



Hewlett Packard
Enterprise

HPE ストレージファイルコントローラー管理 者ガイド

摘要

本書は、HPE ストレージファイルコントローラーを対象に、設置、構成、および維持を行う方法について、システム管理者向けに書かれています。本ガイドの最新バージョンは、<http://www.hpe.com/info/FileController-manuals> から入手できます。

部品番号: P08157-191
発行: 2018 年 9 月
版数: 1

ご注意

本書の内容は、将来予告なしに変更されることがあります。Hewlett Packard Enterprise 製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、脱落に対して、責任を負いかねますのでご了承ください。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、その保有、使用、または複製には、Hewlett Packard Enterprise から使用許諾を得る必要があります。FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェアドキュメンテーション、および商業用製品の技術データ（Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items）は、ベンダー標準の商業用使用許諾のもとで、米国政府に使用許諾が付与されます。

他社の Web サイトへのリンクは、Hewlett Packard Enterprise の Web サイトの外に移動します。Hewlett Packard Enterprise は、Hewlett Packard Enterprise の Web サイト以外の情報を管理する権限を持たず、また責任を負いません。

商標

Intel[®]、Xeon[®] Itanium[®]、Pentium[®]、Intel Inside[®] および Intel Inside ロゴは、インテルコーポレーションまたはその子会社のアメリカ合衆国およびその他の国における商標および登録商標です。

Microsoft[®] および Windows[®] は、米国および/またはその他の国における Microsoft Corporation の登録商標または商標です。

Chrome[®] および Google[®] は、Google LLC の登録商標です。

目次

HPE ストレージファイルコントローラー.....	6
機能.....	6
HPE ストレージファイルコントローラーのハードウェアコンポーネント.....	6
フロントパネルのコンポーネント.....	6
フロントパネルの LED とボタン.....	6
リアパネルのコンポーネント.....	8
リアパネルの LED.....	8
システムボードのコンポーネント.....	9
ホットプラグ対応ドライブ LED の定義.....	12
ファン.....	14
HPE ストレージファイルコントローラーのソフトウェアコンポーネント.....	15
Active Health System.....	15
HPE iLO 5.....	15
HPE ストレージファイルコントローラーの設置.....	15
HPE アレイへの HPE ストレージファイルコントローラーの接続.....	16
HPE 3PAR StoreServ ストレージアレイへの接続.....	16
HPE MSA ストレージアレイへの接続.....	18
HPE Nimble ストレージアレイの接続.....	18
 HPE ストレージファイルコントローラーシステムの構成.....	19
初回のセットアップ.....	19
単一ノードシステムの構成.....	20
クラスターノードの構成.....	51
マルチサイト環境用のフェイルオーバープロパティの構成.....	84
その他のアクセス方式.....	84
リモートデスクトップの使用.....	84
CLI を使用.....	84
 HPE ストレージファイルコントローラーの管理.....	85
ネットワーク構成ツールの使用方法.....	85
通知システム.....	87
 管理ツール.....	89
リモート管理.....	89
ファイルサービスおよび記憶域サービス.....	89
データの重複排除.....	89
 ストレージ管理の概要.....	91
論理コンポーネント.....	91
ストレージ要素の使用.....	92
 ファイルサーバーの管理.....	93
ファイルサービス管理.....	93
アレイ管理ユーティリティ.....	93

ディスクの管理ユーティリティ.....	93
ディスクとボリュームの管理のガイドライン.....	93
最適化のスケジュール.....	94
ストレージの追加.....	94
ボリュームシャドウコピー.....	94
シャドウコピーの計画.....	95
シャドウコピーとドライブの最適化.....	97
マウントされたドライブ.....	97
シャドウコピーの管理.....	98
HPE Nimble アレイからのシャドウコピーの管理.....	101
HPE MSA アレイからのシャドウコピーの管理.....	101
共有フォルダーのシャドウコピー.....	102
Shadow Copy Transport.....	106
フォルダーと共有の管理.....	106
フォルダーの管理.....	107
大規模なネームスペースの管理.....	113
共有の管理.....	114
ファイルサーバーリソースマネージャー.....	115
クォータ管理.....	116
ファイル選別管理.....	116
ストレージレポート.....	116

管理ツール..... 117

クラスター管理..... 118

クラスターの概要.....	118
クラスターの用語とコンポーネント.....	118
ノード.....	118
リソース.....	118
クラスターグループ.....	119
仮想サーバー.....	119
フェイルオーバーとフェイルバック.....	119
クォーラムディスク.....	119
クラスターの概念.....	120
クラスターの計画.....	120
ストレージの計画.....	120
ネットワークの計画.....	120
プロトコルの計画.....	121
クラスターをインストールするための準備.....	122
インストールの開始前.....	122
高可用性を実現するためのマルチパスによるデータパスの使用.....	122
クラスターサーバーのインストール用のチェックリスト.....	122
クラスターのインストール.....	123
ネットワークのセットアップ.....	124
クラスターサービスソフトウェアの構成.....	125
フェールオーバー クラスター管理の使用.....	125
クラスターの作成.....	126
クラスターへのノードの追加.....	126
地理的分散クラスター.....	126
ファイル共有を含むクラスターグループとクラスターリソース.....	126
クラスターグループの概要.....	127
ファイル共有リソースの計画に関する注意事項.....	127
クラスター非対応のファイル共有プロトコル.....	129
クラスターへの新しいストレージの追加.....	130

クラスター環境でのシャドウコピー.....	130
クラスターでの LUN の拡大.....	131
サーバークラスターでの MSNFS 管理.....	131
高度なクラスター管理手順.....	132
フェイルオーバーとフェイルバック.....	132
1 つのクラスターノードの再起動.....	132
1 つのクラスターノードのシャットダウン.....	132
クラスターの電源を切る.....	133
クラスターの電源投入.....	133
トラブルシューティング、サービス、およびメンテナンス.....	134
Hewlett Packard Enterprise のサポートの Web サイト.....	135
Microsoft Systems Center Operations Manager.....	135
ハードウェアコンポーネントの取り外しと交換.....	136
表面スキャン分析.....	136
クラスター固有の注意事項	136
HPE ストレージファイルコントローラーの復旧.....	143
System Recovery DVD.....	143
System Recovery DVD によるシステムデータの保存.....	143
System Recovery DVD によるシステム復旧用 USB フラッシュドライブの作成.....	144
HPE サポートセンターのイメージファイルによる USB フラッシュドライブの作成.....	145
HPE サポートセンターのイメージファイルによる DVD の作成.....	146
DVD または USB フラッシュデバイスによる出荷時イメージの復元.....	146
両方のノードの復旧.....	147
1 台のノードの復旧.....	147
Iternity iCAS.....	150
製品に関するフィードバック.....	151
Web サイト.....	152
サポートと他のリソース.....	153
Hewlett Packard Enterprise サポートへのアクセス.....	153
アップデートへのアクセス.....	153
オープンソースコンポーネントに関する情報	154
カスタマーセルフリペア (CSR)	154
リモートサポート (HPE 通報サービス)	154
保証情報.....	154
規定に関する情報.....	155
Hewlett Packard Enterprise プライバシープラクティス.....	155
ドキュメントに関するご意見、ご指摘.....	155

HPE ストレージファイルコントローラー

HPE ストレージファイルコントローラーを使用すると、ファイルおよびアプリケーションのストレージを簡素化することができます。これにより管理の簡素化、リソース利用の増加、増加の集中管理、データ保護により、所有コストを削減することができます。

機能

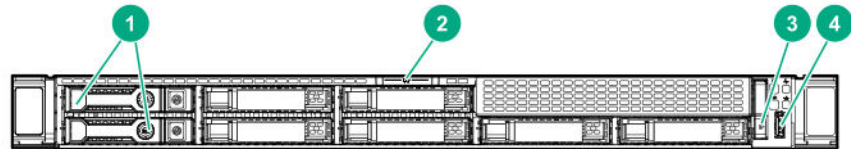
HPE ストレージファイルコントローラーには、以下の利点があります。

- ・ ファイルおよびデータ管理でコストを増やすことなく、リソース使用を効果的に最大化します。
- ・ Microsoft サーバーマネージャーと System Center および HPE Systems Insight Manager と iLO (Integrated Lights Out) を含む、Hewlett Packard Enterprise と Microsoft の管理ソフトを統合します。
- ・ 各システムは、工場で統合されたハードウェアにソフトウェアをプリロードして出荷されるので、導入時間と手順の複雑さが大いに軽減されます。

HPE ストレージファイルコントローラーのハードウェアコンポーネント

フロントパネルのコンポーネント

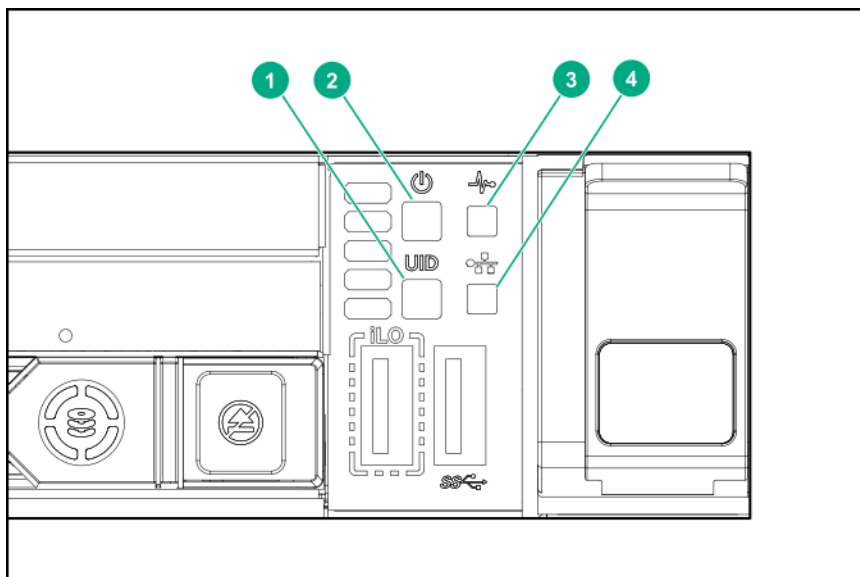
HPE ストレージファイルコントローラーでは、オペレーティングシステムのドライブがベイ 1 と 2 にあることができます。これらのドライブはソリッドステートドライブ (SSD) であり、RAID 1 構成です。



項目	説明
1	SAS/SATA ドライブベイ
2	シリアルラベルプルタブ
3	iLO サービスポート オペレーティングシステムは、このポートを USB ポートとして認識しません。
4	USB 3.0 ポート

フロントパネルの LED とボタン

HPE ストレージファイルコントローラーのフロントパネル LED は、ハードウェアの全体的な状態を示します。さまざまな LED の色と LED の状況 (点滅、点灯、オフ) により、システムが通常の正常な状態であるかどうかわかります。



項目	説明	ステータス
1	UID ボタン/LED*	青色で点灯 = 動作しています。 青色で点滅： ・ 1 Hz = リモート管理またはファームウェアアップグレードが進行中 ・ 4 Hz = iLO の手動再起動シーケンス開始 ・ 8 Hz = iLO の手動再起動シーケンス実行中 消灯 = 動作していません。
2	電源ボタンとシステム電源 LED*	緑色で点灯 = システムに電源が入っています。 緑色で点滅 = 電源投入シーケンスを実行中です。 オレンジ色で点灯 = システムはスタンバイ状態です。 消灯 = 電源が供給されていません。 **
3	ヘルス LED*	緑色で点灯 = 正常 緑色で点滅 = iLO が再起動しています。 オレンジ色で点滅 = システムの性能が劣化しています。 赤色で点滅 = システムに重大な障害が発生しています。 †
4	NIC ステータス LED*	緑色で点灯 = ネットワークにリンクされています。 緑色で点滅 = ネットワークが動作しています。 消灯 = ネットワークが動作していません。

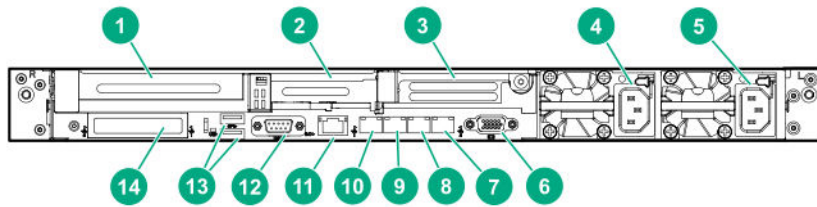
* この表で説明されている 4 つすべての LED が同時に点滅する場合は、電源障害が発生しています。

**電源が供給されていない、電源コードが接続されていない、電源装置が搭載されていない、電源装置が故障している、または電源ボタンケーブルが外れています。

†ヘルス LED が劣化状態またはクリティカル状態を示している場合は、システム IML を確認するか、または iLO を使用してシステムヘルスステータスを確認してください。

リアパネルのコンポーネント

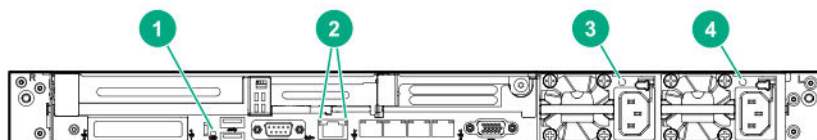
リアパネルのコンポーネントを表に示します。



項目	説明
1	スロット 1 PCIe3
2	スロット 2 PCIe3
3	スロット 3 PCIe3 (オプション - 2 つ目のプロセッサが必要)
4	電源装置 2 (PS2)
5	電源装置 1 (PS1)
6	ビデオポート
7	NIC ポート 4
8	NIC ポート 3
9	NIC ポート 2
10	NIC ポート 1
11	iLO マネジメントポート
12	シリアルポート (オプション)
13	USB 3.0 ポート
14	FlexibleLOM (オプション)

リアパネルの LED

リアパネルの LED は、電源装置、iLO、および NIC ポートのヘルスステータスを示します。

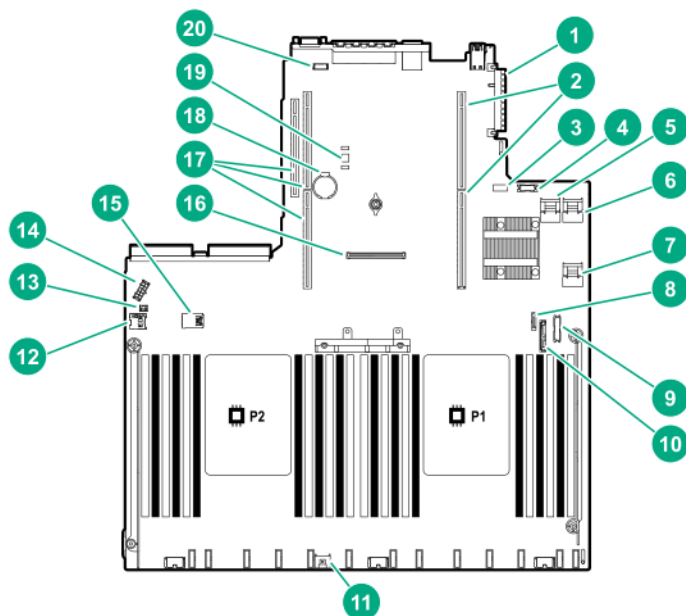


項目	説明	ステータス
1	UID LED	青色で点灯 = 確認機能が使用されています。 青色で点滅 = システムはリモートで管理されています。 消灯 = 確認機能が使用されていません。
2R	iLO 5/Standard NIC 動作 LED	緑色で点灯 = 動作しています。 緑色で点滅 = 動作しています。 消灯 = 動作していません。
2L	iLO 5/Standard NIC リンク LED	緑色で点灯 = 接続されています。 消灯 = リンクされていません。
3	電源装置 2 LED	緑色で点灯 = 正常 消灯 = 以下に示す 1 つまたは複数の状態が発生している可能性があります。 ・ AC 電源が供給されていない ・ 電源装置に障害が発生している ・ 電源装置がスタンバイモードに入っている ・ 電源装置が電流制限を超えた。
4	電源装置 1 LED	緑色で点灯 = 正常 消灯 = 以下に示す 1 つまたは複数の状態が発生している可能性があります。 ・ AC 電源が供給されていない ・ 電源装置に障害が発生している ・ 電源装置がスタンバイモードに入っている ・ 電源装置が電流制限を超えた。

システムボードのコンポーネント

主要なシステムボードコンポーネントを図で示します。

注記: システムボードの交換は HPE 認定技術者が行うようにしてください。



項目	説明
1	FlexibleLOM コネクタ
2	プライマリ（プロセッサ 1）PCIe ライザーコネクタ
3	システムメンテナンススイッチ
4	前面ディスプレイポート/USB 2.0 コネクタ
5	x4 SATA ポート 1
6	x4 SATA ポート 2
7	x2 SATA ポート 3
8	x1 SATA ポート 4
9	フロント電源/USB 3.0 コネクタ
10	オプティカル/SATA ポート 5
11	Smart ストレージバッテリーコネクタ
12	Micro SD カードスロット
13	シャーシ侵入検知コネクタ
14	ドライブバックプレーン電源コネクタ
15	デュアル内部 USB 3.0 コネクタ
16	タイプ a SmartArray コネクタ
17	セカンダリ（プロセッサ 2）PCIe ライザーコネクタ
18	システムバッテリー
19	TPM コネクタ（オプション）
20	シリアルポートコネクタ（オプション）

システムメンテナンススイッチの説明

システムメンテナンススイッチは、システムボード上にあります。変更するのは、HPE テクニカルサポート担当者から指示があった場合だけにしてください。

位置	デフォルト	機能
S1	オフ	オフ = iLO セキュリティを有効にします。 オン = iLO セキュリティを無効にします。
S2	オフ	予約済み
S3	オフ	予約済み
S4	オフ	予約済み
S5	オフ	オフ = 電源投入時パスワードは有効です。 オン = 電源投入時パスワードは無効です。
S6 ¹	オフ	オフ = 動作していません。 オン = 製造時のデフォルト設定を復元します。
S7	オフ	予約済み
S8	—	予約済み
S9	—	予約済み
S10	—	予約済み
S11	—	予約済み
S12	—	予約済み

¹ システムメンテナンススイッチの S6 をオンの位置に設定すると、すべての構成設定を製造時のデフォルト設定に復元できるようになります。

メモリ DIMM

DIMM スロットには、各プロセッサ用に 1 ~ 12 の番号が順に付けられています。HPE ストレージファイルコントローラーはスロット 1 だけを使用します。サポートされる AMP モードは、取り付けのガイドライン用の文字割り当てを使用します。

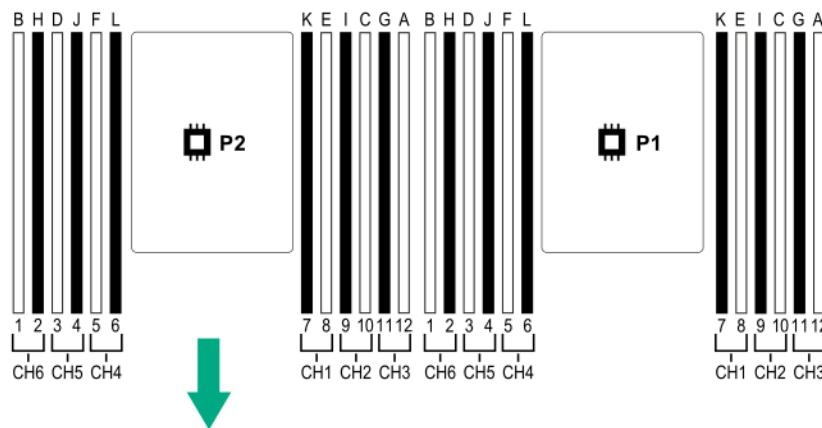
メモリ DIMM は特定の順序で取り付けますが、この順序はシステムのタイプによって異なります。HPE ストレージファイルコントローラーのベースシステムに付属している 1 つの DIMM は、各プロセッサのスロット 8 に取り付けます。DIMM が複数ある場合は、追加のメモリをチャートに従って取り付ける必要があります。

DIMM 数	HPE ストレージファイルコントローラーの DIMM 取り付け順序 スロット 1~12 (プロセッサあたり)			
DIMM 1 基	8			
DIMM 2 基	8	10		
DIMM 3 基	8	10	12	

表は続く

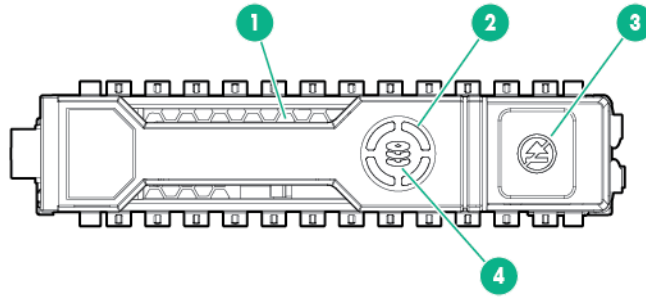
DIMM 数	HPE ストレージファイルコントローラーの DIMM 取り付け順序 スロット 1~12 (プロセッサあたり)											
DIMM 4 基			3		5			8		10		
DIMM 5 基			3		5			8		10		12
DIMM 6 基	1		3		5			8		10		12
DIMM 7 基	1		3		5		7	8		10		12
DIMM 8 基			3	4	5	6	7	8	9	10		
DIMM 9 基	1		3		5		7	8	9	10	11	12
DIMM 10 基	1		3	4	5	6	7	8	9	10		12
DIMM 11 基	1		3	4	5	6	7	8	9	10	11	12
DIMM 12 基	1	2	3	4	5	6	7	8	9	10	11	12

以下に DIMM スロットの位置を示します。緑色の矢印は、システムの正面側を示しています。



ホットプラグ対応ドライブ LED の定義

HPE ストレージファイルコントローラーに含まれているドライブはホットプラグ接続されており、システムの電源を入れたままドライブを取り外して交換できます。表の LED インジケータは、ドライブのヘルスステータスを示します。



項目	LED	ステータス	定義
1	位置確認	青色で点灯	ドライブは、ホストアプリケーションによって識別されています。
		青色の点滅	ドライブキャリアのファームウェアが更新中かまたは更新を必要としています。
2	アクティビティリ ング	緑色で回転	ドライブ動作中。
		オフ	ドライブ動作なし。
3	取り外し禁止	白色で点灯	ドライブを取り外さないでください。ドライブを取り外すと、1つ以上の論理ドライブで障害が発生します。
		オフ	ドライブを取り外しても、論理ドライブで障害は発生しません。
4	ドライブステータ ス	緑色で点灯	ドライブは、1つまたは複数の論理ドライブのメンバーです。
		緑色で点滅	ドライブの動作として以下のいずれかを示します。 ・ 再構築 ・ RAID の移行の実行 ・ ストリップサイズの移行の実行 ・ 容量拡張の実行 ・ 論理ドライブの拡張の実行 ・ 消去 ・ スペア部品のアクティブ化操作
		オレンジ色/緑色で点滅	ドライブは1つまたは複数の論理ドライブのメンバーで、ドライブの障害が予測されています。
		オレンジ色で点滅	ドライブが構成されておらず、ドライブの障害が予測されています。
		オレンジ色で点灯	ドライブに障害が発生しました。
		オフ	ドライブでは、RAID コントローラーまたはスペアドライブによる構成は行われていません。

ファン

HPE ストレージファイルコントローラーには、最低 5 つの標準ファンが付属しています。システムを 2 プロセッサにアップグレードする場合は、ファン数を 7 に増やす必要があります。このファンはホットプラグ対応でないため、システムのパワーダウンが必要になります。

△ 注意: サーバーコンポーネントの損傷を防止するために、シングルプロセッサ構成では、必ずファンベイ 1 と 2 にファンブランクを取り付けてください。

△ 注意: 装置の損傷を防止するために、システムに最適な数のファンが取り付けられていない場合は、システムを長時間動作させないでください。システムが起動することもあります、必要な数のファンが取り付けられて動作していない場合、システムの実行はお勧めできません。

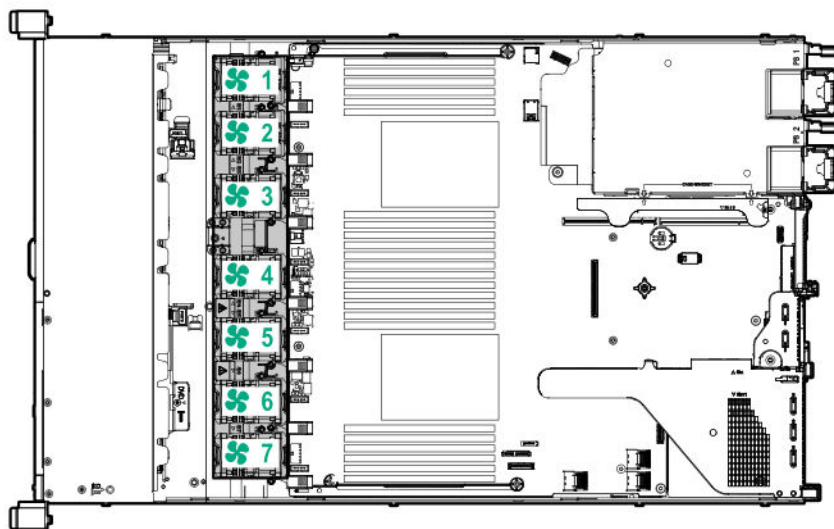
以下の表に、有効なファン構成を示します。

1 プロセッサ構成

ファンベイ 1	ファンベイ 2	ファンベイ 3	ファンベイ 4	ファンベイ 5	ファンベイ 6	ファンベイ 7
ファン	ファン	ファン	ファン	ファン	ブランク	ブランク

2 プロセッサ構成

ファンベイ 1	ファンベイ 2	ファンベイ 3	ファンベイ 4	ファンベイ 5	ファンベイ 6	ファンベイ 7
ファン	ファン	ファン	ファン	ファン	ファン	ファン



1 つのファンローター（1 つの標準的なファン）が失われると、冗長性が損なわれます。2 つのファンローター（2 つの標準的なファン）が失われると、システムでシャットダウンが開始されます。

システムはファンの回転速度の変更をサポートしています。温度が上昇し、ファンの回転速度を上げてシステムを冷却する必要があるまでは、ファンは最小限の速度で回転します。システムは、温度に関連した以下の場合にシャットダウンします。

- ・ 注意レベルの温度が検出された場合、システムは、POST 実行時および OS で、通常の方法のシャットダウンを実行します。通常のシャットダウンが行われる前にシステムハードウェアが重大レベルの温度を検出した場合、システムは即時シャットダウンを実行します。
- ・ 高温シャットダウン機能が BIOS/プラットフォーム構成 (RBSU) で無効に設定されている場合、注意レベルの温度が検出されても、iLO は通常の方法のシャットダウンを実行しません。この機能が無効に

設定されている場合でも、重大な温度レベルが検出されると、システムハードウェアは即時シャットダウンを実行します。

△ 注意: BIOS/プラットフォーム構成 (RBSU) で高温シャットダウン機能が無効に設定されている場合、高温イベントによりサーバーコンポーネントが損傷する場合があります。

HPE ストレージファイルコントローラーのソフトウェアコンポーネント

Windows Storage Server 2016 Standard Edition は、HPE ストレージファイルコントローラー上にプリインストールされ、動作可能な状態で出荷されます。システム構成には、HPE ストレージファイルコントローラーのセットアップおよび管理に使用できる、**初期構成タスクウィンドウ**、**ネットワーク構成タスクウィンドウ**、**サーバーマネージャー**も含まれています。

サーバーマネージャー > ツール > ストレージコントローラーメニューには、HPE ストレージファイルコントローラーの管理に役立つ一連の HPE および Microsoft のユーティリティがあります。**初期構成タスクウィンドウ**では、システム設定、ネットワーク IP の設定、および HPE ストレージファイルコントローラーのドメインなどの項目の構成、電子メールアラートの構成、製品の登録、ストレージのプロビジョニング、サーバーの保護を行うことができるため、初期のアウトオブボックスセットアップを簡単に実行することができます。**サーバーマネージャー > ファイルサービスと記憶域サービス**を使用すると、仮想ディスクを作成し、仮想ディスク上にボリュームを配置することもできます。

Active Health System

Active Health System は、システムハードウェアとシステム構成の変化を監視し、記録します。

Active Health System は、以下の機能を提供します。

- ・ 1,600 を超えるシステムパラメーターの継続的なヘルス監視。
- ・ すべての構成変更のログの取得
- ・ ヘルスおよびサービス通知の統合（正確なタイムスタンプ付き）
- ・ アプリケーションのパフォーマンスに影響を与えないエージェントレスの監視

Active Health System について詳しくは、Hewlett Packard Enterprise の Web サイトにある iLO ユーザーガイドを参照してください。

HPE iLO 5

iLO 5 が、HPE ストレージファイルコントローラーのシステムボードに組み込まれているリモートシステム管理プロセッサです。iLO により、システムを離れた場所から監視および制御できます。iLO 管理は、システムをリモートで構成、更新、監視、および修復するための複数の方法を提供する強力なツールです。iLO は、iLO Advanced Premium Security Edition ライセンスを使用してシステムに事前構成されています。

iLO について詳しくは、Hewlett Packard Enterprise の Web サイトにある iLO ユーザーガイドを参照してください。

HPE ストレージファイルコントローラーの設置

レールキットを取り付けてシステムをラック内にマウントした後で、すべての電源コードを設備の電源に接続してください。

HPE ストレージファイルコントローラーシステムをネットワークに、iLO ネットワークポートを使用してケーブル接続します。iLO ネットワークポートは、HPE ストレージファイルコントローラーハードウェアをリモートで管理するために使用します。管理者はこのポートでシステムに対してリモートコンソール

セッションを起動できます。HPE では、iLO ポートをネットワークに接続することをお勧めします。iLO ポートは、DHCP を介して IP アドレスを取得するように事前構成されています。ご使用の環境が DHCP をサポートしていない場合は、KVM を使用して静的 IP アドレスを使用するように iLO を構成します。詳しくは、[リアパネルのコンポーネント](#)を参照してください。

4 つの 1GbE ネットワークポートは、ストレージネットワーク用、および Active Directory、DNS、NTP などのインフラストラクチャサービスにシステムを接続するために使用します。これらのポートは、分離されたネットワークポートまたはネットワークチームとして構成することができます。スイッチがいずれかの構成用に準備されていることを確認します。

HPE アレイへの HPE ストレージファイルコントローラーの接続

以下に接続できます。

- ・ [HPE 3PAR StoreServ Storage アレイ](#)
- ・ [HPE Nimble アレイ](#)
- ・ [HPE MSA ストレージアレイ](#)

HPE 3PAR StoreServ ストレージアレイへの接続

- ・ [ネットワーク情報の指定](#)
- ・ [HPE ストレージファイルコントローラーシステムへのアクセス](#)
- ・ [クラスターハートビート接続用のケーブル接続](#)

ネットワーク情報の指定

システムのインストールと構成を進める前に、正しいネットワーク情報を得ることが不可欠です。DNS 情報をあらかじめ設定することが必要になることもあります。ネットワーク構成の要件については、システム管理者にお問い合わせください。

-
- ❶ **重要:** HPE ストレージファイルコントローラーシステムを Active Directory ドメインに追加する前に、各ノードとドメインコントローラー間にネットワーク接続があることを確認してください。
-

クラスターシステムを構成する場合は、少なくとも 6 つの IP アドレスが必要です。これらのアドレスは静的に割り当てることも、DHCP によって割り当てることも、両方の方法で割り当てることもできます。静的な IP アドレスを使用するか、DHCP サーバーが自動的に DNS を更新しない場合は、正引きと逆引きの DNS 情報（A レコード、PTR レコード）が DNS サーバーにあらかじめ設定されていることを確認してください。2 ノードクラスターを設定する場合は、HPE ストレージファイルコントローラーの情報を両方とも収集してください。

制限的な Active Directory 環境

HPE ストレージファイルコントローラーシステムが制限的な Active Directory 環境に導入される場合には、Active Directory オブジェクトまたは一部の管理者権限をあらかじめ設定することが必要になる場合があります。詳しくは、次の Microsoft の記事を参照してください。

- ・ <https://docs.microsoft.com/en-us/windows-server/failover-clustering/prestage-cluster-adds>

HPE ストレージファイルコントローラーシステムへのアクセス

HPE ストレージファイルコントローラーの設定を完了するには、直接接続または iLO のいずれかの方法で接続する必要があります。各ストレージファイルコントローラーのメインディスプレイを観察および操作できます。

- ❶ **重要:** ストレージシステムの設置には、直接接続と iLO のアクセス方式しか使用できません。ストレージシステムの設置プロセスが完了し、サーバーの IP アドレスが割り当てられると、ストレージシステムへのアクセス時にリモートデスクトップも使用できるようになります。

手順

1. **直接接続:** ネットワークに DHCP (Dynamic Host Configuration Protocol) サーバーがない場合には、このアクセス方式は必須です。ケーブルを、キーボード、マウス、ネットワークケーブル、モニターケーブル、電源ケーブル順に、ストレージシステムのリアパネルに接続します。

注記: キーボード、マウス、およびモニターは、ストレージシステムには付属していません。

2. **iLO:** iLO リモート管理機能を使用してストレージシステムにアクセスします。

- a. ストレージシステムの背面にある iLO ポートにネットワークケーブルを接続します。
- b. 電源ケーブルをストレージシステムに接続します。
- c. ストレージシステムに添付されている iLO のネットワーク設定タグを見つけ、デフォルトのユーザー名、パスワード、DNS 名を記録します。
- d. リモートコンピューターから標準の Web ブラウザーを開き、ストレージシステムの iLO の管理ホスト名を入力します。

注記: デフォルトでは、iLO はネットワークの DHCP サーバーから管理用の IP アドレスとサブネットマスクを取得します。iLO のタグに記載されているホスト名は、ネットワークの DNS サーバーに自動的に登録されます。DHCP が構成できない、またはシステムが DNS で見つからない場合、直接接続方式を使用して、静的 IP アドレスで iLO を構成します。

- e. iLO のネットワーク設定タグで提供されているデフォルトのユーザー情報を使用して、iLO にログインしてストレージシステムに対するリモートコンソールを起動します。

注記: 初期構成が 2 ノードクラスターの場合は、両方のファイルコントローラーへの直接接続または iLO 接続があることを確認してください。

クラスターハートビート接続用のケーブル接続

2 ノードストレージファイルコントローラーフェイルオーバークラスターは、初期セットアップ中に構成されます。イーサネットケーブルは、下の図に示すように、2 つのファイルコントローラーの間のポート 4 に接続されています。クラスターネットワークインターコネクトとも呼ばれます。設定中に、2 ノードクラスターのセットアップを求められます。このネットワーク接続は、システム間の初期通信を確立するために使用されます。



図 1: システムの接続

HPE MSA ストレージアレイへの接続

MSA アレイを接続します。

- ・ HPE ストレージファイルコントローラー
- ・ (推奨) リモート管理ホスト

MSA ストレージのストレージファイルコントローラーへの接続

直接接続およびスイッチ接続の環境は、MSA ストレージおよびファイルコントローラーの間にサポートされます。MSA ストレージホスト接続ポートは、クラスター環境のファイバーチャネル、iSCSI、または SAS のいずれかになります。スイッチ接続構成の場合は、MSA アレイホスト接続ポートからスイッチのポートにケーブルを接続して、スイッチのポートからファイルコントローラーにケーブルを接続します。

ケーブル接続例（システムへの直接接続など）については、HPE MSA ケーブル接続構成ガイドを参照してください。

MSA アレイの接続ガイドライン

- ・ ホストインターフェイスケーブルは、MSA には付属していません。HPE 提供のケーブルのリストについては、HPE MSA QuickSpecs を参照してください。
- ・ 直接接続展開の場合は、各ホストを両方の MSA アレイの同じポートに接続してください。
- ・ スwitch接続展開の場合は、MSA アレイ A の 1 つのポートおよび MSA アレイ B の対応するポートを 1 台のスイッチに接続し、MSA アレイ A の 2 つ目のポートおよび MSA アレイ B の対応するポートを別のスイッチに接続してください。

MSA アレイのリモート管理ホストへの接続（推奨）

MSA ストレージのリモート管理ポートは、ファイルコントローラーと同じネットワークに接続することをお勧めします。ファイルコントローラーの初期構成時にファイルコントローラーからリモート管理（アウトオブバンド）を構成できます。

RJ-45 イーサネットケーブルを各 MSA ストレージ管理のネットワーク管理ポートから、ファイルコントローラーがアクセスできるスイッチ（可能であれば同じサブネット）に接続します。

HPE Nimble ストレージアレイの接続

HPE Nimble ストレージアレイを、HPE ファイルコントローラーと接続するネットワークに接続します。HPE Nimble ストレージアレイをネットワーク管理ポートへ接続する場合は、初期設定および構成のために HPE ストレージファイルコントローラーと同じネットワーク上で進めることをお勧めします。HPE ストレージファイルコントローラーの初期構成タスク（ICT）中に、構成されていない HPE Nimble ストレージアレイが見つかる場合があります。HPE Nimble ストレージアレイが既に構成されている場合は、ICT 中に HPE Nimble 管理グループの IP アドレスおよび認証情報を使用できることを確認してください。

HPE ストレージファイルコントローラーの構成を開始する前に、HPE Nimble ストレージアレイがインストールおよびケーブルに接続されていることを確認してください。

HPE Nimble ストレージアレイについて詳しくは、[**Infosight**](#) を参照してください。

HPE ストレージファイルコントローラーシステムの構成

HPE ストレージファイルコントローラーシステムは、以下の構成で展開できます。

- ・ スタンドアロン。シングルノードのクラスター構成を構成することも、ノードを既存の Windows フェイルオーバークラスターに参加させることもできます。Windows フェイルオーバークラスターは、1つのクラスター構成内に、最小で 1 ノード、最大で 8 ノードを含むことができます。
- ・ 2 ノードのクラスター。初期時に 2 つのノードを含む新しい Windows フェイルオーバークラスターを作成します。

Windows フェイルオーバークラスター（HPE ストレージファイルコントローラーシステムを使用する、最小で 1 ノード、最大で 8 ノードの構成）。

Windows フェイルオーバークラスターを展開すると、可用性の高いファイルサービスなどの追加機能も提供されます。たとえば、個々のシステムの再起動を要する可能性があるクラスターのメンテナンスを実行している間、ファイル共有をオンラインに維持することができます。

初期構成タスクで構成が完了した後で、Windows フェイルオーバークラスターを作成する際のガイドラインを次の Microsoft Technet 記事で参照してください。[フェイルオーバークラスタリングの概要](#)

最初にシステムに電源を投入したときに、スタンドアロン構成として展開するか、または 2 ノードクラスター構成として展開するかを確認されます。初期構成タスクウィンドウは、選択された構成でシステムをセットアップするための手順を示します。シングルノードのオプションを選択すると、初期構成タスクウィンドウは、スタンドアロンまたはシングルノードクラスターの構成でシステムをセットアップするために必要な手順を示します。

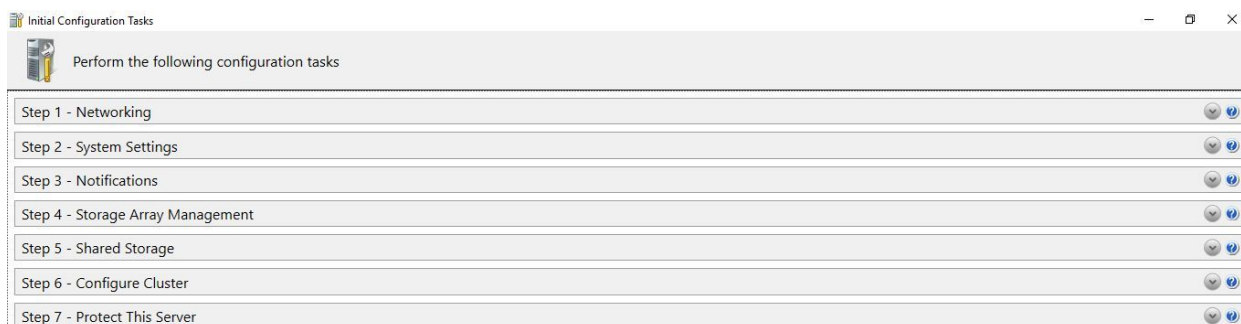
複数ノードのクラスターを作成するときにスタンドアロン構成を選択した場合は、システムに最初に電源を入れたときに、シングルノードクラスターのインストール手順に従ってください。その手順が終了したら、[クラスターの構成](#)セクションの手順に従ってください。既存のクラスターのノードに参加するには、[クラスターの構成](#)の手順に従ってください。

初回のセットアップ

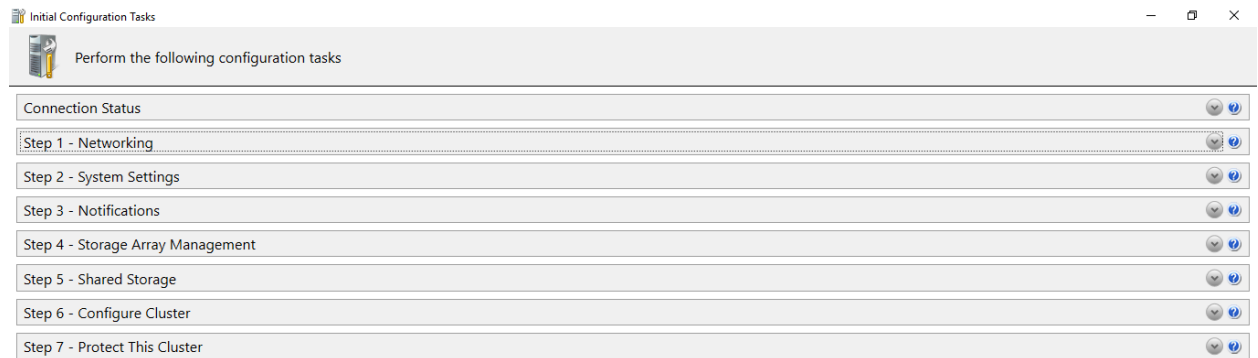
ファイルコントローラーは、単一ノードまたは 2 ノードの Microsoft フェイルオーバークラスターとして構成されます。HPE ストレージファイルコントローラーは、高可用性のために最大 8 つのノードを持つことができます。初回ブート後に、初期構成タスク（ICT）を使用して HPE ストレージファイルコントローラーを構成できます。ICT は、ローカル管理者グループのメンバーがログインすると、自動的に開きます。ログインするたびに ICT ウィンドウが開かないようにするには、[次のログオン時にこのウィンドウを表示しない](#)チェックボックスを選択します。

各タスクは、3 つの列と複数のエキスパンダーで構成されます。最初の列に操作が表示され、2 番目の列に操作に関する説明が表示され、3 番目の列に操作のステータスが表示されます。

単一ノードの ICT ウィンドウ



クラスターノードの ICT ウィンドウ



単一ノードシステムの構成

単一ノードに関するタスクは次のとおりです。

- ・ [ネットワーキング](#)
- ・ [システム設定](#)
- ・ [通知](#)
- ・ [ストレージアレイ管理](#)
- ・ [共用記憶装置](#)
- ・ [ストレージアレイの構成](#)
- ・ [クラスターの構成](#)
- ・ [このサーバーの保護](#)

ネットワーキング

このタスクグループでは、ネットワーク IP およびストレージファイルコントローラーのドメインを設定できます。このグループには、以下のタスクが含まれています。

- ・ [ネットワークの構成](#)
- ・ [コンピューター名とドメインの入力](#)

ネットワークの構成

ネットワーク構成ツールに従って設定していくと、ネットワークチームの構成、VLAN の割り当て、およびネットワークインターフェイス構成のプロセスを実行できます。ネットワーク構成ツールは、プライマリとリモートの両方のノードのネットワークインターフェイスを構成するツールです。

- ・ [ネットワークインターフェイスの設定](#)
- ・ [ネットワークチームの構成](#)
- ・ [ネットワークの VLAN の構成](#)
- ・ [ネットワークインターフェイスの IP 構成](#)
- ・ [ネットワーク構成の概要](#)

- ・ ネットワーク構成の検証
- ・ ネットワーク構成のインポート

手順

1. ネットワーク構成ツールを起動するには、ICT ウィンドウで**ネットワークの構成**をクリックし、**次へ**をクリックします。
あるいは、以下のいずれかの方法で NCT を起動します。
 - ・ コマンドプロンプトまたは PowerShell を開き、NCT と入力する。
 - ・ デスクトップのシステムツールフォルダーをダブルクリックし、**ネットワークの構成**を選択する。
 - ・ スタート画面の**ネットワークの構成**をクリックする。
 - ・ デスクトップにある**ネットワークの構成**アイコンをクリックする。
 - ・ (Nimble アレイの場合) サーバーマネージャーを開き、**ツール > Nimble > ネットワークの構成**の順に選択する。
2. 変更内容を保存して適用するには、**適用**をクリックします。

ネットワークインターフェイスの設定

物理ネットワーク インターフェイスを構成するには、以下の手順に従ってください。

手順

1. 構成対象のインターフェイスの**構成**チェックボックスを選択します。チェックボックスをクリアすると、このインターフェイスはすべての構成から除外され、変更されません。

注記: リモートデスクトッププロトコルに使用される物理ネットワークインターフェイスは、チームの一部として構成できません。このようなインターフェイスは、**構成**チェックボックスが無効になっています。

2. 新しいインターフェイス名を入力します。入力する新しい名前には、\/*? <>|や"などの特殊文字を含めることはできません。
3. **次へ**をクリックして、**ネットワークチームの構成**画面に進みます。

ネットワークチームの構成

注記:

ネットワークチームの構成はオプションです。ネットワークチームを作成しない場合は、**ネットワークチームを今すぐ構成しない**を選択し、**次へ**をクリックして、[ネットワークの VLAN の構成]に進みます。

ネットワークチームの構成画面は、既存のチームが存在しない場合にのみ表示されます。ネットワークチームを使用すると、利用可能な帯域幅を増やしたり、フォールトトレランスとロードバランシングを改善したりできます。

作成できるチームの最大数は、システム上の物理ネットワークインターフェイスの数と同じです。

手順

1. ネットワークチームを今すぐ構成を選択し、作成するチームの数を**チームの数**セクションに入力します。
2. **次へ**をクリックします。
3. ネットワークインターフェイスウィンドウで物理ネットワークインターフェイスを選択し、**次へ**をクリックします。
4. 作成チェックボックスを選択し、
 - a. チーム名を入力します。
 - b. **タイプ**セクションからチームタイプを選択します。デフォルトのチームタイプは、**Switch Independent/Dynamic** です。

注記: 構成または削除の対象として表示されるチームの数は、作成するチーム数によって異なります。たとえば、構成用に 2 つのインターフェイスを選択すると、チームの作成のために 2 行表示されます。

5. **次へ**をクリックします。
現在どのチームにも含まれていないネットワークインターフェイスが表示されます。
6. 新しいチームに含めるネットワークインターフェイスを選択します。
作成するチームごとに、チームの一部ではない物理ネットワークインターフェイスを選択する個別のページが表示されます。
7. **次へ**をクリックして、**ネットワークの VLAN の構成**画面に進みます。

ネットワークチームのガイドライン

ネットワークチームを作成する際に、1 つのネットワークチームによって要求されたネットワークインターフェイスを他のネットワークチームに追加することはできません。インターフェイス名の横に、そのインターフェイスが属しているチームが表示されます。すべてのアダプターが 1 つ以上のチームですでに要求されている場合、警告メッセージが表示されます。元に戻って、以前作成したチームからインターフェイスをいくつか削除するか、またはチームの作成をスキップしてください。

[ネットワークの VLAN 構成] 画面に進むと、ネットワークチームがインターフェイスペインに表示されます。

- ・ チームに含まれている一部の物理ネットワークインターフェイスが切断され、他のインターフェイスは接続されている場合、チームのステータスは劣化と表示されます。
- ・ チームに含まれているすべての物理ネットワークインターフェイスが切断された場合、チームのステータスは切断されましたと表示されます。

