

Dell PowerVault MD3200

および MD3220

ストレージアレイ

導入ガイド



メモ、注意、警告



メモ：コンピュータを使いやすくするための重要な情報を説明しています。



注意：手順に従わない場合は、ハードウェアの損傷やデータの損失の可能性があることを示しています。



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

© 2013 すべての著作権は Dell Inc. にあります。

本書に使用されている商標：Dell™、DELL のロゴ、PowerEdge™、PowerVault™、および OpenManage™ は、Dell Inc. の商標です。Intel® は米国およびその他の国における Intel Corporation の登録商標です。Microsoft®、Windows®、Windows Server®、MS-DOS® および Internet Explorer® は、米国その他の国における Microsoft Corporation の商標または登録商標です。Red Hat® および Red Hat Enterprise Linux® は、米国およびその他の国における Red Hat, Inc. の登録商標です。SUSE® は米国およびその他の国における Novell, Inc. の登録商標です。

2013 年 7 月

Rev. A02

目次

1	はじめに	7
	システム要件	7
	管理ステーションの必要条件	7
	ストレージアレイについて	8
2	ハードウェアの取り付け	11
	ストレージ構成の計画	11
	ストレージアレイの接続	12
	ストレージアレイのケーブル接続	12
	冗長および非冗長構成	12
	シングルコントローラ構成	13
	デュアルコントローラ構成	16
	PowerVault MD1200 シリーズ 拡張エンクロージャの	
	ケーブル接続	21
	以前に構成された PowerVault MD1200 シリーズ拡張	
	エンクロージャで拡張する	21
	新しい PowerVault MD1200 シリーズ拡張	
	エンクロージャで拡張する	23
3	PowerVault MD ストレージソフトウェアの	
	インストール	25
	グラフィカルインストール (推奨)	26
	コンソールインストール	27
	サイレントインストール	27
	PowerVault MD ストレージソフトウェアの	
	アップグレード	28
4	インストール後のタスク	29
	作業を開始する前に	29

iSCSI 設定ワークシート	30
IPv4 設定 — ワークシート	31
IPv6 設定 — ワークシート	32
ストレージアレイの iSCSI の設定	33
モジュラー型ディスク設定ユーティリティ (MDCU) を使用した自動設定	34
接続確立後の手順	37
iSCSI 用のネットワーク設定のガイドライン	37
Microsoft Windows ホストのセットアップ	37
DHCP サーバーを使用する	38
静的 IP アドレス指定を使用する	38
DNS サーバーを使用する	38
WINS サーバーを使用する	38
Linux ホストのセットアップ	39
DHCP を使用する	39
静的 IP アドレスを使用する	40
.	40
5 PowerVault MD Storage ソフトウェアの アンインストール	41
Windows からの MD Storage ソフトウェアの アンインストール	41
Linux からの MD Storage ソフトウェアの アンインストール	42
6 困ったときは	43
システムサービスタグの位置	43
デルへのお問い合わせ	43
マニュアルに対するフィードバック	43
A 付録 — 負荷バランス	45
Windows 負荷バランスポリシー	45

サブセット付きラウンドロビン	45
サブセット付き最小のキューの深さ	45
Windows Server 2008 における負荷 バランスポリシーの変更	46
Linux での負荷バランスポリシーの設定	46
B 付録 — iSCSI の手動設定	47
手順 1：ストレージアレイの検出 (帯域外管理のみ)	48
IPv4 管理ポートのデフォルト設定	48
IPv6 管理ポートのデフォルト設定	48
ストレージアレイの自動検知	49
ストレージアレイの手動検出	50
アレイのセットアップ	50
手順 2：ストレージアレイの iSCSI ポートの設定	51
手順 3：iSCSI イニシエータからのターゲットの検出	53
手順 4：ホストアクセスの設定	55
CHAP 認証について	55
CHAP について	55
ターゲット CHAP	56
相互 CHAP	56
CHAP の定義	57
手順 5：ストレージアレイにおける CHAP 認証の設定 (オプション)	57
ストレージアレイのターゲット CHAP 認証の設定	57
ストレージアレイの相互 CHAP 認証の設定	58
手順 6：ホストサーバーにおける CHAP 認証の設定 (オプション)	59
手順 7：ホストサーバーから ストレージアレイへの接続	62
手順 8：帯域内管理のセットアップ (オプション)	65

はじめに

本ガイドには、Dell PowerVault MD3200 および Dell PowerVault MD3220 ストレージアレイの導入に関する情報を記載しています。導入プロセスには、次の手順が含まれます。

- ハードウェアの取り付け
- Modular Disk Storage Manager (MDSM) ソフトウェアのインストール
- 初期システム設定

その他、システム要件、ストレージアレイの構成、ユーティリティに関する情報が記載されています。



メモ: 製品マニュアルの詳細については、dell.com/support/manuals を参照してください。

管理者は MDSM を使用して、ストレージアレイを最も使いやすい状態に設定し、監視することができます。PowerVault MD シリーズのリソースメディアに含まれる MDSM のバージョンは、PowerVault MD3200 シリーズと以前の PowerVault MD シリーズストレージアレイ両方の管理に使用することができます。MDSM は、Microsoft Windows および Linux の両オペレーティングシステムと互換性があります。

