットワーク上に存在する必要があります。
  - このサブネットから CLI にログインする必要があります。

セキュアな管理用 CLI コマンドの詳細は、**dell.com/support/manuals** で『*Dell FluidFS NAS Solutions CLI Reference Guide*』（Dell FluidFS NAS Solutions CLI レファレンスガイド）を参照してください。

メモ: サブネット上でセキュアな管理を有効にしても、その他のネットワーク上にある既存の管理セッションは切り離されません。そのようなセッションがある場合は警告が発せられます。既存のセッションがないようにするには、報告されたセッションを切り離し、セキュアな管理を無効にしてからセキュアな管理を再度有効にします。その他の管理セッションが報告されていないことを検証してください。

使用される FluidFS NAS ポート

表 2. 必要なポート

FluidFS ポート番号	プロトコル	サービス名
445	TCP および UDP	CIFS/SMB
427	TCP および UDP	SLP
2049 - 2049+（ドメイン番号 - 1）	TCP および UDP	NFS
5001 - 5001+（ドメイン番号 - 1）	TCP および UDP	mount
5051 - 5051+（ドメイン番号 - 1）	TCP および UDP	Quota
4050 - 4050+（ドメイン番号 - 1）	TCP および UDP	nlm（Lock Manager）
4000 - 4000+（ドメイン番号 - 1）	TCP および UDP	Statd
111	TCP および UDP	portmap
44421	TCP	FTP
22	TCP	SSH
80	TCP	HTTP
443	TCP	ウェブ管理 HTTPS
53	UDP	DNS

表 3. 要件に基づく使用ポート

FluidFS ポート番号	プロトコル	サービス名
138	UDP	NetBIOS
139	TCP	NetBIOS
88	TCP および UDP	Kerberos
464	TCP および UDP	Kerberos v5
543	TCP	Kerberos ログイン
544	TCP	Kerberos リモートシェル
749	TCP および UDP	Kerberos 管理
135	TCP	AD - RPC
711	UDP	NIS
714	TCP	NIS
389	TCP および UDP	LDAP
3268	TCP	LDAP グローバルカタログ
3269	TCP	TLS/SSL 上 LDAP グローバルカタログ

FluidFS ポート番号	プロトコル	サービス名
636	TCP	TLS/SSL 上 LDAP
123	UDP	NTP
161	UDP	SNMP エージェント
162	TCP	SNMP トラップ
10000	TCP	NDMP
10560-10568	TCP	レプリケーション
1344	TCP	アンチウィルス - ICAP
8004	TCP	ScanEngine サーバー WebUI（AV ホスト）

11

困ったときは

デルへのお問い合わせ

メモ: デルでは、オンラインおよび電話ベースのサポートとサービスオプションをいくつかご用意しています。アクティブなインターネット接続がない場合は、ご購入時の納品書、出荷伝票、請求書、またはデル製品カタログで連絡先をご確認いただけます。これらのサービスは国および製品によって異なり、お住まいの地域では一部のサービスがご利用いただけない場合があります。

デルのセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

1. dell.com/contactdell にアクセスします。
2. インタラクティブな世界地図からお住まいの国または地域を選択します。
   地域を選択すると、選択した地域内の国が表示されます。
3. 選択した国の下にある適切な言語を選択します。
4. 管轄の営業セグメントを選択します。
   選択したセグメントのメインサポートページが表示されます。
5. 必要に応じて、適切なオプションを選択します。

システムサービスタグの位置

お使いのシステムは、一意のエクスプレスサービスコードおよびサービスタグ番号で識別されます。エクスプレスサービスコードおよびサービスタグは、システムの前面から情報タグを引き出して見ることができます。この情報は、デルがサポートへのお電話を適切な担当者に転送するために使用します。

マニュアルのフィードバック

本マニュアルに対するフィードバックは、documentation_feedback@dell.com まで E-メールを送信してください。または、デルマニュアルページにある **Feedback**（フィードバック）リンクをクリックしてフォームに入力し、**Submit**（送信）をクリックしてフィードバックを送信していただくこともできます。