チームが存在すると、**ネットワークチームの構成**ウィンドウの**削除**チェックボックスが有効になります。**削除**チェックボックスは、チームが存在する場合のみ有効になります。既存のチームを削除すると、そのチームに含まれていた物理ネットワークインターフェイスを、新しいチームで 사용할 ことができます。

ネットワークの VLAN の構成

注記: VLAN 割り当ての構成はオプションです。VLAN 割り当てを構成しない場合は、デフォルトのチームインターフェイスのみが作成されます。**次へ**をクリックしてこの手順をスキップし、[ネットワークインターフェイスの IP 構成] 画面に進んでください。

デフォルトの VLAN ID は 0 ですが、VLAN ID の値には 0~4094 を使用できます。ネットワークチーム用に作成された物理インターフェイスと仮想インターフェイスの両方に VLAN ID を割り当てると、仮想ネットワークインターフェイスが作成されます。物理インターフェイスに VLAN ID が割り当てられた場合、チームは物理インターフェイス単独で作成されます。VLAN ID を持つ仮想インターフェイスは、その後でチーム内に作成されます。

注記: ネットワークチームの作成をスキップし、選択した物理インターフェイス上に VLAN を作成すると、(物理インターフェイス名) チーム - VLAN (VLAN ID) という名前のネットワークチームが自動的に作成されます。

手順

1. **VLAN ID を今すぐ構成**を選択して、**次へ**をクリックします。
2. 以下のオプションのいずれかを選択し、該当するフィールドに VLAN ID を入力します。
 - ・ **単一の VLAN ID を追加** — 単一の VLAN ID を追加します。
 - ・ **個別の VLAN ID を追加** — 複数の VLAN ID をカンマ区切り形式で追加します。
 - ・ **VLAN ID の範囲を追加** — 開始値および終了値に増分を使用して、VLAN ID を指定します。たとえば、開始値が 2、終了値が 20、増分が 5 の場合は、VLAN ID 2、7、12、および 17 が割り当てられます。
3. **デフォルトの仮想ネットワークインターフェイスを削除**チェックボックスを選択して、チームからデフォルトの仮想インターフェイスを削除します (オプション)。

注記: ネットワークチームを作成すると、デフォルトで仮想ネットワークインターフェイスも作成されます。デフォルトの仮想インターフェイスを削除した場合、物理ネットワークインターフェイスと仮想ネットワークインターフェイスに 1 つ以上の VLAN ID が割り当てられていない限り、ネットワークチームでも物理 NIC でもパケットを受信しません。

4. **次へ**をクリックして、**ネットワークインターフェイスの IP 構成**画面に進みます。

[ネットワークインターフェイスの IP 構成] に進むと、VLAN 割り当てがインターフェイスペインに表示されます。

注記: チームおよびアダプターへの VLAN ID 割り当て後に**ネットワークインターフェイスの VLAN ID を今すぐ構成しない**を選択しても、割り当てられた ID は削除されません。チームの VLAN を構成しない場合は、各 VLAN ページを順に進み、すべてのチームおよびアダプターに対して **VLAN ID をこのチームに追加しない**を暗黙的に選択します。

ネットワークインターフェイスの IP 構成

ネットワークインターフェイスの IP 構成では、インターフェイスペインでインターフェイスを選択して IP アドレスを構成します。構成可能な各インターフェイスは、ツールが自動的に有効にします。割り当てる IP アドレスは、静的でも、DHCP を使用して動的に割り当ててもかまいません。

注記: 両方のノード上のインターフェイスを、同じネットワークセグメントを使用するように構成することをお勧めします。たとえば、プライマリノードのネットワークインターフェイス 1 をセグメント 192.168.8.x に接続する場合は、リモートノードのネットワークインターフェイス 1 をネットワークセグメント 192.168.8.x に接続することをお勧めします。

手順

1. 次のいずれかを実行します。

- a. 動的 IP アドレスと静的 IP アドレスを割り当てるには、**IP アドレスとゲートウェイの割り当てに DHCP を使用する**を選択するか、**静的 IP アドレスとゲートウェイの割り当て**を選択します。

❗ **重要:** 静的 IP アドレスとゲートウェイの割り当てを選択する場合は、DNS サーバーのアドレスも静的でなければならず、ネットワークマスクを割り当てる必要もあります。デフォルトゲートウェイアドレスの割り当てはオプションです。

- b. DNS サーバーのアドレスの割り当てに DHCP を使用するまたは DNS サーバーの静的 IP アドレスの割り当てを選択します。前の手順で静的 IP アドレスとゲートウェイの割り当てオプションを選択した場合、DNS サーバーの静的 IP アドレスの割り当てがデフォルトで選択されており、変更することはできません。

この手順を繰り返して、他のネットワークインターフェイスを構成します。

Hewlett Packard Enterprise では、このウィンドウの次へをクリックする前に、各インターフェイスを確認することをお勧めします。

2. 次へをクリックして、[ネットワーク構成の概要] 画面に進みます。

ツールは、IP アドレスとサブネットマスクを使用してゲートウェイを検証します。

ネットワーク構成の概要

[ネットワーク構成の概要] ウィンドウで、すべての構成変更を確認します。必要に応じて、前へをクリックするか、ページの下部にあるナビゲーションリンクを使用して、構成を編集します。適用をクリックして、構成の変更を適用します。

次へをクリックして、構成された各タスクの詳細を表示します。エラーがある場合は、エラータブに表示されます。

構成が正常に変更されると、ネットワーク構成ファイル (NCTConfig.xml) が C:\Program Files\HPE\StoreEasy NetworkConfigurationWizard に自動的に作成されます。このファイルには、ネットワーク構成の詳細が含まれています。

物理ネットワークインターフェイスの構成が正常に行われたが、チームまたは VLAN の作成に失敗した場合は、NCTConfig.xml が引き続き作成されます。ただし、このファイルには物理ネットワークインターフェイスのみが含まれます。物理ネットワークインターフェイスのタスクが失敗した場合、NCTConfig.xml ファイルは作成されません。

このファイルを使用して、1 つのストレージシステムから別のストレージシステムにネットワーク構成をインポートできます。ネットワーク構成のインポートに関する詳細については、「[ネットワーク構成のインポート](#)」を参照してください。

ネットワーク構成の検証

ネットワーク構成の検証画面を使用して、ネットワーク設定を検証します。ネットワークの検証では、テスト対象のすべてのネットワークインターフェイスが接続されている必要があります。

注記:

- ネットワークの検証はオプションです。ただし、Hewlett Packard Enterprise では、このウィザードを使用して、ご使用のネットワーク設定が有効かどうかを確認することをお勧めします。この検証は、ネットワーク環境の問題の診断に役立ちます。
- NCT に戻ってネットワーク検証ウィザードのみを使用するには、コマンドプロンプトまたは PowerShell を開き、NCT -validate コマンドを入力します。

手順

1. ネットワーク構成を今すぐ検証を選択します。
2. (ご使用のシステムが存在するドメイン) の名前とドメインコントローラーの IP アドレスを入力します。システムがドメインに存在しない場合は、これらのフィールドを空白にしておくことができます。
3. 検証をクリックします。

各インターフェイスは順にテストされ、検証の成功または失敗が出力ウィンドウに示されます。検証の進行状況は、タスクバーにも表示されます。検証結果は、`c:\nas\logs\NetworkConfigTool` フォルダーに保存されます。各検証結果が、検証が実行された時刻と日付を使用した名前のファイルに保存されます。検証が完了すると、検証結果は、ICT ウィンドウに表示されます。

ネットワークの検証を実行しない場合は、レジストリキーを使用すると、以下のステータスが表示されます。

ネットワーク構成が検証されていません

構成が検証されていない場合に表示されます。

ネットワーク構成が検証されました

検証が完了したことをキーが示す場合に表示されます。

ネットワークの検証に失敗しました

1 つ以上の検証手順が失敗したことをキーが示す場合に表示されます。

ネットワーク構成のインポート

NCTConfig.xml ファイルを使用すると、別のストレージシステムから、すべてのインターフェイスに対するネットワーク構成の設定を一度にインポートすることができます。利用可能なインターフェイスから目的のネットワークインターフェイスを再構成して、チームを作成したり、既存のチームを削除したりすることができます。

NCTConfig.xml ファイルとその使用法の詳細については、HPE ストレージファイルコントローラー管理者ガイドの「ネットワーク構成ファイルの管理」セクションを参照してください。

ネットワーク構成の設定のインポート

手順

1. ファイル NCTConfig.xml を開き、<AdapterIPConfiguration>タグの詳細を編集します。
2. 必要に応じて、Name タグのインターフェイス名を編集します。

❗ **重要:** インターフェイス名を変更するときは、デフォルトの VLAN に関連付けられているプレフィックスを変更する必要があります。たとえば、インターフェイス名が `Ethernet 2 Team -VLAN Default` である場合は、プレフィックスを変更して `Ethernet 2 Team` とします。`VLAN Default` は、デフォルトの VLAN 名であり、変更することはできません。

3. ファイルを保存し、構成をインポートするストレージサーバー上の `C:\Program Files\HPE\StoreEasy NetworkConfigurationWizard` にコピーします。
4. NCT ウィザードを起動し、プロンプトが表示されたらはいをクリックして、最後に保存された構成を使用します。
NCT ウィザードは、構成の詳細を NCTConfig.xml ファイルからロードして表示します。
5. 検出が完了したら、次へをクリックします。

6. ネットワーク構成の概要画面とネットワーク構成の検証画面で必要なネットワーク構成の変更を行います。
7. ネットワーク構成の概要画面で適用をクリックします。
8. ネットワーク構成の検証画面で検証をクリックします。

ネットワークの検証の詳細については、HPE ストレージファイルコントローラー管理者ガイドを参照してください。

ネットワークの検証が完了し、ステータスメッセージが表示されます。

コンピューター名とドメインの入力

ストレージシステムにリモートでアクセスし、レポートとログを簡単に識別するには、組織内のコンピューターの命名規則に従って、わかりやすい名前を割り当てる必要があります。コンピューター名とドメインを入力をクリックしてシステムのプロパティウィンドウを開き、コンピューター名とドメインを指定します。オペレーティングシステムは、ランダムに生成されたコンピューター名とドメインを使用してインストールされます。プロンプトで新しいコンピューター名とドメインを入力し、システムを再起動します。

コンピューター名のガイドライン

コンピューター名を割り当てる際は、以下の点に注意してください。

- ・ Microsoft では、ほとんどの言語で 15 文字以下にするよう推奨しています。中国語、日本語、韓国語など、文字ごとに多くの保存領域を必要とする言語の場合は、7 文字以下にするよう推奨されています。
追加情報については、<https://technet.microsoft.com/en-us/library/cc731383> を参照してください。
- ・ Hewlett Packard Enterprise では、コンピューター名にインターネット標準文字のみを使用することをお勧めします。標準文字とは、0~9 の数字、A~Z（大文字と小文字）、およびハイフン（-）です。コンピューター名をすべて数字で指定することはできません。
- ・ ネットワークで DNS を使用している場合は、さまざまな種類の文字を使用できます。これらには、Unicode 文字やアンパサンド(&)などの非標準文字が含まれます。非標準文字を使用すると、Microsoft 以外のソフトウェアのネットワーク上での動作に影響を与える場合があります。
- ・ コンピューター名は最長で 63 バイトです。さらに、15 バイト以上の名前には追加の設定手順があります。
- ・ コンピューターがドメインのメンバーである場合は、ドメイン内の別のコンピューターと異なる一意の名前を選択する必要があります。

システム設定

オペレーティングシステムのプロパティをカスタマイズして構成します。

- ・ ローカル管理者パスワードを設定する
- ・ 時刻とタイムゾーンの設定

ローカル管理者パスワードを設定する

管理者パスワードは、システムにアクセスするために必要です。

1. ローカル管理者パスワードを設定するをクリックします。

パスワードの設定ウィンドウが表示されます。

2. 新しいパスワードおよび確認用パスワードフィールドに新しいパスワードを入力します。

注記: HPEStorage! は、システムのデフォルトのパスワードです。

3. OK をクリックします。

- ❶ **重要:** パスワードを忘れた場合は復元できません。新しいパスワードを作成する必要があります。パスワードのリセットユーティリティにアクセスするには、**コントロールパネル > ユーザーアカウント > パスワードリセットディスクの作成**をクリックして、リセットディスクまたは USB を作成する手順を実行します。
-

時刻とタイムゾーンの設定

地理的場所に応じて、時刻とタイムゾーンを設定します。HPE ストレージファイルコントローラー上のクラスターノードの**時刻およびタイムゾーンの設定**オプションは、ネットワーキングセクションで利用可能です。

システムの日付と時刻をインターネット時刻と同期させることができます。また、別のタイムゾーンの時刻を表示するように追加のクロックを構成することもできます。

通知

メールアラートを構成し、HPE 製品通知を登録します。

- ・ [File Controller アラートの構成](#)
- ・ [HPE 製品通知の登録](#)

File Controller アラートの構成

ホストオペレーティングシステムとは無関係に検出されたファイルコントローラーのアラート状態を送信するには、iLO の **iLO アラートメール**を使用します。メールアラートには、ハードウェア障害のような主要なホストシステムイベントが含まれます。アラートは、指定したメールアドレスに送信されます。

注記: 一部のメールサービスプロバイダーでは、スパム、商用コンテンツ、迷惑な容量など、問題のあるメールをブロックするためのフィルターやルールが確立されています。iLO により生成されたメッセージの受信が、これらのツールによってブロックされる場合があります。iLO アラートメールに指定されている送信者のメールアドレスが、受信者メールのホワイトリストにあることを確認して、メールがスパムフォルダーにフィルターされないようにしてください。

アラートメールを有効にする

手順

1. iLO システムにログインします。
2. 左のナビゲーションペインで**マネジメント**を選択してから、**アラートメールタブ**をクリックします。
3. **iLO アラートメールを有効**オプションを選択します。
4. **アラートメールタブ**で以下の情報を指定します。
 - ・ メールアドレス
 - ・ 送信ドメイン

- ・ SMTP ポート
 - ・ SMTP サーバー
5. (オプション) **テストアラートメールを送信**をクリックして、指定されたメールアドレスにテストメッセージを送信します。

注記: **テストアラートメールを送信**ボタンは、**iLO アラートメールを有効**が有効になっている場合にのみ使用できます。

6. 変更を保存するには、**適用**をクリックします。

アラートメールのオプション

メールアドレス

iLO によるメールアラートの宛先メールアドレス。これは最大 63 文字であり、標準のメールアドレス形式でなければなりません。入力できるメールアドレスは 1 つだけです。

送信ドメイン

送信 (送信元) メールアドレスに指定されたドメイン名。送信アドレスは、iLO 名をホスト名として、送信ドメインをドメイン名として使用して構成します。最大 63 文字を使用できます。

SMTP ポート

SMTP サーバーが未認証の SMTP 接続に使用するポート。デフォルト値は 25 です。

SMTP サーバー

SMTP サーバーまたは MSA の IP アドレスまたは DNS 名。このサーバーは、メッセージ転送エージェントと連携してメールを配信します。最大 63 文字を使用できます。

アラートメールを無効にする

手順

1. iLO システムにログインします。
2. 左のナビゲーションペインで**マネジメント**を選択してから、**アラートメールタブ**をクリックします。
3. **iLO アラートメールを有効**オプションをクリアします。
4. 変更を保存するには、**適用**をクリックします。

製品通知の登録

Hewlett Packard Enterprise は、システムの更新、重大な問題、および機能の更新についての通知を受信できるように、ご使用のシステムを登録することをお勧めします。サービスのリリースにアクセスできるようにするには、システムの登録が必須になります。ご使用のシステムがネットワークに接続していない場合は、インターネットアクセスを使用して他のデバイスから製品登録できます。

注記: 登録は、サービスのリリースにアクセスするために必須です。

以下の方法で製品の登録リンクにアクセスすることもできます。

- ・ デスクトップにある **Register For HPE product notifications** アイコンをダブルクリックします。
- ・ スタート画面で**製品の登録**をクリックします。
- ・ サーバーマネージャーを開き、**ツール > (接続するアレイにより次のいずれか) 3PAR、MSA、Nimble > 製品の登録**の順に選択します。

ストレージアレイ管理

HPE ファイルコントローラーのすべての SAN アレイに接続できます。ファイルコントローラーに接続されているストレージシステムに応じて、以下のストレージ管理を実行します。

3PAR StoreServ アレイ

注記: 接続タイプが iSCSI の場合、iSCSI イニシエーターが有効になります。

- ・ [アレイ管理ログイン詳細の設定](#)
- ・ [iSCSI イニシエーターの実行](#)
- ・ [Multi-Path IO の構成](#)

Nimble アレイ

- ・ [Nimble グループの検出](#)
- ・ [Nimble グループに接続](#)
- ・ [iSCSI イニシエーターの実行](#)
- ・ [Multi-Path IO の構成](#)

MSA または他のアレイ

注記: 接続タイプが iSCSI の場合、iSCSI イニシエーターが有効になります。

- ・ [アレイ管理ログイン詳細の設定](#)
- ・ [iSCSI イニシエーターの実行](#)
- ・ [Multi-Path IO の構成](#)

アレイ管理ログイン詳細の設定

手順

1. 接続するストレージアレイの **アレイ IP アドレス** を入力します。
2. **アレイのユーザー ID** と **アレイのパスワード** を入力します。
3. プロトコルを **https** または **http** のいずれかから選択します。
4. **接続タイプ** を **FC** または **iSCSI** のいずれかから選択します。
5. **保存** をクリックします。
メッセージアレイデータは正常に保存されましたが表示されます。
6. アレイ登録ツールを閉じるには、**終了** をクリックします。
ICT ウィンドウの 3 番目の列で、接続されたアレイの IP アドレスを確認できます。

Nimble グループの検出

[Nimble グループの検出] タスクを使用して、**Nimble Setup Manager** を開きます。初期化されていない Nimble アレイを構成できます。

- ・ Nimble アレイの初期化
- ・ Nimble アレイのセットアップ

Nimble アレイの初期化

手順

1. ICT タスクグループで**ストレージアレイ管理 > Nimble グループの検出**をクリックします。

Welcome to Nimble Setup Manager 画面が表示されます。

ストレージファイルコントローラーに接続されている、初期化されていない Nimble アレイが表示されます。

注記: アレイがリストされない場合は、ストレージファイルコントローラーと Nimble アレイのネットワーク接続の両方が同じネットワークセグメントに接続されているかどうか確認します。

2. 初期化するアレイを選択し、**Next** をクリックします。

注記: セキュリティ証明書の問題が発生した場合は、Internet Explorer で JavaScript とアクティブスクリプトを有効にします。

License Agreement screen が表示されます。

3. **License Agreement screen** で、チェックボックスをクリックして、ライセンス条件に同意します。次に、**Proceed** をクリックします。

Nimble Storage group Setup 画面が表示されます。

4. **Set up this array but do not join a group** オプションをクリックします。
5. 以下のパラメーターを入力し、**Finish** をクリックします。
 - a. **Array Name** : 英字、数字、またはダッシュのみを使用します。名前の最初の文字に句読点は使用しないでください。
 - b. **Group Name**: 英字、数字、またはダッシュのみを使用します。名前の最初の文字に句読点は使用しないでください。
 - c. **Management IP**: Nimble アレイの IP アドレスが含まれます。
 - d. **Netmask** : IP アドレスをマスクし、IP アドレスをネットワークアドレスとホストアドレスに分割する 32 ビットの数値。
 - e. **Default Gateway** : さまざまなプロトコルを使用する別のネットワークにアクセスできます。
 - f. **Domain Name** (任意) : HPE ストレージファイルコントローラーのドメイン コントローラーの名前。
 - g. **Password** : Create a new password フィールドと Confirm password フィールドに同じパスワードを入力します。

アレイの初期化に成功したら、アレイをセットアップします。

アレイの詳細については、**InfoSight** のドキュメントを参照してください。

Nimble アレイのセットアップ

前提条件

Nimble アレイを初期化します。

手順

1. ユーザー名とパスワードを入力し、**ログイン**をクリックします。

注記: 画面全体が表示されない場合は、画面の解像度を上げてください。

Nimble Storage セットアップページが表示されます。

2. サブネット構成でデータサブネットの追加をクリックします。
3. インターフェイスの割り当てで、次の情報を入力し、**次へ**をクリックします。

注記: eth1 と eth2 のサブネットが、それぞれ**管理**および**なし**であることを確認します。

- a. IP インターフェイス：このインターフェイスは、管理 IP アドレスとは異なっていなければなりません。
 - b. コントローラー A の IP アドレス
 - c. コントローラー B の IP アドレス
4. ドメインで、以下の情報を入力し**次へ**をクリックします。
 - a. (オプション) ドメイン名
 - b. DNS サーバー：DNS サーバーフィールドには、最大 5 つの IP アドレスを入力できます。
 5. 時間の下で：
 - a. ドロップダウンリストからタイムゾーンを選択します。
 - b. 時刻 (NTP) サーバーのホスト名または IP アドレスを入力します。
 6. サポートで、以下の情報を入力し**終了**をクリックします。
 - a. 差出人アドレス
 - b. 送信先アドレス

注記: 複数の電子メールアドレスを入力するには、カンマで区切って入力するか、個々の行に入力します。

- c. SMTP サーバー
- d. プロキシサーバーを設定する必要がある場合は、**HTTP プロキシサーバーの使用**を選択します。

メッセージ

「セットアップ完了」

が表示されます。

7. 次のいずれかを実行します。

- a. **続行**をクリックします。
- b. WWPN ホスト情報を使用して、イニシエーターグループを作成します。
 - ・ **管理 > イニシエーターグループ**を選択します。
 - ・ グループを選択し、**編集**をクリックして、既存のイニシエーターグループを編集します。
 - ・ 各イニシエーターのエイリアスと WWPN を入力して**保存**をクリックします。

Nimble グループへの接続

Nimble グループに接続をクリックすると、Nimble アレイの管理グループの IP アドレスと認証情報（暗号化済み）が HPE ストレージファイルコントローラのノードに保存されます。この情報は、他のツールによって使用されます。

手順

1. ICT ウィンドウで、**ストレージアレイ管理 > Nimble グループに接続**をクリックします。
Nimble グループに接続ウィンドウが表示されます。
2. **グループ管理 IP** フィールドに、Nimble アレイの構成時に指定した管理グループの IP アドレスを入力します。
3. Nimble 管理グループの構成時に指定した**グループユーザー名**と**グループパスワード**を入力します。
4. **接続**をクリックして、Nimble グループへの接続を確立します。

レジストリに Nimble 管理グループの IP アドレスと認証情報を保存すると、次のいずれかのステータスメッセージが表示されます。

- ・ Nimble グループに接続できませんでした。HPE ストレージファイルコントローラーが Nimble アレイに正常に接続できない場合に表示されます。
- ・ Nimble グループへの接続が完了しました。HPE ファイルストレージファイルコントローラーが、管理 IP アドレスと認証情報を使用して、Nimble アレイを正常に特定して認証できた場合に表示されます。

iSCSI イニシエーターの実行

このリンクをクリックすると、iSCSI イニシエーターツールが起動します。このツールを使用して、iSCSI アレイに接続します。

注記: iSCSI イニシエーターの実行ツールは、選択したアレイの接続タイプが iSCSI である場合にのみ使用できます。

マルチパス IO の構成

注記: MPIO を構成しないと、ドライブが重複してリストされます。

複数のパスを介して仮想ボリュームをファイルコントローラーにエクスポートすると、MPIO 構成は自動で行われます。構成の状態は、ICT ウィンドウに表示されます。管理者特権の PowerShell またはコマンドプロンプトで `mpiocpl` コマンドを入力すると、MPIO のプロパティのアプレットを開くことができます。

マルチパス IO の構成

手順

1. **Multi-Path IO の構成**をクリックします。
[MPIO のプロパティ (mpiocpl.exe)] ウィンドウが開きます。
2. **マルチパスの検出タブ**で、次を選択します。
 - a. iSCSI デバイスのサポートを追加
 - b. iSCSI のマルチイニシエーターを許可

共用記憶装置

このタスクグループでは、ノード間の共有ストレージの結果のステータスを参照することができます。両方のノードは、一意のストレージ識別子をベースとして、同じストレージにアクセスする必要があります。共有ストレージに表示されるメッセージを以下に示します。

- ・ **「共有ストレージが見つかりません」**: システムは、基準に合う共通の共有ストレージを見つけることができませんでした。共有ストレージが利用可能かを検証するには、各サーバーで `get-disk powershell` スクリプトを実行し、2つのサーバーのユニーク ID を比較します。たとえば、`get-disk | select uniqueid,friendlyname,operationalstatus` を実行します。
- ・ **「共有ストレージが見つかりました」**: システムは、監視ディスクに使用可能なストレージを見つけました。両方のノードで同じユニーク ID を持つディスクは、共有として扱われます。

注記: 1 つ以上の LUN がノードにエクスポートされているのに、ユニーク ID が一致しないか、リストされない場合は、各 StoreVirtual ファイルコントローラー上で、昇格した Administrator PowerShell コマンドプロンプトから、`Update-StorageProviderCache -DiscoveryLevel Full` を起動して、ストレージプロバイダーのキャッシュを更新する必要があります。ただし、キャッシュを更新しても問題が解決しない場合は、ストレージの接続に使用されている HBA またはネットワークアダプターが同一であること、ファームウェアおよびドライバーのバージョンが同じであることを確認します。ファームウェアまたはドライバーを変更した場合は、両方のノードを再起動する必要があります。それでもストレージプロバイダーキャッシュの更新で問題が発生する場合は、各ノードで `cmdlet Get-StorageProvider` コマンドを実行し、システムがストレージにアクセスできることを検証してください。詳細は、共有ストレージソリューションのインストールおよびセットアップ情報を参照してください。

ディスクアレイを管理するためにサポートされている 3PAR Management Console ソフトウェアのバージョンについては、3PAR ディスクアレイ製品のマニュアルを参照してください。

注記: 3PAR ディスクアレイへの iSCSI 接続の共有ストレージを参照するには、ICT のネットワークの構成タスクを完了させてください。現在構成中のホストから 3PAR Management Console またはコマンドラインユーティリティを使用するときは、ICT のネットワークの構成タスクを完了させる必要があります。これによりホストは、ネットワークを介して 3PAR ディスクアレイと接続できるようになります。セキュリティを強化し、より良いレベルのストレージサービスをユーザーおよびアプリケーションの両方に対して提供するために、3PAR Virtual Domains ソフトウェアを使用することを検討してください。詳細は、HPE 3PAR StoreServ Storage コンセプトガイドを参照してください。

詳細は、HPE 3PAR Windows Server 2016/2012/2008 実装ガイドを参照してください。

MSA アレイへの接続時に監視ディスク（仮想ボリューム、最小 600 MB）またはその他の仮想ボリュームを準備する

MSA アレイの監視ディスクをプロビジョニングできます。

前提条件

アレイ情報を保存フィールドを使用して、ストレージアレイが構成済みであることを確認します。詳細については、「[アレイ管理ログイン詳細の設定](#)」を参照してください。

手順

1. 監視ディスク（最小 600 MB）に使用する仮想ボリュームまたはその他の仮想ボリュームを準備するをクリックして、MSA アレイのストレージ管理ユーティリティのウィンドウを起動します。
2. 必要なログイン認証情報を入力します。
3. 以下のいずれかの操作を実行します。
 - ・ ホストの作成
 - ・ 仮想ボリュームの作成
 - ・ 仮想ボリュームのエクスポート

ホストの作成

ホストの表示

ホストトピックには、システムで定義されているイニシエーター、ホスト、ホストグループに関する情報がテーブル形式で表示されます。ホストトピックでは、ユーザーがイニシエーターをマッピングし、マップ詳細を表示することもできます。

ホストテーブル

ホストテーブルには、以下の情報が表示されます。デフォルトでは、一度に 10 個のエントリーがテーブルに表示されます。

- ・ グループ。イニシエーターがホストグループにグループ化されている場合にはグループ名を表示し、それ以外の場合は「--」と表示します。
- ・ ホスト。イニシエーターがホストにグループ化されている場合にはホスト名を表示し、それ以外の場合は「--」と表示します。
- ・ ニックネーム。イニシエーターに割り当てられているニックネームを表示します。
- ・ ID。イニシエーターの ID を表示します。この ID は、FC または SAS イニシエーターの WWN であるか、iSCSI イニシエーターの IQN です。
- ・ プロファイル。プロファイル設定が表示されます。
 - 標準。デフォルトのプロファイルです。
 - HP-UX。ホストはフラットスペースアドレッシングを使用します。
 - OpenVMS。LUN 0 は、マッピングに割り当ててはできません。
- ・ 検出済み。検出されたイニシエーターの場合は [はい]、手動で作成されたイニシエーターの場合は [いいえ] が表示されます。
- ・ マッピング済み。ボリュームにマッピングされているイニシエーターの場合は [はい]、マッピングされていないイニシエーターの場合は [いいえ] が表示されます。
- ・ ホストのタイプ。ホストインターフェイスプロトコルを示します。

関連マッピングテーブル

選択したイニシエーターについて、[関連マッピング] テーブルには、以下の情報が表示されます。デフォルトでは、一度に 20 個のエントリーがテーブルに表示されます。

- ・ Group.Host.Nickname。マッピングが適用されるイニシエーターを識別します。
 - initiator-name - マッピングはこのイニシエーターにのみ適用されます。
 - initiator-ID - マッピングはこのイニシエーターのみに適用され、イニシエーターはニックネームを持ちません。
 - host-name.* - マッピングはこのホストのすべてのイニシエーターに適用されます。
 - host-group-name.*.* - マッピングはこのグループのすべてのホストに適用されます。
- ・ ボリューム。マッピングが適用されるボリュームを識別します。
 - volume-name - マッピングはこのボリュームにのみ適用されます。
 - volume-group-name.* - マッピングはこのボリュームグループのすべてのボリュームに適用されます。
- ・ アクセス。マッピングに割り当てられているアクセスのタイプを表示します。
 - 読み取り/書き込み - マッピングで読み書きアクセスが許可されます。
 - 読み取り専用 - マッピングで読み取りアクセスが許可されます。
 - アクセスなし - マッピングでアクセスが禁止されます。
- ・ LUN。マッピングで 1 つの LUN と LUN の範囲のどちらを使用する (*で示されます) かを示します。
- ・ ポート。マッピングが適用されるコントローラーホストポートをリストします。各番号は、両方のコントローラー上で対応するポートを表します。

イニシエーターの作成

イニシエーターは手動で作成することができます。たとえば、スイッチを介してコントローラーポートを物理的にホストに接続する前にイニシエーターを定義したい場合もあります。

手順

1. イニシエーターに使用する FC または SAS WWN、あるいは iSCSI IQN を決定します。
2. ホストトピックで、**操作 > イニシエーターの作成**を選択します。[イニシエーターの作成] パネルが開きます。
3. [イニシエーター ID] フィールドで、WWN または IQN を入力します。WWN の値には、桁の各ペアの間にコロンを含めることができますが、コロンは破棄されます。
4. イニシエーターの名前フィールドに、識別しやすいようにニックネームを入力します。たとえば、MailServer_FCp1 を使用できます。イニシエーター名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , . < \ を含めることはできません。

他のイニシエーターによって名前が使用されている場合には、別の名前を入力するように指示されます。
5. プロファイルリストで、適切なオプションを選択します。

- ・ **標準**。デフォルトのプロファイルです。
- ・ **HP-UX**。ホストはフラットスペースアドレッシングを使用します。
- ・ **OpenVMS**。イニシエーターに LUN 0 を割り当てることはできません。

6. **OK** をクリックします。イニシエーターが作成され、ホストテーブルが更新されます。

イニシエーターの変更

手動で作成したイニシエーターは変更することができます。

手順

1. ホストトピックで、変更するイニシエーターを選択します。
2. **操作 > イニシエーターの変更**を選択します。イニシエーターの変更パネルが開きます。
3. イニシエーターの名前フィールドに、識別しやすいニックネームを入力します。たとえば、**MailServer_FCp2** のように指定できます。イニシエーター名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、", . < \ を含めることはできません。他のイニシエーターによって名前が使用されている場合には、別の名前を入力するように指示されます。
4. プロファイルリストで、適切なオプションを選択します。

- ・ **標準**。デフォルトのプロファイルです。
- ・ **HP-UX**。ホストはフラットスペースアドレッシングを使用します。
- ・ **OpenVMS**。イニシエーターに LUN 0 を割り当てることはできません。

5. **OK** をクリックします。ホストテーブルが更新されます。

イニシエーターの削除

手動で作成したイニシエーターは、グループ化もマッピングもされていなければ、削除することができます。手動で作成したイニシエーターがマッピングされている場合には削除できません。また、検出されたイニシエーターは削除できませんが、削除操作でそのニックネームを削除することは可能です。

手順

1. ホストトピックで、名前の付いた 1~128 のイニシエーターから、ホストに追加する対象を選択します。
2. **操作 > イニシエーターの削除**を選択します。
イニシエーターの削除パネルが開き、削除するイニシエーターがリストされます。
3. **OK** をクリックします。
イニシエーターが削除され、ホストテーブルが更新されます。

ホストへのイニシエーターの追加

名前の付いた既存のイニシエーターを、既存のホストまたは新規ホストに追加できます。ホストにイニシエーターを追加するには、そのイニシエーターのマッピングが、ホスト内の他のすべてのイニシエーターと同じでなければなりません。つまり、そのイニシエーターは、同じアクセス設定、ポート設定、および LUN 設定によって、同じボリュームまたはボリュームグループにマッピングされている必要があります。

手順

1. ホストトピックで、名前の付いた 1~128 のイニシエーターから、ホストに追加する対象を選択します。

操作 > ホストへの追加を選択します。[ホストへの追加] パネルが開きます。

2. 次のいずれかを実行します。

- ・ 既存のホストを使用する場合は、[ホストの選択] リストでその名前を選択します。
- ・ ホストを作成する場合は、[ホストの選択] フィールドにホストの名前を入力します。ホスト名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、", . < \ を含めることはできません。

3. **OK** をクリックします。選択したイニシエーターについて、ホスト値が--から、指定した名前に変わります。

ホストからのイニシエーターの削除

最後のイニシエーターを除くすべてのイニシエーターを、ホストから削除できます。ホストからイニシエーターを削除すると、そのイニシエーターはグループ解除されますが削除されることはありません。すべてのイニシエーターを削除するには、ホストを削除してください。

手順

1. ホストトピックで、ホストから削除する 1~1024 のイニシエーターを選択します。

2. **操作 > ホストからの削除**を選択します。

ホストからの削除パネルが開き、削除するイニシエーターがリストされます。

3. **OK** をクリックします。

選択したイニシエーターについて、ホスト値が--に変わります。

ホストの削除

グループ化されていないホストは削除できます。ホストを削除すると、そのイニシエーターはグループ解除されますが、削除されるわけではありません。

手順

1. ホストトピックで、グループ化されていない 1~512 のイニシエーターを削除対象として選択します。

2. **操作 > ホストの削除**を選択します。

ホストの削除パネルが開き、削除するホストがリストされます。

3. **OK** をクリックします。

選択したホストのイニシエーターについて、ホスト値が--に変わります。

ホスト名の変更

ホストは名前を変更することができます。

手順

1. ホストトピックで、名前を変更するホストに所属するイニシエーターを選択します。

2. **操作 > ホスト名の変更**を選択します。

ホスト名の変更パネルが開きます。

3. 新しいホスト名フィールドに、ホストの新しい名前を入力します。

ホスト名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , . < \ を含めることはできません。他のホストによって名前が使用されている場合には、別の名前を入力するように指示されます。

4. **OK** をクリックします。

ホストテーブルが更新されます。

ホストグループへのホストの追加

既存のホストを、既存のホストグループまたは新規ホストグループに追加できます。

ホストグループにホストを追加するには、そのホストのマッピングが、グループの他のすべてのメンバーと同じでなければなりません。ホストは、同じアクセス設定、ポート設定、および LUN 設定によって、同じボリュームまたはボリュームグループにマップされている必要があります。

手順

1. ホストトピックで、ホストグループに追加したいホストに所属する 1~256 のイニシエーターを選択します。

2. **操作 > ホストグループへの追加**を選択します。

ホストグループへの追加パネルが開きます。

3. 次のいずれかを実行します。

- ・ 既存のホストグループを使用する場合は、ホストグループの選択リストでその名前を選択します。
- ・ ホストグループを作成する場合は、ホストグループの選択フィールドにホストグループの名前を入力します。ホストグループ名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , < \ を含めることはできません。

4. **OK** をクリックします。

選択したホストについて、グループ値が--から、指定したホストグループ名に変わります。

ホストグループからのホストの削除

最後のホストを除くすべてのホストを、ホストグループから削除できます。ホストグループからホストを削除すると、そのホストはグループ解除されますが削除はされません。ホストグループを削除するには、ホストグループの削除を参照してください。

手順

1. ホストトピックで、ホストグループから削除する 1~256 のホストを選択します。

2. **操作 > ホストからの削除**を選択します。

[ホストグループからの削除] パネルが開き、削除するホストがリストされます。

3. **OK** をクリックします。

選択したホストについて、グループ値が--に変わります。

ホストグループの削除

ホストグループを削除することができます。ホストグループを削除するとそのホストはグループ解除されますが、削除はされません。

手順

1. ホストトピックで、削除する 1~32 のホストグループを選択します。
2. **操作 > ホストグループ名の変更**を選択します。
ホストグループの削除パネルが開き、削除するホストグループがリストされます。
3. **OK** をクリックします。
選択したホストグループに含まれていたホストについて、グループ値が--に変わります。

ホストグループ名の変更

ホストグループ名を変更します。

手順

1. ホストトピックで、名前を変更するホストグループを選択します。
2. **操作 > ホストグループ名の変更**を選択します。
ホストグループ名の変更パネルが開きます。
3. 新しいホストグループ名フィールドに、そのホストグループの新しい名前を入力します。
ホストグループ名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , . < \ を含めることはできません。他のホストグループによって名前が使用されている場合には、別の名前を入力するように指示されます。
4. **OK** をクリックします。
ホストテーブルが更新されます。

チャレンジハンドシェイク認証プロトコル (CHAP)

iSCSI では、CHAP (チャレンジハンドシェイク認証プロトコル) を使用して、ログイン要求のイニシエーターとターゲット間で認証を行うことができます。この識別を実行するには、イニシエーターとターゲットに CHAP レコードのデータベースが存在する必要があります。各 CHAP レコードは、イニシエーターだけを認証する (単方向 CHAP) 場合は 1 つ、イニシエーターとターゲットの両方を認証する (相互 CHAP) 場合は 2 つの名前 - シークレットペアを指定できます。iSCSI ホストからコントローラー iSCSI ポートへのログインリクエストの場合は、ホストがイニシエーターで、コントローラーポートがターゲットです。

CHAP が有効で、ストレージシステムが既知の送信者 (イニシエーター) からのログインリクエストの受信者である場合、システムは既知のシークレットを要求します。発信元がそのシークレットを提供すると、接続が許可されます。

CHAP がピア接続されているシステムで使用され、複製で使用される場合には、特別な考慮事項があります。ピア接続では、ストレージシステムはログインリクエストの送信者または受信者として機能できます。送信者として、有効な CHAP レコードによって、CHAP が無効な場合でも CHAP を認証できます。システムがピアの要求する CHAP シークレットを提供し、接続が許可されるため、これが可能になります。

CHAP レコードの追加または変更手順

1. 双方向 CHAP を使用する予定で、コントローラー iSCSI ポートの IQN を確認する必要がある場合は、以下を実行します。

- a. システムトピックを選択します。
 - b. 背面側ビューを選択します。
 - c. 使用したい iSCSI ホストポートにカーソルを合わせます。ポート情報パネルが表示されたら、ID フィールドの値の IQN をメモしてください。
2. ホストトピックで、**操作 > CHAP の設定**を選択します。[CHAP の設定] パネルが開き、既存の CHAP レコードがリストされます。
 3. **認証 (CHAP) の有効化**チェックボックスを選択して、すべての iSCSI ノードで CHAP の使用を有効にし、操作を確認します。

注記: ここで CHAP を有効または無効にすると、[ホストポート設定] パネルの**詳細設定**タブの設定が更新されます。

4. 次のいずれかを実行します。
 - ・ 既存のレコードを変更するには、それを選択します。レコードの値が、編集する CHAP レコードのリストの下フィールドに表示されます。IQN は編集できません。
 - ・ 新しいレコードを追加するには、**新規**をクリックします。
5. 新しいレコードの場合、ノード名 (IQN) フィールドに、イニシエーターの IQN を入力します。値には大文字と小文字の区別があり、最大長は 223 バイトです。0~9、小文字の a~z、ハイフン、コロン、ピリオドを使用できます。
6. シークレットフィールドで、ターゲットがイニシエーターの認証に使用できるシークレットを入力します。このシークレットでは大文字と小文字が区別され、最大 12~16 バイトを指定できます。値には、" <を除くスペースおよび印字可能な UTF-8 文字が使用できます。
7. 相互 CHAP を使用する手順
 - ・ **相互 CHAP** チェックボックスにチェックを入れます。
 - ・ **相互 CHAP 名**フィールドに、手順 1 で取得した IQN を入力します。この値では、大文字と小文字が区別されます。最大 223 バイトで、0~9、小文字の a~z、ハイフン、コロン、およびピリオドを使用できます。
 - ・ **双方向 CHAP シークレット**フィールドで、イニシエーターがターゲットの認証に使用できるシークレットを入力します。シークレットでは大文字小文字が区別され、最大 12~16 バイトで指定できます。また、イニシエータのシークレットとは異なる必要があります。値には、" <を除くスペースおよび印字可能な UTF-8 文字が使用できます。ストレージシステムのシークレットは、両方のコントローラーで共有されます。
8. **適用**または **OK** をクリックします。CHAP レコードのテーブルが更新されます。

CHAP レコードを削除する手順

△ 注意: CHAP レコードを削除すると、ボリュームがアクセス不可になり、それらのボリューム内のデータが使用できなくなる可能性があります。

1. ホストトピックで、**操作 > CHAP の設定**を選択します。[CHAP の設定] パネルが開き、既存の CHAP レコードがリストされます。
2. 削除するレコードを選択します。

3. **削除**を選択します。確認パネルが表示されます。
4. **削除**を選択します。あるいは、**キャンセル**を選択します。[削除]を選択すると、CHAP レコードが削除されます。

仮想ボリュームの作成

仮想プールにはボリュームを追加できます。個別に仮想ボリュームを作成したり、さまざまな設定で複数の仮想ボリュームを作成したり、同じ設定で複数の仮想ボリュームを作成することができます。最後のケースの場合、ボリュームには同じベース名が付き、0000 から始まる数値サフィックスが続いてそれぞれの名前が固有になり、同じプールに配置されます。ボリューム階層の親和性設定を選択して、ボリュームデータの階層を指定することもできます。

手順

1. 次のいずれかを実行します。

- ・ プールトピックのプールテーブルで仮想プールを選択し、**操作 > 仮想ボリュームの作成**の順に選択します。
- ・ ボリュームトピックで、**操作 > 仮想ボリュームの作成**の順に選択します。

仮想ボリュームの作成パネルが開き、各プールの現在の容量の使用率が表示されます。

注記: 仮想プールが存在しない場合、仮想ボリュームを作成するオプションは利用できません。

2. オプション: ボリューム名を変更します。デフォルトは Voln です。n は 0001 から始まり、デフォルト名が付いたボリュームごとに 1 ずつ増加します。ボリューム名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , < \ を含めることはできません。

その名前が別のボリュームによって使用されている場合、その名前は固有になるように自動的に変更されます。たとえば MyVolume は MyVolume0001 に、Volume2 は Volume3 に変更されます。

3. オプション: ボリュームサイズを測定単位も含めて変更します。MiB、GiB、TiB、MB、GB、TB のうちいずれかの単位を使用できます。デフォルトサイズは 100GB です。システムでサポートされる最大ボリュームサイズについては、SMU ヘルプのシステム構成の制限に関するトピックを参照してください。ボリュームサイズは、4.2MB (4MiB) 境界にアライメントされます。ボリュームが作成または拡張される場合、作成または拡張後のサイズが 4.2MB 未満のときは、4.2MB に増やされます。4.2MB より大きな値は、最も近い 4.2MB 境界まで減らされます。
4. オプション: 作成するボリュームの数を変更します。デフォルトは 1 です。プールごとにサポートされるボリュームの最大数については、SMU ヘルプのシステム構成の制限に関するトピックを参照してください。
5. オプション: ボリューム階層の親和性設定を指定し、ボリュームデータを自動的に特定の階層に関連付けて、可能な場合は常にすべてのボリュームデータをその階層に移動するようにします。デフォルトは **アフィニティなし** です。
6. オプション: ボリュームを作成するプールを選択します。プール間でボリュームの負荷分散が行われるため、デフォルトでは、A と B のうちボリュームが少ない方になります。
7. オプション: 異なる設定で別のボリュームを作成するには、**行の追加**をクリックし、設定を変更します。カーソルがある行を削除するには、**行の削除**をクリックします。
8. **OK** をクリックします。

ボリュームの作成によってプール容量がオーバーコミットされる場合は、イベント通知を設定して、プールで物理ストレージが不足する前に警告するように要求されます。

9. 仮想ボリュームが容量を超える場合は、次のように操作します。

- a. はいをクリックして次に進みます。続行しない場合はいいえをクリックします。はいをクリックした場合は、ボリュームが作成されてボリュームテーブルが更新されます。
- b. 確認パネルを閉じるには、OK をクリックします。

HPE 3PAR アレイへの接続時に監視ディスク（仮想ボリューム、最小 600 MB）またはその他の仮想ボリュームを準備する

3PAR StoreServ アレイの監視ディスクをプロビジョニングできます。

前提条件

アレイ情報を保存フィールドを使用して、ストレージアレイが構成済みであることを確認します。詳細については、「[アレイ管理ログイン詳細の設定](#)」を参照してください。

手順

1. 監視ディスク（最小 600 MB）に使用する仮想ボリュームまたはその他の仮想ボリュームを準備するをクリックして、3PAR StoreServ 管理コンソール（SSMC）のログインウィンドウを起動します。
2. 必要なログイン認証情報を入力します。
3. 以下のいずれかの操作を実行します。
 - ・ ホストの作成
 - ・ 仮想ボリュームの作成
 - ・ 仮想ボリュームのエクスポート

ホストの作成

フィールドにマウスカーソルを重ねると、ツールヒントが表示されます。

全般

必須またはオプションの設定に対して、選択肢を入力または選択します。

パス

ホストパスを追加するには、**FC の追加**または**iSCSI の追加**をクリックし、表示されたダイアログの指示に従います。リストからパスを削除するには、その削除アイコン (X)。

Smart SAN パスを編集するには、編集アイコン (✎) をクリックし、表示されたダイアログの指示に従います。

CHAP 設定

iSCSI ホストでは、CHAP セキュリティ設定の選択肢を入力します。

追加設定

ホストのオプション情報を入力するには、**記述子展開アイコン** (▶) をクリックします。

選択が完了したら、**作成**をクリックし、アクションを開始してダイアログを閉じるか、または**作成 +**をクリックし、アクションを開始してダイアログを開いたままにします。

仮想ボリュームの作成

フィールドにマウスカーソルを重ねると、ツールヒントが表示されます。

ヒント：ダイアログの上部にある**詳細オプション**チェックボックスを選択すると、CPG の割り当て警告と割り当て制限（サポートされている場合）オプション、および仮想ボリュームの**特殊属性**オプションを指定することができます。

全般

必須およびオプションの設定に対して、選択肢を入力または選択します。

保護と追加設定

ボリューム

コピー CPG、ボリューム数、およびボリュームセットなどの設定を指定するには、**ボリューム展開**アイコン（▶）をクリックします。

スナップショット

作成済みのポリシーからスナップショットポリシーを選択するには、**スナップショット展開**アイコン（▶）をクリックします。スナップショットポリシーは、ポリシー名、スケジュール、保持期間、有効期限、および名前パターンを指定します。利用可能なデフォルトポリシーは、**毎時**、**日次**、および**週次**です。

すでにスナップショットポリシーが直接割り当てられている仮想ボリュームセットの一部である仮想ボリュームにスナップショットポリシーを割り当てようとすると、警告メッセージが表示されます。

Remote Copy グループ

仮想ボリュームを追加する必要がある Remote Copy グループを表示するには、**Remote Copy グループ**展開アイコン（▶）をクリックします。ドロップダウンに、RC グループ名、モード、および構成が表示されます。仮想ボリュームにターゲットアレイが割り当てられていない場合、表示する Remote Copy グループはありません。

RMC 保護

使用可能なポリシーから、関連付けられた仮想ボリュームの保護ポリシーを指定できます。**RMC 保護**ドロップダウンはデフォルトで展開されます。

ポリシーの追加をクリックし、表示されたダイアログの手順に従います。

エクスポート

仮想ボリュームの作成時にホストへ新しい仮想ボリュームをエクスポートするには、**エクスポート展開**アイコン（▶）をクリックし、**追加**をクリックして、表示されたダイアログの指示に従います。

特殊属性

仮想ボリュームのボリューム ID を指定する、失効したスナップショット、1 ホスト限定のエクスポート、ゼロ検出、保持時間、および有効期限などのオプションを有効または無効にするは、**特殊属性展開**アイコン（▶）をクリックします。

詳細オプションに対して、選択肢を入力または選択できます。

選択が完了したら、**作成**をクリックし、アクションを開始してダイアログを閉じるか、または**作成 +**をクリックし、アクションを開始してダイアログを開いたままにします。

仮想ボリュームのエクスポート

フィールドにマウスカーソルを重ねると、ツールヒントが表示されます。

全般

このパネルには、仮想ボリューム画面で選択された仮想ボリュームのストレージシステムおよび仮想ドメインが表示されます。

仮想ボリューム

仮想ボリューム画面で選択された仮想ボリュームは、このパネルにリストされます。

エクスポート先

エクスポート先のホストまたはホストセットを選択するには、このパネルの**追加**をクリックし、表示されたダイアログの指示に従います。

次と共にエクスポート

LUN ボックスの LUN 値を受け入れるかまたは選択します。または、**自動**チェックボックスを選択します。

- ・ 1つのホストへ1つの仮想ボリュームをエクスポートする場合、次に利用可能な LUN が **LUN** ボックスに表示されます。
- ・ 複数の仮想ボリュームをエクスポートする場合、次に利用可能な LUN 範囲が **LUN** ボックスに表示されます。
- ・ 別の LUN または LUN 範囲を指定するには、リストから1つまたは複数の LUN を選択します。また、LUN 番号を1つ入力することも、カンマで区切った LUN 番号（例: 1, 2, 3）を入力することも、またはダッシュを使用して LUN 範囲（例: 1-5）を入力することもできます。

自動オプションの使用

- ・ 自動オプションを指定して複数のホストにエクスポートすると、各仮想ボリュームは、各ホストの、異なる LUN に割り当てられます。
- ・ 自動オプションを指定せずに複数のホストにエクスポートすると、各仮想ボリュームは、各ホストの、同じ LUN に割り当てられます。

選択が完了したら、**エクスポート**をクリックし、アクションを開始してダイアログを閉じます。

監視ディスクボリュームまたは他のディスクボリュームのプロビジョニング

監視ディスクは、実際のディスクで、クラスターに共通のディスクストレージによって用意されます。ノードは、ディスクへの排他的アクセスを調整します。このディスクには、クラスター構成データが格納されます。

ディスクの管理を起動するには、このリンクをクリックします。マップした仮想ディスク上にボリュームを作成できます。

Nimble アレイ用 HPE ストレージファイルコントローラーでのストレージアレイの構成

ストレージアレイの構成タスクグループでは、HPE ストレージファイルコントローラーと Nimble アレイ間の通信プロトコルを確立できます。このストレージ構成により、Nimble Storage ボリュームを Windows ボリュームとしてプロビジョニングすることができます。

タスクには以下が含まれます。

- ・ [イニシエーターグループの作成とグループへのホストの割り当て](#)
- ・ [Nimble アレイボリュームのプロビジョニング](#)
- ・ [Windows ボリュームのプロビジョニング](#)

イニシエーターグループの作成とグループへのホストの割り当て

イニシエーターは、HPE ストレージファイルコントローラー上のポートで、Nimble アレイ上のターゲットポートとの接続を開始します。イニシエーターは、iSCSI ファブリックを介して1つ以上のターゲットポートへの接続を開始する Ethernet ネットワークインターフェイスカード（NIC）ポート、またはファイバーチャネルファブリックを介して1つ以上のターゲットポートへの接続を開始するファイバーチャネルホストバスアダプター（HBA）ポートです。

イニシエーターグループは、単一ユニットとして管理される iSCSI イニシエーターまたはファイバーチャネルイニシエーターの集合です。HPE ストレージファイルコントローラーをクラスターに設定する場合は、すべてのノードの適切なポートをすべて同じイニシエーターグループに設定してください。

注記: FC および iSCSI イニシエーターグループは、HPE ストレージファイルコントローラーに接続されている Nimble 管理グループのタイプに基づいて自動で選択されます。

手順

1. ウィンドウの**ストレージアレイの構成 > イニシエーターグループ**を作成し、ホストをグループに割り当てをクリックします。
2. **イニシエーターグループの作成**フィールドにイニシエーターグループの名前を入力します。
名前の割り当てには、最大 64 個の英数字を使用できます。2 番目以降の文字にはハイフン (-) とピリオド (.) を使用できます。たとえば、myobject-5 のように指定できます。名前にアンダースコア記号は使用しないでください。
3. 各イニシエーターの**エイリアス**セクションに代替名を入力します。
4. ファイバーチャネルイニシエーターグループの場合は、**WWPN** ドロップダウンリストからワールドワイドポート名 (WWPN) を選択します。iSCSI イニシエーターグループの場合は、IP アドレスを入力し、**IQN** ドロップダウンメニューから **IQN** を選択します。
5. **列を追加**をクリックして列を追加するか、**列を削除**をクリックして列を削除します。
エイリアスまたは名前には最大 10 行を追加できます。IQN/WWPN 番号に基づいて、イニシエーターグループにエイリアスを追加できます。
6. **イニシエーターグループを作成**をクリックします。
イニシエーターグループが作成されましたというメッセージが表示されます。
7. **OK** をクリックして終了します。

ファイバーチャネルイニシエーターグループ

ファイバーチャネルイニシエーターグループは、1 つ以上のイニシエーターの集合で、それぞれのイニシエーターには固有のワールドワイドポート名 (WWPN) があります。各 WWPN は、ファイバーチャネルベースのクライアント上にある 1 つのホストバスアダプター (HBA) ポートを Windows サーバー、ESXi、または Linux ホストの形式で表します。Nimble アレイでファイバーチャネルイニシエーターグループを構成します。

注記: デフォルトでは、ファイバーチャネルボリュームはイニシエーターへのアクセスを拒否します。イニシエーターグループ内のイニシエーターがボリュームにアクセスできるようにするには、目的のイニシエーターを含む ACL を設定し、ボリュームに接続する必要があります。

iSCSI イニシエーターグループ

iSCSI イニシエーターグループは、1 つ以上の iSCSI イニシエーターの集合で、それぞれのイニシエーターに固有の iSCSI 修飾名 (IQN) と IP アドレスがあります。各 IQN は、iSCSI ベースのクライアント上にある単一のネットワークインターフェイスカード (NIC) を Windows サーバー、ESXi、または Linux ホストの形式で表します。Nimble アレイに iSCSI イニシエーターグループを設定し、ベンダーの推奨に従って、クライアント側の iSCSI イニシエーターを設定します。

注記: デフォルトでは、iSCSI ボリュームはイニシエーターへのアクセスを拒否します。イニシエーターグループ内のイニシエーターがボリュームにアクセスできるようにするには、目的のイニシエーターを含む ACL を設定し、ボリュームに接続する必要があります。

Nimble アレイボリュームのプロビジョニング

1. **ストレージレイの構成 > Nimble アレイボリュームをプロビジョニングする**をクリックします。
2. **作成または既存のボリュームを使用する**を選択します。
3. **名前セクション**に、ボリュームの名前を入力します。
英字（大文字と小文字）、数字、およびアンダースコア（_）を使用できます。他の特殊文字は使用しないでください。
4. **説明セクション**に説明を入力します。
テキスト内にスペースがある場合は、テキストを引用符で囲んでください。
5. **場所**ドロップダウンメニューから、場所を選択します。
6. **パフォーマンスポリシー**ドロップダウンメニューから、パフォーマンスポリシーのタイプを選択します。
パフォーマンスポリシーは、特定のアプリケーションのパフォーマンスを最適に設定するためのものです。パフォーマンスポリシーは、ボリュームを使用するアプリケーションの期待される特性に基づいて、ボリュームのパフォーマンスを最適化するのに役立ちます。パフォーマンスポリシーでは、クォータを超えたときの、関連するボリュームの動作を定義します。既存のパフォーマンスポリシーとボリュームを関連付けることができます。
7. ボリュームのサイズは、MiB、GiB、または TiB で指定します。
サイズはゼロより大きい値でなければなりません。
8. **データ保護**ドロップダウンメニューから、データ保護のタイプを選択します。
 - ・ **ボリュームコレクションがありません**：ボリュームのスナップショットは作成されません。
 - ・ **ボリュームコレクションに参加**：既存のボリュームコレクションのルールを選択して、このボリュームに適用します。
 - ・ **新しいボリュームコレクションを作成**：このボリュームのボリュームコレクションのルールを作成します。
9. **アクセス**ドロップダウンメニューからアクセスのタイプを選択して、ボリュームをストレージファイルコントローラーと接続します。
10. （オプション）**ボリュームのキャッシュフィールド**で、**ピン留め済み**または**通常**のいずれかを選択します。
ピン留め済みを選択すると、
キャッシュは、共有リソースです。ボリュームをピン留めすると、ボリュームのパフォーマンスに影響を及ぼす可能性があります。この設定は、最大のパフォーマンスが必要なワークロードに対してのみ使用してください。というメッセージが表示されます。
11. **作成**をクリックします。
メッセージボリュームが正常に作成されましたが表示されます。
12. **OK** をクリックします。

Nimble アレイボリュームのプロビジョニング

1. **ストレージレイの構成 > Nimble アレイボリュームをプロビジョニングする**をクリックします。
2. **作成または既存のボリュームの使用**を選択します。
3. **名前セクション**に、ボリュームの名前を入力します。

英字（大文字と小文字）、数字、およびアンダースコア（_）を使用できます。特殊文字は使用しないでください。

4. **説明セクション**に説明を入力します。
テキスト内にスペースがある場合は、テキストを引用符で囲んでください。
5. **場所**ドロップダウンメニューから、場所を選択します。
6. **パフォーマンスポリシー**ドロップダウンメニューから、パフォーマンスポリシーのタイプを選択します。
パフォーマンスポリシーは、特定のアプリケーションのパフォーマンスを最適に設定するためのものです。パフォーマンスポリシーは、ボリュームを使用するアプリケーションの期待される特性に基づいて、ボリュームのパフォーマンスを最適化するのに役立ちます。パフォーマンスポリシーでは、クォータを超えたときの、関連するボリュームの動作を定義します。既存のパフォーマンスポリシーとボリュームを関連付けることができます。
7. ボリュームのサイズは、MiB、GiB、または TiB で指定します。
サイズはゼロより大きい値でなければなりません。
8. **データ保護**ドロップダウンメニューから、データ保護のタイプを選択します。
 - ・ **ボリュームコレクションがありません**：ボリュームのスナップショットは作成されません。
 - ・ **ボリュームコレクションに参加**：既存のボリュームコレクションのルールを選択して、このボリュームに適用します。
 - ・ **新しいボリュームコレクションを作成**：このボリュームのボリュームコレクションのルールを作成します。
9. **アクセス**ドロップダウンメニューからアクセスのタイプを選択して、ボリュームをストレージファイルコントローラーと接続します。
10. （オプション）**ボリュームのキャッシュフィールド**で、**ピン留め済み**または**通常**のいずれかを選択します。
ピン留め済みを選択すると、
キャッシュは、共有リソースです。ボリュームをピン留めすると、ボリュームのパフォーマンスに影響を及ぼす可能性があります。この設定は、最大のパフォーマンスが必要なワークロードに対してのみ使用してください。というメッセージが表示されます。
11. **作成**をクリックします。
メッセージ「ボリュームが正常に作成されました」が表示されます。
12. **OK** をクリックします。

Nimble 用ストレージでの Windows ボリュームのプロビジョニング

Nimble アレイを使用すると、ボリュームがプロビジョニングされ、Windows OS に raw ディスクとして提供されます。Windows ボリュームは、データの格納に使用する前に、このディスクに作成する必要があります。**Windows ボリュームをプロビジョニングするオプション**を使用すると、以下のことが可能になります。

- ・ ディスクの初期化
- ・ ファイルシステムによるディスクのフォーマット
- ・ シンプルボリュームの作成
- ・ ディスクのドライブ文字の指定

手順

1. ストレージアレイの構成 > Windows ボリュームをプロビジョニングするをクリックします。
ディスクの管理コンソールが表示されます。
2. 使用可能なディスクのいずれかを右クリックします。
新しいシンプルボリューム画面が表示されます。
3. 新しいシンプルボリューム画面でボリュームのサイズを指定し、次へをクリックします。
4. 簡単にアクセスするためのドライブ文字またはパスを指定し、次へをクリックします。
5. ファイルシステムと割り当てユニットサイズを選択し、ボリュームの名前を入力して、ボリュームをフォーマットしデータを格納します。
6. クイックフォーマットするを選択し、次へをクリックします。
新しいシンプルボリュームの完了画面が表示されます。
7. ボリュームが正常に作成されたら、完了をクリックします。
ICT のステータス列に、ステータスとパスが表示されます。

クラスタを構成する

Witness ディスクが検出されない場合、またはドメインが参加していない場合、クラスタ構成タスクは無効になります。クラスタタスクは次のとおりです。

- ・ クラスタの作成
- ・ クラスタに参加

クラスタ名の指定の要件

クラスタ名を割り当てるときは、次の点を確認します。

- ・ クラスタ名は最長で 15 文字です。
- ・ 名前に、\/*? <>| “などの特殊文字が含まれていないこと。
- ・ 名前が一意であること。ドメイン内の他のシステムまたはクラスタと同じ名前にすることはできません。

HPE 3PAR StoreServ および MSA アレイのクラスタの構成

前提条件

- ・ ファイルコントローラーがドメインに接続されていることを確認します。
- ・ ドメインユーザーの認証情報でファイルコントローラーにログインしていることを確認します。
- ・ Witness ディスクが構成されていることを確認します。

手順

1. クラスタ名を指定するフィールドでクラスタ名を指定します。
2. ノードの検証またはクラスタの作成をクリックします。

ノードでクラスタをホストできるようになっている場合は、ノードの検証オプションを使用します。

クラスターの作成

クラスター名の指定の要件については、クラスター名の指定の要件を参照してください。

手順

1. ICT のクラスターを構成するタスクグループで、**クラスターの作成**をクリックします。
クラスター構成ツールが起動します。
2. クラスター名を**クラスター名を指定する**に入力します。
3. (オプション) **クラスターの検証**をクリックして、ノードを検証します。
4. **クラスターの作成**をクリックします。
クラスターが正常に作成されましたメッセージが表示されます。

クラスターへの参加

クラスター名の指定の要件については、クラスター名の指定の要件を参照してください。

手順

1. ICT のクラスターを構成するタスクグループで、**クラスターに参加**をクリックします。
クラスター構成ツールが起動します。
2. クラスター名を**クラスター名を指定する**に入力します。
3. **ノードの検証**をクリックして、ノードを検証します。
4. **クラスターに参加**をクリックして、ノードをクラスターに参加させます。
クラスターに正常に参加しましたメッセージが表示されます。

HPE Nimble Storage アレイのクラスターの構成

監視ディスクの準備 (Nimble)

Nimble ボリュームが作成され、イニシエーターグループが HPE ストレージファイルコントローラーに割り当てられます。

600 MB の最小サイズのボリュームを作成します。Hewlett Packard Enterprise では、ボリュームの目的を簡単に識別できるように、ボリュームに **Quorum** または **Witness** の名前を付けることをお勧めします。Windows でドライブをフォーマットする場合、**W** または **Q** をドライブ文字として割り当てることができます。ただし、他のファイル共有リソース用のボリュームが必要な場合、ドライブ文字を入力する必要はありません。

クラスターの作成

クラスター名の指定の要件については、クラスター名の指定の要件を参照してください。

手順

1. ICT のクラスターを構成するタスクグループで、**クラスターの作成**をクリックします。
クラスター構成ツールが起動します。
2. クラスター名を**クラスター名を指定する**に入力します。
3. (オプション) **クラスターの検証**をクリックして、ノードを検証します。
4. **クラスターの作成**をクリックします。

クラスターが正常に作成されましたメッセージが表示されます。

クラスターへの参加

クラスター名の指定の要件については、クラスター名の指定の要件を参照してください。

手順

1. ICT のクラスターを構成するタスクグループで、**クラスターに参加**をクリックします。
クラスター構成ツールが起動します。
2. クラスター名を**クラスター名を指定する**に入力します。
3. **ノードの検証**をクリックして、ノードを検証します。
4. **クラスターに参加**をクリックして、ノードをクラスターに参加させます。
クラスターに正常に参加しましたメッセージが表示されます。

このサーバーの保護

ご使用のサーバーを保護できます。

- ・ 自動更新を有効にする
- ・ ディザスタ管理とリカバリを確保する

自動更新を有効にする

オペレーティングシステムのアップデートは、Windows 更新プログラムにより簡素化されているため、時間を節約できます。Windows Update の各機能は、ローカルコンピューターの管理者による設定が可能です。**自動更新を有効にする**のリンクをクリックすると、**Windows 更新プログラムの設定**ダイアログボックスが開きます。**更新プログラムの設定の詳細**オプションをクリックし、Windows 更新プログラムのダウンロードおよびインストール方法を選択します。

Hewlett Packard Enterprise では、更新が適用されるように、以下の作業を行うことをお勧めします。詳細オプションを開いて Windows 更新プログラムを実行する場合、Microsoft 製品の更新方法の構成が可能です。

- ・ 予期しないシステムの再起動を回避するため、自動更新は選択しないでください。
- ・ **重要な更新プログラム**で次のいずれかのオプションを選択します。
 - **更新プログラムのダウンロードのみ、Windows 更新プログラムを使用するが、インストールするかどうかは選択する（デフォルトオプション）**
 - **更新プログラムを確認するが、ダウンロードとインストールを行うかどうかは選択する**
- ・ 推奨される更新プログラムで、**推奨される更新プログラムについても重要な更新プログラムと同様に通知する**を選択します。
- ・ クイックリストアプロセスが終了したらすぐに**更新プログラムのダウンロードとインストール**を実行します。

Subscriber's Choice を使用して、Hewlett Packard Enterprise のカスタマーアドバイザーに登録します。HPESC で利用できるシステムの情報に基づいて、ファームウェアと関連デバイスドライバーが最新であることを確認してください。

通常のストレージファイルコントローラーのサービスリリースを適用します。

Carbonite ソフトウェア

Carbonite ポートフォリオには、障害回復と高可用性に対応するレプリケーションソフトウェアが含まれています。このリンクをクリックすると、Double-Take Availability ソフトウェアのトライアルバージョンのインストールについて表示する HTML ページが開きます。このトライアルバージョンにより、ご使用の環境でこのソフトウェアを評価することができます。デスクトップにある **Carbonite ソフトウェア** アイコンをダブルクリックすることで、HTML ページに直接アクセスすることもできます。

クラスターノードの構成

クラスターノードの ICT タスクは、単一ノードのタスクと似ています。ただし、クラスターノードの場合は、プライマリノードでのみタスクを実行する必要があり、クラスター内の他のノードでは自動的にタスクが実行されます。

単一ノードをクラスターに変換すると、デフォルトで、クラスター内のすべてのノードで ICT ウィンドウが起動します。後で ICT を起動する場合は、Windows 実行コマンドプロンプトに、`C:\Windows\System32\oemooobe \oemooobe.exe` コマンドを入力します。

接続ステータス

2 ノードクラスターを作成する場合に、ストレージファイルコントローラーの電源を投入すると、第 1 ノードが第 2 ノードを検出します。このデフォルト接続は、2 つのノード間に物理的な接続が存在する場合にのみ発生します。システムの接続の図に示すように、各ノードにケーブルを物理的に接続する必要があります。デフォルト接続が発生せず、第 2 ノードが見つかりませんというメッセージが表示される場合は、ノードが正しく接続されているかどうかを（システムの接続の図に従って）確認してください。



図 2: システムの接続

接続ステータスオプションを使用して、セカンダリノードの IP アドレスを再入力します。

第 2 ノードへの接続

第 2 ノードの IP アドレスを確認するには、以下の手順に従ってください。

手順

1. ブラウザーを使って、iLO を搭載した第 2 ノードへのリモートコンソールを開きます。システムへの iLO アクセスについて詳しくは、お手持ちのクイックスタートガイドまたは管理者ガイドを参照してください。
2. システムの管理者パスワード（デフォルトでは HPEStorage!）を使って、第 2 ノードの Windows にログインします。
3. デスクトップのスタート画面から **コントロールパネル > ネットワークとインターネット > ネットワークと共有センター** を順に選択します。

注記: Windows Storage Server 2016 では、Windows のアイコンが最下部のタスクバーに表示されます。スタート画面にアクセスするには、左下にある、タスクバー内の Windows アイコンをクリックします。画面下部にある下向き矢印をクリックすると、スタート画面から利用可能なすべてのメニューおよびアプリケーションが表示されます。キーボードの **Windows** キーを押しても、スタート画面にアクセスできます。

4. **アクティブなネットワークの表示** セクションで、**内部クラスター** を選択します。
5. **詳細** をクリックします。

6. ネットワーク接続の詳細の IP アドレスを書き留めます。この IP アドレスを使って、第 2 ノードに手動で接続します。

注記: IP アドレスが静的にまたは DHCP を介して割り当てられていない限り、アドレスは 169.254.0.1 ~ 169.254.255.254 の、自動プライベート IP アドレス指定 (APIPA) の IP アドレスが使用されます。

7. ICT で第 2 ノードに手動で接続するには、以下の手順に従ってください。

- a. 第 2 ノードに接続をクリックします。

リモートノードへの接続ダイアログボックスが表示されます。

- b. 第 2 ノードの IP アドレスを入力し、適用をクリックします。

トラブルシューティングの詳細については、[トラブルシューティング](#)を参照してください。

注記:

- ・ Windows Storage Server 2016 では、複数の IP アドレスを入力することができます。Hewlett Packard Enterprise では、ICT による 2 ノードクラスターの作成のみをサポートします。クラスターのメンバーとなる第 2 ノードのアドレスのみを入力してください。
 - ・ クラスター内 (ハートビート) ネットワークでは IPV6 対応のままにしておくことをお勧めします。
-

ネットワークング

ネットワークの IP アドレスと HPE ストレージファイルコントローラーのドメインを設定します。以下のタスクを実行できます。

- ・ [ネットワークの構成](#)
- ・ [クラスター名とドメインの入力](#)

ネットワークの構成

ネットワーク構成ツールに従って設定していくと、ネットワークチームの構成、VLAN の割り当て、およびネットワークインターフェイス構成のプロセスを実行できます。ネットワーク構成ツールは、プライマリとリモートの両方のノードのネットワークインターフェイスを構成するツールです。

- ・ [ネットワークインターフェイスの設定](#)
- ・ [ネットワークチームの構成](#)
- ・ [ネットワークの VLAN の構成](#)
- ・ [ネットワークインターフェイスの IP 構成](#)
- ・ [ネットワーク構成の概要](#)
- ・ [ネットワーク構成の検証](#)
- ・ [ネットワーク構成のインポート](#)

手順

1. ネットワーク構成ツールを起動するには、ICT ウィンドウでネットワークの構成をクリックし、次へをクリックします。

あるいは、以下のいずれかの方法で NCT を起動します。

- ・ コマンドプロンプトまたは PowerShell を開き、NCT と入力する。
- ・ デスクトップのシステムツールフォルダーをダブルクリックし、**ネットワークの構成**を選択する。
- ・ スタート画面の**ネットワークの構成**をクリックする。
- ・ デスクトップにある**ネットワークの構成**アイコンをクリックする。
- ・ (Nimble アレイの場合) サーバーマネージャーを開き、**ツール > Nimble > ネットワークの構成**の順に選択する。

2. 変更内容を保存して適用するには、**適用**をクリックします。

ネットワークインターフェイスの設定

物理ネットワーク インターフェイスを構成するには、以下の手順に従ってください。

手順

1. 構成対象のインターフェイスの**構成**チェックボックスを選択します。チェックボックスをクリアすると、このインターフェイスはすべての構成から除外され、変更されません。

注記: リモートデスクトッププロトコルに使用される物理ネットワークインターフェイスは、チームの一部として構成できません。このようなインターフェイスは、**構成**チェックボックスが無効になっています。

2. 新しいインターフェイス名を入力します。入力する新しい名前には、\/*?<>|や"などの特殊文字を含めることはできません。
3. **次へ**をクリックして、**ネットワークチームの構成**画面に進みます。

ネットワークチームの構成

注記:

ネットワークチームの構成はオプションです。ネットワークチームを作成しない場合は、**ネットワークチームを今すぐ構成しない**を選択し、**次へ**をクリックして、[ネットワークの VLAN の構成]に進みます。

ネットワークチームの構成画面は、既存のチームが存在しない場合にのみ表示されます。ネットワークチームを使用すると、利用可能な帯域幅を増やしたり、フォールトトレランスとロードバランシングを改善したりできます。

作成できるチームの最大数は、システム上の物理ネットワークインターフェイスの数と同じです。

手順

1. **ネットワークチームを今すぐ構成**を選択し、作成するチームの数を**チームの数**セクションに入力します。
2. **次へ**をクリックします。
3. **ネットワークインターフェイス**ウィンドウで物理ネットワークインターフェイスを選択し、**次へ**をクリックします。
4. **作成**チェックボックスを選択し、

- a. チーム名を入力します。
- b. タイプセクションからチームタイプを選択します。デフォルトのチームタイプは、**Switch Independent/Dynamic** です。

注記: 構成または削除の対象として表示されるチームの数は、作成するチーム数によって異なります。たとえば、構成用に 2 つのインターフェイスを選択すると、チームの作成のために 2 行表示されます。

5. **次へ**をクリックします。

現在どのチームにも含まれていないネットワークインターフェイスが表示されます。

6. 新しいチームに含めるネットワークインターフェイスを選択します。

作成するチームごとに、チームの一部ではない物理ネットワークインターフェイスを選択する個別のページが表示されます。

7. **次へ**をクリックして、**ネットワークの VLAN の構成**画面に進みます。

ネットワークの VLAN の構成

注記: VLAN 割り当ての構成はオプションです。VLAN 割り当てを構成しない場合は、デフォルトのチームインターフェイスのみが作成されます。**次へ**をクリックしてこの手順をスキップし、[ネットワークインターフェイスの IP 構成] 画面に進んでください。

デフォルトの VLAN ID は 0 ですが、VLAN ID の値には 0~4094 を使用できます。ネットワークチーム用に作成された物理インターフェイスと仮想インターフェイスの両方に VLAN ID を割り当てると、仮想ネットワークインターフェイスが作成されます。物理インターフェイスに VLAN ID が割り当てられた場合、チームは物理インターフェイス単独で作成されます。VLAN ID を持つ仮想インターフェイスは、その後でチーム内に作成されます。

注記: ネットワークチームの作成をスキップし、選択した物理インターフェイス上に VLAN を作成すると、(物理インターフェイス名) チーム - VLAN (VLAN ID) という名前のネットワークチームが自動的に作成されます。

手順

1. **VLAN ID を今すぐ構成**を選択して、**次へ**をクリックします。
2. 以下のオプションのいずれかを選択し、該当するフィールドに VLAN ID を入力します。
 - ・ **単一の VLAN ID を追加** — 単一の VLAN ID を追加します。
 - ・ **個別の VLAN ID を追加** — 複数の VLAN ID をカンマ区切り形式で追加します。
 - ・ **VLAN ID の範囲を追加** — 開始値および終了値に増分を使用して、VLAN ID を指定します。たとえば、開始値が 2、終了値が 20、増分が 5 の場合は、VLAN ID 2、7、12、および 17 が割り当てられます。
3. **デフォルトの仮想ネットワークインターフェイスを削除**チェックボックスを選択して、チームからデフォルトの仮想インターフェイスを削除します (オプション)。

注記: ネットワークチームを作成すると、デフォルトで仮想ネットワークインターフェイスも作成されます。デフォルトの仮想インターフェイスを削除した場合、物理ネットワークインターフェイスと仮想ネットワークインターフェイスに 1 つ以上の VLAN ID が割り当てられていない限り、ネットワークチームでも物理 NIC でもパケットを受信しません。

4. 次へをクリックして、ネットワークインターフェイスの IP 構成画面に進みます。

[ネットワークインターフェイスの IP 構成] に進むと、VLAN 割り当てがインターフェイスペインに表示されます。

注記: チームおよびアダプターへの VLAN ID 割り当て後にネットワークインターフェイスの VLAN ID を今すぐ構成しないを選択しても、割り当てられた ID は削除されません。チームの VLAN を構成しない場合は、各 VLAN ページを順に進み、すべてのチームおよびアダプターに対して **VLAN ID をこのチームに追加しない**を暗黙的に選択します。

ネットワークインターフェイスの IP 構成

ネットワークインターフェイスの IP 構成では、インターフェイスペインでインターフェイスを選択して IP アドレスを構成します。構成可能な各インターフェイスは、ツールが自動的に有効にします。割り当てられた IP アドレスは、静的でも、DHCP を使用して動的に割り当ててもかまいません。

注記: 両方のノード上のインターフェイスを、同じネットワークセグメントを使用するように構成することをお勧めします。たとえば、プライマリノードのネットワークインターフェイス 1 をセグメント 192.168.8.x に接続する場合は、リモートノードのネットワークインターフェイス 1 をネットワークセグメント 192.168.8.x に接続することをお勧めします。

手順

1. 次のいずれかを実行します。

- a. 動的 IP アドレスと静的 IP アドレスを割り当てるには、**IP アドレスとゲートウェイの割り当てに DHCP を使用する**を選択するか、**静的 IP アドレスとゲートウェイの割り当て**を選択します。

❗ **重要:** 静的 IP アドレスとゲートウェイの割り当てを選択する場合は、DNS サーバーのアドレスも静的でなければならず、ネットワークマスクを割り当てる必要もあります。デフォルトゲートウェイアドレスの割り当てはオプションです。

- b. DNS サーバーのアドレスの割り当てに DHCP を使用するまたは DNS サーバーの静的 IP アドレスの割り当てを選択します。前の手順で静的 IP アドレスとゲートウェイの割り当てオプションを選択した場合、DNS サーバーの静的 IP アドレスの割り当てがデフォルトで選択されており、変更することはできません。

この手順を繰り返して、他のネットワークインターフェイスを構成します。

Hewlett Packard Enterprise では、このウィンドウの**次へ**をクリックする前に、各インターフェイスを確認することをお勧めします。

2. 次へをクリックして、[ネットワーク構成の概要] 画面に進みます。

ツールは、IP アドレスとサブネットマスクを使用してゲートウェイを検証します。

ネットワーク構成の概要

[ネットワーク構成の概要] ウィンドウで、すべての構成変更を確認します。必要に応じて、**前へ**をクリックするか、ページの下部にあるナビゲーションリンクを使用して、構成を編集します。**適用**をクリックして、構成の変更を適用します。

次へをクリックして、構成された各タスクの詳細を表示します。エラーがある場合は、エラータブに表示されます。

構成が正常に変更されると、ネットワーク構成ファイル (NCTConfig.xml) が C:\Program Files\HPE\StoreEasy NetworkConfigurationWizard に自動的に作成されます。このファイルには、ネットワーク構成の詳細が含まれています。

物理ネットワークインターフェイスの構成が正常に行われたが、チームまたは VLAN の作成に失敗した場合は、NCTConfig.xml が引き続き作成されます。ただし、このファイルには物理ネットワークインターフェイスのみが含まれます。物理ネットワークインターフェイスのタスクが失敗した場合、NCTConfig.xml ファイルは作成されません。

このファイルを使用して、1つのストレージシステムから別のストレージシステムにネットワーク構成をインポートできます。ネットワーク構成のインポートに関する詳細については、「ネットワーク構成のインポート」を参照してください。

ネットワーク構成の検証

ネットワーク構成の検証画面を使用して、ネットワーク設定を検証します。ネットワークの検証では、テスト対象のすべてのネットワークインターフェイスが接続されている必要があります。

注記:

- ・ ネットワークの検証はオプションです。ただし、Hewlett Packard Enterprise では、このウィザードを使用して、ご使用のネットワーク設定が有効かどうかを確認することをお勧めします。この検証は、ネットワーク環境の問題の診断に役立ちます。
- ・ NCT に戻ってネットワーク検証ウィザードのみを使用するには、コマンドプロンプトまたは PowerShell を開き、NCT -validate コマンドを入力します。

手順

1. ネットワーク構成を今すぐ検証を選択します。
2. (ご使用のシステムが存在するドメイン) の名前とドメインコントローラーの IP アドレスを入力します。システムがドメインに存在しない場合は、これらのフィールドを空白にしておくことができます。
3. 検証をクリックします。

各インターフェイスは順にテストされ、検証の成功または失敗が出力ウィンドウに示されます。検証の進行状況は、タスクバーにも表示されます。検証結果は、c:\nas\logs\NetworkConfigTool フォルダーに保存されます。各検証結果が、検証が実行された時刻と日付を使用した名前のファイルに保存されます。検証が完了すると、検証結果は、ICT ウィンドウに表示されます。

ネットワークの検証を実行しない場合は、レジストリキーを使用すると、以下のステータスが表示されます。

ネットワーク構成が検証されていません

構成が検証されていない場合に表示されます。

ネットワーク構成が検証されました

検証が完了したことをキーが示す場合に表示されます。

ネットワークの検証に失敗しました

1つ以上の検証手順が失敗したことをキーが示す場合に表示されます。

HPE ストレージファイルコントローラー上でのネットワーク設定のインポート

NCTConfig.xml ファイルを使用すると、ネットワーク構成の設定を1つのストレージシステムから別のストレージシステムにインポートし、そのネットワーク構成の設定をすべてのインターフェイスに対して

一度に適用することができます。設定を正常にインポートした後、NCT を起動すると、確認メッセージが表示されます。これは、最後に使用されたネットワーク構成の設定を使用することを示します。はいをクリックすると、NCT ウィザードはネットワーク構成の詳細を NCTConfig.xml ファイルからロードし、チームの詳細と共に既存のインターフェイスの詳細を表示します。利用可能なインターフェイスから目的のネットワークインターフェイスを再構成して、チームを作成したり、既存のチームを削除したりすることができます。

- ❗ **重要:** インターフェイス名を変更するときは、デフォルトの VLAN に関連付けられているプレフィックスのみを変更する必要があります。たとえば、完全なインターフェイス名が Ethernet 2 Team -VLAN Default である場合は、プレフィックスのみを変更して、Ethernet 2 Team とします。デフォルトの VLAN 名は変更できません（この例では VLAN Default です）。

NCTConfig.xml ファイルによる作業で重要な考慮事項は、以下のとおりです。

- ・ ファイル内の XML タグの名前を変更しないでください。タグの名前を変更すると、構成の適用中にエラーが発生する可能性があります。
- ・ ファイル NCTConfig.xml の名前は変更しないでください。
- ・ エラーが発生するため、PciKey タグの内容を編集しないでください。
- ・ 編集できるのは、Name、AdapterIPConfiguration、AdapterHWInformation などの特定の XML タグのみです。
- ・ ファイル NCTConfig.xml が壊れているかまたはタグが誤っている場合、その旨のメッセージが画面上に表示されます。同じファイルを再利用することはできません。このような場合、NCT は以降の構成で、システム検出状態を使用します。

NCTConfig.xml ファイルからネットワーク構成の設定をインポートするには、以下の手順に従ってください。

1. NCTConfig.xml ファイルを開き、<AdapterIPConfiguration>タグの、アダプターの IP 構成を編集します。
2. 必要に応じて、インターフェイス名を編集します。
3. ファイルを保存し、構成をインポートするストレージシステム上の C:\Program Files\HPE\StoreEasy NetworkConfigurationWizard にコピーします。
4. NCT を起動し、プロンプトが表示されたらはいをクリックして、最後に保存された構成を使用します。
5. NCT ウィザードは、構成の詳細を NCTConfig.xml ファイルからロードして表示します。
6. 検出が完了したら、次へをクリックします。
7. それぞれのウィンドウで、ネットワーク構成について必要な変更を行います。
8. 変更を適用するには、ネットワーク構成の概要ウィンドウで適用をクリックします。
9. 変更を検証するには、ネットワーク構成の検証ウィンドウで検証をクリックします。

以下の理由により、XML ファイルのインポートに失敗する可能性があります。

- ・ ファイルが壊れている。
- ・ XML ファイル中のアダプターの数と、ファイルをインポートするシステムのアダプターの数不一致。
- ・ ファイル名が NCTConfig.xml ではない。

- ・ ファイルが別の場所またはフォルダーにコピーされた。
- ・ 編集可能でないXML タグが編集された。

NCTConfig.xml ファイルとその使用法の詳細については、HPE ストレージファイルコントローラー管理者ガイドを参照してください。

クラスター名とドメインの入力

クラスター名とドメインを入力を選択して、クラスター名とドメイン参加ウィザードを開きます。ウィザードの指示に従います。タスクを完了するため、ウィザードでは特に次の情報が必要です。

- ・ **Active Directory ドメイン** — 両方のノードとも、メンバーサーバーとしてこのドメインに参加します。
- ・ **ドメインユーザーアカウント** — ドメイン内では「コンピューターオブジェクトの作成」および「すべてのプロパティの読み取り」のアクセス許可が必要です。
- ・ **任意のクラスター管理名およびクラスターノード名** — クラスターノード名はクラスター名から自動的に取得されますが、個別に変更することが可能です。
- ・ **新しいローカル管理者のパスワード** — セットアップを簡単にするため、新しいパスワードは両方のノードに適用されますが、後で一方または両方のノードで変更できます。両方のノードで、同じパスワードを使用する必要はありません。

ウィザードを完了すると、両方のノードが再起動します。再起動後、フェイルオーバークラスターを管理するための適切な権限を持つドメインログインアカウントを使用してログインします。

システム設定

オペレーティングシステムのプロパティをカスタマイズして構成します。

時刻とタイムゾーンの設定

時刻とタイムゾーンの設定

地理的場所に応じて、時刻とタイムゾーンを設定します。HPE ストレージファイルコントローラー上のクラスターノードの**時刻およびタイムゾーンの設定**オプションは、ネットワーキングセクションで利用可能です。

システムの日付と時刻をインターネット時刻と同期させることができます。また、別のタイムゾーンの時刻を表示するように追加のクロックを構成することもできます。

通知

メールアラートを構成し、HPE 製品通知を登録します。

- ・ **File Controller アラートの構成**
- ・ **HPE 製品通知の登録**

File Controller アラートの構成

ホストオペレーティングシステムとは無関係に検出されたファイルコントローラーのアラート状態を送信するには、iLO の **iLO アラートメール**を使用します。メールアラートには、ハードウェア障害のような主要なホストシステムイベントが含まれます。アラートは、指定したメールアドレスに送信されます。

注記: 一部のメールサービスプロバイダーでは、スパム、商用コンテンツ、迷惑な容量など、問題のあるメールをブロックするためのフィルターやルールが確立されています。iLO により生成されたメッセージの受信が、これらのツールによってブロックされる場合があります。iLO アラートメールに指定されている送信者のメールアドレスが、受信者メールのホワイトリストにあることを確認して、メールがスパムフォルダーにフィルターされないようにしてください。

アラートメールを有効にする

手順

1. iLO システムにログインします。
2. 左のナビゲーションペインで**マネジメント**を選択してから、**アラートメール**タブをクリックします。
3. **iLO アラートメールを有効**オプションを選択します。
4. **アラートメール**タブで以下の情報を指定します。

- ・ メールアドレス
- ・ 送信ドメイン
- ・ SMTP ポート
- ・ SMTP サーバー

5. (オプション) **テストアラートメールを送信**をクリックして、指定されたメールアドレスにテストメッセージを送信します。

注記: **テストアラートメールを送信**ボタンは、**iLO アラートメールを有効**が有効になっている場合にのみ使用できます。

6. 変更を保存するには、**適用**をクリックします。

アラートメールのオプション

メールアドレス

iLO によるメールアラートの宛先メールアドレス。これは最大 63 文字であり、標準のメールアドレス形式でなければなりません。入力できるメールアドレスは 1 つだけです。

送信ドメイン

送信（送信元）メールアドレスに指定されたドメイン名。送信アドレスは、iLO 名をホスト名として、送信ドメインをドメイン名として使用して構成します。最大 63 文字を使用できます。

SMTP ポート

SMTP サーバーが未認証の SMTP 接続に使用するポート。デフォルト値は 25 です。

SMTP サーバー

SMTP サーバーまたは MSA の IP アドレスまたは DNS 名。このサーバーは、メッセージ転送エージェントと連携してメールを配信します。最大 63 文字を使用できます。

アラートメールを無効にする

手順

1. iLO システムにログインします。
2. 左のナビゲーションペインで**マネジメント**を選択してから、**アラートメール**タブをクリックします。

3. iLO アラートメールを有効オプションをクリアします。

4. 変更を保存するには、**適用**をクリックします。

製品通知の登録

Hewlett Packard Enterprise は、システムの更新、重大な問題、および機能の更新についての通知を受信できるように、ご使用のシステムを登録することをお勧めします。サービスのリリースにアクセスできるようにするには、システムの登録が必須になります。ご使用のシステムがネットワークに接続していない場合は、インターネットアクセスを使用して他のデバイスから製品登録できます。

注記: 登録は、サービスのリリースにアクセスするために必須です。

以下の方法で製品の登録リンクにアクセスすることもできます。

- ・ デスクトップにある **Register For HPE product notifications** アイコンをダブルクリックします。
- ・ スタート画面で**製品の登録**をクリックします。
- ・ サーバーマネージャーを開き、**ツール > ストレージファイルコントローラー > 製品の登録**を選択します。

ストレージアレイ管理

HPE ファイルコントローラーのすべての SAN アレイに接続できます。ファイルコントローラーに接続されているストレージシステムに応じて、以下のストレージ管理を実行します。

3PAR StoreServ アレイ

注記: 接続タイプが iSCSI の場合、iSCSI イニシエーターが有効になります。

- ・ [アレイ管理ログイン詳細の設定](#)
- ・ [iSCSI イニシエーターの実行](#)
- ・ [Multi-Path IO の構成](#)

Nimble アレイ

- ・ [Nimble グループの検出](#)
- ・ [Nimble グループに接続](#)
- ・ [iSCSI イニシエーターの実行](#)
- ・ [Multi-Path IO の構成](#)

MSA または他のアレイ

注記: 接続タイプが iSCSI の場合、iSCSI イニシエーターが有効になります。

- ・ [アレイ管理ログイン詳細の設定](#)
- ・ [iSCSI イニシエーターの実行](#)
- ・ [Multi-Path IO の構成](#)

アレイ管理ログイン詳細の設定

手順

1. 接続するストレージアレイの**アレイ IP アドレス**を入力します。
2. **アレイのユーザー ID**と**アレイのパスワード**を入力します。
3. プロトコルを **https** または **http** のいずれかから選択します。
4. **接続タイプ**を **FC** または **iSCSI** のいずれかから選択します。
5. **保存**をクリックします。
メッセージ**アレイデータは正常に保存されました**が表示されます。
6. アレイ登録ツールを閉じるには、**終了**をクリックします。
ICT ウィンドウの 3 番目の列で、接続されたアレイの IP アドレスを確認できます。

Nimble グループの検出

[Nimble グループの検出] タスクを使用して、**Nimble Setup Manager** を開きます。初期化されていない Nimble アレイを構成できます。

- ・ **Nimble アレイの初期化**
- ・ **Nimble アレイのセットアップ**

Nimble アレイの初期化

手順

1. ICT タスクグループで**ストレージアレイ管理 > Nimble グループの検出**をクリックします。

Welcome to Nimble Setup Manager 画面が表示されます。

ストレージファイルコントローラーに接続されている、初期化されていない Nimble アレイが表示されます。

注記: アレイがリストされない場合は、ストレージファイルコントローラーと Nimble アレイのネットワーク接続の両方が同じネットワークセグメントに接続されているかどうか確認します。

2. 初期化するアレイを選択し、**Next** をクリックします。

注記: セキュリティ証明書の問題が発生した場合は、Internet Explorer で JavaScript とアクティブスクリプトを有効にします。

License Agreement screen が表示されます。

3. **License Agreement screen** で、チェックボックスをクリックして、ライセンス条件に同意します。
次に、**Proceed** をクリックします。

Nimble Storage group Setup 画面が表示されます。

4. **Set up this array but do not join a group** オプションをクリックします。
5. 以下のパラメーターを入力し、**Finish** をクリックします。

- a. **Array Name** : 英字、数字、またはダッシュのみを使用します。名前の最初の文字に句読点は使用しないでください。
- b. **Group Name**: 英字、数字、またはダッシュのみを使用します。名前の最初の文字に句読点は使用しないでください。
- c. **Management IP**: Nimble アレイの IP アドレスが含まれます。
- d. **Netmask** : IP アドレスをマスクし、IP アドレスをネットワークアドレスとホストアドレスに分割する 32 ビットの数値。
- e. **Default Gateway** : さまざまなプロトコルを使用する別のネットワークにアクセスできます。
- f. **Domain Name** (任意) : HPE ストレージファイルコントローラーのドメイン コントローラーの名前。
- g. **Password** : Create a new password フィールドと Confirm password フィールドに同じパスワードを入力します。

アレイの初期化に成功したら、アレイをセットアップします。

アレイの詳細については、[InfoSight](#) のドキュメントを参照してください。

Nimble アレイのセットアップ

前提条件

Nimble アレイを初期化します。

手順

1. ユーザー名とパスワードを入力し、**ログイン**をクリックします。

注記: 画面全体が表示されない場合は、画面の解像度を上げてください。

Nimble Storage セットアップページが表示されます。

2. **サブネット構成**で**データサブネットの追加**をクリックします。
3. **インターフェイスの割り当て**で、次の情報を入力し、**次へ**をクリックします。

注記: eth1 と eth2 のサブネットが、それぞれ**管理**および**なし**であることを確認します。

- a. **IP インターフェイス** : このインターフェイスは、管理 IP アドレスとは異なっていなければなりません。
 - b. **コントローラー A の IP アドレス**
 - c. **コントローラー B の IP アドレス**
4. **ドメイン**で、以下の情報を入力し**次へ**をクリックします。
 - a. (オプション) **ドメイン名**
 - b. **DNS サーバー** : DNS サーバーフィールドには、最大 5 つの IP アドレスを入力できます。
 5. **時間**の下で :

- a. ドロップダウンリストからタイムゾーンを選択します。
 - b. 時刻 (NTP) サーバーのホスト名または IP アドレスを入力します。
6. サポートで、以下の情報を入力し**終了**をクリックします。
- a. 差出人アドレス
 - b. 送信先アドレス

注記: 複数の電子メールアドレスを入力するには、カンマで区切って入力するか、個々の行に入力します。

- c. SMTP サーバー
- d. プロキシサーバーを設定する必要がある場合は、**HTTP プロキシサーバーの使用**を選択します。

メッセージ

「セットアップ完了」

が表示されます。

7. 次のいずれかを実行します。
- a. **続行**をクリックします。
 - b. WWPN ホスト情報を使用して、イニシエーターグループを作成します。
 - ・ **管理** > **イニシエーターグループ**を選択します。
 - ・ グループを選択し、**編集**をクリックして、既存のイニシエーターグループを編集します。
 - ・ 各イニシエーターのエイリアスと WWPN を入力して**保存**をクリックします。

Nimble グループへの接続

Nimble グループに接続をクリックすると、Nimble アレイの管理グループの IP アドレスと認証情報（暗号化済み）が HPE ストレージファイルコントローラのノードに保存されます。この情報は、他のツールによって使用されます。

手順

1. ICT ウィンドウで、**ストレージアレイ管理** > **Nimble グループに接続**をクリックします。

Nimble グループに接続ウィンドウが表示されます。
2. **グループ管理 IP** フィールドに、Nimble アレイの構成時に指定した管理グループの IP アドレスを入力します。
3. Nimble 管理グループの構成時に指定した**グループユーザー名**と**グループパスワード**を入力します。
4. **接続**をクリックして、Nimble グループへの接続を確立します。

レジストリに Nimble 管理グループの IP アドレスと認証情報を保存すると、次のいずれかのステータスメッセージが表示されます。

- ・ Nimble グループに接続できませんでした。HPE ストレージファイルコントローラーが Nimble アレイに正常に接続できない場合に表示されます。
- ・ Nimble グループへの接続が完了しました。HPE ファイルストレージファイルコントローラーが、管理 IP アドレスと認証情報を使用して、Nimble アレイを正常に特定して認証できた場合に表示されます。

iSCSI イニシエーターの実行

このリンクをクリックすると、iSCSI イニシエーターツールが起動します。このツールを使用して、iSCSI アレイに接続します。

注記: iSCSI イニシエーターの実行ツールは、選択したアレイの接続タイプが iSCSI である場合にのみ使用できます。

マルチパス IO の構成

注記: MPIO を構成しないと、ドライブが重複してリストされます。

複数のパスを介して仮想ボリュームをファイルコントローラーにエクスポートすると、MPIO 構成は自動で行われます。構成の状態は、ICT ウィンドウに表示されます。管理者特権の PowerShell またはコマンドプロンプトで `mpiocpl` コマンドを入力すると、MPIO のプロパティのアプレットを開くことができます。

マルチパス IO の構成

手順

1. **Multi-Path IO の構成**をクリックします。
[MPIO のプロパティ (mpiocpl.exe)] ウィンドウが開きます。
2. **マルチパスの検出タブ**で、次を選択します。
 - a. iSCSI デバイスのサポートを追加
 - b. iSCSI のマルチイニシエーターを許可

共用記憶装置

このタスクグループでは、ノード間の共有ストレージの結果のステータスを参照することができます。両方のノードは、一意のストレージ識別子をベースとして、同じストレージにアクセスする必要があります。共有ストレージに表示されるメッセージを以下に示します。

- ・ **「共有ストレージが見つかりません」**: システムは、基準に合う共通の共有ストレージを見つけることができませんでした。共有ストレージが利用可能かを検証するには、各サーバーで `get-disk powershell` スクリプトを実行し、2 つのサーバーの **ユニーク ID** を比較します。たとえば、`get-disk | select uniqueid,friendlyname,operationalstatus` を実行します。
- ・ **「共有ストレージが見つかりました」**: システムは、監視ディスクに使用可能なストレージを見つけました。両方のノードで同じユニーク ID を持つディスクは、共有として扱われます。

注記: 1 つ以上の LUN がノードにエクスポートされているのに、ユニーク ID が一致しないか、リストされない場合は、各 StoreVirtual ファイルコントローラー上で、昇格した Administrator PowerShell コマンドプロンプトから、`Update-StorageProviderCache -DiscoveryLevel Full` を起動して、ストレージプロバイダーのキャッシュを更新する必要があります。ただし、キャッシュを更新しても問題が解決しない場合は、ストレージの接続に使用されている HBA またはネットワークアダプターが同一であること、ファームウェアおよびドライバーのバージョンが同じであることを確認します。ファームウェアまたはドライバーを変更した場合は、両方のノードを再起動する必要があります。それでもストレージプロバイダーキャッシュの更新で問題が発生する場合は、各ノードで `cmdlet Get-StorageProvider` コマンドを実行し、システムがストレージにアクセスできることを検証してください。詳細は、共有ストレージソリューションのインストールおよびセットアップ情報を参照してください。

ディスクアレイを管理するためにサポートされている 3PAR Management Console ソフトウェアのバージョンについては、3PAR ディスクアレイ製品のマニュアルを参照してください。

注記: 3PAR ディスクアレイへの iSCSI 接続の共有ストレージを参照するには、ICT のネットワークの構成タスクを完了させてください。現在構成中のホストから 3PAR Management Console またはコマンドラインユーティリティを使用するときは、ICT のネットワークの構成タスクを完了させる必要があります。これによりホストは、ネットワークを介して 3PAR ディスクアレイと接続できるようになります。セキュリティを強化し、より良いレベルのストレージサービスをユーザーおよびアプリケーションの両方に対して提供するために、3PAR Virtual Domains ソフトウェアを使用することを検討してください。詳細は、HPE 3PAR StoreServ Storage コンセプトガイドを参照してください。

詳細は、HPE 3PAR Windows Server 2016/2012/2008 実装ガイドを参照してください。

MSA アレイへの接続時に監視ディスク（仮想ボリューム、最小 600 MB）またはその他の仮想ボリュームを準備する

MSA アレイの監視ディスクをプロビジョニングできます。

前提条件

アレイ情報を保存フィールドを使用して、ストレージアレイが構成済みであることを確認します。詳細については、「[アレイ管理ログイン詳細の設定](#)」を参照してください。

手順

1. 監視ディスク（最小 600 MB）に使用する仮想ボリュームまたはその他の仮想ボリュームを準備するをクリックして、MSA アレイのストレージ管理ユーティリティのウィンドウを起動します。
2. 必要なログイン認証情報を入力します。
3. 以下のいずれかの操作を実行します。
 - ・ ホストの作成
 - ・ 仮想ボリュームの作成
 - ・ 仮想ボリュームのエクスポート

ホストの作成

ホストの表示

ホストトピックには、システムで定義されているイニシエーター、ホスト、ホストグループに関する情報がテーブル形式で表示されます。ホストトピックでは、ユーザーがイニシエーターをマッピングし、マップ詳細を表示することもできます。

ホストテーブル

ホストテーブルには、以下の情報が表示されます。デフォルトでは、一度に 10 個のエントリーがテーブルに表示されます。

- ・ **グループ**。イニシエーターがホストグループにグループ化されている場合にはグループ名を表示し、それ以外の場合は「--」と表示します。
- ・ **ホスト**。イニシエーターがホストにグループ化されている場合にはホスト名を表示し、それ以外の場合は「--」と表示します。
- ・ **ニックネーム**。イニシエーターに割り当てられているニックネームを表示します。
- ・ **ID**。イニシエーターの ID を表示します。この ID は、FC または SAS イニシエーターの WWN であるか、iSCSI イニシエーターの IQN です。
- ・ **プロファイル**。プロファイル設定が表示されます。
 - **標準**。デフォルトのプロファイルです。
 - **HP-UX**。ホストはフラットスペースアドレッシングを使用します。
 - **OpenVMS**。LUN 0 は、マッピングに割り当ててはできません。
- ・ **検出済み**。検出されたイニシエーターの場合は [はい]、手動で作成されたイニシエーターの場合は [いいえ] が表示されます。
- ・ **マッピング済み**。ボリュームにマッピングされているイニシエーターの場合は [はい]、マッピングされていないイニシエーターの場合は [いいえ] が表示されます。
- ・ **ホストのタイプ**。ホストインターフェイスプロトコルを示します。

関連マッピングテーブル

選択したイニシエーターについて、[関連マッピング] テーブルには、以下の情報が表示されます。デフォルトでは、一度に 20 個のエントリーがテーブルに表示されます。

- ・ **Group.Host.Nickname**。マッピングが適用されるイニシエーターを識別します。
 - **initiator-name** - マッピングはこのイニシエーターにのみ適用されます。
 - **initiator-ID** - マッピングはこのイニシエーターのみに適用され、イニシエーターはニックネームを持ちません。
 - **host-name.*** - マッピングはこのホストのすべてのイニシエーターに適用されます。
 - **host-group-name.*.*** - マッピングはこのグループのすべてのホストに適用されます。
- ・ **ボリューム**。マッピングが適用されるボリュームを識別します。
 - **volume-name** - マッピングはこのボリュームにのみ適用されます。
 - **volume-group-name.*** - マッピングはこのボリュームグループのすべてのボリュームに適用されます。
- ・ **アクセス**。マッピングに割り当てられているアクセスのタイプを表示します。
 - **読み取り/書き込み** - マッピングで読み書きアクセスが許可されます。
 - **読み取り専用** - マッピングで読み取りアクセスが許可されます。
 - **アクセスなし** - マッピングでアクセスが禁止されます。

- ・ LUN。マッピングで 1 つの LUN と LUN の範囲のどちらを使用する（*で示されます）かを示します。
- ・ ポート。マッピングが適用されるコントローラーホストポートをリストします。各番号は、両方のコントローラー上で対応するポートを表します。

イニシエーターの作成

イニシエーターは手動で作成することができます。たとえば、スイッチを介してコントローラーポートを物理的にホストに接続する前にイニシエーターを定義したい場合もあります。

手順

1. イニシエーターに使用する FC または SAS WWN、あるいは iSCSI IQN を決定します。
2. ホストトピックで、**操作 > イニシエーターの作成**を選択します。[イニシエーターの作成] パネルが開きます。
3. [イニシエーター ID] フィールドで、WWN または IQN を入力します。WWN の値には、桁の各ペアの間にコロンを含めることができますが、コロンは破棄されます。
4. イニシエーターの名前フィールドに、識別しやすいようにニックネームを入力します。たとえば、`MailServer_FCp1` を使用できます。イニシエーター名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、`"`、`,`、`.`、`<`、`\`を含めることはできません。
他のイニシエーターによって名前が使用されている場合には、別の名前を入力するように指示されます。
5. プロファイルリストで、適切なオプションを選択します。
 - ・ **標準**。デフォルトのプロファイルです。
 - ・ **HP-UX**。ホストはフラットスペースアドレッシングを使用します。
 - ・ **OpenVMS**。イニシエーターに LUN 0 を割り当ててはできません。
6. **OK** をクリックします。イニシエーターが作成され、ホストテーブルが更新されます。

イニシエーターの変更

手動で作成したイニシエーターは変更することができます。

手順

1. ホストトピックで、変更するイニシエーターを選択します。
2. **操作 > イニシエーターの変更**を選択します。イニシエーターの変更パネルが開きます。
3. イニシエーターの名前フィールドに、識別しやすいニックネームを入力します。たとえば、**MailServer_FCp2** のように指定できます。イニシエーター名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、`"`、`,`、`.`、`<`、`\`を含めることはできません。他のイニシエーターによって名前が使用されている場合には、別の名前を入力するように指示されます。
4. プロファイルリストで、適切なオプションを選択します。

- ・ **標準**。デフォルトのプロファイルです。
- ・ **HP-UX**。ホストはフラットスペースアドレッシングを使用します。
- ・ **OpenVMS**。イニシエーターに LUN 0 を割り当てることはできません。

5. **OK** をクリックします。ホストテーブルが更新されます。

イニシエーターの削除

手動で作成したイニシエーターは、グループ化もマッピングもされていなければ、削除することができます。手動で作成したイニシエーターがマッピングされている場合には削除できません。また、検出されたイニシエーターは削除できませんが、削除操作でそのニックネームを削除することは可能です。

手順

1. ホストトピックで、名前の付いた 1~128 のイニシエーターから、ホストに追加する対象を選択します。
2. **操作 > イニシエーターの削除**を選択します。
イニシエーターの削除パネルが開き、削除するイニシエーターがリストされます。
3. **OK** をクリックします。
イニシエーターが削除され、ホストテーブルが更新されます。

ホストへのイニシエーターの追加

名前の付いた既存のイニシエーターを、既存のホストまたは新規ホストに追加できます。ホストにイニシエーターを追加するには、そのイニシエーターのマッピングが、ホスト内の他のすべてのイニシエーターと同じでなければなりません。つまり、そのイニシエーターは、同じアクセス設定、ポート設定、および LUN 設定によって、同じボリュームまたはボリュームグループにマッピングされている必要があります。

手順

1. ホストトピックで、名前の付いた 1~128 のイニシエーターから、ホストに追加する対象を選択します。
操作 > ホストへの追加を選択します。[ホストへの追加] パネルが開きます。
2. 次のいずれかを実行します。
 - ・ 既存のホストを使用する場合は、[ホストの選択] リストでその名前を選択します。
 - ・ ホストを作成する場合は、[ホストの選択] フィールドにホストの名前を入力します。ホスト名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、", . <\>を含めることはできません。
3. **OK** をクリックします。選択したイニシエーターについて、ホスト値が--から、指定した名前に変わります。

ホストからのイニシエーターの削除

最後のイニシエーターを除くすべてのイニシエーターを、ホストから削除できます。ホストからイニシエーターを削除すると、そのイニシエーターはグループ解除されますが削除されることはありません。すべてのイニシエーターを削除するには、ホストを削除してください。

手順

1. ホストトピックで、ホストから削除する 1~1024 のイニシエーターを選択します。
2. **操作 > ホストからの削除**を選択します。
ホストからの削除パネルが開き、削除するイニシエーターがリストされます。
3. **OK** をクリックします。
選択したイニシエーターについて、ホスト値が--に変わります。

ホストの削除

グループ化されていないホストは削除できます。ホストを削除すると、そのイニシエーターはグループ解除されますが、削除されるわけではありません。

手順

1. ホストトピックで、グループ化されていない 1~512 のイニシエーターを削除対象として選択します。
2. **操作 > ホストの削除**を選択します。
ホストの削除パネルが開き、削除するホストがリストされます。
3. **OK** をクリックします。
選択したホストのイニシエーターについて、ホスト値が--に変わります。

ホスト名の変更

ホストは名前を変更することができます。

手順

1. ホストトピックで、名前を変更するホストに所属するイニシエーターを選択します。
2. **操作 > ホスト名の変更**を選択します。
ホスト名の変更パネルが開きます。
3. 新しいホスト名フィールドに、ホストの新しい名前を入力します。
ホスト名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , . < \ を含めることはできません。他のホストによって名前が使用されている場合には、別の名前を入力するように指示されます。
4. **OK** をクリックします。
ホストテーブルが更新されます。

ホストグループへのホストの追加

既存のホストを、既存のホストグループまたは新規ホストグループに追加できます。

ホストグループにホストを追加するには、そのホストのマッピングが、グループの他のすべてのメンバーと同じでなければなりません。ホストは、同じアクセス設定、ポート設定、および LUN 設定によって、同じボリュームまたはボリュームグループにマップされている必要があります。

手順

1. ホストトピックで、ホストグループに追加したいホストに所属する 1~256 のイニシエーターを選択します。
2. **操作 > ホストグループへの追加**を選択します。

ホストグループへの追加パネルが開きます。

3. 次のいずれかを実行します。

- ・ 既存のホストグループを使用する場合は、ホストグループの選択リストでその名前を選択します。
- ・ ホストグループを作成する場合は、ホストグループの選択フィールドにホストグループの名前を入力します。ホストグループ名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , < \ を含めることはできません。

4. OK をクリックします。

選択したホストについて、グループ値が--から、指定したホストグループ名に変わります。

ホストグループからのホストの削除

最後のホストを除くすべてのホストを、ホストグループから削除できます。ホストグループからホストを削除すると、そのホストはグループ解除されますが削除はされません。ホストグループを削除するには、ホストグループの削除を参照してください。

手順

1. ホストトピックで、ホストグループから削除する 1~256 のホストを選択します。

2. 操作 > ホストからの削除を選択します。

[ホストグループからの削除] パネルが開き、削除するホストがリストされます。

3. OK をクリックします。

選択したホストについて、グループ値が--に変わります。

ホストグループ名の変更

ホストグループ名を変更します。

手順

1. ホストトピックで、名前を変更するホストグループを選択します。

2. 操作 > ホストグループ名の変更を選択します。

ホストグループ名の変更パネルが開きます。

3. 新しいホストグループ名フィールドに、そのホストグループの新しい名前を入力します。

ホストグループ名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , . < \ を含めることはできません。他のホストグループによって名前が使用されている場合には、別の名前を入力するように指示されます。

4. OK をクリックします。

ホストテーブルが更新されます。

ホストグループの削除

ホストグループを削除することができます。ホストグループを削除するとそのホストはグループ解除されますが、削除はされません。

手順

1. ホストトピックで、削除する 1~32 のホストグループを選択します。
2. **操作 > ホストグループ名の変更**を選択します。
ホストグループの削除パネルが開き、削除するホストグループがリストされます。
3. **OK** をクリックします。
選択したホストグループに含まれていたホストについて、グループ値が--に変わります。

チャレンジハンドシェイク認証プロトコル (CHAP)

iSCSI では、CHAP (チャレンジハンドシェイク認証プロトコル) を使用して、ログイン要求のイニシエーターとターゲット間で認証を行うことができます。この識別を実行するには、イニシエーターとターゲットに CHAP レコードのデータベースが存在する必要があります。各 CHAP レコードは、イニシエーターだけを認証する (単方向 CHAP) 場合は 1 つ、イニシエーターとターゲットの両方を認証する (相互 CHAP) 場合は 2 つの名前 - シークレットペアを指定できます。iSCSI ホストからコントローラー iSCSI ポートへのログインリクエストの場合は、ホストがイニシエーターで、コントローラーポートがターゲットです。

CHAP が有効で、ストレージシステムが既知の送信者 (イニシエーター) からのログインリクエストの受信者である場合、システムは既知のシークレットを要求します。発信元がそのシークレットを提供すると、接続が許可されます。

CHAP がピア接続されているシステムで使用され、複製で使用される場合には、特別な考慮事項があります。ピア接続では、ストレージシステムはログインリクエストの送信者または受信者として機能できます。送信者として、有効な CHAP レコードによって、CHAP が無効な場合でも CHAP を認証できます。システムがピアの要求する CHAP シークレットを提供し、接続が許可されるため、これが可能になります。

CHAP レコードの追加または変更手順

1. 双方向 CHAP を使用する予定で、コントローラー iSCSI ポートの IQN を確認する必要がある場合は、以下を実行します。
 - a. システムトピックを選択します。
 - b. 背面側ビューを選択します。
 - c. 使用したい iSCSI ホストポートにカーソルを合わせます。ポート情報パネルが表示されたら、ID フィールドの値の IQN をメモしてください。
2. ホストトピックで、**操作 > CHAP の設定**を選択します。[CHAP の設定] パネルが開き、既存の CHAP レコードがリストされます。
3. **認証 (CHAP) の有効化**チェックボックスを選択して、すべての iSCSI ノードで CHAP の使用を有効にし、操作を確認します。

注記: ここで CHAP を有効または無効にすると、[ホストポート設定] パネルの**詳細設定**タブの設定が更新されます。

4. 次のいずれかを実行します。
 - ・ 既存のレコードを変更するには、それを選択します。レコードの値が、編集する CHAP レコードのリストの下フィールドに表示されます。IQN は編集できません。
 - ・ 新しいレコードを追加するには、**新規**をクリックします。

5. 新しいレコードの場合、ノード名 (IQN) フィールドに、イニシエーターの IQN を入力します。値には大文字と小文字の区別があり、最大長は 223 バイトです。0~9、小文字の a~z、ハイフン、コロン、ピリオドを使用できます。
6. シークレットフィールドで、ターゲットがイニシエーターの認証に使用できるシークレットを入力します。このシークレットでは大文字と小文字が区別され、最大 12~16 バイトを指定できます。値には、"<"を除くスペースおよび印字可能な UTF-8 文字が使用できます。
7. 相互 CHAP を使用する手順
 - ・ **相互 CHAP** チェックボックスにチェックを入れます。
 - ・ **相互 CHAP 名** フィールドに、手順 1 で取得した IQN を入力します。この値では、大文字と小文字が区別されます。最大 223 バイトで、0~9、小文字の a~z、ハイフン、コロン、およびピリオドを使用できます。
 - ・ **双方向 CHAP シークレット** フィールドで、イニシエーターがターゲットの認証に使用できるシークレットを入力します。シークレットでは大文字小文字が区別され、最大 12~16 バイトで指定できます。また、イニシエータのシークレットとは異なる必要があります。値には、"<"を除くスペースおよび印字可能な UTF-8 文字が使用できます。ストレージシステムのシークレットは、両方のコントローラーで共有されます。
8. **適用**または **OK** をクリックします。CHAP レコードのテーブルが更新されます。

CHAP レコードを削除する手順

 **注意:** CHAP レコードを削除すると、ボリュームがアクセス不可になり、それらのボリューム内のデータが使用できなくなる可能性があります。

1. ホストトピックで、**操作 > CHAP の設定**を選択します。[CHAP の設定] パネルが開き、既存の CHAP レコードがリストされます。
2. 削除するレコードを選択します。
3. **削除**を選択します。確認パネルが表示されます。
4. **削除**を選択します。あるいは、**キャンセル**を選択します。[削除]を選択すると、CHAP レコードが削除されます。

仮想ボリュームの作成

仮想プールにはボリュームを追加できます。個別に仮想ボリュームを作成したり、さまざまな設定で複数の仮想ボリュームを作成したり、同じ設定で複数の仮想ボリュームを作成することができます。最後のケースの場合、ボリュームには同じベース名が付き、0000 から始まる数値サフィックスが続いてそれぞれの名前が固有になり、同じプールに配置されます。ボリューム階層の親和性設定を選択して、ボリュームデータの階層を指定することもできます。

手順

1. 次のいずれかを実行します。
 - ・ プールトピックのプールテーブルで仮想プールを選択し、**操作 > 仮想ボリュームの作成**の順に選択します。
 - ・ ボリュームトピックで、**操作 > 仮想ボリュームの作成**の順に選択します。仮想ボリュームの作成パネルが開き、各プールの現在の容量の使用率が表示されます。

注記: 仮想プールが存在しない場合、仮想ボリュームを作成するオプションは利用できません。

2. オプション: ボリューム名を変更します。デフォルトは Voln です。n は 0001 から始まり、デフォルト名が付いたボリュームごとに 1 ずつ増加します。ボリューム名には大文字と小文字の区別があり、最大長は 32 バイトです。システムにある名前は使用できず、" , < \ を含めることはできません。

その名前が別のボリュームによって使用されている場合、その名前は固有になるように自動的に変更されます。たとえば MyVolume は MyVolume0001 に、Volume2 は Volume3 に変更されます。

3. オプション: ボリュームサイズを測定単位も含めて変更します。MiB、GiB、TiB、MB、GB、TB のうちいずれかの単位を使用できます。デフォルトサイズは 100GB です。システムでサポートされる最大ボリュームサイズについては、SMU ヘルプのシステム構成の制限に関するトピックを参照してください。ボリュームサイズは、4.2MB (4MiB) 境界にアライメントされます。ボリュームが作成または拡張される場合、作成または拡張後のサイズが 4.2MB 未満のときは、4.2MB に増やされます。4.2MB より大きな値は、最も近い 4.2MB 境界まで減らされます。
4. オプション: 作成するボリュームの数を変更します。デフォルトは 1 です。プールごとにサポートされるボリュームの最大数については、SMU ヘルプのシステム構成の制限に関するトピックを参照してください。
5. オプション: ボリューム階層の親和性設定を指定し、ボリュームデータを自動的に特定の階層に関連付けて、可能な場合は常にすべてのボリュームデータをその階層に移動するようにします。デフォルトは **アフィニティなし** です。
6. オプション: ボリュームを作成するプールを選択します。プール間でボリュームの負荷分散が行われるため、デフォルトでは、A と B のうちボリュームが少ない方になります。
7. オプション: 異なる設定で別のボリュームを作成するには、**行の追加** をクリックし、設定を変更します。カーソルがある行を削除するには、**行の削除** をクリックします。
8. **OK** をクリックします。
ボリュームの作成によってプール容量がオーバーコミットされる場合は、イベント通知を設定して、プールで物理ストレージが不足する前に警告するように要求されます。
9. 仮想ボリュームが容量を超える場合は、次のように操作します。
 - a. はいをクリックして次に進みます。続行しない場合はいいえをクリックします。はいをクリックした場合は、ボリュームが作成されてボリュームテーブルが更新されます。
 - b. 確認パネルを閉じるには、**OK** をクリックします。

HPE 3PAR アレイへの接続時に監視ディスク（仮想ボリューム、最小 600 MB）またはその他の仮想ボリュームを準備する

3PAR StoreServ アレイの監視ディスクをプロビジョニングできます。

前提条件

アレイ情報を保存フィールドを使用して、ストレージアレイが構成済みであることを確認します。詳細については、「[アレイ管理ログイン詳細の設定](#)」を参照してください。

手順

1. **監視ディスク（最小 600 MB）**に使用する仮想ボリュームまたはその他の仮想ボリュームを準備するをクリックして、3PAR StoreServ 管理コンソール (SSMC) のログインウィンドウを起動します。
2. 必要なログイン認証情報を入力します。
3. 以下のいずれかの操作を実行します。

- ・ ホストの作成
- ・ 仮想ボリュームの作成
- ・ 仮想ボリュームのエクスポート

ホストの作成

フィールドにマウスカーソルを重ねると、ツールヒントが表示されます。

全般

必須またはオプションの設定に対して、選択肢を入力または選択します。

パス

ホストパスを追加するには、**FC の追加**または**iSCSI の追加**をクリックし、表示されたダイアログの指示に従います。リストからパスを削除するには、その削除アイコン (✕)。

Smart SAN パスを編集するには、編集アイコン (✎) をクリックし、表示されたダイアログの指示に従います。

CHAP 設定

iSCSI ホストでは、CHAP セキュリティ設定の選択肢を入力します。

追加設定

ホストのオプション情報を入力するには、**記述子展開**アイコン (▶) をクリックします。

選択が完了したら、**作成**をクリックし、アクションを開始してダイアログを閉じるか、または**作成 +**をクリックし、アクションを開始してダイアログを開いたままにします。

仮想ボリュームの作成

フィールドにマウスカーソルを重ねると、ツールヒントが表示されます。

ヒント：ダイアログの上部にある**詳細オプション**チェックボックスを選択すると、CPG の割り当て警告と割り当て制限（サポートされている場合）オプション、および仮想ボリュームの**特殊属性**オプションを指定することができます。

全般

必須およびオプションの設定に対して、選択肢を入力または選択します。

保護と追加設定

ボリューム

コピー CPG、ボリューム数、およびボリュームセットなどの設定を指定するには、**ボリューム展開**アイコン (▶) をクリックします。

スナップショット

作成済みのポリシーからスナップショットポリシーを選択するには、**スナップショット展開**アイコン (▶) をクリックします。スナップショットポリシーは、ポリシー名、スケジュール、保持期間、有効期限、および名前パターンを指定します。利用可能なデフォルトポリシーは、**毎時**、**日次**、および**週次**です。

すでにスナップショットポリシーが直接割り当てられている仮想ボリュームセットの一部である仮想ボリュームにスナップショットポリシーを割り当てようとすると、警告メッセージが表示されます。

Remote Copy グループ

仮想ボリュームを追加する必要がある Remote Copy グループを表示するには、**Remote Copy グループ**展開アイコン (▶) をクリックします。ドロップダウンに、RC グループ名、モード、および構成が表示

されます。仮想ボリュームにターゲットアレイが割り当てられていない場合、表示する Remote Copy グループはありません。

RMC 保護

使用可能なポリシーから、関連付けられた仮想ボリュームの保護ポリシーを指定できます。**RMC 保護**ドロップダウンはデフォルトで展開されます。

ポリシーの追加をクリックし、表示されたダイアログの手順に従います。

エクスポート

仮想ボリュームの作成時にホストへ新しい仮想ボリュームをエクスポートするには、**エクスポート**展開アイコン (▶) をクリックし、**追加**をクリックして、表示されたダイアログの指示に従います。

特殊属性

仮想ボリュームのボリューム ID を指定する、失効したスナップショット、1 ホスト限定のエクスポート、ゼロ検出、保持時間、および有効期限などのオプションを有効または無効にするは、**特殊属性**展開アイコン (▶) をクリックします。

詳細オプションに対して、選択肢を入力または選択できます。

選択が完了したら、**作成**をクリックし、アクションを開始してダイアログを閉じるか、または**作成 +**をクリックし、アクションを開始してダイアログを開いたままにします。

仮想ボリュームのエクスポート

フィールドにマウスカーソルを重ねると、ツールヒントが表示されます。

全般

このパネルには、仮想ボリューム画面で選択された仮想ボリュームのストレージシステムおよび仮想ドメインが表示されます。

仮想ボリューム

仮想ボリューム画面で選択された仮想ボリュームは、このパネルにリストされます。

エクスポート先

エクスポート先のホストまたはホストセットを選択するには、このパネルの**追加**をクリックし、表示されたダイアログの指示に従います。

次と共にエクスポート

LUN ボックスの LUN 値を受け入れるかまたは選択します。または、**自動**チェックボックスを選択します。

- ・ 1 つのホストへ 1 つの仮想ボリュームをエクスポートする場合、次に利用可能な LUN が **LUN** ボックスに表示されます。
- ・ 複数の仮想ボリュームをエクスポートする場合、次に利用可能な LUN 範囲が **LUN** ボックスに表示されます。
- ・ 別の LUN または LUN 範囲を指定するには、リストから 1 つまたは複数の LUN を選択します。また、LUN 番号を 1 つ入力することも、カンマで区切った LUN 番号 (例: 1, 2, 3) を入力することも、またはダッシュを使用して LUN 範囲 (例: 1-5) を入力することもできます。

自動オプションの使用

- ・ 自動オプションを指定して複数のホストにエクスポートすると、各仮想ボリュームは、各ホストの、異なる LUN に割り当てられます。
- ・ 自動オプションを指定せずに複数のホストにエクスポートすると、各仮想ボリュームは、各ホストの、同じ LUN に割り当てられます。

選択が完了したら、エクスポートをクリックし、アクションを開始してダイアログを閉じます。

監視ディスクボリュームまたは他のディスクボリュームのプロビジョニング

監視ディスクは、実際のディスクで、クラスターに共通のディスクストレージによって用意されます。ノードは、ディスクへの排他的アクセスを調整します。このディスクには、クラスター構成データが格納されます。

ディスクの管理を起動するには、このリンクをクリックします。マップした仮想ディスク上にボリュームを作成できます。

クラスター構成

HPE ストレージファイルコントローラーの物理的な設置が完了したら、社内に新しいシステムを展開する前に、システムを構成する必要があります。ローカル管理者グループのメンバーユーザーのログオン時に自動的に開く初期構成タスク (ICT) ウィンドウを使用して、システムを構成することができます。ICT の複数のインスタンスを同時に開くことはできません。

システム構成やクラスターの展開は、すべて第 1 ノード（つまりローカルノード）から実行されます。システム内の第 1 ノードは、お手持ちのストレージシステムのクイックスタートガイドに記載のとおり、最初に Windows セットアップウィザードを実行するように選択されています。ICT のタスクを順番に実行します。

注記:

- ・ クラスターの作成時には、両方のノードのハードウェア構成、ファームウェア、および Windows Update が同じであることを確認してください。
- ・ ウィンドウの右下のメッセージが示すとおり、ICT は定期的に更新されます。更新中に ICT タスクを選択すると、そのタスク用のアプリケーションの起動が遅くなります。**F5** を押して ICT を更新することもできます。
- ・ ICT が第 2 ノードに接続できる場合にのみ有効となるタスクが複数あります。
- ・ ICT は初期セットアップを目的としているため、初期セットアップが完了した後は、ウィンドウの下部にある**次のログオン時にこのウィンドウを表示しない**チェックボックスを選択できます。後で ICT を起動する場合は、`c:\windows\system32\oemoobe\oemoobe.exe` コマンドを入力してください。

ICT には以下のタスクが含まれています。

- ・ **接続ステータス**
- ・ **ネットワーキング**
- ・ **システム設定**
- ・ **通知**
- ・ **ストレージアレイ管理**
- ・ **共用記憶装置**
- ・ **クラスターの構成**
- ・ **このクラスターの保護**

HPE 3PAR StoreServ および MSA アレイのクラスターの構成

前提条件

- ・ ファイルコントローラーがドメインに接続されていることを確認します。
- ・ ドメインユーザーの認証情報でファイルコントローラーにログインしていることを確認します。
- ・ Witness ディスクが構成されていることを確認します。

クラスターの検証と作成

前提条件

このタスクを実行するには、ローカル管理者グループのメンバーであるドメインアカウントを使用してください。このタスクは、ICT が第 2 ノードに接続されていて、その両方のノードがクラスターの一部でない場合にのみ有効となります。

手順

1. **クラスターの検証と作成**を選択します。
フェイルオーバークラスターマネージャーウィザードが表示されます。
2. ウィザードの右ペインにある**クラスターの作成**リンクをクリックします。
クラスターの作成ウィザードが表示されます。
3. 表示された情報を確認し、**次へ**をクリックします。
4. クラスターの一部にするサーバーの IP アドレスを追加し、**次へ**をクリックします。

注記: 少なくともひとつのサーバーを追加してください。

サーバーを 1 つしか追加しないと、クラスター名の入力を促すメッセージが表示され、単一ノードの検証はスキップされます。

複数のサーバーを追加すると、検証テストの実行を促すメッセージが表示されます。

5. **はい**をクリックします。
構成の検証ウィザードが表示されます。
6. **すべてのテストを実行する（推奨）**または**テストのみを実行する**ボタンのいずれかを選択して、**次へ**をクリックします。

注記: HPE では、クラスターを作成する前に検証テストを実行することを強くお勧めします。

7. **次へ**をクリックして確認します。
このプロセスは、完了までに数分かかります。
8. **レポートの表示**をクリックします。
検証レポートが表示されます。
9. **終了**をクリックします。
クラスターの作成ウィザードが表示され、**構成の検証**ウィザードが終了します。
10. クラスター名を入力し、**次へ**をクリックします。
概要画面が表示されます。
11. **次へ**をクリックします。
フェイルオーバークラスターが作成されたことを示す確認画面が表示されます。

12. レポートの表示をクリックします。
 クラスター作成レポートが表示されます。
13. 終了をクリックします。

Nimble アレイに接続されているクラスターの構成

共有ストレージが検出されなかった場合、クラスター構成のタスクは無効になります。クラスターの構成では、以下のタスクを実行できます。

クラスターを構成するには、以下の手順に従ってください。

1. イニシエーターグループの作成とグループへのホストの割り当て
2. Nimble アレイボリュームのプロビジョニング
3. 共有ストレージのプロビジョニング
4. Windows ボリュームのプロビジョニング
5. 監視ディスクストレージのプロビジョニング
6. クラスターの検証と作成

イニシエーターグループを作成し、ホストグループに割り当て

イニシエーターは、Nimble アレイに接続された HPE ストレージファイルコントローラー上のポートで、ストレージアレイ上のターゲットポートとの接続を開始します。iSCSI ファブリックを介して 1 つ以上のターゲットポートへの接続を開始する Ethernet ネットワークインターフェイスカード (NIC) ポート、またはファイバーチャネルファブリックを介して 1 つ以上のターゲットポートへの接続を開始するファイバーチャネルホストバスアダプター (HBA) ポートです。

イニシエーターグループは、単一ユニットとして管理される iSCSI イニシエーターまたはファイバーチャネルイニシエーターの集合です。HPE ストレージファイルコントローラーをクラスターに設定する場合は、すべてのノードの適切なポートをすべて同じイニシエーターグループに設定してください。

・ iSCSI イニシエーターグループ

iSCSI イニシエーターグループは、1 つ以上の iSCSI イニシエーターの集合で、それぞれのイニシエーターに固有の iSCSI 修飾名 (IQN) と IP アドレスがあります。各 IQN は、iSCSI ベースのクライアント上にある単一のネットワークインターフェイスカード (NIC) を Windows サーバー、ESXi、または Linux ホストの形式で表します。Nimble アレイに iSCSI イニシエーターグループを設定し、ベンダーの推奨に従って、クライアント側の iSCSI イニシエーターを設定します。

注記: デフォルトでは、iSCSI ボリュームはイニシエーターへのアクセスを拒否します。イニシエーターグループ内のイニシエーターがボリュームにアクセスできるようにするには、目的のイニシエーターを含む ACL を設定し、ボリュームに接続する必要があります。

・ ファイバーチャネルイニシエーターグループ

ファイバーチャネルイニシエーターグループは、1 つ以上のイニシエーターの集合で、それぞれのイニシエーターには固有のワールドワイドポート名 (WWPN) があります。各 WWPN は、ファイバーチャネルベースのクライアント上にある 1 つのホストバスアダプター (HBA) ポートを Windows サーバー、ESXi、または Linux ホストの形式で表します。Nimble アレイでファイバーチャネルイニシエーターグループを構成します。

注記: デフォルトでは、ファイバーチャネルボリュームはイニシエーターへのアクセスを拒否します。イニシエーターグループ内のイニシエーターがボリュームにアクセスできるようにするには、目的のイニシエーターを含む ACL を設定し、ボリュームに接続する必要があります。

イニシエーターグループを作成するには、以下を実行します。

注記: FC および iSCSI イニシエーターグループは、HPE ストレージファイルコントローラーに接続されている Nimble 管理グループのタイプに基づいて自動で選択されます。

1. ICT タスクグループの **クラスタを設定 > イニシエーターグループを作成し、ホストグループに割り当て** をクリックします。
2. **イニシエーターグループを作成** ウィザードにイニシエーターグループの名前を入力します。
名前の割り当てには、64 個の英数字の文字列を使用できます。ハイフンとドットは、2 番目以降の文字に使用できます。たとえば、myobject-5 のように指定できます。イニシエーターグループ名にアンダースコア記号は使用しないでください。
3. 各イニシエーターの **エイリアス** セクションに代替名を入力します。
4. ファイバーチャネルイニシエーターグループの場合は、**WWPN** ドロップダウンリストからワールドワイドポート名 (WWPN) を選択します。
iSCSI イニシエーターグループの場合は、IP アドレスを入力し、**IQN** ドロップダウンメニューから **IQN** を選択します。
5. **列を追加** をクリックして列を追加するか、**列を削除** をクリックして列を削除します。
6. **イニシエーターグループを作成** をクリックします。
イニシエーターグループが作成されましたというメッセージが表示されます。
7. **OK** をクリックして終了します。

Nimble アレイボリュームのプロビジョニング

1. **ストレージアレイの構成 > Nimble アレイボリュームをプロビジョニングする** をクリックします。
2. **作成または既存のボリュームを使用する** を選択します。
3. **名前** セクションに、ボリュームの名前を入力します。
英字 (大文字と小文字)、数字、およびアンダースコア () を使用できます。他の特殊文字は使用しないでください。
4. **説明** セクションに説明を入力します。
テキスト内にスペースがある場合は、テキストを引用符で囲んでください。
5. **場所** ドロップダウンメニューから、場所を選択します。
6. **パフォーマンスポリシー** ドロップダウンメニューから、パフォーマンスポリシーのタイプを選択します。
パフォーマンスポリシーは、特定のアプリケーションのパフォーマンスを最適に設定するためのものです。パフォーマンスポリシーは、ボリュームを使用するアプリケーションの期待される特性に基づいて、ボリュームのパフォーマンスを最適化するのに役立ちます。パフォーマンスポリシーでは、クォータを超えたときの、関連するボリュームの動作を定義します。既存のパフォーマンスポリシーとボリュームを関連付けることができます。
7. ボリュームのサイズは、MiB、GiB、または TiB で指定します。

サイズはゼロより大きい値でなければなりません。

8. **データ保護**ドロップダウンメニューから、データ保護のタイプを選択します。

- ・ **ボリュームコレクションがありません**：ボリュームのスナップショットは作成されません。
- ・ **ボリュームコレクションに参加**：既存のボリュームコレクションのルールを選択して、このボリュームに適用します。
- ・ **新しいボリュームコレクションを作成**：このボリュームのボリュームコレクションのルールを作成します。

9. **アクセス**ドロップダウンメニューからアクセスのタイプを選択して、ボリュームをストレージファイルコントローラーと接続します。

10. (オプション) **ボリュームのキャッシュフィールド**で、**ピン留め済み**または**通常**のいずれかを選択します。

ピン留め済みを選択すると、

キャッシュは、共有リソースです。ボリュームをピン留めすると、ボリュームのパフォーマンスに影響を及ぼす可能性があります。この設定は、最大のパフォーマンスが必要なワークロードに対してのみ使用してください。というメッセージが表示されます。

11. **作成**をクリックします。

メッセージボリュームが正常に作成されましたが表示されます。

12. **OK** をクリックします。

共有ストレージのプロビジョニング

このタスクグループでは、ノード間の共有ストレージの結果のステータスを参照することができます。両方のノードは、一意のストレージ識別子をベースとして、同じストレージにアクセスする必要があります。共有ストレージは、ファイルコントローラー内のディスクです。共有ストレージに表示されるメッセージを以下に示します。

- ・ **共有ストレージが見つかりません**：システムは、基準に合う共通の共有ストレージを見つけることができませんでした。共有ストレージが利用可能かどうかを検証するには、各サーバーで PowerShell スクリプト「get-disk」を実行し、2つのサーバーの**ユニーク ID**を比較します。

たとえば、`get-disk | select uniqueid,friendlyname,operationalstatus`を実行します。

- ・ **共有ストレージが見つかりました**：監視ディスクに使用可能なストレージが見つかりました。両方のノードで同じユニーク ID を持つディスクは、共有として扱われます。

Nimble 用ストレージでの Windows ボリュームのプロビジョニング

Nimble アレイを使用すると、ボリュームがプロビジョニングされ、Windows OS に raw ディスクとして提供されます。Windows ボリュームは、データの格納に使用する前に、このディスクに作成する必要があります。**Windows ボリュームをプロビジョニングする**オプションを使用すると、以下のことが可能になります。

- ・ ディスクの初期化
- ・ ファイルシステムによるディスクのフォーマット
- ・ シンプルボリュームの作成
- ・ ディスクのドライブ文字の指定

手順

1. ストレージアレイの構成 > Windows ボリュームをプロビジョニングするをクリックします。
ディスクの管理コンソールが表示されます。
2. 使用可能なディスクのいずれかを右クリックします。
新しいシンプルボリューム画面が表示されます。
3. 新しいシンプルボリューム画面でボリュームのサイズを指定し、次へをクリックします。
4. 簡単にアクセスするためのドライブ文字またはパスを指定し、次へをクリックします。
5. ファイルシステムと割り当てユニットサイズを選択し、ボリュームの名前を入力して、ボリュームをフォーマットしデータを格納します。
6. クイックフォーマットするを選択し、次へをクリックします。
新しいシンプルボリュームの完了画面が表示されます。
7. ボリュームが正常に作成されたら、完了をクリックします。
ICT のステータス列に、ステータスとパスが表示されます。

監視ディスクストレージのプロビジョニング

監視ディスクストレージのプロビジョニングリンクをクリックすると、Nimble ボリュームをプロビジョニングするためのオンラインヘルプのプロセスへのリンクが開きます。Nimble ボリュームは HPE ストレージファイルコントローラー用に作成し、イニシエーターグループを割り当てる必要があります。

最小サイズが 600 MB のボリュームを作成し、ボリュームの目的がわかるように、ボリュームに、Quorum または Witness の名前を付けることをお勧めします。Windows でドライブをフォーマットするときには、ドライブ文字 (W または Q) を割り当てます。これが他のファイル共有リソースで必要な場合は、ドライブ文字を入力する必要はありません。

クラスタの検証と作成

前提条件

このタスクを実行するには、ローカル管理者グループのメンバーであるドメインアカウントを使用してください。このタスクは、ICT が第 2 ノードに接続されていて、その両方のノードがクラスタの一部でない場合にのみ有効となります。

手順

1. クラスタの検証と作成を選択します。
フェイルオーバークラスタマネージャーウィザードが表示されます。
2. ウィザードの右ペインにあるクラスタの作成リンクをクリックします。
クラスタの作成ウィザードが表示されます。
3. 表示された情報を確認し、次へをクリックします。
4. クラスタの一部にするサーバーの IP アドレスを追加し、次へをクリックします。

注記: 少なくともひとつのサーバーを追加してください。

サーバーを 1 つしか追加しないと、クラスタ名の入力を促すメッセージが表示され、単一ノードの検証はスキップされます。

複数のサーバーを追加すると、検証テストの実行を促すメッセージが表示されます。

5. はいをクリックします。
構成の検証ウィザードが表示されます。
6. すべてのテストを実行する（推奨）またはテストのみを実行するボタンのいずれかを選択して、次へをクリックします。

注記: HPE では、クラスターを作成する前に検証テストを実行することを強くお勧めします。

7. 次へをクリックして確認します。
このプロセスは、完了までに数分かかります。
8. レポートの表示をクリックします。
検証レポートが表示されます。
9. 終了をクリックします。
クラスターの作成ウィザードが表示され、構成の検証ウィザードが終了します。
10. クラスター名を入力し、次へをクリックします。
概要画面が表示されます。
11. 次へをクリックします。
フェイルオーバークラスターが作成されたことを示す確認画面が表示されます。
12. レポートの表示をクリックします。
クラスター作成レポートが表示されます。
13. 終了をクリックします。

このクラスターの保護

クラスター対応更新を使用して、サーバーが、重要なソフトウェア更新と拡張機能を Windows Update から直接受信できるようにします。

- ・ クラスター対応更新
- ・ Carbonite ソフトウェア

クラスター対応更新の使用

CAU（Cluster-Aware Updating：クラスター対応更新）は、自動化かつ統合された信頼性の高い更新機能であり、クラスター化されたサーバーの更新を、その処理中に可用性をほとんどあるいはまったく損なうことなく行うことができます。

更新する際に、CAU が以下のタスクを実行します。

手順

1. クラスターの各ノードをノードメンテナンスモードにする。
2. クラスターの役割をノード外に移動する。
3. 更新とすべての依存更新をインストールする。
4. 必要に応じて再起動を実行する。
5. ノードのメンテナンスモードを終了する。

6. クラスターの役割をノード上で復元する。

7. 次のノードの更新に移る。

CAU は、クラスターの更新処理全体を以下の 2 つのモードで調整できます。

- ・ **自動更新モード** — CAU のクラスター化対応の役割はフェイルオーバークラスターでワークロードとして構成されており、Windows Update をクラスターノードに適用するためのプロセスを制御するスケジューラを管理します。クラスターは、デフォルトまたはカスタムの更新実行 (Updating Run) プロファイルを使用して、スケジュールされた時間に自己更新します。更新の実行中に、CAU 更新コーディネータープロセスが、CAU のクラスター化された役割を所有しているノードから開始され、以降のクラスターノードが順次更新されます。自己更新モードでは、CAU は完全に自動化されたエンドツーエンドの更新プロセスを使用することで、フェイルオーバークラスターを更新できます。このモードでは、管理者がオンデマンドで更新を開始したり、あるいは必要に応じてリモート更新手法を使用することができます。自己更新モードでは、管理者はクラスターに接続して `Get-CauRun Windows` PowerShell コマンドレットを実行することによって、進行中の更新に関する要約情報を得ることができます。
- ・ **リモート更新モード** — Windows Storage Server 2016 が動作しているリモートコンピューターが、CAU ツールで更新コーディネーターとして構成されます。更新コーディネーターは、更新実行中に更新されるクラスターのメンバーではありません。管理者は、デフォルトまたはカスタムの更新実行プロファイルを使用することで、リモートコンピューターから更新実行をオンデマンドで開始できます。リモート更新モードは、更新実行中の進捗状況のリアルタイム監視と、Windows Storage Server 2016 のサーバーコアで動作しているクラスターで役立ちます。

注記:

- ・ 各クラスターノードは、Windows Storage Server 2016 でデフォルトで有効になっている WinRM Remoting を許可するように構成する必要があります。
- ・ クラスター内の各ノードの Windows Update 機能は、クラスターノードを自動更新しないように構成する必要があります。ただし、Hewlett Packard Enterprise では、クラスターノードで Windows Update を自動ダウンロードするように設定して、更新実行の時間を最小限に短縮し、計画された IT メンテナンス期間内に完了する確率を高めることをお勧めします。なお、各クラスターノードで Windows Update の自動ダウンロード機能を無効にした場合でも、CAU は機能します。
- ・ クラスター対応更新は、Microsoft 更新サービスおよびエンタープライズレベルの WSUS (Windows サーバー更新サービス) の両方で動作します。

CAU について詳しくは、次の Microsoft Technet の記事を参照してください。 [クラスター対応更新の概要](#)

CAU を使用するには、以下の手順に従ってください。

- ・ クラスター対応更新セクションで、**クラスター対応更新**を使用してこのクラスターを安全で最新の状態に保つをクリックします。
クラスター対応更新画面が表示されます。
- ・ クラスターの更新に必要なオプションを選択します。画面の各種オプションの詳細については、CAU オンラインヘルプを参照してください。

Carbonite ソフトウェア

Carbonite ポートフォリオには、障害回復と高可用性に対応するレプリケーションソフトウェアが含まれています。このリンクをクリックすると、Double-Take Availability ソフトウェアのトライアルバージョンのインストールについて表示する HTML ページが開きます。このトライアルバージョンにより、ご使用の

環境でこのソフトウェアを評価することができます。デスクトップにある **Carbonite** ソフトウェアアイコンをダブルクリックすることで、HTML ページに直接アクセスすることもできます。

マルチサイト環境用のフェイルオーバープロパティの構成

Peer Persistence を HPE 3PAR StoreServ アレイで、Cluster Extension を他のストレージアレイで使用してマルチサイト環境用のフェイルオーバープロパティを構成できます。

その他のアクセス方式

HPE ストレージファイルコントローラーの設置プロセスが完了し、システムの IP アドレスが割り当てられると、システムへのアクセス時にリモートデスクトップや CLI 方式も使用できるようになります。

リモートデスクトップの使用

リモートデスクトップでは、任意のクライアントからサーバーにログオンして、サーバーをリモート管理することができます。リモートデスクトップは、リモート管理用にインストールされ、同時に 2 つのセッションを実行できます。セッションの実行には 1 つのライセンスが必要になるため、他のユーザーに影響する場合があります。2 つのセッションが実行中の場合、他のユーザーはアクセスが拒否されます。

HPE ストレージファイルコントローラーシステムをリモートデスクトップ方式でネットワークに接続するには、以下の手順に従ってください。

手順

1. PC クライアントで、**スタート > Windows PowerShell** を選択します。msc と入力して **Enter** キーを押します。
2. コンピューターボックスに、HPE ストレージファイルコントローラーの IP アドレスを入力して、**接続** をクリックします。
3. 管理者のユーザー名とパスワードで、HPE ストレージファイルコントローラーにログオンします。

CLI を使用

アレイにログインして、コマンドを実行します。詳しくは、次を参照してください。

- ・ [HPE 3PAR StoreServ CLI リファレンスガイド](#)
- ・ [HPE Nimble アレイコマンドリファレンスガイド](#)

HPE ストレージファイルコントローラーの管理

ICT ウィンドウを使用してシステムの初期セットアップを完了した後は、システムの管理にはサーバーマネージャーを使用します。サーバーマネージャーは、ICT を閉じると自動的に起動されます。サーバーマネージャーは、タスクバーにあるショートカットアイコンをクリックすることで、HPE ストレージファイルコントローラーデスクトップから起動することもできます。Microsoft TechNet の記事（[サーバーマネージャーを使用して複数のリモートサーバーを管理する](#)）で説明されているように、ローカルの HPE ストレージファイルコントローラーシステムのほか、他の Windows サーバーも管理できます。

リモートサーバー管理ツールは、Windows 8/10 クライアントにインストールすると、HPE ストレージファイルコントローラーのリモート管理にも使用できます。このツールをダウンロードするには、[Microsoft Download Center](#) に移動してください。

注記: ローカルシステムにのみ適用されます。

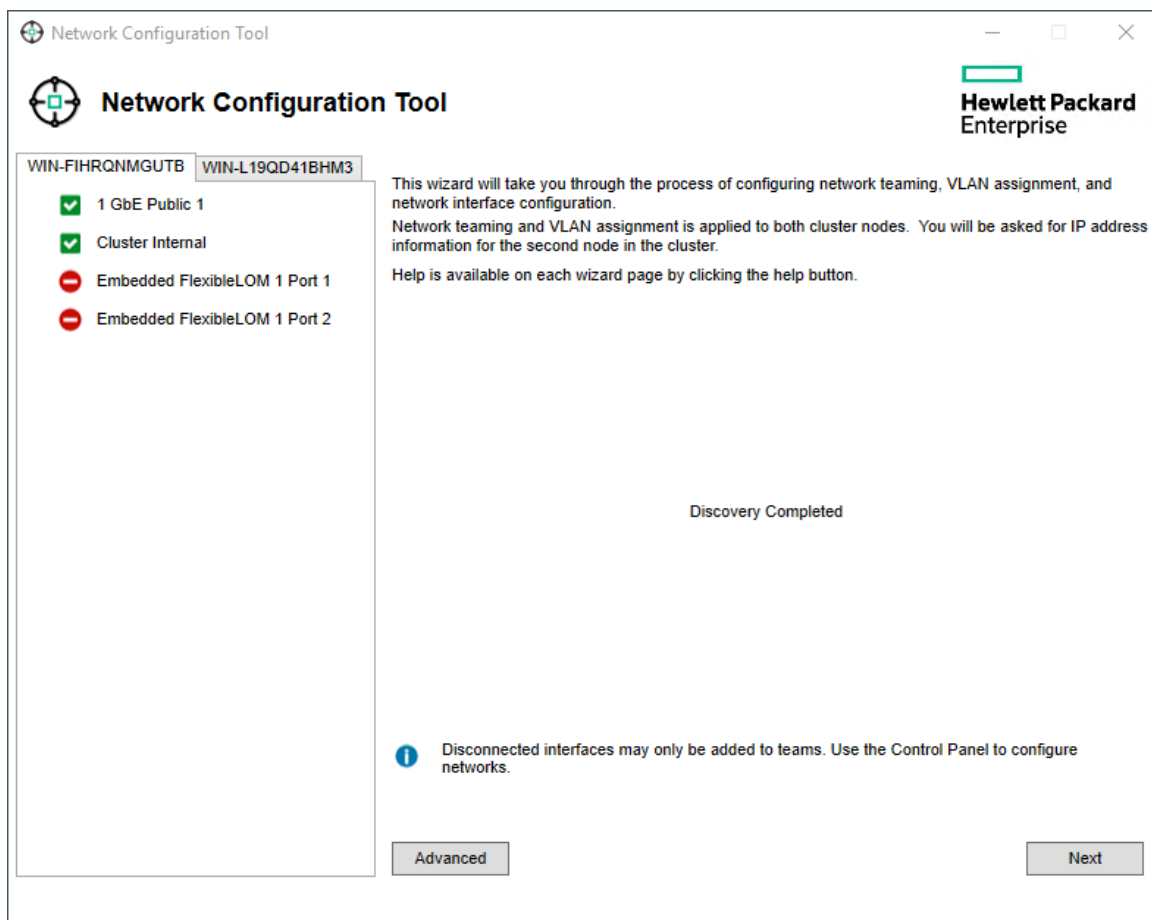
ストレージ関連のタスクの多くは、サーバーマネージャーのファイルサービスと記憶域サービスから実行できます。ツールメニューには、Windows 管理者が使い慣れている一般的なユーティリティが含まれています。ツール > HPE ストレージファイルコントローラーメニューグループには、HPE 固有の管理ツールと、HPE ストレージファイルコントローラーシステムの管理に関係する、使用頻度の高い Windows ツールも含まれています。ツール > HPE ストレージファイルコントローラーメニューには、以下のオプションが含まれています。

- ・ **システムレポートの収集** — データ収集および診断ツールが起動されます。システムレポートの収集は、データ収集および診断ツールです。このツールは、HPE ストレージファイルコントローラーの状態について広範なデータを収集します。これらのデータは、HPE サポートが問題の診断に利用します。データ収集の進捗が表示され、収集が完了すると、Windows Explorer で、収集された情報が含まれるタイムスタンプ付きの.cab アーカイブを含むフォルダーが開きます。フォルダーは C:\Windows\HPSReports\Enhanced\Report\cab です。HPE サポートは、.cab ファイルをアップロードできる FTP サイトを提供します。
- ・ **電子メールアラートの構成** — ハードウェアイベントが通知される電子メール受信者を構成することができるイベント通知設定ウィザードが起動されます。
- ・ **ネットワークの構成** — ネットワークの構成ツールを起動します。
- ・ **ドキュメント** — オンラインヘルプが起動されます。
- ・ **重複排除機能設定の評価** - Windows の ddpeval.exe ツールが起動されます。このツールを使用して、特定のボリュームで重複排除を有効にした場合に削減されるストレージ容量を評価できます。
- ・ **ファイル共有スナップショット** - ファイル共有のスナップショットを作成するためのストレージのスケジュール設定および構成を行う Windows ツールが起動されます。
- ・ **iLO 設定** — Lights-Out オンライン構成ユーティリティが起動されます。
- ・ **製品の登録** — 製品を登録するための [HPE 製品の登録](#) ページが起動されます。

ネットワーク構成ツールの使用方法

NCT ウィザードを使用すると、HPE ストレージファイルコントローラーのネットワークインターフェイスを構成することができます。NCT は、システムのすべての利用可能なネットワークインターフェイスを分析し、間違った構成を行う可能性を低くするために別のネットワーク構成を選択できるようにします。また、ネットワーク環境でのエラーのトラブルシューティングに役立てるために、構成の検証も行います。

- ❗ **重要:** HPE では、このツールを使用してネットワークインターフェイスを構成することを強くお勧めします。



ネットワーク構成ファイルを使用してネットワーク構成をインポートすることもできます。ネットワーク構成ファイルについて詳しくは、**ネットワーク構成のインポート**を参照してください。

以下の方法で NCT（ネットワーク構成ツール）を直接起動できます。

- ・ コマンドプロンプトまたは PowerShell を開き、NCT と入力する。
- ・ サーバーマネージャーを開き、ツール > HPE ストレージファイルコントローラー > ネットワークの構成の順に選択する。
- ・ デスクトップのシステムツールフォルダーをダブルクリックし、ネットワークの構成をクリックする。
- ・ スタート画面のネットワークの構成をクリックする。
- ・ デスクトップにあるネットワークの構成アイコンをクリックする。

NCT は、2 つのペインに分かれています。ネットワークインターフェイスを構成するため、またはネットワーク構成を検証するために NCT を起動すると、ネットワーク構成の検出が開始されます。システムの検出が完了すると、左ペイン（インターフェイスペイン）に、検出されたインターフェイスとその動作状態が表示されます。右ペインには、現在の構成手順についての説明が表示されます。インターフェイスペイン内のネットワークインターフェイス上にホバーすると、デバイス名、インターフェイス名、およびステータスが表示されます。たとえば、インターフェイスは、無効です、切断されています、または有効ですになっています。

-
- ❗ **重要:** NCT の使用中に別のツールを使用してシステムのネットワーク構成を変更した場合、その変更は NCT を閉じて再起動したときだけ NCT に反映されます。
-

NCT ウィザードには、以下のセクションがあります。

- ・ ネットワークインターフェイス
- ・ ネットワークチームの構成
- ・ ネットワークの VLAN の構成
- ・ ネットワークインターフェイスの IP 構成
- ・ ネットワーク構成の概要
- ・ ネットワーク構成の検証

通知システム

通知システム機能を使用すると、空き領域、未割り当て領域、および使用済み領域などの各種のシステムパラメーターの電子メールアラートを設定することができます。電子メールアラートは、指定されたルールおよび通知パラメーターをベースに比較し、比較が true の場合に送信されます。たとえば、使用済み領域パラメーターの値として 100 MB を設定すると、メールアラートは、システム内の使用済み領域が 100 MB に達したときに送信されます。

注記: 電子メールアラートは、システム全体のストレージについて送信されます（特定のドライブについてではありません）。

以下の方法で通知システムダイアログボックスにアクセスできます。

- ・ デスクトップにある **HPE ストレージファイルコントローラー通知システム**アイコンをダブルクリックする。
- ・ サーバーマネージャーを開き、ツール > HPE ストレージファイルコントローラーをクリックし、**通知システム**を選択する。
- ・ スタート画面の**通知システム**をクリックする。

メールアラートを設定するには、以下の手順に従ってください。

手順

1. **連絡先情報**グループに、フルネーム、アラートを送信および受信する電子メールアドレス、および SMTP サーバー名を入力します。
2. **テスト**をクリックして、SMTP サーバーの検証を行います。この手順はオプションです。

注記: 検証が成功すると、指定されたメールアドレスにメールが送信され、確認メッセージが画面に表示されます。検証が失敗すると、SMTP サーバーの詳細を確認する必要があるというメッセージが表示されます。

3. **通知パラメーター**グループで、パラメーターと比較を選択してから、パラメーター値に対して比較する値を入力します。**毎日通知**チェックボックスを選択すると、電子メール通知が毎日送信されます。**毎日通知**チェックボックスをオフにすると、メール通知が 1 回だけ送信されます。ただし、通知ルールが変更されると、電子メール通知が送信されます。

パラメーター	比較	値
・ 空き領域	・ 等しい	・ 100 MB
・ 未割り当て領域	・ 等しくない	・ 100 MiB
・ 使用済み領域	・ 未滿	・ 5%
	・ 以下	「空き領域」に対してのみ
	・ より大きい	
	・ 以上	

注記: 通知システムにおけるパラメーターの値を指定する際に単位を指定しない場合、デフォルトの単位は「バイト」とみなされます。たとえば、空き領域のパラメーターに対し、GB などの単位を指定せずに 100 という値を入力した場合、この値はデフォルトで 100 バイトとみなされます。

4. OK をクリックします。

ルールが正常に保存されましたメッセージが表示されます。

既存のルールを削除するには、**削除**をクリックしてください。

管理ツール

HPE ストレージファイルコントローラーシステムには、ストレージシステムの管理タスクを簡略化する管理ツールが複数あります。

管理ツールは、初期サーバー構成、ストレージおよび共有フォルダーの簡易セットアップと管理、iSCSI ターゲットのためのユーザーインターフェイスを提供します。ネットワーク接続ストレージ専用調整されています。

リモート管理

システムのリモート管理には次のツールを使用できます。

- ・ リモートデスクトップ
- ・ RSAT ツール経由での Windows 8 または 10 クライアント上のサーバーマネージャー
- ・ リモート PowerShell

ファイルサービスおよび記憶域サービス

ファイルサービスおよび記憶域サービスに含まれるテクノロジーは、1 つまたは複数のファイルコントローラーシステムをセットアップして管理する場合に役立ちます。

管理者はファイルサービスおよび記憶域サービス役割を使用して、サーバーマネージャーや Windows PowerShell を使用することで、複数のファイルコントローラーシステムとそれぞれの記憶域をセットアップおよび管理することができます。特定のアプリケーションでは、次のことを行うことができます。

- ・ サーバーマネージャーを使用して複数のファイルコントローラーシステムを 1 つのウィンドウからリモートで管理します。
- ・ Windows PowerShell を使用して、ファイルコントローラーの管理タスクの大半を自動化します。

データの重複排除

データの重複排除とは、データの重複を検出し、データの正確さや整合性を損なうことなくその重複を削除することです。この目的は、ファイルを小さな可変サイズのチャンク（32KB~128KB）に分割して重複するチャンクを識別し、各チャンクのコピーを 1 つだけ保持することによって、より多くのデータをより小さな領域に格納することです。重複するチャンクのコピーは、1 つのコピーへの参照に置き換えられます。チャンクは圧縮され、「System Volume Information」フォルダーの特別なコンテナファイルにまとめられます。

重複排除を有効にし、データを最適化した後では、ボリュームには、次のものが含まれます。

- ・ **最適化されなかったファイル** — たとえば、設定されているファイルエイジのポリシーに適合しないファイル、システム状態ファイル、代替データストリーム、暗号化されたファイル、拡張属性を含むファイル、32KB より小さいファイル、その他の再解析ポイントファイル、他のアプリケーションで使われているファイルなどがあります。
- ・ **最適化されたファイル** — 再解析ポイントとして保持されているファイルで、このファイルには、チャンクストアに含まれる個々のチャンクのマップへのポインターが含まれています。これらのポインターはファイルを復元する際に必要となります。
- ・ **チャンクストア** — 最適化されたファイルデータが保存されている場所です。
- ・ **追加の空き領域** — 最適化されたファイルおよびチャンクストアが占める領域は、最適化前と比較して大幅に少なくなります。

ボリューム上でデータの重複排除を有効にするには、以下の手順に従ってください。

手順

1. Windows サーバーマネージャーを開きます。
2. ファイルサービスと記憶域サービスを選択し、**ボリューム**を選択します。
3. データボリュームを右クリックし、**データ重複除去の構成**を選択します。
重複除去設定ウィンドウが表示されます。
4. 次の操作を実行します。
 - a. ボリュームのワークロードを選択します。
 - b. ファイルの作成日からファイルの重複排除を実行するまでの日数を入力します。
 - c. 重複排除を実行しないファイルタイプの拡張子を指定します。
 - d. **追加**をクリックして、重複排除を実行しないファイルを格納しているフォルダーを表示します。
5. **適用**をクリックしてこれらの設定を適用するか、または**重複除去スケジュールの設定**をクリックして重複排除のスケジュールを構成します。

詳しくは、Windows Storage Server 2016 のヘルプを参照してください。

ストレージ管理の概要

本章では、HPE ストレージファイルコントローラーシステムのストレージ構造を構成する一部のコンポーネントの概要を提供します。

論理コンポーネント

ボリューム

ボリュームがファイルとフォルダーを保存するために作成されて使用されます。ボリュームが作成される（たとえば、仮想ディスクごとに 1 つのボリューム）と、ファイル情報の保存に使用できる、ファイルシステムレイアウトが確立されます。HPE ストレージファイルコントローラーでは、NTFS および ReFS ファイルシステムフォーマットを使用できます。

NTFS フォーマットでは、汎用のファイルストレージに必要なほとんどの機能をサポートします。ReFS フォーマットにより導入された以下の機能により、従来不足していた機能の一部が補われています。

- ・ チェックサムによるメタデータ整合性。
- ・ オプションのユーザーデータ整合性のための整合性ストリーム。
- ・ 堅牢なディスクアップデート（書き込み時コピー）のための書き込み時割り当てトランザクションモデル。
- ・ ボリューム、ファイル、およびディレクトリサイズの拡大。
- ・ フォールトトレランスの場合のパフォーマンスおよび冗長性の確保のためのデータストライピング。
- ・ 潜在的なディスクエラーに対する保護のためのディスクのスクラブ。
- ・ すべてのケースで最大のボリューム可用性を実現するための、破損時のサルベージによる回復。

ただし、ReFS では、お使いのファイルデータストレージ環境で重要となるすべての機能を使用できるわけではありません。NTFS では、より適切なオプションがある可能性があります。ファイルシステムフォーマットを選択する前に、以下の表で、各機能が使用可能かどうか確認してください。

ファイルシステムの機能	NTFS	ReFS
大文字と小文字を区別するファイル名	はい	はい
ファイル名の太文字/小文字種別の保持	はい	はい
Unicode ファイル名	はい	はい
ACL の保持と強制	はい	はい
スパースファイル	はい	はい
リパースポイント	はい	はい
ファイル ID でのオープン	はい	はい
USN ジャーナル	はい	はい

表は続く

ファイルシステムの機能	NTFS	ReFS
ハードリンク	はい	いいえ
ファイルベースの圧縮	はい	いいえ
重複排除	はい	いいえ
オブジェクト ID	はい	いいえ
暗号化ファイルシステム	はい	いいえ
名前付きストリーム	はい	いいえ
トランザクション	はい	いいえ
拡張属性	はい	いいえ

ファイル共有 - SMB と NFS

以下のファイル共有プロトコルは、ボリュームに保存されているファイルおよびフォルダーへのリモートアクセスに使用できます。

- ・ サーバーメッセージブロック (SMB)
- ・ ネットワークファイルシステム (NFS)
- ・ ファイル転送プロトコル (FTP)
- ・ Hypertext Transfer Protocol (HTTP)

Windows クライアントと macOS クライアントで最もよく使用されるプロトコルは SMB です。Linux および UNIX オペレーティングシステムでは、NFS が使用されます。ファイル共有が、ボリュームのルートを含むあらゆるディレクトリツリーレベル（たとえば D:\）で作成されます。

ストレージ要素の使用

要素を作成する最後の手順は、要素のドライブ文字またはマウントポイントを決定し、要素をフォーマットすることです。作成された各要素は、ドライブ文字（利用可能な場合）、または既存のフォルダーまたはドライブ文字のマウントポイントとして存在することができます。いずれの方法もサポートされています。ただし、マウントポイントは、Microsoft Services for Unix を使用して共有される共有には使用できません。マウントポイントはいずれの方法でもセットアップできますが、NFS 共有と組み合わせて使用すると NFS 共有が不安定になります。

ファイルサーバーの管理

この章では、ファイルサーバーの管理に有用な多くのタスクとユーティリティについて説明します。

ファイルサービス管理

SAN 環境の HPE ストレージファイルコントローラーシステムに関する情報は、HPE の Web サイト (<http://www.hpe.com/info/SDGmanuals>) にある SAN Design Reference Guide で入手できます。

アレイ管理ユーティリティ

RAID アレイおよび LUN 用のストレージデバイスは、アレイ管理ユーティリティを使用して作成および管理します。Smart アレイでは、SSA を使用してください。

ディスクの管理ユーティリティ

ディスクの管理ツールは、ハードディスクやボリューム、またはそれらが保持しているパーティションを管理するために使用します。ディスクの管理は、ディスクの初期化、ボリュームの作成、NTFS および ReFS によるボリュームのフォーマットに使用します。

注記: リモートデスクトップ接続を介してディスクの管理ユーティリティにアクセスする場合、この接続は、サーバー上のディスクおよびボリュームの管理以外には使用できません。

ディスクとボリュームの管理のガイドライン

- ・ 1 つの論理ドライブが HPE ストレージファイルコントローラーのオペレーティングシステム用に構成されており、どのような形でも変更してはなりません。この論理ドライブは予約済みのボリュームであり、そのままの状態に維持する必要があります。
- ・ HPE ストレージファイルコントローラーでは、複数のアレイコントローラーにまたがるダイナミックボリュームをサポートしていません。また、ソフトウェア RAID ベースのダイナミックボリュームの使用もお勧めしません。ソフトウェアベースの RAID 構成よりも効率的であるため、Smart アレイコントローラーのハードウェアベースの RAID 構成機能を使用する必要があります。
- ・ 意味の通るボリュームラベルを使用するために、可能であれば、ボリュームラベルに組み込む対象のドライブ文字を指定します。識別する唯一の手段がボリュームラベルであるという場合も多く見られます。
- ・ システムのリストアに備えて、すべてのボリュームラベルとドライブ文字を記録しておきます。
- ・ 最後のディスクパーティションのみを拡張できます。
- ・ ベーシックディスクには最大で 4 つのプライマリパーティションを含めることができます。
- ・ スナップショット、パフォーマンス、最適化のサポートを最善の状態にするには、16K の割り当て（アロケーション）サイズでドライブをフォーマットします。
- ・ 重複排除シャドウコピー、暗号化、圧縮を最高レベルで提供できるため、NTFS 形式でフォーマットされたドライブの使用をお勧めします。
- ・ NTFS ボリュームのサイズは、重複排除またはボリュームシャドウコピーサービス（VSS）を使用したい場合、64TB 以下のサイズにする必要があります。また、64TB を超える書き込み可能スナップショットもサポートされていません。
- ・ ベーシックディスクが 2TB を超える場合は、GUID パーティションテーブル（GPT）スタイルでフォーマットしなければなりません。

最適化のスケジュール

最適化は、ローカルボリュームを分析し、断片化されたファイルやフォルダーがボリューム上で1つの連続した領域にまとまるように連結するプロセスです。これによって、ファイルシステムのパフォーマンスが向上します。最適化は、ファイルとフォルダーを連結し、ボリューム上の空き領域を連結します。このため、新しいファイルが断片化される可能性が低くなります。

ボリュームの最適化は、都合のよいときに自動的に行われるようにスケジュールできます。最適化は1回または繰り返し実行されるように設定できます。

注記: 特定の時刻前に実行する最適化をスケジュールすることによって、その時刻以降に最適化プロセスが実行されるのを防ぐことができます。その時刻になったときに最適化プロセスが実行されていた場合、プロセスは停止されます。この設定は、サーバーアクセスの要求が増える前に、最適化プロセスを必ず終了させるのに役立ちます。

シャドウコピーが有効になっているボリュームを最適化する場合、フォーマット時のクラスター（またはアロケーションユニット）サイズは16KB以上を使用してください。16KB以上を使用しないと、最適化がシャドウコピープロセスによる変更として登録します。これによって、キャッシュファイルの上限に達したときに、シャドウコピーにスナップショットを強制的に削除させる変更の回数が増えます。

△ 注意: アロケーションユニットサイズは、ドライブを再フォーマットしないと変更できません。再フォーマットされたドライブ上のデータは復旧できません。

ストレージの追加

ストレージの拡大/拡張は、次の3つの形式のいずれかで実行できます。

- ・ 元のLUNから、割り当てられていない容量を拡大します。
- ・ LUNに変更を加えて、追加のストレージを収容します。
- ・ 新しいLUNをシステムに追加します。

ストレージの拡張

拡張とは、すでに構成されているアレイに物理ディスクを追加するプロセスです。拡張を実行する前にアレイに存在していた論理ドライブ（またはボリューム）は変更されません。アレイ内の空き容量のみが変化します。拡張プロセスは、オペレーティングシステムから完全に独立しています。

注記:

アレイ上のストレージを拡張する方法については、ストレージアレイハードウェアのユーザードキュメントを参照してください。

Windows Storage Utilities によるストレージの拡大

ボリュームを拡大すると、論理ドライブのストレージ容量が増加します。このプロセス中、管理者は、通常はアレイを拡張した後で、同じアレイ上の既存の論理ドライブに新しいストレージ容量を追加します。

ボリュームシャドウコピー

ボリュームシャドウコピーサービスは、ボリュームのある時点でのスナップショット（シャドウコピー）を作成するための環境を提供します。シャドウコピーでは、ボリュームごとに最低64個のシャドウコピーをサポートします。

シャドウコピーには、指定された時点にボリューム上にあったファイルまたはフォルダーの以前のバージョンが含まれます。シャドウコピーのメカニズムを管理している間、以前のバージョンのファイルと

フォルダーは、クライアントからネットワークを通じてのみ入手可能で、ボリューム全体としてではなくフォルダーまたはファイルごとに表示されます。

シャドウコピー機能はデータブロックを使用します。ファイルシステムへの変更が行われると、シャドウコピーサービスは元のブロックを特殊なキャッシュファイルにコピーして、特定時点におけるファイルの一貫したビューが保持されます。スナップショットには元のブロックのサブセットだけが含まれるため、通常、キャッシュファイルは元のボリュームよりも小さくなります。スナップショットの元の形式では、ディスクへの更新が生じるまでブロックは移動されないため、スナップショットは場所を占有しません。

シャドウコピーを使用することにより、HPE ストレージファイルコントローラーシステムでは、選択したボリューム上のすべてのファイルの以前のバージョンを保持できます。エンドユーザーは、Windows のエクスプローラーでファイルを表示するための各クライアントのアドオンプログラムを使用して、ファイルまたはフォルダーにアクセスできます。ファイルの以前のバージョンまたはシャドウコピーにアクセスすることで、以下のことができます。

- ・ 誤って削除されたファイルを復旧する。以前のバージョンを開いて、安全な場所にコピーできます。
- ・ 誤って上書きされたファイルを復旧する。ファイルの以前のバージョンにアクセスできます。
- ・ 作業中にファイルの以前の数バージョンを見比べる。以前のバージョンを使用して、ファイルの 2 つのバージョンにおける変更点を見比べます。

シャドウコピーは、現在のバックアップ、アーカイブ、またはビジネスリカバリシステムに置き換わるものではありませんが、復元手順を簡略化できます。スナップショットには、元のデータブロックの部分だけが含まれ、シャドウコピーではメディアの故障によるデータ消失を防ぐことはできません。ただし、スナップショットの長所はシャドウコピーからデータをただちに復旧でき、テープからデータを復元するのに要する時間が短縮されます。

シャドウコピーの計画

セットアップをサーバー上で起動し、クライアントインターフェイスをエンドユーザーが使用できるようにする前に、以下の点を考慮します。

- ・ どのボリュームからシャドウコピーを取るか。
- ・ どのくらいのディスク容量をシャドウコピーに割り当てる必要があるか。
- ・ シャドウコピーを保存するのに別々のディスクを使用するかどうか。
- ・ どのくらいの周期でシャドウコピーを取るか。

ボリュームの識別

シャドウコピーはボリューム全体に対して作成されますが、特定のディレクトリは作成されません。シャドウコピーが最も効果を発揮するのは、ドキュメント、スプレッドシート、プレゼンテーション、画像、またはデータベースファイルなどのユーザーファイルがサーバーに保存されている場合です。

注記:

シャドウコピーは、アプリケーションまたは電子メールデータベースの以前のバージョンへアクセスする目的では使用しないでください。

シャドウコピーは、グループポリシーまたはユーザーがデータを保存するその他の共有フォルダーを使用してリダイレクトされるホームディレクトリやマイドキュメントフォルダーなど、ユーザーデータを保存するボリューム用に設計されています。

シャドウコピーは、圧縮または暗号化されたファイルを扱い、シャドウコピーの作成時にそのファイルに設定されていたすべてのアクセス権をそのまま保持します。たとえば、ファイルを読み取るためのアクセス権を持たないユーザーは、ファイルの以前のバージョンを復元したり、復元されたファイルを読み取ることはできません。

シャドウコピーはボリューム全体に対して作成されますが、ユーザーがシャドウコピーにアクセスするには共有フォルダーを使用する必要があります。また、ローカルサーバーの管理者がシャドウコピーにアクセスするには、`\\servername\sharename` パスを指定する必要があります。管理者またはエンドユーザーが、共有フォルダー内にないファイルの以前のバージョンにアクセスするには、まず管理者がそのフォルダーを共有化する必要があります。

注記:

シャドウコピーは NTFS でだけ使用でき、FAT または FAT32 ボリュームでは使用できません。

シャドウコピーを使用して記録されたファイルまたはフォルダーは、元のデータが変更中であっても、静的に見えます。

ディスクスペースの割り当て

シャドウコピーを保存するために割り当てる容量を決める際、コピーが変更される周期だけでなく、コピーされるファイルの数とサイズの両方を考慮します。たとえば、毎月 100 ファイルだけ変更される場合は、毎日 10 ファイル変更される場合に比べて必要になるストレージ容量は少なくなります。各ファイルへの変更の頻度が多いため、シャドウコピーの保存用に割り当てられた容量を超過した場合、シャドウコピーはまったく作成されなくなります。

管理者は、ユーザーが使用したいと考えるバージョンはいくつまでなのかも考慮に入れる必要があります。エンドユーザーが 1 つのシャドウコピーが使用できればよいと考える場合もあれば、3 日間または 3 週間分のシャドウコピーを要求する場合があります。ユーザーが多くのシャドウコピーを要求する場合、管理者はシャドウコピーを保存するためにより多くのストレージ容量を割り当てる必要があります。

制限を低く設定しすぎた場合、使用するディスク容量が管理者による設定に制限されるため、シャドウコピー技術を使用するバックアッププログラムにも影響を及ぼします。

注記:

シャドウコピーに割り当てられるボリューム容量に関係なく、すべてのボリュームには最大 64 個のシャドウコピーがあります。65 個目のシャドウコピーが作成されると、最も古いシャドウコピーが消去されます。

指定できる最小限のストレージ容量は 350MB です。デフォルトの制限は、コピー元のボリュームの 10% です。シャドウコピーが別々のボリュームに保存されている場合、**コピー元のボリューム**ではなく**ストレージボリューム**に使用可能な容量が反映されるように、デフォルト設定を変更してください。ストレージの制限に達すると、シャドウコピーの古いバージョンは削除されてしまい、復元できません。

△ 注意:

ストレージボリュームを変更するには、シャドウコピーを削除する必要があります。元のストレージボリュームに残っている既存のファイル変更履歴は失われます。この問題を避けるには、最初に選択したストレージボリュームの大きさが十分であることを確認します。

ストレージ領域の識別

同じファイルサーバー上にもう 1 つのボリュームのシャドウコピーを保存するために、ボリュームをそれぞれ別のディスク専用に設定できます。たとえば、ユーザーファイルが H:\ に保存される場合、S:\ など他のボリュームをシャドウコピーを保存するために使用できます。異なるディスク上の異なるボリュームを使用する方がパフォーマンスが向上するため、頻繁に使用される HPE ストレージファイルコントローラシステムの場合はこの使用方法をお勧めします。

異なるボリュームが（シャドウコピーが保存されている）ストレージ領域用に使用される場合、（ユーザーファイルが保存されている）コピー元のボリュームではなく、ストレージ領域で使用できる容量に反映させるために、最大サイズを**無制限**に変更する必要があります。

シャドウコピー用のディスク容量は、コピー元のファイルと同じボリュームか別のボリュームのいずれかに割り当てることができます。使いやすさと保守の容易さを取るか、パフォーマンスと信頼性を取るかをシステム管理者が判断する必要があります。

同じボリューム上でシャドウコピーを保存すると設定や保守が容易にできるという潜在的利益がありますが、パフォーマンスと信頼性は低くなります。

△ 注意: シャドウコピーがユーザーファイルと同じボリュームに保存される場合、ディスク入出力 (I/O) のバーストによってすべてのシャドウコピーが削除される可能性があることに注意してください。シャドウコピーの突然の消失は、管理者やエンドユーザーにとって受け入れられない事態でしょう。そのため、異なるディスク上の個々のボリュームを使用して、シャドウコピーを保存することが最善であると言えます。

作成頻度の決定

シャドウコピーをより頻繁に作成すれば、エンドユーザーが必要なバージョンを入手できる可能性が高くなります。ただし、ボリュームごとにシャドウコピーを保存できるのは 64 個までなので、シャドウコピーを作成する頻度を取るか、以前のバージョンのファイルを入手するのに時間を費やすことを取るかを判断する必要があります。

デフォルトで HPE ストレージファイルコントローラーシステムは、月曜日から金曜日まで午前 7 時と正午 12 時にシャドウコピーを作成します。シャドウコピースケジュールがエンドユーザーの要件に合うように、管理者はこれらの設定を容易に変更できます。

シャドウコピーとドライブの最適化

シャドウコピーが起動されているボリュームでディスクの最適化機能を実行すると、最も古いシャドウコピーから順にすべてまたはいくつかのシャドウコピーが失われます。

シャドウコピーが有効になっているボリュームを最適化する場合は、16KB 以上のスナップショットのクラスター（アロケーションユニット）サイズを使用してください。このアロケーションユニットサイズを使用することにより、スナップショットでのコピー回数が少なくなります。アロケーションユニットサイズを使用しないと、最適化プロセスによる変更の回数が原因で、シャドウコピーが予想よりも早く削除されることになります。ただし、クラスターサイズが 4KB 以下の場合、NTFS 圧縮だけがサポートされることに注意してください。

注記:

ボリュームのクラスターサイズを確認するには、`fsutil fsinfo ntfsinfo` コマンドを使用します。データが含まれるボリューム上のクラスターサイズを変更するには、ボリューム上でデータをバックアップし、新しいクラスターサイズを使用して再フォーマットし、データを復元します。

マウントされたドライブ

マウントされたドライブは、NTFS ボリューム上で（マウントポイントと呼ばれる）空のフォルダーに接続されるローカルボリュームです。マウントされたドライブが含まれるボリュームでシャドウコピーが有効になっている場合、マウントされたドライブは、シャドウコピーの作成時には含まれません。また、マウントされたドライブが共有され、シャドウコピーが有効になっているときに、（マウントポイントが保存される）ホストボリュームからマウントされたドライブにトラバースしている場合、ユーザーはシャドウコピーにアクセスできません。

たとえば、フォルダー `F:\data\users` があり、`Users` フォルダーが `G:\` のマウントポイントであるとして、`F:\` と `G:\` の両方でシャドウコピーが有効になっている場合、`F:\data` は `\\server1\data` として、`G:\data\users` は `\\server1\users` として共有されます。この例では、ユーザーは `\\server1\data` と `\\server1\users` の以前のバージョンにアクセスできますが、`\\server1\data\users` の以前のバージョンにはアクセスできません。

シャドウコピーの管理

vssadmin ツールは、ボリュームシャドウコピーを作成、表示、サイズ変更、および削除するコマンドライン機能を提供します。システム管理者は、「Shadow Copies for Shared Folders」機能を通じて、ユーザーがシャドウコピーを使用できるようにすることができます。管理者は、**プロパティメニュー（共有フォルダーのシャドウコピーのシステム管理ビューを参照）**を使用して、シャドウコピー機能をオンにし、コピーするボリュームを選択し、シャドウコピーを作成する頻度を決定します。

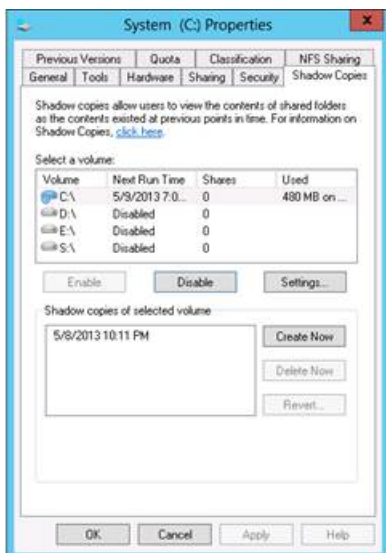


図 3: 共有フォルダーのシャドウコピーのシステム管理ビュー

シャドウコピーキャッシュファイル

デフォルトのシャドウコピー設定では、コピー元のボリュームの 10%（最小で 350MB）が割り当てられ、元のボリュームと同じボリュームにシャドウコピーが保存されます。（**コピー元のボリュームに保存されるシャドウコピー**を参照してください）。キャッシュファイルは、シャドウコピーが有効になっている各ボリュームのルートにある、「System Volume Information」という名前の保護された隠しディレクトリに格納されます。

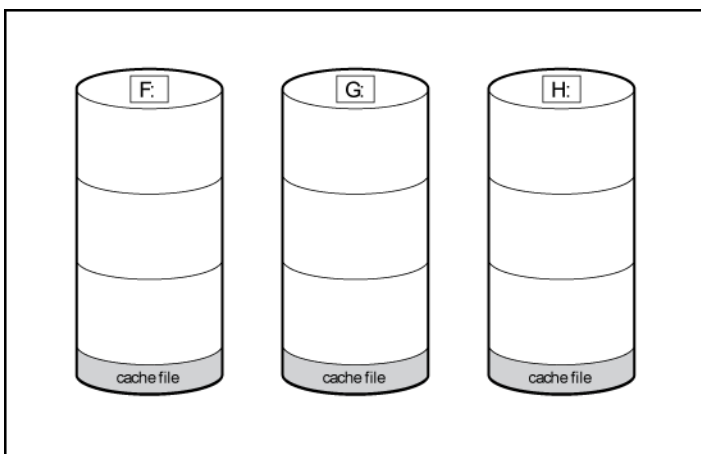


図 4: コピー元のボリュームに保存されるシャドウコピー

ファイル共有を含むボリュームとは別の専用ボリュームに、キャッシュファイルを格納するように、キャッシュファイルの場所を変更できます。（**別のボリュームに保存されるシャドウコピー**を参照してください）。

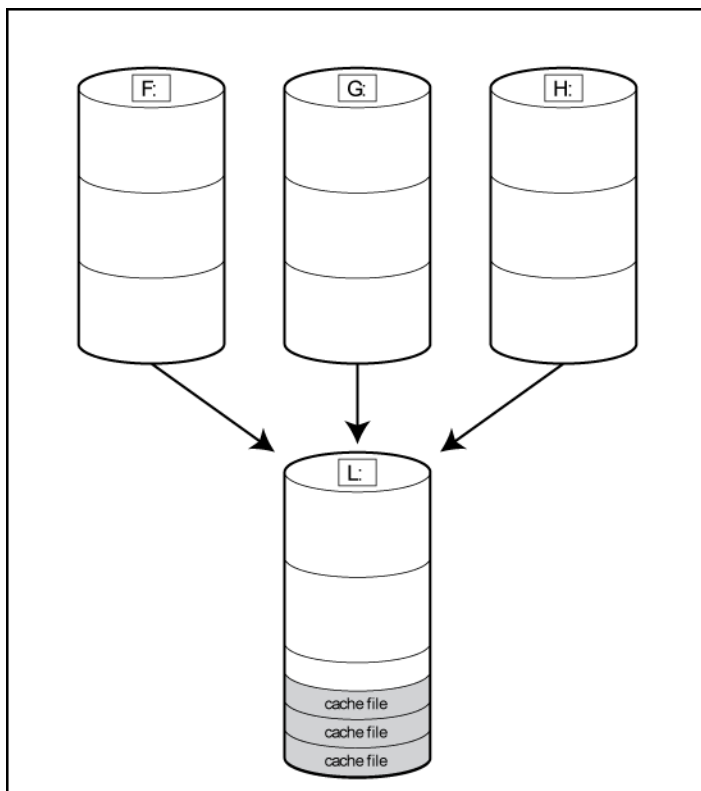


図 5: 別のボリュームに保存されるシャドウコピー

シャドウコピーを別のボリュームに保存する主な利点は、管理のしやすさとパフォーマンスです。コピー元のボリュームにあるシャドウコピーは、継続的に監視される必要があり、ファイル共有のために作成された領域を使用できます。制限の設定が高すぎると、貴重なストレージ容量をふさいでしまいます。制限の設定が低すぎると、シャドウコピーがすぐに消去されてしまうか、まったく作成されないことがあります。別のボリュームにシャドウコピーを保存することにより、通常、制限を高めに設定したり、制限なしに設定したりできます。キャッシュファイルの位置を変更する手順については、オンラインヘルプを参照してください。

△ 注意: 別のボリューム L: 上のデータが失われた場合、シャドウコピーを復元できません。

シャドウコピーの有効化と作成

ボリューム上でシャドウコピーを有効にすると、自動的に次の操作が行われます。

- ・ 選択したボリュームのシャドウコピーを作成します。
- ・ シャドウコピーの最大ストレージ容量を設定します。
- ・ シャドウコピーが特定のタイムゾーンで、月曜から金曜までの午前 7 時と正午 12 時に行われるようスケジュールします。

注記:

- ・ シャドウコピーを作成すると、ボリュームのコピーが 1 つだけ作成され、スケジュールは作成されません。
 - ・ 1 つ目のシャドウコピーが作成された後は、移動できません。シャドウコピーを有効にする前に、プロパティでキャッシュファイルの場所を変更することによって、キャッシュファイルを移動できます。**シャドウコピーのプロパティの表示**を参照してください。
-

シャドウコピーの一覧の表示

ボリュームのシャドウコピーの一覧を表示するには、以下の手順に従ってください。

手順

1. ディスクの管理にアクセスします。
2. ボリュームまたは論理ドライブを選択し、それを右クリックします。
3. プロパティを選択します。
4. シャドウ コピータブを選択します。

すべてのシャドウコピーが一覧表示され、作成された日時によって並べられます。

注記:

新しいシャドウコピーを作成するか、このページからシャドウコピーを削除できます。

スケジュールの設定

シャドウコピースケジュールは、ボリュームのシャドウコピーを作成する周期を制御します。ある組織におけるシャドウコピーの最も効果的なスケジュールを判断するのに役立つ要素がいくつかあります。要素として仕事の習慣やユーザーの居場所などがあります。たとえば、ユーザーごとにタイムゾーンまたは勤務日程が違っている場合に、このような違いを考慮して毎日のシャドウコピースケジュールを調整できます。

シャドウコピーは、1 時間に 1 回を超える頻度にならないようにスケジュールしてください。

注記:

シャドウコピーのスケジュールを削除しても、その操作が既存のシャドウコピーに影響することはありません。

シャドウコピーのプロパティの表示

シャドウ コピーのプロパティページは、コピーの数、最新のシャドウコピーが作成された日時、最大サイズの設定が表示されます。

注記:

現在シャドウコピーが存在しないボリュームでは、キャッシュファイルの場所を変更できます。キャッシュファイルは別々のディスクで管理することをお勧めします。

△ 注意:

すべてのシャドウコピーに対するサイズ制限を減らす場合は注意してください。すべてのシャドウコピーで現在使用されているサイズの合計よりも少なくサイズが設定された場合、新しい制限に合わせて合計サイズを減らすために多数のシャドウコピーが削除されます。削除されたシャドウコピーは復旧できません。

シャドウコピーの別のボリュームへのリダイレクト

- ① **重要:** シャドウコピーを別のボリュームにリダイレクトするには、まず、現在のボリューム上でシャドウコピーを無効にする必要があります。有効なシャドウコピーを無効にすると、そのボリューム上の既存のすべてのシャドウコピーが永久に削除されることを通知するメッセージが表示されます。

シャドウコピーを別のボリュームにリダイレクトするには、以下の手順に従ってください。

手順

1. ディスクの管理にアクセスします。
2. ボリュームまたは論理ドライブを選択し、それを右クリックします。
3. プロパティを選択します。
4. シャドウ コピータブを選択します。
5. シャドウコピーをリダイレクトするボリュームを選択し、ボリュームのシャドウコピーが無効になっていることを確認します。有効になっている場合は、**無効**をクリックします。
6. **設定**をクリックします。
7. 次のボリューム上に**配置**フィールドで、リストから使用できる代替りのボリュームを選択します。

注記: シャドウコピーのデフォルトスケジュール設定を変更する場合は、**スケジュール**をクリックします。

8. **OK** をクリックします。
9. シャドウ コピータブで、ボリュームが選択されていることを確認し、**有効**をクリックします。

以上で、シャドウコピーが別のボリュームに作成されるようにスケジュール設定されました。

シャドウコピーの無効化

ボリューム上のシャドウコピーを無効にすると、ボリューム上のすべての既存のシャドウコピーが削除されます。また、新しいシャドウコピーを作成するスケジュールも削除されます。

△ 注意:

シャドウコピーサービスが無効になっている場合、一部のボリュームのすべてのシャドウコピーが削除されます。削除されたシャドウコピーは復元できません。

HPE Nimble アレイからのシャドウコピーの管理

シャドウコピーについて詳しくは、[Infosight](#) をご覧ください。

HPE MSA アレイからのシャドウコピーの管理

VSS 機能には、シャドウコピーの作成、削除、および管理が含まれます。

スナッププールにまだ割り当てられていない標準リニアボリュームのシャドウコピーを作成するには、SMU または CLI を使用してスナッププールを作成してから、CLI を使用して既存の標準ボリュームをマスターボリュームに変換し（ボリュームのシャドウコピーを有効化）します。

先にスナップショットを作成しようとするリニアボリュームがマスターボリュームに変換されていない場合、HPE MSAVSS ハードウェアプロバイダは、ボリュームサイズの約 20% のバッキングストア（ただし 6GB 以上）を割り当てた後で、自動的にマスターボリュームに変換しようとします。最後のスナップショットが削除されると、ボリュームは変換されて通常のボリュームに戻り、その後でさらなるボリュームのスナップショット作成に必要なリソースが解放されます。

仮想プールでボリュームのシャドウコピーを作成するには、下の手順 2 に進んでください。

手順

1. ボリュームがリニアボリュームの場合は、SMU または CLI を使用してスナッププールを作成してから、CLI を使用して既存の標準ボリュームをマスターボリュームに変換することで、ボリュームのスナップショット（シャドウコピー）が有効になります。リニアボリュームがまだマスターボリュームでない場合、CLI の `convert std-to-master` コマンドを使用してマスターボリュームに変換します。HPE MSA VSS ハードウェアプロバイダは自動的にスナッププールを割り当てて、標準ボリュームをマスターボリュームに変換しようとします。ただし、以下の手順を前もって実行することでストレージの割り当てをより制御可能になり、操作が成功しない場合により良いフィードバックが得られます。
2. ディスクシャドウ（Windows Server 2008 以降に付属）のような VSS リクエスターや VShadow（microsoft.com から Windows SDK の一部としてダウンロード可能）を使用して、シャドウコピーを作成します。
 - ・ ハードウェアプロバイダがインストールされた後で、バックアップソフトウェアがそれを使用して、バックアップが実行されたときシステム上で一時的なハードウェアスナップショットを作成する場合があります。
 - ・ HPE MSA VSS ハードウェアプロバイダはシャドウコピーをすぐに（5 秒未満）で作成しますが、Microsoft VSS サブシステムは新しいシャドウコピーを認識してインポートするのに時間がかかることがあります。シャドウコピーを作成してインポートするのに最大で 90 秒かかる場合があります。複数の RAID パーティションが同じシャドウコピーセットに含まれている場合は、さらに時間がかかります。

共有フォルダーのシャドウコピー

シャドウコピーは、ネットワーク経由で、サポートされる各クライアントとプロトコルによってアクセスされます。サポートされるプロトコルは、SMB と NFS の 2 種類あります。これ以外のすべてのプロトコル、HTTP、FTP、AppleTalk、NetWare Shares などはサポートされません。SMB サポートでは、共有フォルダーのシャドウコピーというクライアント側アプリケーションが必要になります。クライアント側アプリケーションは、Windows XP、Windows 2000 SP3+ およびそれ以降のバージョンのオペレーティングシステム版のものを使用できます。

NFS 共有に保存されたファイルの以前のバージョンを UNIX ユーザーが独自に取得する場合、必要となる追加のソフトウェアはありません。

注記:

- ・ 共有フォルダーのシャドウコピーは、ネットワーク共有のシャドウコピーの取得だけをサポートします。ローカルフォルダーのシャドウコピーの取得はサポートしません。
- ・ 共有フォルダーのシャドウコピーは、HTTP、FTP、AppleTalk、または NetWare 共有では使用できません。そのため、これらのプロトコルのユーザーが共有フォルダーのシャドウコピーを使用して、ファイルの以前のバージョンを独自に取得することはできません。ただし、管理者がこのようなユーザーのために、共有フォルダーのシャドウコピークライアントを使用してファイルを復元することは可能です。

SMB シャドウコピー

Windows ユーザーは独自に、共有フォルダーのシャドウコピークライアントを通じて、SMB 共有に保存されたファイルの以前のバージョンへアクセスできます。シャドウコピークライアントがユーザーのコンピューターにインストールされた後で、共有のシャドウコピーにアクセスするには、共有を右クリックしてプロパティウィンドウを表示させて**以前のバージョン**タブをクリックし、目的のシャドウコピーを選択します。ユーザーは、使用できるすべてのシャドウコピーを表示、コピー、復元できます。

シャドウコピークライアントは、元のフォルダーとファイルのアクセス制御リスト（ACL）に設定するアクセス権を維持します。したがって、各ユーザーはアクセス権のある共有のシャドウコピーにだけアクセスできます。つまり、ユーザーが共有に対するアクセス権を持っていない場合、その共有のシャドウコピーへのアクセス権也没有ありません。

Shadow Copies of Shared Folders クライアントパックは、ネットワーク共有上のファイルとフォルダーの**プロパティ**ウィンドウ内に**以前のバージョン**タブをインストールします。

ユーザーがシャドウコピーにアクセスするには、Windows のエクスプローラーを使用して**以前のバージョン**タブから**開く**、**コピー**、または**復元**を選択します。（クライアント GUI を参照してください）。個々のファイルとフォルダーが両方とも復元できます。

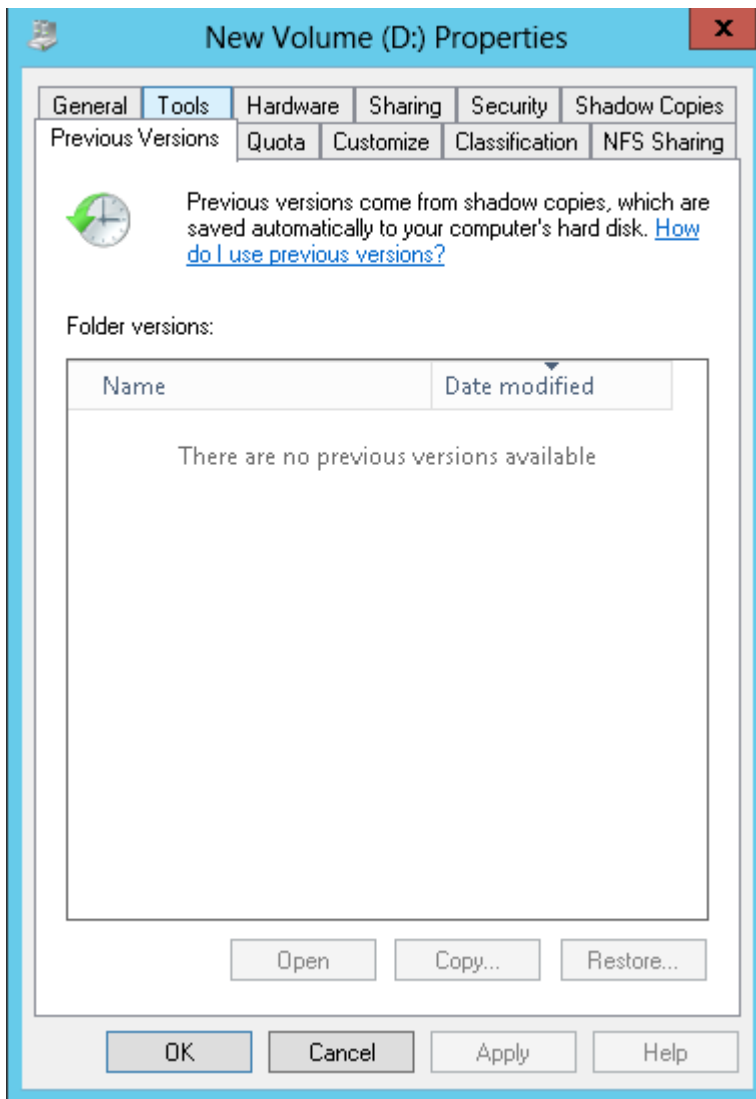


図 6: クライアント GUI

シャドウコピーが有効な HPE ストレージファイルコントローラーにホストされているネットワークフォルダーを、ユーザーが表示する場合、ファイルまたはディレクトリの古いバージョン（スナップショットの前のバージョン）が使用できます。ファイルまたはフォルダーのプロパティを表示すると、他のファイルやフォルダーと同じような、フォルダーまたはファイル履歴、つまり、ファイルまたはフォルダーコンテンツの読み取り専用のある時点のコピーが示されます。ユーザーは、フォルダー履歴内のファイルを表示したり、フォルダー履歴からファイルをコピーしたりできます。

NFS シャドウコピー

UNIX ユーザーは独自に、NFS クライアントを通じて NFS 共有に保存されたファイルの以前のバージョンにアクセスできます。このために必要となる追加のソフトウェアはありません。NFS サーバーは、共有の使用可能なシャドウコピーを共有の疑似サブディレクトリとして公開します。これらの各疑似サブディレクトリは、通常のサブディレクトリとまったく同じように表示されます。

各疑似サブディレクトリの名前には、`..@GMT-YYYY.MM.DD-HH:MM:SS` という形式でシャドウコピーの作成時刻が反映されます。一般的なツールで疑似サブディレクトリが必要以上に列挙されないように、それぞれの疑似サブディレクトリの名前はドット文字で始まり、非表示になります。

以下の例では、2003 年 4 月 27 日、28 日、29 日の午前 4 時に記録された、3 つのシャドウコピーがある「NFSShare」という NFS 共有が表示されます。

NFSShare

.@GMT-2003.04.27-04:00:00

.@GMT-2003.04.28-04:00:00

.@GMT-2003.04.29-04:00:00

NFS シャドウコピーの疑似サブディレクトリへのアクセスは、ファイルシステムに保存されたアクセス権を使用して、通常のアクセス制御方式で管理されます。ユーザーは、シャドウコピーが取られた時点に読み取りアクセス権を持っていたシャドウコピーだけにアクセスできます。ユーザーがシャドウコピーを変更できないようにするには、ユーザーの所有権またはアクセス権、あるいは元のファイルに設定されたアクセス権に関係なく、すべての疑似サブディレクトリに読み取り専用マークを付けます。

NFS サーバーは、シャドウコピーの到着または削除に関して、システムを定期的に登録して、それに応じてルートディレクトリビューを更新します。また、次回共有のルートでディレクトリを発行するときに、クライアントでは更新されたビューをキャプチャします。

削除されたファイルまたはフォルダーの復旧

削除されたファイルまたはフォルダーをフォルダー内に復旧するには、以下の手順に従ってください。

手順

1. 削除されたファイルが保存されていたフォルダーにアクセスします。
2. カーソルをフォルダー内の余白の上に置きます。カーソルをファイルの上に置くと、そのファイルが選択されます。
3. マウスを右クリックして、メニューの下部から**プロパティ**を選択します。**以前のバージョン**タブを選択します。
4. ファイルが削除されたときに、そのファイルが格納されていたフォルダーのバージョンを選択し、**開く**をクリックします。
5. フォルダーを表示し、復旧するファイルまたはフォルダーを選択します。複数のフォルダーに移動していくことができます。
6. **復元**を選択して、ファイルまたはフォルダーを元の場所に復元します。**コピー**を選択すると、ファイルまたはフォルダーが新しい場所に復元されます。

上書きされたファイルまたは破損したファイルの復旧

上書きされたファイルまたは破損したファイルの復旧は、フォルダーではなくファイル自体を右クリックできるため、削除されたファイルの復旧よりも簡単です。上書きされたファイルまたは破損したファイルを復旧するには、以下の手順に従ってください。

手順

1. 上書きされたファイルまたは破損したファイルを右クリックし、**プロパティ**をクリックします。
2. **以前のバージョン**をクリックします。
3. 古いバージョンを表示するには、**開く**をクリックします。古いバージョンをほかの場所にコピーするには、**コピー**をクリックします。現在のバージョンを古いバージョンで置き換えるには、**復元**をクリックします。

フォルダーの復旧

フォルダーを復旧するには、以下の手順に従ってください。

手順

1. カーソルを復旧するフォルダー内の余白の上に置きます。カーソルをファイルの上に置くと、そのファイルが選択されます。
2. マウスを右クリックして、メニューの下部から**プロパティ**を選択します。**以前のバージョン**タブを選択します。
3. **コピー**または**復元**をクリックします。

復元をクリックすると、フォルダーおよびすべてのサブフォルダーを復元できます。**復元**を選択してもファイルが削除されることはありません。

Shadow Copy Transport

Shadow Copy Transport は、ストレージエリアネットワーク (SAN) でデータを伝達する機能を提供します。ストレージレイと VSS 対応ハードウェアプロバイダーにより、1 台のサーバーでシャドウコピーを作成し、別のサーバーにインポートすることができます。このプロセスは実質的に「仮想」伝達であり、データのサイズにかかわらず、数分で完了します。

Shadow Copy Transport は、次のようなさまざまな目的で使用できます。

- ・ テープバックアップ

従来のテープバックアップの代わりに、実運用環境のサーバーからバックアップサーバーにシャドウコピーを移動します。シャドウコピーは、そのバックアップサーバー上で、テープにバックアップできます。他の 2 つの方法のように、この方法でも実運用環境のサーバーからバックアップトラフィックがなくなります。一部のバックアップアプリケーションはトランスポートを可能にするハードウェアプロバイダーソフトウェアとともに設計されていますが、サポートされていない場合もあります。管理者は、バックアップアプリケーションにこの機能が付属しているか確認する必要があります。

- ・ データマイニング

特定の実運用環境のサーバーで使用しているデータは、しばしば、組織内の別のグループや部門でも有用です。別のサーバーにトランスポートすることで、実運用環境のサーバーのトラフィックが増加することなく、データのシャドウコピーが使用可能になります。元のサーバーの性能に影響を与えずに、シャドウコピーを異なる目的で利用することができます。

トランスポートプロセスは、一連の DISKRAID コマンドを通じて実行します。

1. ソースサーバー上のソースデータのシャドウコピーを作成します (読み取り専用)。
2. ソースサーバーからシャドウコピーを隠します。
3. ターゲットサーバーでシャドウコピーを見えるようにします。
4. オプションで、シャドウコピーの読み取り専用フラグをクリアします。

これでデータが使用可能になります。

フォルダーと共有の管理

HPE ストレージファイルコントローラーは、NFS、FTP、HTTP、Microsoft SMB など、複数のファイル共有プロトコルをサポートしています。この項では、概要の他、サポートされているプロトコル用にファイル共有をセットアップしたり、管理したりする手順について説明します。また、ファイル単位および共有単位のセキュリティについても説明します。

注記: 一部のサーバーは、クラスター構成と非クラスター構成のどちらでも展開できます。この項では、非クラスター展開での共有のセットアップ方法を説明します。

フォルダーの管理

ボリュームとフォルダーは、任意のシステムでデータを整理するために使用されます。システムの規模を問わず、ボリュームとフォルダーの構造と命名規則を系統的にすると、管理作業が軽減されます。ボリューム、フォルダー、共有の順に移動するのに伴い、ユニットに保存されているデータタイプと許可されているセキュリティアクセスのレベルが細分化されます。

フォルダーは、サーバーマネージャーを使用して管理できます。タスクの内容は、次のとおりです。

- ・ 特定のボリュームまたはフォルダーのアクセス
- ・ 新しいフォルダーの作成
- ・ フォルダーの削除
- ・ フォルダープロパティの変更
- ・ ボリュームまたはフォルダー用の新しい共有の作成
- ・ ボリュームまたはフォルダー用の共有の管理

ファイル単位のアクセス権の管理

ファイル単位のセキュリティは、Windows のエクスプローラーを使用して管理します。

ファイル単位のセキュリティには、個々のファイルのアクセス許可、所有権、および監査の設定が含まれます。

ファイルのアクセス権を入力するには、以下の手順に従ってください。

1. Windows のエクスプローラーを使用して、変更する必要があるフォルダーまたはファイルまで移動し、そのフォルダーを右クリックします。
2. **プロパティ**をクリックし、**セキュリティタブ**をクリックします。

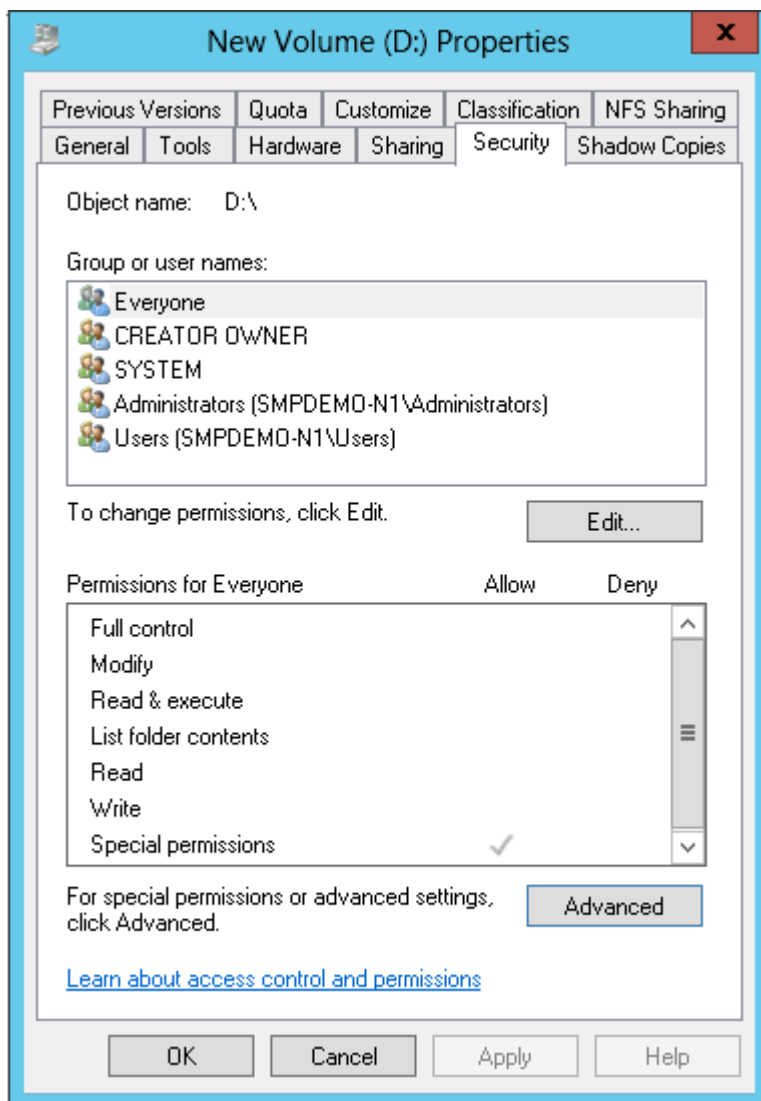


図 7: プロパティ画面、セキュリティタブ

セキュリティタブのダイアログボックスには、複数のオプションがあります。

- ・ アクセス許可リストにユーザーやグループを追加するには、**追加**をクリックします。ダイアログボックスの指示に従います。
- ・ アクセス許可リストからユーザーやグループを削除するには、削除するユーザーまたはグループを強調表示して**削除**をクリックします。
- ・ セキュリティタブの中央セクションに、アクセス権レベルのリストが表示されます。アクセス許可リストに新しいユーザーまたはグループを追加するときは、該当するボックスを選択し、共通のファイルアクセスレベルを構成します。

3. ファイルの所有権を変更したり、個々のファイルアクセスレベルのアクセス権を変更するには、**詳細設定**をクリックします。

セキュリティの詳細設定画面、アクセス許可タブに、**セキュリティの詳細設定画面**で利用できるプロパティを示します。

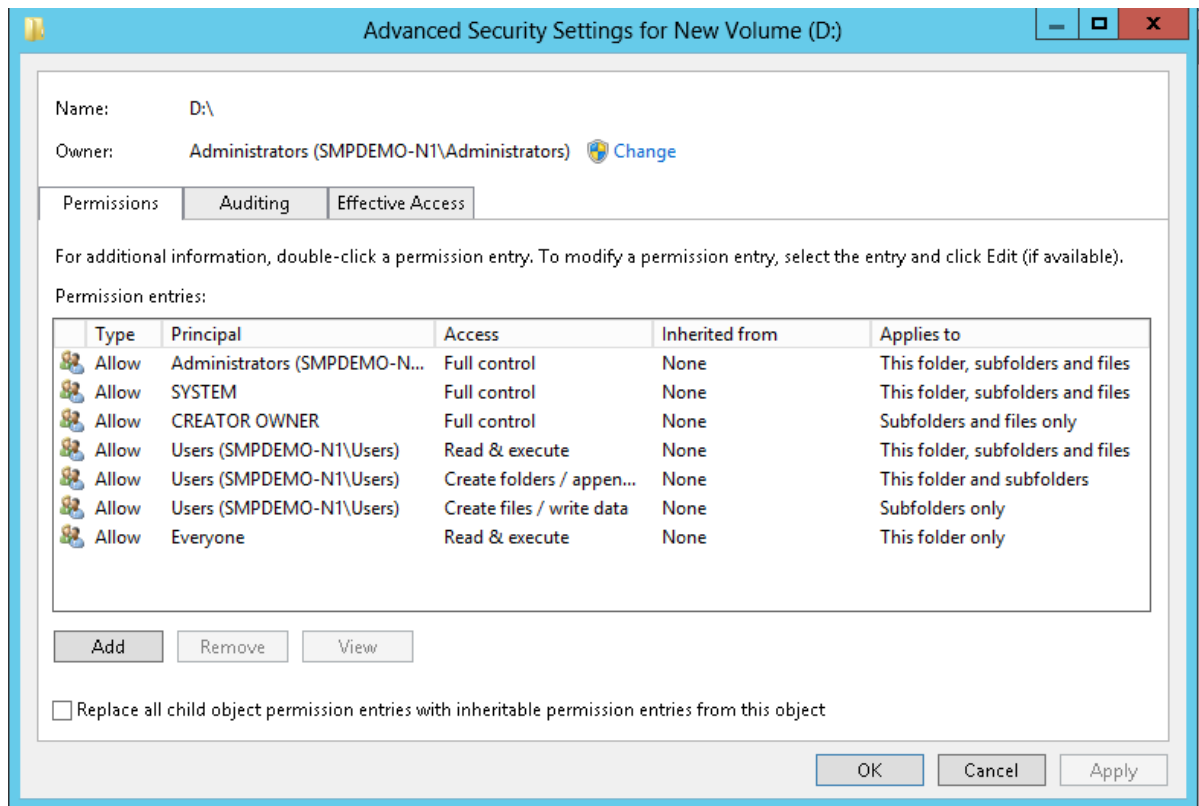


図 8: セキュリティの詳細設定画面、アクセス許可タブ

セキュリティの詳細設定画面で利用できる他の機能は、セキュリティの詳細設定画面、アクセス許可タブに表示されていますが、それらは以下のとおりです。

- ・ **新しいユーザーまたはグループを追加する** — **追加**をクリックし、ダイアログボックスの指示に従います。
 - ・ **ユーザーまたはグループを削除する** — **削除**をクリックします。
 - ・ **子オブジェクトのアクセス許可エントリすべてを、このオブジェクトからの継承可能なアクセス許可エントリで置き換える** — これを選択すると、デフォルトで、すべての子フォルダーとファイルが、現在のフォルダーアクセス権を継承します。
 - ・ **特定のユーザーまたはグループに割り当てられている具体的なアクセス権を変更する** — 変更したいユーザーまたはグループを選択し、**編集**をクリックします。
4. アクセス許可を有効にするには、**許可**ボックスを選択し、アクセス許可を無効にするには、**拒否**ボックスを選択します。いずれのボックスも選択しないと、アクセス許可は自動的に無効になります。ユーザーまたはグループに関するアクセス許可エントリ画面に、**編集**画面と一部のアクセス権を示します。

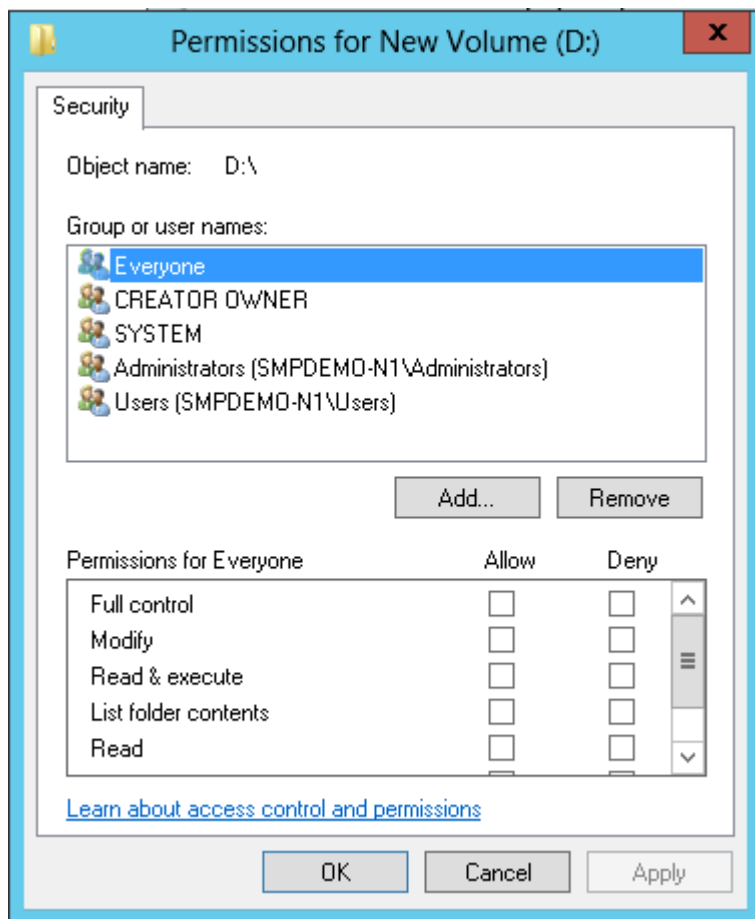


図 9: ユーザーまたはグループに関するアクセス許可エントリ画面

セキュリティの詳細設定の別の領域は、**監査**タブです。監査タブを使用すると、ファイルまたはフォルダーへのアクセスまたはアクセス試行の監査ルールを設定できます。**セキュリティの詳細設定の監査**タブからは、ユーザーまたはグループの追加、削除、表示、または変更を実行できます。

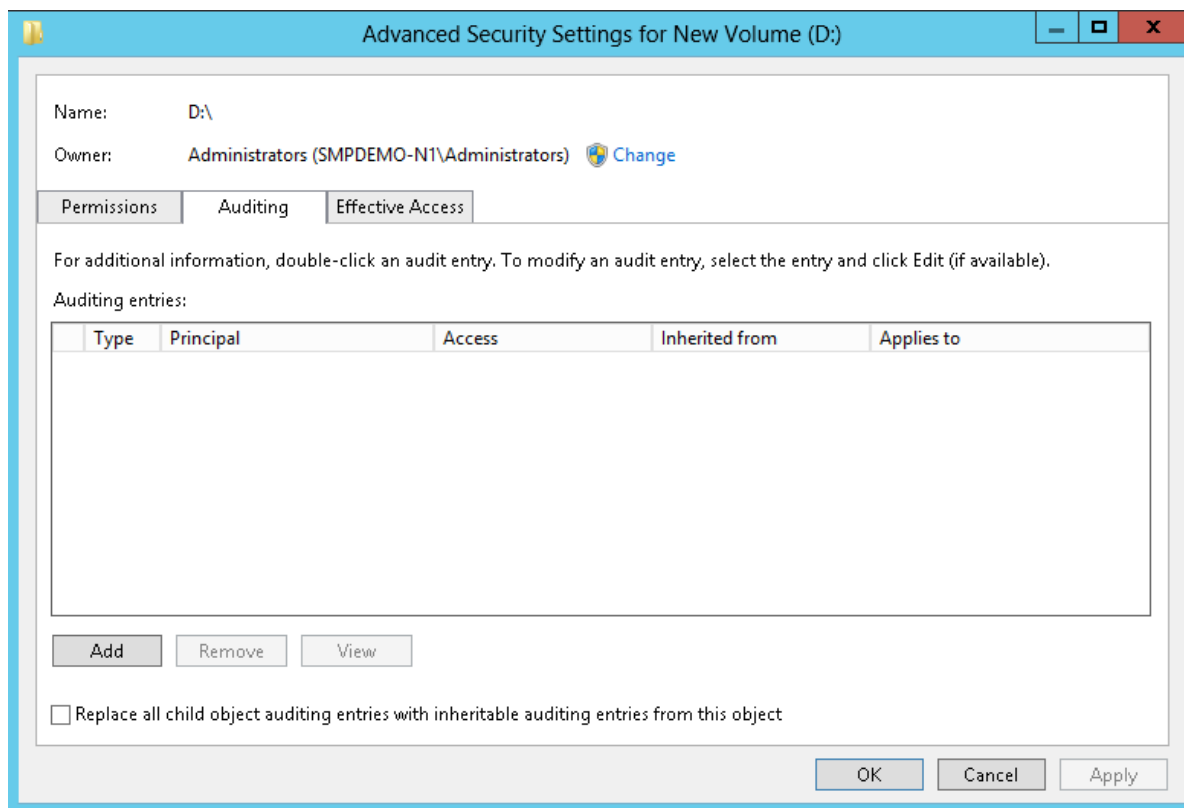


図 10: セキュリティの詳細設定画面、監査タブ

5. 追加をクリックして監査エントリ画面を表示します。

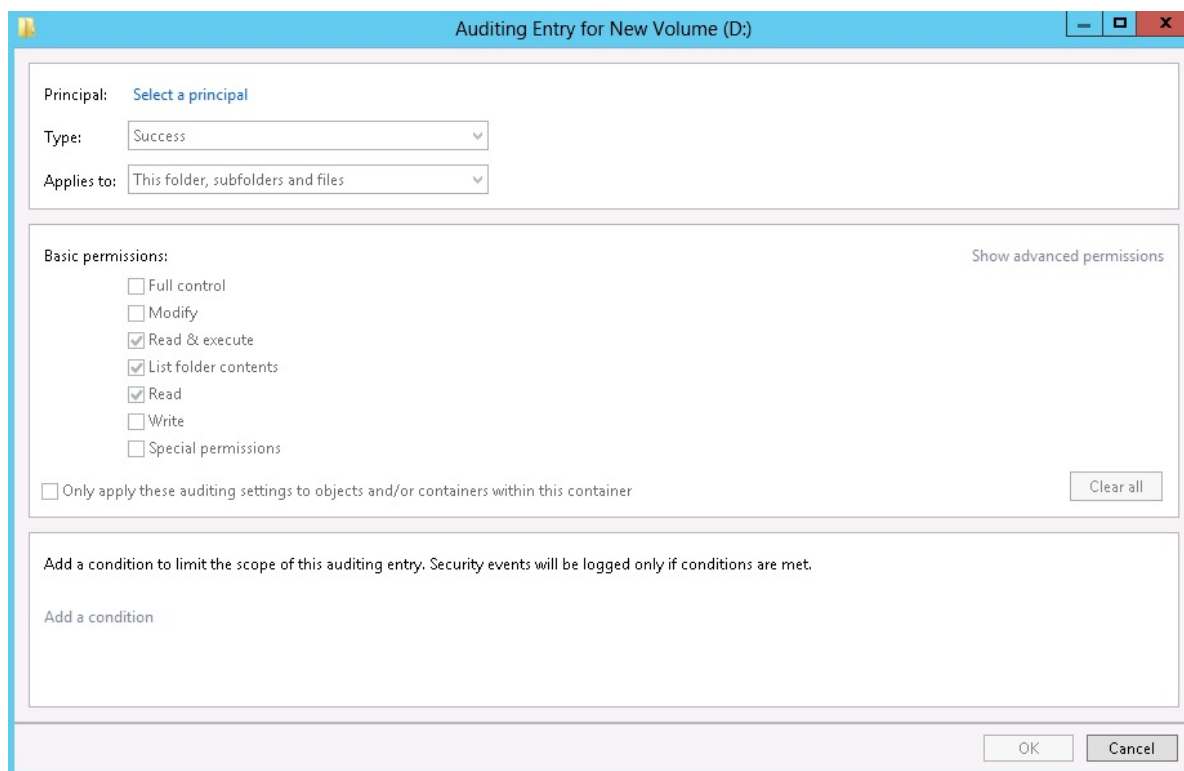


図 11: 新規ボリュームの監査エントリ画面

6. プリンシパルの選択をクリックしてユーザーまたはグループの選択画面を表示します。

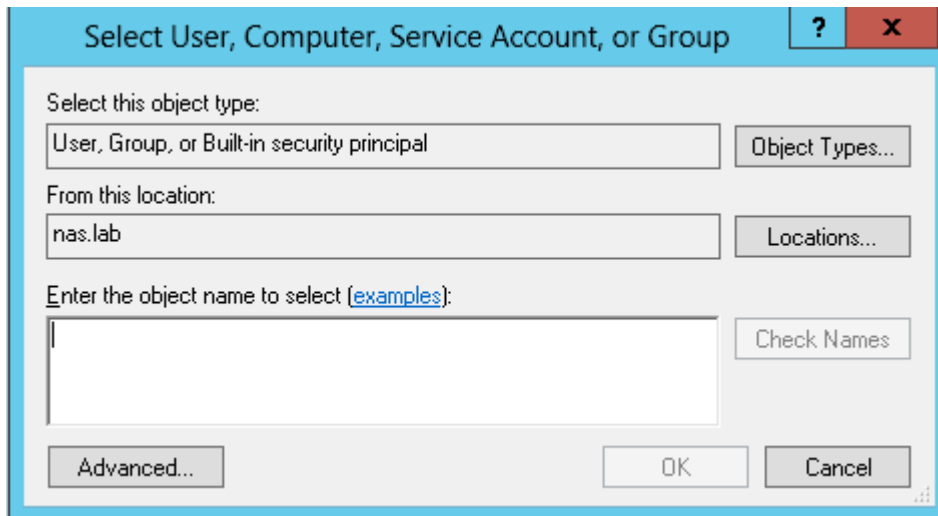


図 12: ユーザーまたはグループの選択画面

注記: ユーザーまたはグループを検索するには詳細設定をクリックします。

7. ユーザーまたはグループを選択します。
8. **OK** をクリックします。
9. ユーザーまたはグループについて、設定したい**成功監査**と**失敗監査**を選択します。
10. **OK** をクリックします。

注記: この情報を構成するには、監査を有効にする必要があります。ローカルコンピューターポリシーエディターを使用して、HPE ストレージファイルコントローラーの監査ポリシーを構成します。

所有者タブを使用すると、ファイルの所有権を取得できます。通常、管理者は、ファイルの ACL が完全でないかまたは破損しているとき、この領域を使用してファイルの所有権を取得します。所有権を取得することで、ファイルにアクセスして、手動で適当なセキュリティ構成を適用します。

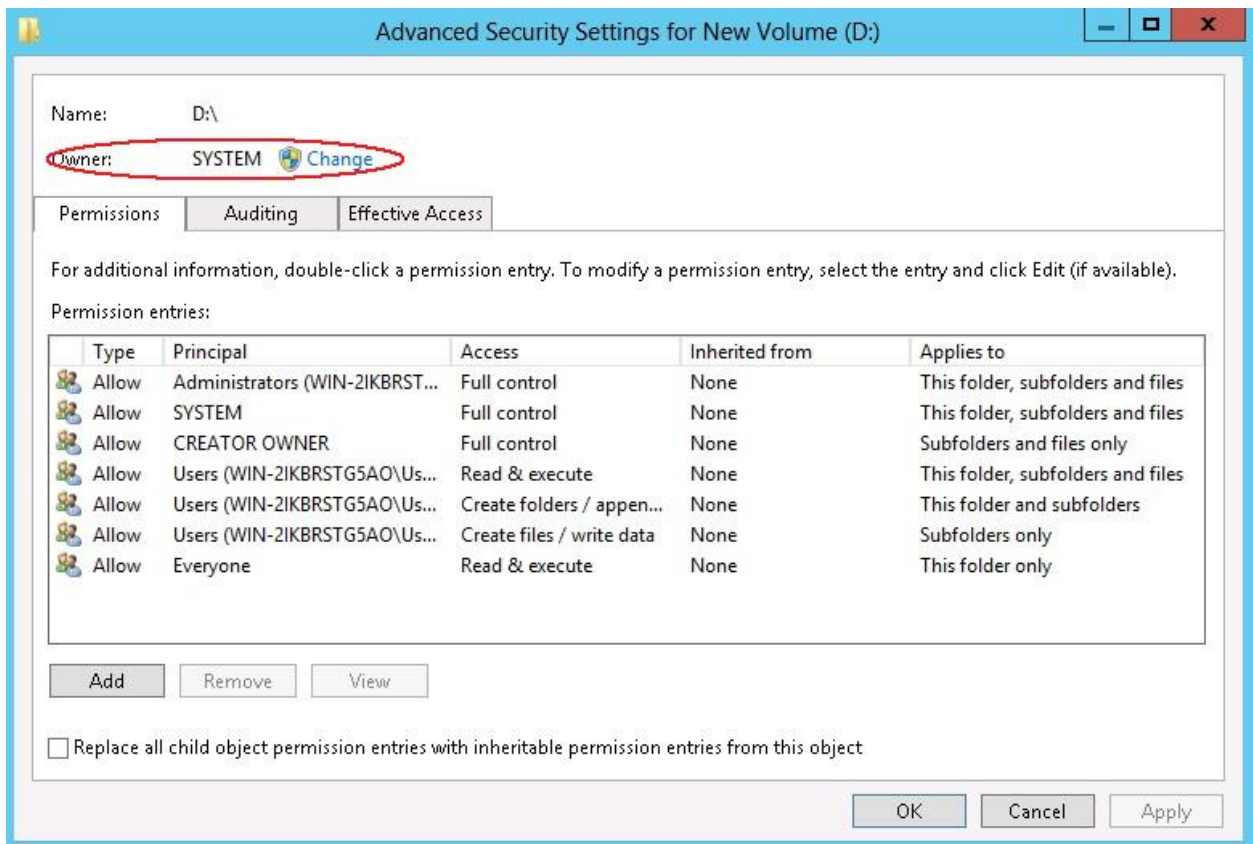


図 13: セキュリティの詳細設定画面

画面の一番上に、ファイルまたはフォルダーの現在の所有者が表示されます。所有権を取得するには、以下の手順に従ってください。

1. 所有者の変更リストから、該当するユーザーまたはグループを選択します。
2. サブフォルダーとファイルの所有権も取得する必要がある場合は、サブコンテナとオブジェクトの所有者を置き換えるボックスを有効にします。
3. OK をクリックします。

大規模なネームスペースの管理

手順

1. DFS 名前空間 (DFS N) と DFS レプリケーション (DFS R) : DFS 名前空間 : 組織内の共有フォルダーの仮想ビューです。異なるサーバー上の複数の共有フォルダーを、論理的に構造化された 1 つ以上のネームスペースにグループ化できます。

DFS レプリケーション: LAN または WAN ネットワーク接続にわたって、複数のサーバー上のフォルダーを同期させることができる、マルチマスタレプリケーション エンジンです。

詳細は、<https://technet.microsoft.com/en-us/library/jj127250.aspx> を参照してください。

2. ボリュームマウントポイント: NFS の場合、回避策として、DFS-N の代わりにボリュームマウントポイントが使用されます。

詳細は、<https://technet.microsoft.com/en-us/library/cc938934.aspx> を参照してください。

共有の管理

共有の設定や管理は、複数の方法で実行できます。Windows のエクスプローラー、コマンドラインインターフェイス、またはサーバーマネージャーを使用する方法があります。

注記: 一部のサーバーは、クラスター構成と非クラスター構成のどちらでも展開できます。この章では、非クラスター展開での共有のセットアップ方法を説明します。

すでに述べたように、HPE ストレージファイルコントローラーのファイル共有セキュリティモデルは、NTFS ファイルレベルのセキュリティモデルに基づいています。共有セキュリティは、ファイルセキュリティにシームレスに統合されています。ここでは、共有の管理に加えて、共有セキュリティについても説明します。

共有に関する注意事項

HPE ストレージファイルコントローラー上の共有の内容、サイズ、分散を計画すると、性能、管理性、使いやすさを強化できます。

共有の内容は、特定の共有が多すぎたり、汎用的な共有が少なすぎたりといった 2 種類の一般的な落とし穴に陥らないよう、慎重に選択しなければなりません。たとえば、汎用的な共有は、最初のセットアップは簡単ですが、後で問題を引き起こす場合があります。一般に、特定の目的やユーザーのグループを考慮して、別々の共有を作成する必要があります。ただし、作成される共有が多すぎるのも問題です。たとえば、ユーザーのホームディレクトリ用に 1 つの共有を作成すれば十分な場合は、ユーザーごとに別々の共有を作成する代わりに、1 つの「homes」共有を作成します。

共有や他のリソースの数を低く抑えると、HPE ストレージファイルコントローラーの性能が最適化されます。たとえば、個々のユーザーのホームディレクトリをそれぞれの共有として共有化する代わりに、最上位ディレクトリを共有化し、ユーザー各自が個人用ドライブをそれぞれのサブディレクトリにマッピングするようにします。

アクセス制御リストの定義

アクセス制御リスト (ACL) には、共有にアクセスできるユーザーと許可されているアクセスタイプを指定する情報が入っています。NTFS ファイルシステムの共有ごとに、複数のユーザーアクセス権が関連付けられた 1 つの ACL があります。たとえば、ACL は、User1 が共有に読み取り/書き込みアクセスでき、User2 が共有に読み取り専用アクセスでき、User3 が共有にアクセスできないといったようにアクセス権を定義できます。また、ACL には、グループ内のすべてのユーザーに適用されるグループアクセス情報も入っています。ACL を「アクセス権」と呼ぶ場合もあります。

Windows ドメイン環境へのローカルファイルシステムのセキュリティの統合

ACL には、特定のワークグループサーバーまたはドメイン環境からのユーザーとグループに固有のプロパティ情報が含まれています。マルチドメイン環境では、複数のドメインからのユーザーとグループのアクセス権を、同じデバイスに保存されたファイルに適用できます。HPE ストレージファイルコントローラーのローカルのユーザーとグループには、デバイスが管理している共有へのアクセスを許可することができます。ストレージシステムのドメイン名は、ユーザーまたはグループが認識されるコンテキストを提供します。アクセス権の構成は、サーバーが存在するネットワークとドメインのインフラストラクチャによって異なります。

ファイル共有プロトコル (NFS を除く) は、ネットワーク経由のすべての接続について、ユーザーとグループ単位のコンテキストを提供します。(NFS は、マシン単位のコンテキストを提供します)。それらのユーザーまたはマシンによって新しいファイルが作成されると、該当する ACL が適用されます。

構成ツールは、クライアントがアクセス権を共有する機能を提供します。これらの共有アクセス権はファイルシステム ACL 全体に適用され、ネットワーク経由で新しいファイルが作成されると、ファイルを作成しているユーザーがファイルの所有者になります。共有内の特定のサブディレクトリが共有自体と異なるアクセス権を持つ場合は、代わりにサブディレクトリの NTFS アクセス権が適用されます。この方法の結果が階層型セキュリティモデルであり、ネットワークプロトコルアクセス権とファイルアクセス権の組み合わせによって、デバイスに存在する共有のセキュリティが決定されます。

注記: 共有のアクセス権とファイルレベルのアクセス権は、別々に実装されます。ファイルシステムのファイルへのアクセス権が、共有に適用されるアクセス権と異なる場合があります。このような場合、共有のアクセス権よりファイルレベルのアクセス権が優先されます。

管理（隠し）共有と標準的な共有の比較

SMB は、管理共有と標準的な共有をサポートしています。

- ・ 管理共有とは、最後の文字が\$である共有です。管理共有は、クライアントが SMB サーバーで使用できる共有を参照するとき、共有リストに表示されません。
- ・ 標準的な共有とは、最後の文字が\$でない共有です。標準的な共有は、SMB クライアントが SMB サーバーで使用できる共有を参照するとき、常に表示されます。

HPE ストレージファイルコントローラーは、SMB の管理共有と標準的な共有の両方をサポートしています。管理共有を作成するには、共有作成時に、名前の最後に\$文字を付けます。標準的な共有を作成するときは、共有名の最後に\$文字を付けないでください。

共有の管理

共有は、サーバーマネージャーを使用して管理できます。タスクの内容は、次のとおりです。

- ・ 新しい共有の作成
- ・ 共有の削除
- ・ 共有プロパティの変更
- ・ DFS への公開

注記:

一部のサーバーでは、これらの機能はクラスター環境でも動作しますが、非クラスター対応の共有のみに対して使用するのが妥当です。クラスター用の共有を管理するには、クラスター アドミニストレーターを使用します。このページにクラスター共有リソースが表示されます。

△ 注意:

共有を削除する前に、すべてのユーザーにその共有の使用を終了するように警告し、だれも共有を使用していないことを確認してください。

ファイルサーバーリソースマネージャー

ファイルサーバーリソースマネージャー (FSRM) は、管理者が HPE ストレージファイルコントローラーに保存されているデータの量とタイプを理解、制御、および管理できるツールの集合です。たとえば、以下のタスクを実行できます。

- ・ クォータ管理
- ・ ファイルスクリーニング管理
- ・ ストレージレポート

Server Manager で FSRM タスクを利用できます。

クォータ管理

ファイルサーバーリソースマネージャスナップインのクォータ管理ノードでは、以下のタスクを実行することができます。

- ・ ボリュームやフォルダーに割り当てることができるクォータを作成し、クォータに近づいたり、クォータを超えたときに通知を生成する。
- ・ ボリュームやフォルダー内のすべての既存のフォルダーと将来作成される新しいサブフォルダーに適用する自動クォータを生成する。
- ・ 新しいボリュームやフォルダーに簡単に適用でき、組織全体で利用できるクォータテンプレートを定義する。

ファイル選別管理

ファイルサーバーリソースマネージャスナップインのファイル選別管理ノードでは、以下のタスクを実行できます。

- ・ ユーザーが保存できるファイルのタイプをコントロールし、ユーザーがブロックされているファイルを保存しようとしたときに通知を送信するファイルスクリーンを作成する。
- ・ 新しいボリュームやフォルダーに簡単に適用でき、組織全体で利用できるファイル選別テンプレートを定義する。
- ・ ファイル選別ルールの柔軟性を拡張するファイル選別例外を作成する。

ストレージレポート

ファイルサーバーリソースマネージャスナップインのストレージレポートノードでは、以下のタスクを実行できます。

- ・ ディスク使用量の傾向を把握できる周期的なストレージレポートをスケジュールする。
- ・ すべてのユーザーまたは一部のユーザーグループが許可されていないファイルを保存しようとしなかったかを監視する。
- ・ 瞬時にストレージレポートを生成する。

管理ツール

アップデートツール

アップデートツールは、ホットフィックスおよび更新された HPE コンポーネントを、HPE ストレージファイルコントローラーシステムにインストールするためのものです。アップデートツールユーティリティは、クラスター対応アップデート (CAU) 機能を利用する、統合されて拡張された、シームレスなエンドユーザーエクスペリエンスを提供するように設計されています。このツールは、ローカルおよびリモートのプロセッサからスタンドアロンノードおよびクラスターノードをアップグレードするための、統一されたグラフィカルユーザーインターフェイスを提供します。それに加えて、このインターフェイスは、下層のフレームワークを利用する高度なパラメーター選択を提供しながら、完全な操作を最小限のクリック数で実行できるようにしています。

アップデートツールによるアップデートのインストール手順

1. ツールを起動するため、デスクトップの Update Tool アイコンをダブルクリックします。アップデートをインストールするために使用できるモードが表示されます。
2. モードを選択します。スタンドアロン、コーディネーター、またはクラスターモード
3. 次へをクリックします。

モードに応じて以下の作業を行います。

- ・ スタンドアロンモードを選択した場合、システム構成サマリーページに移動します。
- ・ クラスターモードまたはコーディネーターモードを選択した場合、クラスター、ドメイン資格情報の入力ページに移動します。

4. クラスター、ドメイン資格情報の入力ページで、必要な設定を入力して次へをクリックします。システム構成サマリーページが表示されます。
5. インストールをクリックします。インストールが開始し、アップデートツールの結果ページに移動します。このページでは、インストールの状態が表示されます。

注記: スタンドアロンモードでは、インストールを開始後はインストールをキャンセルできません。

6. アップデートのインストール中にシステムで生成されたログファイルを表示するには、ログを開くをクリックします。

注記: クラスターシステムでは、個別のノードを選択して、ログを開くをクリックして特定のノードのログを表示する必要があります。

7. システムを再起動するとアップデートはインストールを終了します。

OK をクリックしてツールを終了します。

SR パッケージに含まれるいずれのコンポーネントも再起動が不要な場合、アプリケーションが終了します。

クラスター管理

HPE ストレージファイルコントローラーシステムには、シングルノードとして、または 1 つのクラスターとして動作可能であるという重要な機能があります。この章では、クラスターのインストールとクラスター管理に関する注意事項を説明します。

クラスターの概要

フェイルオーバークラスターは、アプリケーションおよびサービスの可用性を向上するために連携して動作する独立したコンピューターのグループです。クラスター構成の各サーバー（ノードと呼ばれます）は、物理的なケーブルとソフトウェアで接続されています。いずれかのクラスターノードで障害が発生すると、別のノードがサービスの提供を開始します（この処理はフェイルオーバーと呼ばれます）。ユーザーに影響するサービスの中断は、最小限に抑えられます。

最大 8 台のサーバーノードを相互接続し、単一点障害の防止（no-single-point-of-failure、NSPOF）クラスターとして展開することができます。プライベートネットワークの利用により、各クラスターノードがお互いの状態を継続的に確認するために通信できます。各ノードはもう一方のノードに対して周期的なメッセージを送信します。このメッセージを「ハートビート」と呼びます。一方のノードがハートビートの送信を停止した場合、クラスターサービスはそのノードが保有しているあらゆるリソースを、もう一方のノードへフェイルオーバーします。たとえば、クォーラムディスクを保有しているノードが何かの理由でシャットダウンした場合、そのハートビートは停止します。他のノードはハートビートが欠落したことを検出し、別のノードがクォーラムディスクとクラスターの所有権を取得します。

クラスター化サーバーは、問題が発生した場合でもファイル共有を他のストレージシステムにフェイルオーバーできるので、ファイルサービスの可用性を大幅に高めます。ファイル共有リソースがあるサーバーノードから他のノードへ移行する場合も、サービス中断は短時間で済みます。

クラスターの用語とコンポーネント

ノード

クラスターの最も基本的なパーツはサーバーですが、これを「ノード」と呼びます。サーバーノードは、クラスター内にある個別のサーバー、言い換えるとクラスターのメンバーです。

リソース

クラスターサービスによって管理されているハードウェアコンポーネントとソフトウェアコンポーネントをクラスターリソースと呼びます。クラスターリソースには、以下に定義する 3 つの特性があります。

- ・ オンラインまたはオフラインにできます。
- ・ クラスター内で管理できます。
- ・ 一度にただ 1 つのノードを所有できます。

クラスターリソースの例は、IP アドレス、ネットワーク名、物理ディスクリソース、およびファイル共有です。リソースは、個別のシステムコンポーネントを表します。これらのグループは編成されてグループになり、1 つのグループとして管理されます。一部のリソースはシステムにより自動的に作成されますが、他のリソースは手動でセットアップする必要があります。リソースの種類には、以下のようなものがあります。

- ・ IP アドレスリソース
- ・ クラスター名リソース
- ・ クラスタークォーラムディスクリソース
- ・ 物理ディスクリソース

- ・ 仮想サーバー名リソース
- ・ SMB ファイル共有リソース
- ・ NFS ファイル共有リソース
- ・ FTP ファイル共有リソース
- ・ iSCSI リソース

クラスターグループ

クラスターリソースは、クラスターグループにまとめられています。グループは、複数のノード間でフェイルオーバーを実行するための基本単位です。リソースは、個別にフェイルオーバーしません。代わりに、自らが所属しているグループを単位としてフェイルオーバーします。

仮想サーバー

仮想サーバーとは、スタティックな IP アドレスリソースと 1 つのネットワーク名リソースを使用する、1 つのクラスターグループのことです。複数の仮想サーバーを作成することもできます。仮想サーバーの所有権を他のサーバーノードに割り当てることにより、ストレージシステムの処理負荷をクラスター内にある複数のノードに分散できます。

仮想サーバーを作成すると、仮想サーバーに依存するリソースを、複数のクラスターノード間でフェイルオーバーおよびフェイルバックできます。クラスターリソースは、仮想サーバーに割り当てられます。これにより、リソースのサービスは中断することなく確実にクライアントに提供され続けます。

フェイルオーバーとフェイルバック

クラスターグループとリソースのフェイルオーバーは、次の状況で発生します。

- ・ グループをホストするノードが非アクティブになったとき。
- ・ あるグループの中にあるリソースのすべてが特定のリソースに依存していて、そのリソースの障害が発生した場合。
- ・ 管理者が強制的にフェイルオーバーを実施した場合。

リソースと、リソースに依存するものは、同じグループ内に配置する必要があります。その結果、特定のリソースがフェイルオーバーする場合、そのリソースに依存するものすべてもフェイルオーバーします。

リソースがフェイルオーバーする場合、クラスターサービスは特定の手順を実行します。最初に、リソース依存性によって定義された順序で、リソースすべてがオフラインになります。2 番目に、クラスターサービスは優先所有者リストで次の位置にあるノードへ、グループを転送することを試みます。転送が成功した場合、リソース依存性構造に従って、リソースはオンラインになります。

システムフェイルオーバーポリシーは、グループ内にある個別のリソースの障害をクラスターがどのように検出し、どのように応答するかを定義します。フェイルオーバーが発生し、クラスターが元の状態に戻った後、ポリシーに基づいてフェイルバックを自動的に発生させることもできます。以前に障害が発生したノードがオンラインに復帰した後、クラスターサービスはグループを元のホストへフェイルバックさせることができます。フェイルオーバーが発生する前に、フェイルバックポリシーを設定する必要があります。その結果、フェイルバックは意図したとおりに機能します。

クォーラムディスク

偶数個のクラスターノードで構成されるクラスターには、クォーラムディスクを使用することをお勧めします。クォーラムディスクは、複数のクラスターノードが内部のクラスター状態を調整する目的で使用する共有ストレージです。共通のクラスターディスクアレイ内にあるこの物理ディスクは、クラスターの動作にとって非常に重要な役割を果たします。クォーラムディスクは、持続性のあるストレージという手段を提供します。このディスクは、クラスターのすべてのノードからアクセスできる物理ストレージを提供

します。あるノードが起動時にクォーラムリソースを制御する場合、そのノードはクラスターを起動できません。さらに、そのノードが、クォーラムリソースを所有する他のノードと通信できる場合、後者のノードはクラスターに参加するか、クラスターにとどまることができます。

クォーラムディスクは、次の方法でデータ整合性を維持します。

- ・ クラスターデータベースの最新バージョンを保存します。
- ・ アクティブに通信している一連のノードのうち、ただ 1 つのセットがクラスターとしての動作を許可されていることを保証します。

クラスターの概念

Microsoft フェールオーバークラスタリングを使用すると、可用性、スケーラビリティ、管理性、およびワークロード管理を改善するために、個々のシステムがグループ化されます。クラスターのノード数が増えるほど、より一層改善されます。HPE では、Windows フェールオーバークラスタリングの実装を計画する場合は、docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster を参照することをお勧めします。

クラスターの計画

クラスターの利点を活用するための要件は、以下のとおりです。

- ・ ストレージの計画
- ・ ネットワークの計画
- ・ プロトコルの計画

ストレージの計画

HPE ストレージファイルコントローラーシステムは、以下の論理データ層に分かれています。

- ・ 物理ディスク
- ・ チャンクレット
- ・ 論理ディスク
- ・ CPG
- ・ 仮想ボリューム

ネットワークの計画

スタンドアロンシステムに比べると、クラスターはより洗練されたネットワーク配置を必要とします。クラスター名、仮想サーバー名、およびユーザー情報とグループ情報を記録するために、Windows NT ドメインまたは Active Directory ドメインを動作させる必要があります。クラスターは、ドメイン以外の環境に配備できません。

どのようなクラスター配備でも最低、ネットワークアドレスは 6 つ、ネットワーク名は 4 つ必要です。詳細を以下に示します。

- ・ クラスター名（一意の NETBIOS 名）と IP アドレス
- ・ ノード A の名前と IP アドレス
- ・ ノード B の名前と IP アドレス

- ・ 仮想サーバー A に対応する、少なくとも 1 つの仮想サーバー名と IP アドレス
- ・ ノード A とノード B それぞれに対応するクラスター相互接続の静的 IP アドレス

マルチノード配備では、追加のネットワークアドレスも必要です。追加のノードごとに、3 つの静的 IP アドレスが必要です。

仮想名とアドレスは、ネットワーク上のクライアントが使用する唯一の識別情報です。名前とアドレスは仮想的なので、フェイルオーバーが発生したときはその所有権が一方のノードから他方のノードへ移行しますが、クラスターグループに含まれるリソースへ引き続きアクセスできます。

クラスターは各ノードに対して少なくとも 2 つのネットワーク接続を使用します。

- ・ クラスター内の相互接続、つまり「ハートビート」用のクロスオーバーケーブルは、各クラスターノードにある複数のネットワークポートの 1 つに接続します。マルチノード配備では、クラスター相互接続の目的で、スイッチまたはハブを使用したプライベート VLAN が必要です。
- ・ パブリッククライアントネットワークのサブネットは、各クラスターノードの残りのネットワークポートに接続します。クラスターノード名と仮想サーバー名には、それらのサブネット内に存在する IP アドレスを割り当てます。

注記:

フェイルオーバーが続いている間も共有を使用可能にするには、各クラスターノードを同じネットワークサブネットに接続する必要があります。クラスターノードは、自らと接続していないネットワークに対してデータをサービスすることはできません。

プロトコルの計画

すべてのファイル共有プロトコルがクラスターリングによってメリットを受けるとは限りません。プロトコルがクラスターリングをサポートしていない場合、クラスターリソースを保持できないため、クラスターグループをフェイルオーバーできません。フェイルオーバーが発生した場合、プロトコルがクラスターグループと共にフェイルオーバーできないため、クライアントは仮想名または仮想 IP アドレスを使用して共有にアクセスできなくなります。クライアントは、最初のノードがオンライン状態に戻るまで共有にアクセスできません。

HPE では、クラスター対応のプロトコルと、クラスター非対応のプロトコルは、異なるファイル共有に配置することをお勧めします。

表 1: 共有プロトコルのクラスターサポート

プロトコル	クライアントの種類	クラスター対応（フェイルオーバーをサポート）	クラスターノードでのサポート
SMB	Windows	はい	はい
NFS	UNIX	はい	はい
	Linux		
HTTP	Web	いいえ	はい

表は続く

プロトコル	クライアントの種類	クラスター対応（フェイルオーバーをサポート）	クラスターノードでのサポート
FTP	さまざま	はい	はい
iSCSI	標準ベースの iSCSI イニシエーター	はい	はい

クラスターをインストールするための準備

この項では、HPE ストレージファイルコントローラーのクラスター化に必要な手順を説明します。

インストールの開始前

先へ進む前に、以下の仕様が満たされていることを確認します。

- ・ 共有ストレージから作成したクォーラムディスクに、最低でも 50MB の容量が必要です（500MB をお勧めします）。共有ディスクリソースとして使用するために、付加的な LUN を提供することもできます。
- ・ 高可用性を実現するために、クラスター構成はデュアルデータパスを使用して配備するのが妥当です。各ノードからデュアルデータパスを提供することにより、一方のパスで障害が発生した場合でも、そのノードのフェイルオーバーが発生せずに済みます。シングルパスを使用してクラスターを構成することも可能ですが、そのパスで障害が発生した場合、すべてのノードリソースがもう一方のノードへフェイルオーバーする結果を招きます。

高可用性を実現するためのマルチパスによるデータパスの使用

HPE では、高可用性を実現するために、クラスター構成はデュアルデータパスを使用して配備することをお勧めします。シングルパスを使用してクラスターを構成することも可能ですが、そのパスで障害が発生した場合、すべてのノードリソースがもう一方のノードへフェイルオーバーする結果を招きます。ストレージへのマルチパスが望ましいまたは必須の場合、構成の一部としてパスソフトウェアが必須です。マルチパスソフトウェアを使用すると、データパスの障害が原因でノードがフェイルオーバーすることがなくなります。

クラスターサーバーのインストール用のチェックリスト

これらのチェックリストは、インストールの準備を支援します。チェックリストの後に、ステップ単位の指示が続きます。

ネットワーク要件

- ・ 一意の NetBIOS クラスター名。
- ・ クラスター内に配備された各ノードは、以下の静的 IP アドレスを必要とします。
 - プライベートネットワーク内のネットワークアダプター用に 1 つ。
 - パブリックネットワーク内のネットワークアダプター用に 1 つ。
 - 仮想サーバー自体に 1 つ。

クラスター全体も、1 つのクラスター用静的 IP アドレスを必要とします。

- ・ クラスターサービス用のドメインユーザーアカウント（すべてのノードが、同じドメインのメンバーであることが必要です）。
- ・ 各ノードは、少なくとも 2 つのネットワークアダプターを必要とします。1 つはパブリックネットワークとの接続用、もう 1 つはノード相互間のプライベートクラスターネットワーク用です。ただ 1 つのネットワークアダプターを両方の接続に使用する構成はサポートされていません。HCL 承認を受けるには、個別のプライベートネットワークアダプターが必須です。

共有ディスクの要件

注記:

少なくとも 1 つのノードにクラスターサービスをインストールし、そのノードをオンラインにするまでは、一度に複数のノードが共有ストレージデバイスにアクセスしないようにしてください。セレクトティブストレージプレゼンテーション、SAN のゾーニング、または常に 1 つのノードのみをオンラインにすることで、この対策を実現できます。

- ・ クォーラムディスクを含むすべての共有ディスクは、すべてのノードからアクセスできる必要があります。ノードと LUN の間の接続確認を実施する場合、一度に 1 台のノードから LUN にアクセスしてください。
- ・ すべての共有ディスクは、（ダイナミックではなく）ベーシックとして構成する必要があります。
- ・ ディスク上にあるすべてのパーティションは、NTFS 形式でフォーマットする必要があります。

クラスターのインストール

インストールプロセスを実行している間、ノードのシャットダウンとリブートが発生します。これらの手順により、共有ストレージバスに接続されているディスク上のデータが失われず、破損もしないことが保証されます。クラスターソフトウェアによるディスクの保護がまだ行われていない状態で、複数のノードが同時に同じディスクへの書き込みを試みた場合、破損などが発生する可能性があります。

クラスターインストール時の電源シーケンスを使用して、各手順でどのノードとストレージデバイスの電源が投入されているべきか確認してください。

表 2: クラスターインストール時の電源シーケンス

手順	ノード 1	追加ノード	ストレージ	コメント
ネットワークのセットアップ	オン	オン	提供しない	共有バス上にあるすべてのストレージデバイスが提供されていないことを確認します。すべてのノードの電源を入れます。
共有ディスクのセットアップ（クォーラムディスクを含む）	オン	オフ	提供する	すべてのノードをシャットダウンします。共有ストレージを提供し、次にノード 1 の電源を入れます。
ディスク構成の確認	オフ	オン	提供する	ノード 1 をシャットダウンし、追加ノードの電源を入れます。すべてのクラスターノードに対して、このプロセスを繰り返します。

表は続く

手順	ノード1	追加ノード	ストレージ	コメント
ノード1の構成	オン	オフ	提供する	すべてのノードをシャットダウンします。ノード1の電源を入れます。
追加ノードの構成	オン	オン	提供する	ノード1の構成が正常に完了した後、追加ノードの電源を入れます。すべてのクラスターノードに対して、このプロセスを完了します。
インストール後	オン	オン	提供する	この時点で、すべてのクラスターノードはオンになっています。

ストレージシステムでクラスターサービスを構成するには、各ノードに対して管理特権を持つアカウントが必要です。

ネットワークのセットアップ

すべてのネットワーク接続が正しいことを確認します。プライベートネットワークアダプターは他のプライベートネットワークアダプターのみに接続され、パブリックネットワークアダプターはパブリックネットワークに接続されています。

プライベートネットワークアダプターの構成

次の手順は、Microsoft からベストプラクティスとして提供されているものであり、プライベートネットワークアダプターを構成する際に従う必要があります。

- ・ プライベートネットワーク接続のプロパティを開き、**ネットワークタブ**で、TCP/IP だけが選択されていることを確認します。
- ・ インターネットプロトコル (TCP/IP) のプロパティを開き、詳細設定を開きます。DNS タブの**この接続のアドレスを DNS に登録する**が選択されていないことを確認します。
- ・ すべての状況で、プライベートネットワークアダプター用の静的 IP アドレスを設定します。

パブリックネットワークアダプターの構成

DHCP サーバーが使用可能な場合、パブリックネットワークアダプターの IP アドレスは自動的に取得することもできますが、クラスターノードの場合、自動的な取得はおすすめしません。クラスター内では、プライベートとパブリックの両方で、すべてのネットワークアダプターに対して静的 IP アドレスを設定することをお勧めします。DHCP を介して IP アドレスを取得した場合、DHCP サーバーがダウンしたときは、クラスターノードへのアクセスが不可能になる可能性があります。パブリックネットワークアダプターで DHCP を使用する必要がある場合、DHCP サービスが一時的に失われた状況でも動的に割り当てられたリースアドレスが有効な状態にとどまるよう、長いリース期間を使用してください。クラスターサービスが認識するネットワークインターフェイスがサブネットにつき 1 つだけであることを考慮してください。

ローカルエリア接続アイコンの名前変更

HPE では、ネットワーク接続の名前を、分かりやすいものに変更することをお勧めします。分かりやすい名前を使用すると、ネットワークの識別および正しい役割の割り当てを簡単に行うことができます。たとえば、プライベートネットワークを「Cluster interconnect」、パブリックネットワークを「Public connection」という名前にします。

接続と名前解決の確認

名前解決を確認するために、クライアントから各ノードに対して ping を実行します。ノードの IP アドレスではなく、ノードのマシン名を使用します。

ドメインメンバーシップの確認

クラスター内にあるすべてのノードは、同じドメインのメンバーであること、およびドメインコントローラーと DNS サーバーにアクセスできることが必要です。

クラスターアカウントのセットアップ

クラスターサービスは、クラスターサービスを実行するためのドメインユーザーアカウントを必要とします。クラスターサービスのインストールを開始する前に、このユーザーアカウントを作成する必要があります。セットアップは、ユーザー名とパスワードを必要とするからです。このユーザーアカウントは、一意のドメインアカウントで、このクラスターを管理する目的で作成されたものでなければなりません。このユーザーアカウントに対して、管理者特権を割り当てる必要があります。

クォーラムディスクの説明

HPE では、クォーラムディスクに関して、以下のことをお勧めします。

- ・ Microsoft がクォーラムディスクとして必要としている最小サイズは、512 MB です。
- ・ ワークロードやユースケースに基づいた、推奨される 3PAR 構成を使用します。選択する RAID レベルは、書き込みと読み取りの I/O 動作によって異なります。
- ・ クォーラムディスクにドライブ文字を割り当てる場合は、ドライブ文字 Q をお勧めします。オプションとして、**Quorum** または **Witness** などの識別名をクォーラムディスクに指定することもできます。

共有ディスクの構成

Windows ディスクの管理ユーティリティを使用して、追加の共有ディスクリソースを構成します。すべての共有ディスクが NTFS 形式でフォーマットされ、ベーシックディスクとして指定されていることを確認します。

クラスターサービスをインストールする過程で、追加の共有ディスクリソースは、クラスターに対して物理ディスクリソースとして自動的に追加されます。

ディスクアクセスと動作の確認

各共有ディスクリソースにファイルを書き込み、正常に動作していることを確認します。

この時点でノード 1 をシャットダウンし、1 台の追加ノードの電源を入れ、「ディスクアクセスと動作の確認」の手順を繰り返します。すべてのクラスターノードで、この作業を行います。すべてのノードがこれらのディスクの読み取りと書き込みを行えることを確認した後、クラスターノードの電源を切り、ノード 1 の電源を入れ、本書の作業を続行します。

クラスターサービスソフトウェアの構成

フェールオーバー クラスター管理は、クラスターとクラスターリソースを管理、監視、作成、および変更する機能を提供します。

フェールオーバー クラスター管理の使用

フェールオーバー クラスター管理は、すべてのクラスターに存在するグループとリソースに関する情報およびクラスターに関する特定の情報を表示します。

クラスターの作成

クラスターの作成中に、フェールオーバー クラスター管理はハードウェアとソフトウェア構成を分析および確認し、潜在的な問題を特定します。詳細で読みやすいレポートが作成され、クラスターを作成する前に、構成に関する潜在的な注意事項が列挙されます。

発生する可能性のある注意事項のいくつかは、以下のとおりです。

- ・ クォーラムディスクとして使用する共有ディスクがありません。少なくとも 512MB のサイズを持つ NTFS パーティションを使用して、共有ディスクを作成する必要があります。
- ・ ネットワーク接続に DHCP アドレスが使用されています。クラスター構成の中では、すべてのネットワークアダプターは静的 IP アドレスを使用して構成する必要があります。
- ・ File Services for Macintosh と Service for NetWare は、クラスター構成ではサポートされていません。
- ・ クラスター構成では、ダイナミックディスクはサポートされていません。
- ・ まだ構成されていないネットワークアダプター、またはアクティブリンクのないネットワークアダプターでエラーが発生しているようです。そのネットワークアダプターを使用しない場合は、無効にする必要があります。

クラスターへのノードの追加

追加するノードがクラスターのメンバーになるまでの間は、追加するノードがアクセスできるディスクをクォーラムディスクに限定してください。クラスターへの参加が完了するまでは、新しいノードはクラスター内の他の LUN にアクセスすべきではありません。クラスターへの参加が完了した後、新しいノードに対して LUN を提供できます。物理ディスクリソースを新しいノードに移動し、正常に動作することを確認します。

△ 注意:

非クラスターシステムに対して他の LUN を提供すると、データの破損を引き起こす可能性があります。

地理的分散クラスター

クラスターノードを地理的に分散させて、フォールトトレランスの水準を高めることもできます。地理的分散クラスターを、「遠隔クラスター」と呼ぶこともあります。

地理的分散クラスターでは、以下の規則に従う必要があります。

- ・ 遅延時間が 500ms（ミリ秒）以下のネットワーク接続は、クラスターの整合性が維持されることを保証します。ネットワークの遅延時間が 500ms より長い場合、クラスターの整合性を容易に維持できません。
- ・ すべてのノードは、同じサブネット内に存在する必要があります。

ファイル共有を含むクラスターグループとクラスターリソース

フェールオーバー クラスター管理ツールは、すべてのクラスター管理作業に関する詳細なオンラインヘルプを用意しています。

クラスターリソースには、管理タイプのリソースとファイル共有が含まれます。以下の段落では、クラスターグループ、クラスターリソース、およびクラスター化ファイル共有の概要と計画に関する注意事項を説明します。

これらのリソースとグループの作成と管理を行うには、フェールオーバー クラスター管理を使用する必要があります。

クラスターグループの概要

クラスターを最初に作成する際に、デフォルトのクラスターグループが自動的に作成されます。このデフォルトクラスターグループには、インターネットプロトコル (IP) アドレスリソース、ネットワーク名リソース、およびクォーラムディスクリソースが割り当てられています。新しいクラスターの作成時に、セットアップ時に指定された IP アドレスとクラスター名が、デフォルトクラスターグループの IP アドレスおよびネットワーク名として設定されます。

△ 注意:

クラスターグループや IP アドレスは、削除も名前変更もしないでください。そのような作業をした場合、クラスターが失われて、クラスターを再インストールする必要が生じます。

グループを作成する際の管理者にとっての最優先事項は、グループとグループのリソースをどのように管理するのかを理解することです。ノードごとに 1 つのリソースグループと 1 つの仮想サーバーを作成し、そのノードが所有しているすべてのリソースをその中に含める方針を選択することがあります。または、物理ディスクリソースごとに 1 つのリソースグループと仮想サーバーを作成する方針を選択することもあります。さらに、クラスター内でグループとそのリソースの負荷を、ノード間で均衡を取るように試みる必要もあります。

ノードベースのクラスターグループ

1 つのノードにつきリソースグループを 1 つと仮想サーバーを 1 つだけ作成すると、グループ管理とリソース管理が簡単になります。このセットアップを使用すると、管理者はすべてのファイル共有リソースを 1 つのグループに含めることができます。クライアントは、ノードが所有しているすべてのリソースを、仮想サーバー名を介してアクセスします。

ノードベースのクラスターグループでは、各グループには独自のネットワーク名と IP アドレスがあります。管理者は、各物理ディスクリソースをどのノードに配置するのかを決定します。この構成では、細分化が非常に大雑把になります。特定のグループ内にあるすべてのリソースは、同じノード内に配置されている必要があります。必要なのは、2 つの IP アドレスとネットワーク名のみです。この構成では、リソース管理とネットワーク管理のオーバーヘッドは少なく済みます。このアプローチで考えられる欠点は、多くのファイル共有を作成した場合、リソースグループが非常に大きくなる可能性があることです。

ロードバランス

仮想サーバーごとに個別のクラスターグループを作成する場合、2 つのノード間でクラスター内処理負荷の均衡を取る際に、柔軟性が高くなります。優先所有者パラメーターを使用して、各クラスターグループをクラスターノードに割り当てることができます。たとえば、2 つのクラスターグループが存在する場合、最初のクラスターグループをノード A が所有し、2 番目のクラスターグループをノード B が所有するように設定することができます。この結果、両方のデバイスがネットワーク負荷を同時に処理できます。ただ 1 つのクラスターグループが存在する場合、そのグループを所有できるのはただ 1 つのノードです。もう一方のノードはネットワークトラフィックに対してサービスを提供できません。

ファイル共有リソースの計画に関する注意事項

SMB と NFS はクラスター対応プロトコルであり、アクティブ/アクティブのクラスターモデルをサポートしています。そのため、リソースは分散され、両方のノードで同時に処理されます。たとえば、いくつかの NFS ファイル共有リソースを、ノード A に対応する仮想サーバーによって所有されているグループに割り当て、残りの NFS ファイル共有リソースを、ノード B に対応する仮想サーバーによって所有されているグループに割り当てることができます。

ファイル共有をクラスター共有として構成することにより、可用性の高いファイル共有を実現できます。リソースはグループ内に配置されるので、必要な場合は、ファイルの所有権を一方のノードからもう一方のノードへ容易に移動できます。ファイル共有グループを所有しているクラスターノードをシャットダウンする必要が生じた場合、または障害が発生した場合、そのノードがオンラインに復帰するまで、クラスター内にあるもう一方のノードは該当ディレクトリの共有を行います。元のノードがオンラインに復帰した時点で、グループとそのリソースの所有権は元の所有者ノードに戻ります。

リソースの計画

手順

1. クラスタ内の各ノードに対応するクラスターグループを作成します。IP アドレスリソースとネットワーク名リソースも同時に作成します。

クラスターリソースグループは、サーバーの処理負荷の均衡を取る目的で使用されます。グループの所有権は、仮想サーバー間で分散してください。

2. NFS 環境では、NFS サーバーを構成します。

NFS 固有の手順として、監査情報とファイルロック情報の入力、およびクライアントグループとユーザー名マッピングをセットアップすることが挙げられます。これらの手順は、クラスター化配備に固有のものではありません。詳細は、「Other network file and print services」の章の「Microsoft Services for NFS」を参照してください。NFS セットアップ情報に変更を加えた場合、その変更はクラスター内のすべてのノード間で自動的に複製されます。

3. ファイル共有リソースを作成します。

4. ファイル共有リソースの所有権は、リソースグループに割り当てます。

- a. ファイル共有リソースの所有権を、各リソースグループに分配します。その後、それらは複数の仮想サーバーに対して分散され、効率的なロードバランスを実現します。
- b. このファイル共有に関する物理ディスクリソースも、このグループに含まれていることを確認します。
- c. リソースが仮想サーバーに依存していること、およびファイル共有の配置先となる物理ディスクリソースが作成されたことを確認します。

共有リソースのアクセス許可とアクセス権

ファイル共有と NFS 共有のアクセス許可は、フェールオーバー クラスタ管理ツールを介して管理する必要があります。一方、ファイルシステム上にある個別の共有は、Windows のエクスプローラーを介して管理します。フェールオーバー クラスタ管理ツールを介してこれらを管理すると、一方のノードからもう一方のノードへアクセス許可を移行できます。さらに、エクスプローラーを使用して確立されたアクセス許可は、共有の障害が発生した後、またはオフラインになった後は失われます。

NFS クラスタ固有の注意事項

すべての推奨事項を、以下にまとめて示します。

- ・ ユーザーマッピングとグループマッピングをバックアップします。

複雑で高度なマッピングがシステム障害時に消失しないように、マッピングを変更したり、新しいマッピングを追加したときは、必ず、マッピングをバックアップしてください。

- ・ 矛盾なくマッピングします。

正しいファイルアクセスを保証するために、相互にマッピングされるグループには同じユーザーを入れ、グループのメンバーが相互に正しくマッピングされている必要があります。

- ・ 正しくマッピングします。
 - 有効な UNIX ユーザーを有効な Windows ユーザーにマッピングする必要があります。
 - 有効な UNIX グループを有効な Windows グループにマッピングする必要があります。

- ・ マッピングされる Windows ユーザーは、「ネットワークからこのコンピューターにアクセスする権限」を持つ必要があります。そうでない場合、マッピングは無効化されます。
- ・ マッピングされる Windows ユーザーは、アクティブなパスワードを持つ必要があります。そうでない場合、マッピングは無効化されます。
- ・ クラスター化配備では、ドメインユーザーアカウントを使用してユーザー名マッピングを作成します。
ローカルアカウントのセキュリティ識別子を認識するのはローカルサーバーだけなので、クラスター内にあるもう一方のノードは、フェイルオーバーの際にそれらのアカウントを解決できません。ローカルユーザーアカウントとローカルグループアカウントを使用してマッピングを作成しないでください。
- ・ クラスター化配備では、信頼されている側のドメインに所属するコンピューターを使用して、ユーザー名マッピングを管理します。
クラスターの所属ドメインから信頼されていないドメインに所属するコンピューターを使用して、NFS 管理タスクを実行した場合、そのクラスター内にあるノードの間では変更が正しく複製されません。
- ・ クラスター化配備では、PCNFS のパスワードとグループファイルを使用してユーザー情報とグループ情報を提供する場合、システムの各ノードにそれらのファイルを配置する必要があります。
例: パスワードファイルとグループファイルがノード 1 の `c:\maps` に配置されている場合、ノード 2 の `c:\maps` にもそれらを配置する必要があります。パスワードファイルとグループファイルの内容は、両方のノードで一致している必要があります。
各サーバーノードにあるこれらのパスワードファイルとグループファイルは、整合性を維持するためおよび、ユーザーまたはグループが誤って無効化されることを防止するために、定期的に更新する必要があります。

Network File System ユーザーマッピング

Network File System (NFS) とは、ネットワーク経由でファイルへのリモートアクセスを可能にするネットワークファイル共有プロトコルであり、UNIX、Linux、または Mac OS などのオペレーティングシステムを実行するコンピューターのネットワークで一般的に使用されます。NFS は、すべての HPE ストレージファイルコントローラーシステムでサポートされています。

以下の種類の NFS アカウントマッピングがサポートされています。

- ・ Active Directory® ドメインサービス (AD DS) にマッピングされたユーザーアクセス
- ・ マッピングされていない匿名ユーザーアクセス
- ・ マッピングされていない UNIX ユーザーアクセス

NFS について詳しくは、次の Microsoft の Web サイトを参照してください。

[The Storage Team at Microsoft - File Cabinet Blog](#)

クラスター非対応のファイル共有プロトコル

Services for Macintosh (SFM)、File and Print Services for NetWare、HTTP の各ファイル共有プロトコルはクラスター非対応であり、クラスター化リソースにインストールした場合、リソースのフェイルオーバーイベントが発生したときにサービスが一時停止します。サービスの一時停止は、サーバーが停止した場合に発生する状態に似ています。一時停止より前の時点でディスクに保存されていなかったデータは、失われます。SFM の場合、クラスター環境ではプロトコル自体がサポートされていません。SFM は状態情報をメモリに保存するからです。特に、Macintosh ポリュームのインデックスは、ページングされたプールメモリに格納されます。クラスター化モードでの SFM の使用はサポートされていません。また、SFM の基にあるリソースを保持するサーバーがダウンし、もう一方のサーバーへフェイルオーバーされた場合、データが失われる可能性があります。

クラスターへの新しいストレージの追加

新しいストレージは、クラスター内の 1 つのノードに対して提供します。セレクトティブストレージプレゼンテーション (SSP) または、SAN のゾーニングを介して、この作業を実行できます。

以下で説明するタスクを使用して、クラスターにストレージを追加します。詳細は、クラスタリングのオンラインヘルプを参照してください。

物理ディスクリソースの作成

物理ディスクリソースは、クラスターグループ内に配置する必要があります。既存のクラスターグループを使用することもできます。それ以外の場合、新しいクラスターグループを作成する必要があります。ディスクリソースを作成する情報については、クラスターのオンラインヘルプトピック物理ディスクリソースの種類を参照してください。

注記:

- ・ 物理ディスクリソースでは通常、依存性を何も設定しません。
- ・ マルチノードクラスターでは、グループの移動先となるノードを指定する必要があります。クラスターグループをもう一方のノードへ移動した場合、そのグループ内にあるすべてのリソースも移動されます。
- ・ あるノードが物理ディスクリソースを所有している場合、他のすべてのクラスターノードからは、そのディスクは未知の読み出し不可能なディスクのように見えます。これは正常な状況です。物理ディスクリソースがもう一方のノードへ移動された後、そのディスクリソースは読み出し可能になります。

ファイル共有リソースの作成

ファイル共有リソースを作成するには、フェールオーバークラスター管理のオンラインヘルプトピックを参照してください。

- ・ クラスター管理のファイル共有を作成する (Create a cluster-managed file share)
- ・ 多数のファイル共有があるサーバークラスターを使用する (Using a server cluster with large numbers of file shares)

注記:

- ・ ファイル共有リソースは、配置先となる物理ディスクリソースと同じクラスターグループに配置する必要があります。
- ・ この手順で指定した物理ディスクリソースは、このウィザードの最初で指定したのと同じクラスターグループに配置する必要があります。

NFS 共有リソースの作成

NFS 共有リソースを作成するには、サーバークラスターでの MSNFS 管理を参照してください。

クラスター環境でのシャドウコピー

キャッシュファイルの場所は、オリジナルのデータとは異なるディスクにすることをお勧めします。この場合、キャッシュファイルディスク用の物理ディスクリソースは、対象となるシャドウコピーリソース、およびスナップショットが有効となるボリュームと同じクラスターグループ内に作成する必要があります。シャドウコピーを確立する前に、このリソースを作成する必要があります。シャドウコピーリソースは、オリジナルの物理ディスクリソースと、キャッシュファイルを保持する物理ディスクリソースの両方に依存することになります。

詳しくは、フェールオーバークラスター管理のオンラインヘルプトピックを参照してください。

- ・ サーバークラスターで共有フォルダーのシャドウコピーを使用する
- ・ クラスターで共有フォルダーのシャドウコピーを有効にする

クラスターでの LUN の拡大

クラスター内のストレージアレイ上の LUN を拡大するには、ストレージアレイのハードウェアプロバイダーを使用してストレージを拡大または拡張する際の要件と方法を確認します。

サーバークラスターでの MSNFS 管理

Microsoft Services for NFS のオンラインヘルプに、以下の内容に関するサーバークラスター情報が記載されています。

- ・ サーバークラスター上の共有フォルダーを構成する
 - クラスターリソースとして NFS 共有を構成する
 - NFS 共有のクラスターリソースを変更する
 - NFS 共有のクラスターリソースを削除する
- ・ サーバークラスターで NFS 用 Microsoft サービスを使用する
 - サーバークラスターでの NFS サーバーの機能とは
 - サーバークラスターで NFS サーバーを使用する
- ・ サーバークラスターにユーザー名マッピングを構成する

詳しくは、Microsoft Services for NFS のオンラインヘルプを参照してください。

サーバークラスターで NFS サーバーを実行するためのベストプラクティス

- ・ サーバークラスターを停止する前に NFS サーバーを停止します。
- ・ ノードが故障した場合の共有の可用性を確保します。
- ・ 適切なツールを使用して Network File System (NFS) 共有クラスターリソースを管理します。
- ・ 競合する共有名の使用を避けます。
- ・ 監査ログの可用性を確保します。
- ・ NFS サーバーを停止する前にファイル共有を移動するか、オフラインにします。
- ・ リソースを変更する前にリソースをオフラインにします。
- ・ 信頼されるドメイン内のコンピューターから NFS サーバーを管理します。
- ・ クラスターサービスが再起動した後で NFS サーバーサービスを再起動します。
- ・ 適切な共有モードを選択します。
- ・ NFS 共有クラスターリソースを作成したり変更したりする場合は、コマンドラインを正しく使用します。
- ・ ハードマウントを使用します。
- ・ 正しい仮想サーバー名を使用します。

高度なクラスター管理手順

フェイルオーバーとフェイルバック

すでに述べたように、一方のノードがオフラインになった場合、そのノードに従属しているすべてのリソースはもう一方のノードへ自動的にフェイルオーバーされます。処理は続行されますが、速度は低下します。残りのノードですべての操作を処理する必要があるからです。3つ以上のノードからなるクラスターの場合、付加的なフェイルオーバー規則を適用することもできます。たとえば、障害が発生したノードが処理していた作業負荷を均衡の取れた方法で分散するために、グループを複数のノードへフェイルオーバーするよう構成することができます。リソースが特定のノードでオンラインになることを防止するために、実行可能な所有者リストからノードを除外することもできます。最後に、優先所有者リストの順序を設定し、フェイルオーバーノードの順序設定済みリストを用意することもできます。これらのツールを使用することにより、マルチノードクラスター環境でリソースのフェイルオーバーを制御し、制御されて均衡の取れたフェイルオーバー手法を確立し、増加した作業負荷の均衡を取ることができます。

オペレーティング環境はさまざまに異なるため、(リソースグループごとに編成された)リソースが元のノードへ自動的にフェイルバックするのか、またはリソースがフェイルオーバーしたままとして手動で元のノードへ戻されるまで待つのか、管理者が指定する必要があります。

注記:

リソースを指定の所有者へ自動的にフェイルバックするようストレージシステムを設定していない場合、フェイルオーバーが発生するたびにリソースを手動で元のノードへ戻す必要があります。

1つのクラスターノードの再起動

△ 注意:

1つのクラスターノードを再起動する前に、クラスター内にある他のノードが正常に動作していることを確認してください。再起動しようとするノード上のリソースに接続しているユーザーに対して、適切な警告を送信してください。ターミナルサービスを使用すると、ストレージシステムデスクトップのサーバーマネージャーから使用中の接続を表示できます。フェイルオーバークラスターマネージャーから、ファイルサーバーの役割を選択し、その役割の共有を表示します。

クラスター内にあるノードのいずれかを再起動する物理的なプロセスは、シングルノード環境でストレージシステムを再起動する場合と同じです。ただし、特別な注意が必要です。

あるクラスターノードを再起動すると、有効になっているフェイルオーバーポリシーに基づき、そのノードがサービスしているすべてのクラスターリソースが、クラスター内の他のノードへフェイルオーバーされます。フェイルオーバープロセスが完了するまで、現時点で実行されている読み出しと書き込みの操作は失敗します。再起動されたノードが正常に動作してリソースが戻されるまでは、余分な作業により、クラスター内にある他のノードの負荷が通常より大きくなります。

1つのクラスターノードのシャットダウン

△ 注意:

1つのクラスターノードをシャットダウンする前に、クラスター内にある他のノードが正常に動作していることを確認してください。シャットダウンしようとするノード上のリソースに接続しているユーザーに対して、適切な警告を送信してください。

1つのクラスターノードをシャットダウンすると、そのノードが提供しているすべてのクラスターリソースが、クラスター内の他のノードへフェイルオーバーされます。その結果、クラスターフェイルオーバープロセスが完了するまで、現時点で実行されている、クライアントの読み出しと書き込みの操作は失敗します。シャットダウンされたノードに電源が投入されクラスターに再参加するまでは、余分な作業により、クラスター内にある他のノードの負荷が通常より大きくなります。

クラスターの電源を切る

ストレージシステムクラスターの電源を切るプロセスは、シングルノードの場合と同じです。ただし、クラスターの場合、ストレージサブシステムとシャットダウンの順序に関して、特別に注意が必要です。

電源を切るプロセスは、2つの主要な手順に分割できます。

手順

1. クラスターノードをシャットダウンする。
2. クラスターノードの電源を切る。

これらの手順の順序は、非常に重要です。デバイスは、ストレージサブシステムより先にシャットダウンする必要があります。ノードとストレージサブシステムのシャットダウンを不適切に実行すると、データが破損したり失われたりすることがあります。

△ 注意: クラスターノードの電源を切る前に、すでに説明したシャットダウンの適切な手順に従ってください。1つのクラスターノードのシャットダウンを参照してください。一度に1つのノードのみをシャットダウンする必要があります。

クラスターの電源投入

ストレージシステムクラスターの電源を入れるプロセスは、シングルノードの場合より複雑です。ストレージサブシステムに注意を払う必要があるためです。

電源を入れる順序は非常に重要です。電源の投入を不適切に実行すると、データが破損したり失われたりすることがあります。

△ 注意: ストレージサブシステムの電源を入れ、正常に動作していることを確認するまでは、クラスターノードの電源を入れないでください。

ノードの電源投入は、個別に行う必要があります。次の追加のノードの電源を入れる前に、前のノードがクラスターを形成するまで待ってください。クラスターノードの電源を入れるには、以下の手順に従ってください。

手順

1. ストレージサブシステムが正常に動作していることを確認した後、1台のノードの電源を入れます。それ以降のノードの電源を入れる前に、最初のノードが完全に起動するまで待ってください。
一度に複数のノードの電源を入れた場合、最初にシーケンスを完了したノードがクラスターのクォーラムの所有権を取得し、クラスターデータベースを制御するようになります。必ず特定のノードの電源を最初に入れ、他のクラスターノードの電源が入る前に完全に再起動されるようにすることで、そのノードをクラスタークォーラムの通常の所有者として指定してください。
2. 追加のクラスターノードの電源を入れます。各ノードが完全に起動されてから、それ以降のノードを起動してください。

トラブルシューティング、サービス、およびメンテナンス

HPE ストレージファイルコントローラーには、いくつかの監視およびトラブルシューティングのオプションがあります。以下のトラブルシューティング用警告とソリューションを使用してシステムの正常性を保持します。

- ・ 通知アラート
- ・ System Management Homepage (SMH)
- ・ ハードウェアコンポーネントの LED
- ・ HPE および Microsoft のサポート用 Web サイト
- ・ HPE Insight Remote Support ソフトウェア
- ・ Microsoft Systems Center Operations Manager (SCOM) と Microsoft の Web サイト
- ・ クラスター固有のトラブルシューティング
- ・ HPE SIM 7.6 以降 (HPE ストレージファイルコントローラー/HPE SIM の適切な統合に必要)

注記:

- HPE SIM の最新版は、HPE SPOCK の Web サイト (<http://www.hpe.com/storage/spock>) を参照してください。
- HPE SIM との統合は WBEM/WMI インターフェイスを使用する場合のみサポートします。HPE SIM を ProLiant SNMP エージェントを使用するように構成しないでください。テスト未実施でありサポートされていません。HPE ストレージファイルコントローラー上では ProLiant SNMP エージェントがデフォルトで有効化されています。これらのエージェントは内部の管理機能に使用されるため、無効化しないでください。ProLiant SNMP エージェントが外部のクライアントに対して有効になっている場合、HPE SIM を、これらのエージェントと通信しないように構成する必要があります。

-
- ❗ **重要:** 最初にストレージデバイスをサーバーに接続するときに、Update-StorageProviderCache -DiscoveryLevel 3 -PassThru コマンドを実行する必要があります。
-

Windows イベントベースの一般的なトラブルシューティング

イベントの分析には、イベントビューアーを使用できます。イベントビューアーを開くと、左側のペインには、異なるすべてのイベントログが示されたフォルダービューが表示されます。また、多数のログのイベントを同時に取り扱うことができる、カスタマイズ可能なビューも表示されます。たとえば、最近のバージョンの Windows では、管理イベントビューに、アプリケーションログまたはシステムログから生成されたエラー、警告、および重大なすべてのイベントが表示されます。中央のペインには、イベントのリストが表示されます。ここでイベントをクリックすると、イベントの詳細がプレビューペインに表示されます。または、イベントをダブルクリックすると、詳細は別ウィンドウに表示されます。これは、大規模なイベントセットを参照して、重要なすべての事項を、インターネット検索を開始する前に見つけたい場合に便利です。右側のペインを使用すると、カスタムビューの作成、フィルター処理、または特定のイベントをベースとしてスケジュール化されたタスクの作成などのアクションに素早くアクセスすることができます。

Hewlett Packard Enterprise のサポートの Web サイト

HPE ストレージファイルコントローラーの問題のトラブルシューティングを行うには、HPE サポート & ドライバーの Web サイト (<https://www.hpe.com/support>) で、HPE Server, Storage and Networking を選択します。HPE ストレージファイルコントローラーと入力するか、またはコンポーネント情報（たとえば、SAS I/O モジュール）を入力します。詳細情報を入力した後に、以下のリンクを使用してトラブルシューティング情報を入手します。

- ・ ドライバー、ソフトウェア、およびファームウェアオペレーティングシステム用のドライバーとソフトウェアが掲載されています。
- ・ 重要な問題およびソリューション、該当製品またはコンポーネントの、お客様へのお知らせ、アドバイザリ、資料などが掲載されています。
- ・ マニュアル、製品またはコンポーネントに該当する、最新のユーザードキュメントが掲載されています。ユーザーガイドには、トラブルシューティングに役立つ情報が掲載されています。以下の ProLiant サーバーマニュアルは、HPE ストレージファイルコントローラーに対して有用なトラブルシューティング情報を提供しています。
 - 以下のガイドには、特定のサーバーのトラブルシューティング情報が記載されています。
 - HPE ProLiant DL360 Gen10 Maintenance and Service Guide
 - HPE ProLiant Gen10 サーバートラブルシューティングガイド

これらのマニュアルは、<http://www.hpe.com/support/proliantgen10/docs> で参照できます。

- ❗ **重要:** ProLiant サーバーのドキュメントに記載されている一部のトラブルシューティング手順は、HPE ストレージファイルコントローラーの特定のモデルには適用できない場合があります。必要に応じて、HPE のサポート窓口にお問い合わせください。

HPE ストレージファイルコントローラーのマニュアルは、[HPE ストレージファイルコントローラーマニュアル](#)をご覧ください。

ソフトウェア関連のコンポーネントと問題については、オンラインヘルプまたはユーザーガイドに有用なトラブルシューティング情報が記載されています。既知の問題、対応策、およびサービスリリースについては、このガイドまたはリリースノートに記述されています。

- Customer notices - HPE ストレージファイルコントローラーに関する情報を記述しています。
- Customer advisories - 既知の問題と解決策または対応策を記述しています。

注記: お客様へのお知らせやアドバイザリを受信するには、「メールニュース配信」に登録する必要があります。

Microsoft Systems Center Operations Manager

Microsoft Systems Center Operations Manager (SCOM) は、Windows OS およびアプリケーションプラットフォームを保守するための総合的な監視、パフォーマンス管理、および分析ツールを提供します。このソリューションにより、Microsoft Windows 環境と HPE ストレージ製品を、共通の OpsMgr コンソールから監視することができます。Hewlett Packard Enterprise management packs for Microsoft System Center Operations Manager を、インストール、構成、および使用のためのドキュメントと共にダウンロードするには、下記の **Hewlett Packard Enterprise Management Packs for Microsoft Systems Center** サイトにアクセスします。

https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=System_Center

ハードウェアコンポーネントの取り外しと交換

ハードウェアコンポーネントの取り外しや交換について詳しくは、該当する ProLiant ユーザーガイドにある、コンポーネントの取り外しと交換についての手順に従ってください。HPE ストレージファイルコントローラー製品の ProLiant モデルを以下に示します。

HPE ストレージファイルコントローラー— HPE ProLiant DL360 Gen10 CTO サーバー

注記: システムボードを交換した後、システム BIOS に正しい製品 ID が反映されたこと、および取り付けられた部品に製品名がインストールされていることを確認する必要があります。正しい製品名は、System Insight Manager や Insight Remote Support などのアプリケーションで重要です。正しい製品名をインストールするには、C:\nas\Components\Support\NAMING フォルダーに移動します。ご使用のシステムに適用される Smart Component を見つけて実行します。Smart Component の実行後、変更を有効にするために、システムをシャットダウンして、再起動する必要があります。HPE ストレージファイルコントローラーシステムのようなマルチノードクラスターでは、名前を変更するノードをシャットダウンする前に、クラスターリソースを他のノードに移動することをお勧めします。正しい Smart Component を実行しなかった場合、製品名が誤って設定されます。しかし、システムにそれ以外の影響はありません。

表面スキャン分析

Hewlett Packard Enterprise Smart アレイコントローラーは、アクティブでない期間中にすべてのドライブを継続的にスキャンし、メディア不良を見つけます。Hewlett Packard Enterprise Smart アレイコントローラーは、頻繁に使用されている期間中も、不要セクターにアクセスしたときに、メディア不良を検出することができます。回復可能なメディア不良を検出した場合、Hewlett Packard Enterprise Smart アレイコントローラーは、ディスクドライブ上の予約領域に不要セクターを自動的に再マッピングします。回復不可能なメディア不良を検出した場合、フォールトトレラント論理ドライブが構成されていれば、コントローラーは自動的にデータを再生成し、ディスクドライブ上の再マッピングされた予約領域に書き込みます。表面スキャン分析の間隔は、UI から調整することができます。ただし、表面スキャン分析を無効にすると、コントローラーがディスク表面の不良を事前に検出して修正することができなくなり、データ紛失につながる可能性があるため、注意してください。

クラスター固有の注意事項

この項では、クラスター固有の問題およびトラブルシューティング方法について説明します。

QR プロセス中、iLO 画面が真っ白になる

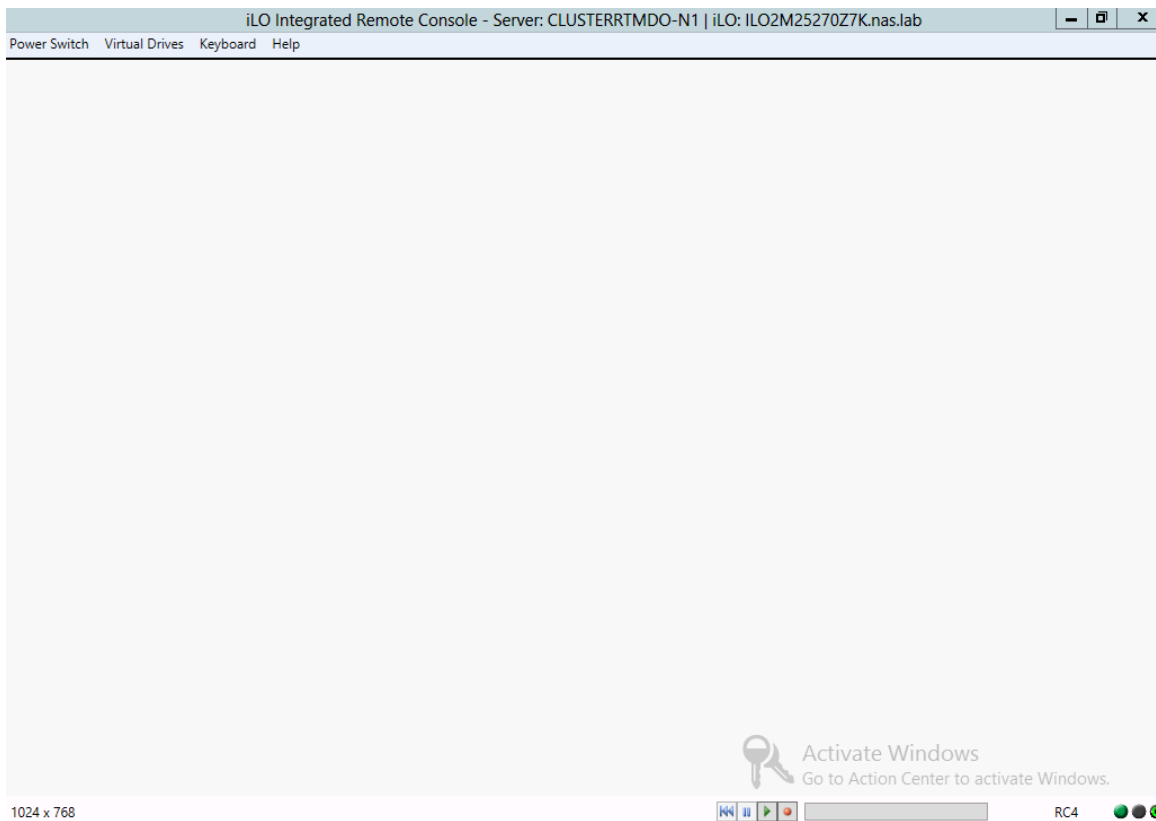


図 14: 真っ白な iLO 画面

この問題を回避するには、以下の手順を実行してください。

- ・ サーバーをリセットします。
- ・ **F9** キーを押します。
- ・ **System Configuration⇒BIOS/Platform Configuration (RBSU) ⇒PCI Device Enable/Disable** を選択します。
- ・ **Slot 2: HP Store Fabric 8Gb Dual Port PCI-e FC HBA - FC** を選択して無効にします。

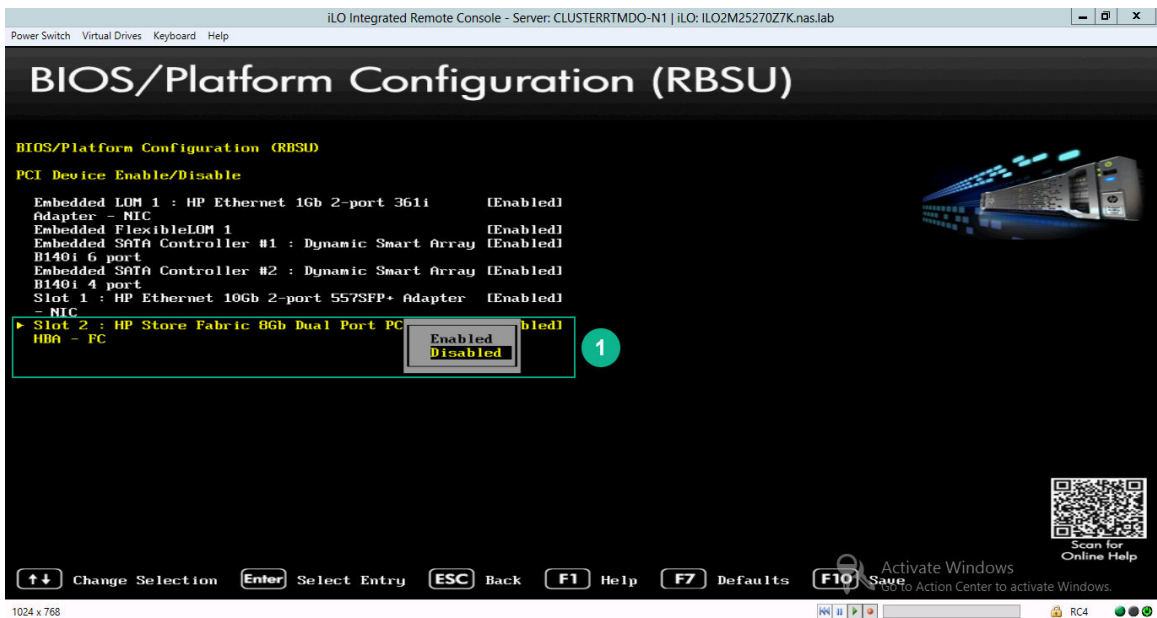


図 15: システム設定

- ・ F10 キーを押して、変更を保存します。その後、終了し、再起動します。

System Installation and Recovery screen の QR プロセス中、No disk found in Slot0b ポップアップが表示される

USB を使用してサーバーを QR しているときに、USB が NTFS でフォーマットされていると、No disk found in Slot0b ポップアップが表示されます。このポップアップが表示されないようにするには、USB を NTFS ではなく、FAT32 でフォーマットしてください。

QR プロセス中、System Installation and Recovery ウィンドウに Not a valid configuration... ポップアップが表示される

この問題を回避するには、以下の手順を実行してください。

- ・ サーバーをリセットします。
- ・ F10 (Intelligent Provisioning) を押します。
- ・ HP Smart Storage Administrator (HPSSA) を選択します。
- ・ 論理ドライブをすべて削除し、新しい論理ドライブを作成します。
- ・ サーバーを再度リセットし、QR プロセスを実行します。

クラスターの検証がフェイルオーバークラスターマネージャーで失敗し、構成がクラスタリングに適さないことが示されていますというメッセージが表示される

上記の問題を解決するには、以下の手順を実行してください。

- ・ 検証レポートを確認します。
- ・ ストレージの障害の場合、共有ストレージを、クラスターが作成される両方のノードへマッピングします。
- ・ ネットワークの障害の場合、内部のクラスターのケーブル接続を確認します。

クラスターサービスが services.msc で実行されていない

この場合、まず、両方のクラスターノードが動作していることを確認します。powershell の Get-cluster コマンドを、クラスターサービスが実行されていないノードの管理者として実行します。

エラーが引き続き発生する場合は、ノードがクラスターの一部ではなくなったことを示しています。この場合、フェイルオーバークラスターマネージャーからクラスターへの接続を使用して、ノードをクラスターに再参加させます。

ローカルコンピュータ上でクラスターサービスを起動できない

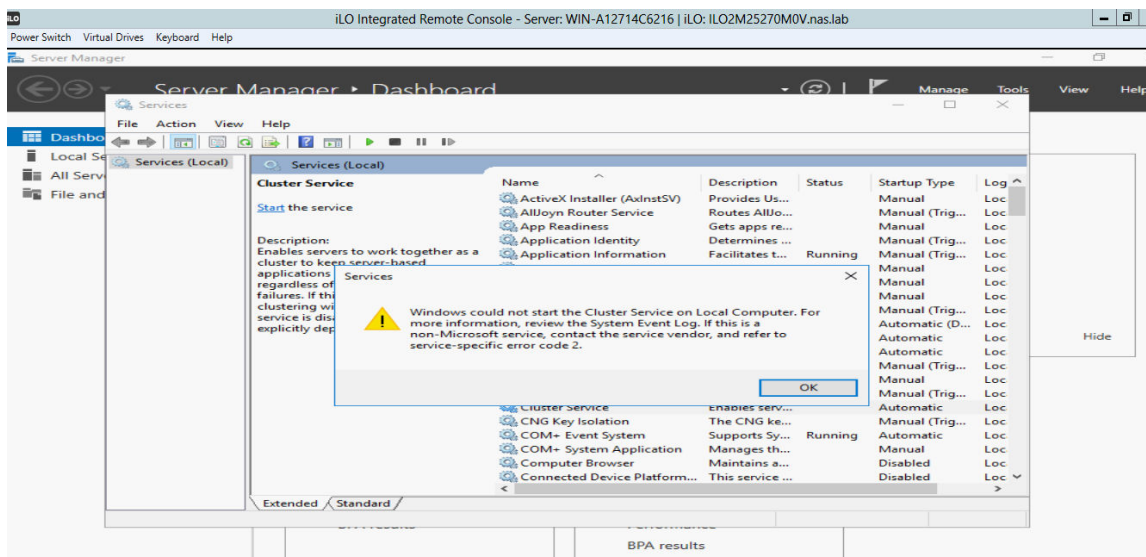


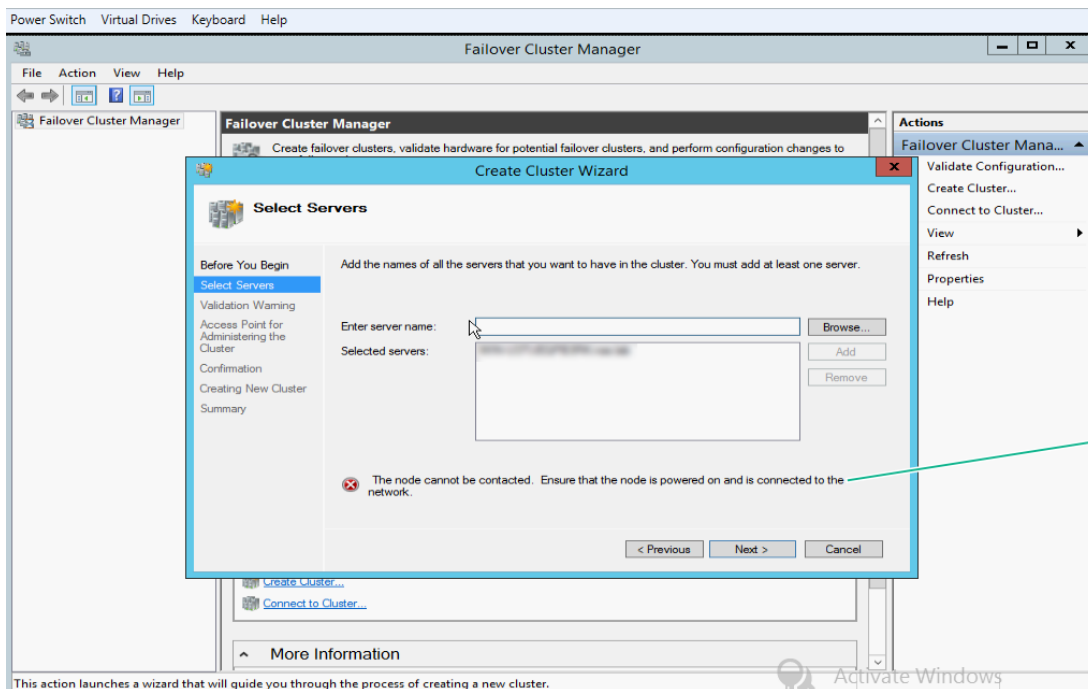
図 16: Services.msc

すべてが正しく実行されていることを確認します。クラスターサービスを停止して再起動するか、またはノードを除外して使用できないようにしてからクラスターを完全に再作成します。

クラスターの作成ウィザードのエラー

フェイルオーバークラスターマネージャーで、クラスターが作成されるノードの IP アドレスを追加しているときに、The node cannot be contacted. Ensure the node is powered on and connected to network というエラーメッセージが表示されます。

ノードの電源がオンであることを確認します。



フェイルオーバークラスターマネージャーでは、クラスターが作成されるノードの IP アドレスを追加しているときに、The computer <computer name> is joined to a cluster というエラーメッセージが表示されます。

このノードを新しいクラスターの一部にするには、ノードを以前のクラスターから切断し、powershell を実行します。

powershell の `Remove-ClusterNode` コマンドを（管理者として）実行し、ノードをフェイルオーバークラスターから削除します。そして、そのノードをフェイルオーバークラスターに再度追加します。

注記: ノードを削除すると、クラスターに追加し直さない限り、クラスターの一部としては機能しなくなります。

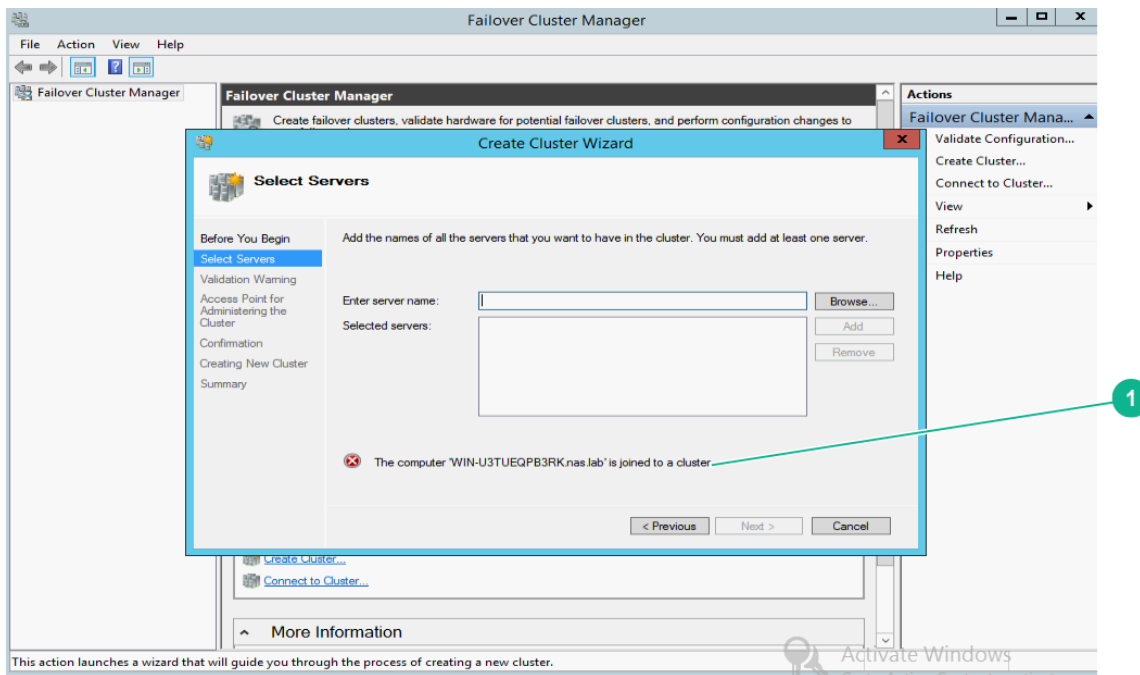


図 17: クラスターの作成ウィザードの問題 2

フェイルオーバークラスターの障害

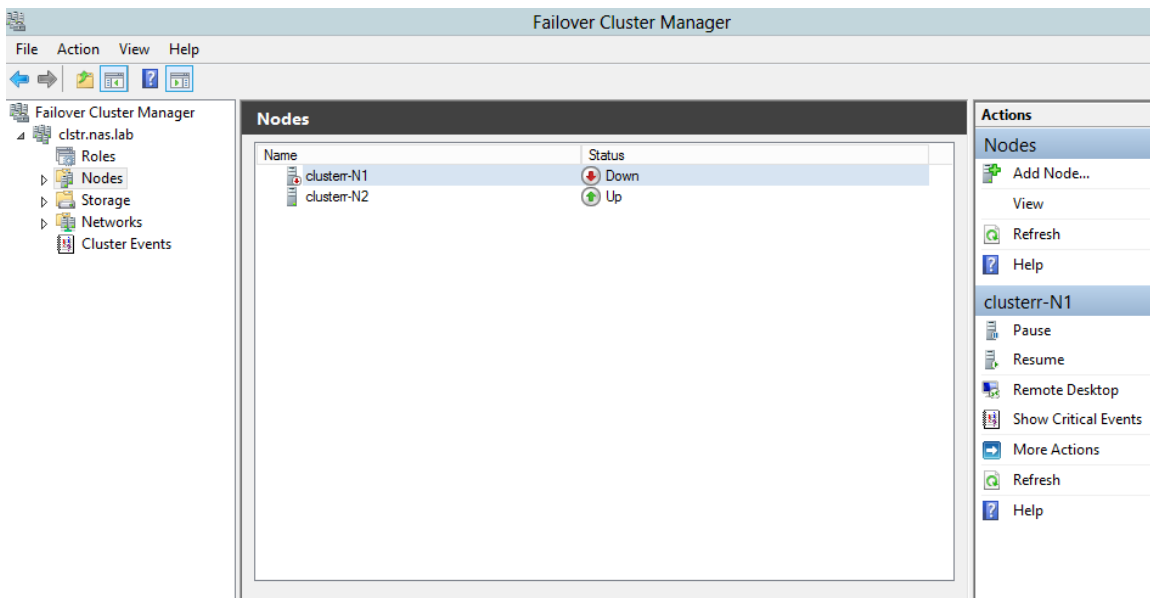


図 18: フェイルオーバークラスターの障害

フェイルオーバークラスターのフェイルオーバーエラーは、2 ノードのクラスターの 1 つのノードのハードウェア障害か、またはオペレーティングシステムの障害が原因です。

ハードウェア障害は、SCSI カードまたはオペレーティングシステムの障害によって発生する可能性があります。このような場合、Powershell の `Remove-ClusterNode` コマンド（管理者として実行）を使用して、障害が発生したノードをフェイルオーバークラスターから削除するか、またはフェイルオーバークラスターマネージャーからノードを削除します。コンピューターをオフラインにしてハードウェア障害に対応し、マシンを稼働状態に戻して、修理したノードを既存のクラスターに追加し直します。

オペレーティングシステムの障害の場合は、ノードはオフラインになっていても、回復不可能な故障ではありません。このため、再度ノードを回復し、検証します。必要な修理を行い、コンピューターを稼働状態に戻して、フェイルオーバーしたクラスターインスタンスに、修理したノードを追加し直します。

詳しくは、以下の Web サイトを参照してください。

- ・ <https://msdn.microsoft.com/en-in/library/ms189117.aspx>

HPE ストレージファイルコントローラーの復旧

この章では、HPE ストレージファイルコントローラーシステムを工場出荷時のデフォルトの状態に復旧する方法について説明します。System Recovery DVD（注文した場合）を使用すると、システムの復旧を実行できます。System Recovery DVD を注文しなかった場合は、**HPE サポートセンター**からシステム回復イメージをダウンロードし、イメージファイルを USB フラッシュドライブまたは DVD に保存し、システムの復旧を実行することができます。システム復旧用の USB フラッシュドライブまたは DVD の作成については、**HPE サポートセンターのイメージファイルによる USB フラッシュドライブの作成**および**HPE サポートセンターのイメージファイルによる DVD の作成**を参照してください。

注記: サーバーを起動してイメージを復旧する前に、外付けストレージを取り外してください。取り外さないと、システムが外付けディスク内のボリュームを数えようとして、ハングすることがあります。

System Recovery DVD

System Recovery DVD は、HPE ストレージファイルコントローラーのオプションで注文することができます。System Recovery DVD を使用すると、イメージのインストールや、壊滅的な障害から復旧させることができます。

いつでも、DVD から起動して、サーバーを出荷時の状態に復元することができます。これにより、他のすべての手順でサーバーの起動が失敗した場合に、システムを復旧することができます。

復旧プロセスは既存のデータボリュームを保持しようとしませんが、システムを復旧する前にデータをバックアップする必要があります。

❗ **重要:** 復旧処理の過程で、元の OS の論理ドライブのデータはすべて消去されます。

システム復旧の中で、既存のドライブを、同じサイズまたはより大きなサイズのドライブと置き換えることができます。HPE では、置き換えるドライブは、元のドライブと同じタイプにすることをお勧めしますが、必須ではありません。ただし、同じ RAID グループ内のドライブは同じタイプにする必要があります（RAID グループ内で異なるドライブタイプを混在させることはできません）。

ディスクドライブを交換した後、システム復旧を実施する場合、交換ドライブに論理ドライブが含まれていないことを確認する必要があります。論理ドライブを削除するには Option ROM Configuration for Arrays（ORCA）ユーティリティを使用してください。ORCA について詳しくは、下記のサイトで HPE Smart アレイコントローラーでのアレイの構成リファレンスガイドを参照してください。

<http://www.hpe.com/support/manuals>

System Recovery DVD によるシステムデータの保存

System Recovery DVD をブートし、プロンプトが表示されたら、**Windows Recovery Environment** を選択します。次の手順を実行します。

手順

1. キーボードレイアウトを選択します。
2. **Troubleshoot > Advanced Options > Command Prompt** を選択します。
3. `WPEINIT` と入力し、約 10 秒待ってから次に進みます。
4. コマンドプロンプトで `IPCONFIG` と入力し、ネットワークインターフェイスに IP アドレスがあることを確認します。

注記:

- ・ ネットワークが DHCP を使用していない場合は、IP アドレスおよび DNS 情報を手動で割り当ててください。手動で IP アドレスを割り当てるコマンドの例を以下に示します。
 - `netsh interface ip set address "connection name" static 192.168.0.101 255.255.255.0 192.168.0.1`
 - `netsh interface ip add dns "connection name" 208.67.222.222`
 - `netsh interface ip add dns "connection name" 208.67.220.220 index=2`
- ・ netsh コマンドの使用方法についての詳細は、<https://technet.microsoft.com/en-us/library/bb490943.aspx> を参照してください。
- ・ ネットワークを開始するには、時間がかかる場合があります。有効な IP アドレスがネットワークインターフェイスに割り当てられるまでは、次の手順に進まないでください。

5. コマンドプロンプトで `NET USE Z: \\servername\sharename` と入力します。\\servername\sharename は、データがコピーされるネットワーク共有への UNC パスです。

6. プロンプトが表示されたら、共有にアクセスするためのユーザー名とパスワードを入力します。

共有がドライブ Z: にマッピングされたら、Robocopy を使用してシステムからネットワーク共有にファイルをコピーできます。Robocopy の詳細については、<https://technet.microsoft.com/library/cc733145.aspx> を参照してください。

復旧後のドライブ文字の割り当て

既存のデータボリューム（非オペレーティングシステムボリューム）があるシステムを System Recovery DVD で復元した場合、データボリュームにはドライブ文字が割り当てられていません。これは設計によるものです。ボリュームラベルは維持されるので、これらを使用してデータボリュームを識別できます。

diskpart.exe またはディスクの管理を使用して、ボリュームにドライブ文字を割り当てられます。

ディスクの管理を使用するには以下の手順に従ってください。

1. スタート→Windows PowerShell をクリックします。

Windows PowerShell ウィンドウが開きます。

2. `diskmgmt.msc` と入力して Enter を押します。

ディスクの管理ウィンドウが開きます。

3. ドライブ文字を割り当てるディスクとパーティションを右クリックし、ドライブ文字とパスの変更を選択します。

System Recovery DVD によるシステム復旧用 USB フラッシュドライブの作成

USB フラッシュドライブを使用して System Recovery DVD のバックアップコピーを作成すれば、USB フラッシュドライブを使用してシステムを復元できます。

System Recovery DVD を使用してシステム復旧用 USB フラッシュドライブを作成するには、以下の手順を実行します。

手順

1. 8GB 以上の空の USB フラッシュドライブを用意します。
2. USB フラッシュデバイスをワークステーションまたはラップトップに挿入します。
3. 管理者特権のコマンドプロンプトを開きます。
4. コマンドプロンプトで、`diskpart` と入力します。
5. `diskpart` プロンプトで、`list disk` と入力します。
6. Flash ドライブに対応するディスク番号を特定します。通常は、表示された最後のディスクです。
7. `sel disk <USB drive number>` (たとえば、`sel disk 4`) と入力します。
8. `clean` と入力します。このコマンドにより、USB フラッシュドライブからすべてが消去されます。このため、正しいディスクを選択したことを確認してください。
9. `create par primary` と入力します。
10. `sel par 1` と入力します。
11. `format fs=fat32 quick` と入力します。
12. パーティションを Active とするために、`active` と入力します。
13. USB ドライブにドライブ文字をアサインするために、`assign letter=<drive letter>` (たとえば、`assign letter=U`) と入力します。
14. `exit` と入力して、`diskpart` コンテキストコマンドを終了します。
15. コンピューターに System Recovery DVD を挿入します。
16. Windows のエクスプローラーまたは同等のユーティリティを使用し、隠しファイルやシステムファイルを含むすべてのコンテンツが表示されるように DVD を開きます。
17. DVD 上のすべてのファイル (bootmgr を含む) を選択します。
18. 選択したすべてのファイルを USB フラッシュドライブのルートにコピーします。

HPE サポートセンターのイメージファイルによる USB フラッシュドライブの作成

HPE サポートセンターのイメージファイルでシステム復旧用の USB フラッシュドライブを作成するには、以下の手順を実行します。

手順

1. イメージファイルをダウンロードしたら、その ISO をローカルにマウントし、ファイルにアクセスできるようにします。システムに USB フラッシュドライブを挿入します。
2. 管理者権限のある昇格コマンドプロンプトを開き、`diskpart` と入力して、**Enter** を押します。
3. `list disk` と入力し、USB フラッシュドライブ番号またはドライブ文字を調べ、**Enter** を入力します。
4. USB フラッシュドライブのドライブ番号またはドライブ文字をメモします。
5. `select disk <x>` (<x> は、USB フラッシュドライブのドライブ番号またはドライブ文字) と入力し、**Enter** を押します。

6. `clean` と入力して USB フラッシュドライブからデータを削除し、**Enter** を押します。
7. `create part pri` と入力して USB フラッシュドライブに新しいプライマリパーティションを作成し、**Enter** を押します。
8. `select part 1` と入力して、作成したパーティションを選択し、**Enter** を押します。
9. パーティションを FAT32 としてフォーマットするには、`format fs=fat32 quick` と入力し、**Enter** を押してください。

❗ **重要:** サーバープラットフォームは Unified Extensible Firmware Interface (UEFI) で構成されているため、USB フラッシュドライブを NTFS ではなく、FAT32 としてフォーマットする必要があります。パーティションを FAT32 としてフォーマットするには、3PAR File controller `formatfs=fat32 quick` と入力し、**Enter** を押してください。

10. `active` と入力してパーティションをアクティブとしてマークし、**Enter** を押します。
11. `Exit` と入力して `diskpart context` コマンドを終了し、**Enter** を押します。
12. ディスクイメージファイル (ISO) に含まれているインストールファイルを、USB フラッシュドライブの `root` にコピーします。

HPE サポートセンターのイメージファイルによる DVD の作成

HPE サポートセンターのイメージファイルでシステム復旧用の DVD を作成するには、以下の手順を実行します。

手順

1. ドライブに空き DVD (2 層式) を挿入します。
2. システム上の ISO イメージファイルを見つけ、ダブルクリックします。
Windows ディスクイメージ書き込みツールウィンドウが表示されます。
3. 使用するディスクイメージ書き込みツールを選択します。この手順は、複数のディスクイメージ書き込みツールがある場合だけ実行します。
4. **書き込み後のディスクの確認**を選択し、ISO イメージが正しく書き込まれていることを確認するようにします。
5. **書き込み**をクリックします。
完了すると、該当するステータスが画面に表示されます。

DVD または USB フラッシュデバイスによる出荷時イメージの復元

手順

1. 次のいずれかを実行します。

- a. 直接アクセスを行うには、System Recovery DVD またはブート可能な USB フラッシュデバイス (System Recovery イメージが準備されたもの) を挿入します。
 - b. リモート管理アクセスを行うには、iLO を使用してクライアント PC からサーバーに接続します。クライアント PC に System Recovery DVD を挿入します。または、System Recovery イメージを準備したブート可能な USB フラッシュデバイスを接続します。
2. USB フラッシュデバイスまたは USB DVD ドライブでサーバーブレードを再起動します。
- システム BIOS は、デフォルトで最初に USB デバイスから起動しようとします。ブート中にモニター出力を監視して、必要に応じてキーを押して USB メディアから起動します。
-
- 注記:** 直接接続の場合は、適切なブートシーケンスを行うために BIOS の設定を変更する必要がある場合があります。リモート接続の場合は、適切なブートシーケンスを行うために一部の iLO 設定を変更する必要がある場合があります。
-
3. HPE ストレージファイルコントローラーシステムリカバリのオプションをクリックします。
- 復旧処理が実行されます。その間、ユーザーによる操作はほとんどありません。サーバーは自動的に数回再起動します。
-
- ❗ **重要:** 復旧処理は中断しないでください。
-
- 復旧処理が完了すると、Windows の設定ウィザードが表示されます。以降の手順は、復旧しているのが両方のノードか (**両方のノードの復旧**を参照)、あるいは 1 台のノードか (**1 台のノードの復旧**を参照) に応じて異なります。
4. 直接接続した DVD またはフラッシュデバイス (または、リモートで接続した iLO 仮想 DVD またはフラッシュデバイス) をサーバーから取り外します。先に進む前に、取り外してあった外付けストレージを再度取り付けて、サーバーを再起動してください。

両方のノードの復旧

両方のノードを復旧する場合の手順は、工場から出荷された新しい HPE ストレージファイルコントローラーシステムを構成する作業と同様です。

注記: 復旧処理では HPE ストレージファイルコントローラーシステムを工場出荷バージョンに復元しますが、EMU および iLO アドレスの構成は工場出荷時のデフォルト値には復元しません。EMU および iLO アドレスの構成は、システムの復旧前と同じです。

各サーバーとも、**DVD または USB フラッシュデバイスを使用した工場出荷イメージの復元**の手順に従ってください。

1 台のノードの復旧

クラスターの 2 台のノードのうちの 1 台のみを復旧する場合は、復旧したノードを既存の Windows フェイルオーバークラスターに参加させるため、少し手順が複雑です。動作している (少なくとも 1 つのノードを含む) Windows のフェイルオーバークラスターがない場合は、**両方のノードの復旧**の手順に従います。

以下の手順は、HPE ストレージファイルコントローラーシステムのノードのうち 1 台のイメージを再作成して、Windows フェイルオーバークラスターにそのノードを再度参加させる方法を示しています。

手順

1. **DVD または USB フラッシュデバイスによる出荷時イメージの復元**の手順に従います。
2. Windows セットアップウィザードが表示されたら、言語、地域の設定、およびキーボードのレイアウトを選択して、使用許諾契約書に同意します。ウィザードが完了すると、2 番目のノードの検出が試みられます。検出が失敗して、以下のエラーメッセージが表示されます。

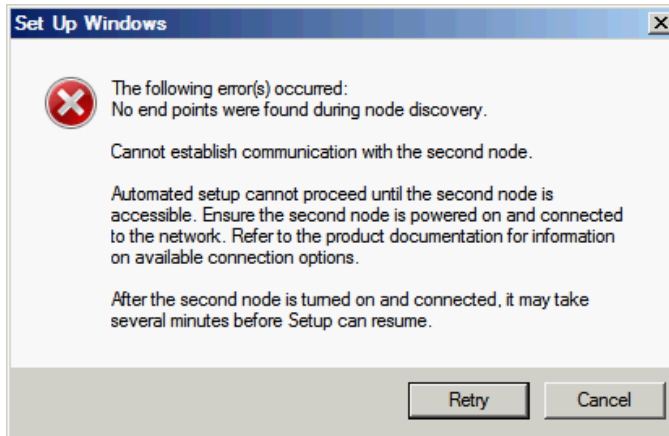


図 19: 2 番目のノード検索中のエラーメッセージ

3. **キャンセル**をクリックします。次のメッセージを表示したポップアップウィンドウが開きます。
2 番目のノードを無視しますか? 無視した場合、後でウィザードを手動で実行して 2 番目のノードを構成する必要があります。
4. **はい**をクリックします。
インストールが続行され、最後にノードが再起動されます。再起動後、Windows により自動的にローカル管理者としてログオンされ、初期構成タスク (ICT) ウィンドウが起動されます。ただし、ICT を使用してノードを構成しません。
5. ウィンドウの左下の**次のログオン時にこのウィンドウを表示しない**ボックスをチェックして、ICT ウィンドウを閉じます。ノード間の不整合について警告するメッセージが表示されます。ICT ウィンドウを閉じることを確認します。
6. **CTRL+ALT+DELETE** キーを押して、ローカル管理者アカウントのパスワードを変更します。(iLO リモートコンソールを使用している場合は、キーボードメニューから **CTRL-ALT-DEL** 項目を選択します。) **パスワードの変更**を選択します。システムを最初に構成したときに使用していた古いパスワードを入力し、続いて新しいパスワードを入力します。
7. タスクバーの右下隅に表示される時刻と日付を選択します。**日付と時刻の設定の変更**リンクをクリックします。ノードのタイムゾーンに、もう一方の HPE ストレージファイルコントローラーサーバーおよびドメインコントローラーと同じタイムゾーンを設定します。必要な場合は、時刻を調整します。
8. ICT ウィンドウが閉じるときに、サーバーマネージャーが開きます。開かない場合は、Windows のスタートボタンの右側のタスクバーにあるショートカットから起動します。
9. コンピューター名/ドメインの変更画像に示すように、コンピューター名をクリックし、**システムのプロパティ**ウィンドウで**変更**をクリックします。ノードの新しいコンピューター名を入力して**ドメイン**を選択し、ノードを参加させる Active Directory のドメイン名を指定します。指定するドメインは、既存の 1 ノードクラスターを含むドメインと同じドメインである必要があります。ドメインにコンピューターを追加する権限を持つドメインアカウントの認証情報の入力を求められます。変更を行ったら、サーバーの再起動を求めるプロンプトに同意します。

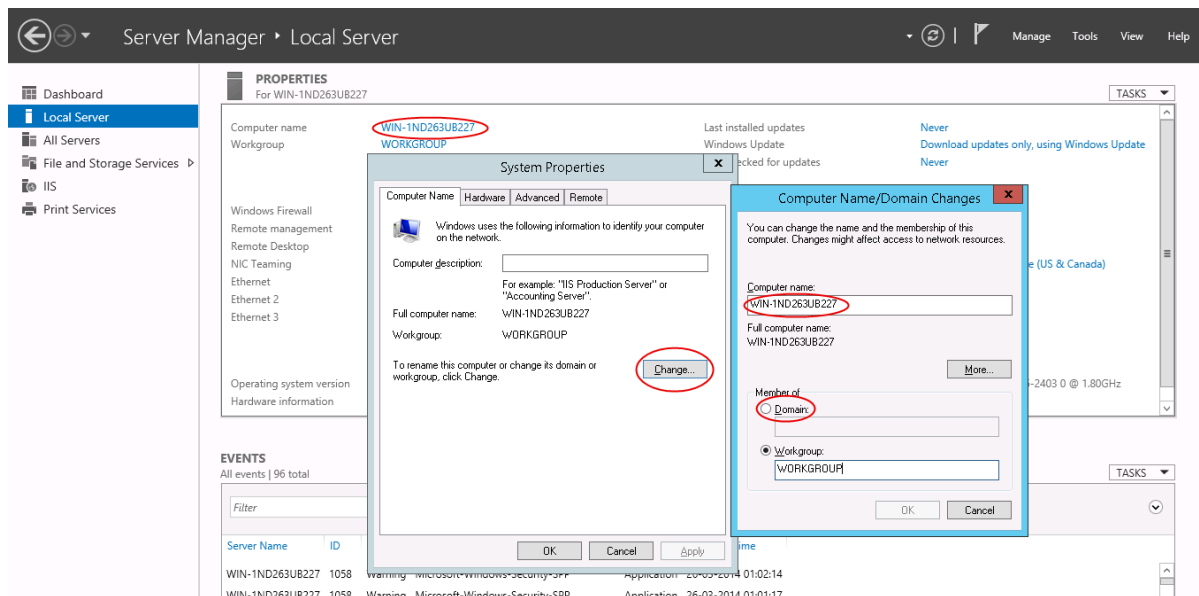


図 20: コンピューター名/ドメインの変更

10. サーバーの再起動後に、ローカル管理者としてログオンします。今後、クラスターメンバーとしてサーバーを管理するために、ローカル管理者グループのメンバーとして少なくとも 1 人のドメインユーザーを使用してください。サーバーマネージャーで**構成 > ローカルユーザーとグループ**を選択してドメインユーザーを管理者グループに追加します。
11. 復旧したノードをクラスターに戻す前に、クラスターから故障したノードを削除（排除）します。詳しくは、次の Microsoft の記事を参照してください。
12. [http://technet.microsoft.com/ja-jp/library/cc784955\(v=WS.10\).aspx](http://technet.microsoft.com/ja-jp/library/cc784955(v=WS.10).aspx)
13. 復旧したサーバーをクラスターに追加するには、もう一方のサーバー（既存の 1 ノードクラスターのメンバーであるサーバー）にドメインユーザーとしてログオンします。初期構成タスク（ICT）ウィンドウは使用しないでください。以下の日本語の Web サイトの説明に従って復旧したサーバーをクラスターに追加します。
14. <http://technet.microsoft.com/ja-jp/library/cc730998.aspx>

Iternity iCAS

HPE ストレージファイルコントローラーで iTernity Compliant Archive Solution (iCAS) を使用すると、オープンで、柔軟性があり、拡張可能な長期のアーカイブ機能入手することができます。SEC 17a-4 (f) 要件を満たしていることを、今すぐ確認してください。**iCAS** へのショートカットが、デスクトップ上およびスタート画面上にあります。iCAS および無償試用版のサインアップについて詳しくは、Iternity の Web サイトを参照してください。

製品に関するフィードバック

製品に関するフィードバック機能を使用すると、HPE ストレージファイルコントローラーの改善についてのご意見、ご提案、またはフィードバックを storeeasyproductfeedback@hpe.com へ送信することができます。以下の方法で製品に関するフィードバックダイアログボックスにアクセスできます。

- ・ デスクトップにある **Product Feedback** アイコンをダブルクリックする。
- ・ スタート画面の **Product Feedback** をクリックする。

Web サイト

全般的な Web サイト

Hewlett Packard Enterprise Information Library

<http://www.hpe.com/info/EIL>

Single Point of Connectivity Knowledge (SPOCK) ストレージ互換性マトリックス

<http://www.hpe.com/storage/spock>

ストレージのホワイトペーパーおよび分析レポート

<http://www.hpe.com/storage/whitepapers>

その他の Web サイトについては、[サポートと他のリソース](#)を参照してください。

サポートと他のリソース

Hewlett Packard Enterprise サポートへのアクセス

- ・ ライブアシスタンスについては、Contact Hewlett Packard Enterprise Worldwide の Web サイトにアクセスします。

<http://www.hpe.com/assistance>

- ・ ドキュメントとサポートサービスにアクセスするには、Hewlett Packard Enterprise サポートセンターの Web サイトにアクセスします。

<http://www.hpe.com/support/hpesc>

ご用意いただく情報

- ・ テクニカルサポートの登録番号（該当する場合）
- ・ 製品名、モデルまたはバージョン、シリアル番号
- ・ オペレーティングシステム名およびバージョン
- ・ ファームウェアバージョン
- ・ エラーメッセージ
- ・ 製品固有のレポートおよびログ
- ・ アドオン製品またはコンポーネント
- ・ 他社製品またはコンポーネント

アップデートへのアクセス

- ・ 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるソフトウェアアップデート方法を確認してください。
- ・ 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

Hewlett Packard Enterprise サポートセンター

<http://www.hpe.com/support/hpesc>

Hewlett Packard Enterprise サポートセンター：ソフトウェアのダウンロード

<http://www.hpe.com/support/downloads>

Software Depot

<http://www.hpe.com/support/softwaredepot>

- ・ eNewsletters およびアラートをサブスクライブするには、以下にアクセスします。

<http://www.hpe.com/support/e-updates-ja>

- ・ お客様の資格を表示したりアップデートしたり、契約や保証をお客様のプロファイルにリンクしたりするには、Hewlett Packard Enterprise サポートセンターの **More Information on Access to Support Materials** ページにアクセスします。

<http://www.hpe.com/support/AccessToSupportMaterials>

- ❗ **重要:** 一部のアップデートにアクセスするには、Hewlett Packard Enterprise サポートセンターからアクセスするときに製品資格が必要になる場合があります。関連する資格を使って HPE パスポートをセットアップしておく必要があります。

オープンソースコンポーネントに関する情報

HPE StoreEasy management console は、特定の開発用オープンソースライブラリを使用しており、ソフトウェアインストールの一部として配布されます。関連するオープンソースのライセンスニーズに従って、ライセンスファイルとソースコードに関する情報を皆さまがご確認できるようにしています。詳しくは、[オープンソースのダウンロードサイト](#)をご覧ください。

カスタマーセルフリペア（CSR）

Hewlett Packard Enterprise カスタマーセルフリペア（CSR）プログラムでは、ご使用の製品をお客様ご自身で修理することができます。CSR 部品を交換する必要がある場合、お客様のご都合のよいときに交換できるよう直接配送されます。一部の部品は CSR の対象になりません。Hewlett Packard Enterprise もしくはその正規保守代理店が、CSR によって修理可能かどうかを判断します。

リモートサポート（HPE 通報サービス）

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。リモートサポートは、インテリジェントなイベント診断を提供し、ハードウェアイベントを Hewlett Packard Enterprise に安全な方法で自動通知します。これにより、ご使用の製品のサービスレベルに基づいて、迅速かつ正確な解決が行われます。ご使用のデバイスをリモートサポートに登録することを強くおすすめします。

ご使用の製品にリモートサポートの追加詳細情報が含まれる場合は、検索を使用してその情報を見つけてください。

リモートサポートおよびプロアクティブケア情報

HPE 通報サービス

<http://www.hpe.com/jp/hpalert>

HPE プロアクティブケアサービス

<http://www.hpe.com/services/proactivecare-ja>

HPE プロアクティブケアサービス：サポートされている製品のリスト

<http://www.hpe.com/services/proactivecaresupportedproducts>

HPE プロアクティブケアアドバンスドサービス：サポートされている製品のリスト

<http://www.hpe.com/services/proactivecareadvancedsupportedproducts>

保証情報

ご使用の製品の保証に関する情報を表示するには、以下のリンクを参照してください。

HPE ProLiant と IA-32 サーバーおよびオプション

<http://www.hpe.com/support/ProLiantServers-Warranties>

HPE Enterprise および Cloudline サーバー

<http://www.hpe.com/support/EnterpriseServers-Warranties>

HPE ストレージ製品

<http://www.hpe.com/support/Storage-Warranties>

HPE ネットワーク製品

<http://www.hpe.com/support/Networking-Warranties>

規定に関する情報

安全、環境、および規定に関する情報については、Hewlett Packard Enterprise サポートセンターからサーバー、ストレージ、電源、ネットワーク、およびラック製品の安全と準拠に関する情報を参照してください。

<http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

規定に関する追加情報

Hewlett Packard Enterprise は、REACH（欧州議会と欧州理事会の規則 EC No 1907/2006）のような法的な要求事項に準拠する必要に応じて、弊社製品の含有化学物質に関する情報をお客様に提供することに全力で取り組んでいます。この製品の含有化学物質情報レポートは、次を参照してください。

<http://www.hpe.com/info/reach>

RoHS、REACH を含む Hewlett Packard Enterprise 製品の環境と安全に関する情報と準拠のデータについては、次を参照してください。

<http://www.hpe.com/info/ecodata>

社内プログラム、製品のリサイクル、エネルギー効率などの Hewlett Packard Enterprise の環境に関する情報については、次を参照してください。

<http://www.hpe.com/info/environment>

Hewlett Packard Enterprise プライバシープラクティス

名前、電話番号、IP アドレスやメール アドレスなどの個人情報の共有はシステムの問題が検出された際に HPE から要求される場合があります。個人のデータは、サポート提供と最適化目的にのみ使用されます。HPE のプライバシーに関する詳細は、[HPE のプライバシーに関する声明を参照](#)。

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterprise では、お客様により良いドキュメントを提供するように努めています。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、ドキュメントフィードバック担当 (docsfeedback@hpe.com) へお寄せください。この電子メールには、ドキュメントのタイトル、部品番号、版数、およびドキュメントの表紙に記載されている刊行日をご記載ください。オンラインヘルプの内容に関するフィードバックの場合は、製品名、製品のバージョン、ヘルプの版数、およびご利用規約ページに記載されている刊行日もお知らせください。