システム要件

PowerVault MD3200 シリーズのハードウェアとソフトウェアを設置し、設定する前に、対応オペレーティングシステムがインストールされていること、および最小システム要件が満たされていることを確認します。詳細については、dell.com/support/manuals で『Support Matrix』（サポートマトリクス）を参照してください。

管理ステーションの必要条件

管理ステーションは、MDSM を使用してネットワーク全体のストレージアレイを設定および管理します。管理ステーションは、次の最小システム要件を満たしている必要があります。

- Intel Pentium または同等のプロセッサ（1333 MHz 以上）、512 MB RAM（1024 MB を推奨）。
- 1 GB のディスク空き容量。
- 画面解像度 1024x768、1600 万色（1280x1024 32 ビット推奨）。

- Microsoft Windows、Red Hat Enterprise Linux、または SUSE Linux Enterprise Server。



メモ：対応オペレーティングシステムには、ネイティブおよびゲストオペレーティングシステムの両方が含まれます。



メモ：サポートされるハイパーバイザーは、Microsoft Hyper-V、Citrix XenServer、および VMware ESX と ESXi です。対応バージョンについての情報は、dell.com/support/manuals で『Support Matrix』（サポートマトリクス）を参照してください。

- システム管理者またはそれと同等の権限。

ストレージレイについて

RAID コントローラモジュールを通じてアクセスされる物理ディスクを含むエンクロージャは、RAID エンクロージャと呼ばれています。ストレージレイには、物理ディスク、RAID コントローラモジュール、ファン、電源ユニットなどのさまざまなハードウェアコンポーネントが含まれており、これらがエンクロージャ内に収められています。

ストレージレイに接続されている 1 台または複数のホストサーバーは、ストレージレイ上のデータにアクセスできます。どのパスが 1 つだけ失われても（ホストサーバーポートの障害などにより）、ストレージレイに保存されているデータへのアクセスが全面的に失われることがないように、ホストとストレージレイの間に複数の物理パスを確立することも可能です。

ストレージレイは、次で実行されている MDSM で管理されます。

- ホストサーバー — ホストサーバーシステムでは、MDSM とストレージレイは SAS 接続を経由して管理リクエストとイベント情報を通信します。
- 管理ステーション — 管理ステーションでは、MDSM はストレージレイ管理ポートへのイーサネット接続、またはホストサーバーへのイーサネット接続を経由してストレージレイと通信します。イーサネット接続は SAS 接続を使って管理ステーションとストレージレイの間で管理情報をやりとりします。

MDSM を使用して、ストレージレイ内の物理ディスクを構成し、ディスクグループと呼ばれる論理コンポーネントを作成します。次に、ディスクグループを仮想ディスクに分割します。ディスクグループは、ストレージレイの未設定容量内に作成されます。仮想ディスクは、ディスクグループの空き容量内に作成されます。

未設定容量は、ディスクグループにまだ割り当てられていない物理ディスクで構成されます。未設定の容量を使用して仮想ディスクを作成すると、ディスクグループが自動的に作成されます。ディスクグループ内の唯一の仮想ディスクが削除されると、そのディスクグループも削除されます。空き容量とは、仮想ディスクに割り当てられていないディスクグループ内の容量です。

データは、RAID テクノロジを使用してストレージレイ内の物理ディスクに書き込まれます。データがどんな方法で物理ディスクに書き込まれるかは、RAID のレベルによって決まります。RAID のレベルが異なれば、アクセスの容易さ、冗長性、容量のレベルが異なります。ストレージレイ上の各ディスクグループと仮想ディスクについて、特定の RAID レベルを設定できます。

RAID の使用およびストレージステーション内でのデータ管理の詳細については、dell.com/support/manuals で『Owner's Manual』（オーナーズマニュアル）を参照してください。

ハードウェアの取り付け

本ガイドを使用する前に、次の手順を確認するようにしてください。

- 『Getting Started Guide』（はじめに） — トレージアレイに付属の『Getting Started Guide』には、システムの初期セットアップを設定するための情報が記載されています。
- 『Owner's Manual』（オーナーズマニュアル）の計画の項 — 計画の項では、ストレージソリューションのセットアップ前に知っておく必要のある重要なコンセプトについて説明されています。
dell.com/support/manuals で『Owner's Manual』（オーナーズマニュアル）を参照してください。

ストレージ構成の計画

ストレージアレイを設置する前に、次の点を検討してください。

- データストレージのニーズと管理上の必要条件を評価します。
- 可用性の要求を計算します。
- 完全バックアップを毎週、差分バックアップを毎日行うなど、バックアップの頻度とレベルを決めます。
- パスワード保護、およびエラーが発生した場合の電子メールアラート通知など、ストレージアレイのオプションを検討します。
- データ構成計画に従って、仮想ディスクとディスクグループの構成を設計します。たとえば、1つの仮想ディスクを在庫管理に、2つ目を財務・税務情報に、3つ目を顧客情報に使います。
- 障害の発生した物理ディスクと自動的に置き換わるホットスペアのためのスペースを設けるかどうかを決めます。

ストレージレイの接続

ストレージレイは、2 台のホットスワップ対応 RAID コントローラモジュールでホストに接続されます。RAID コントローラモジュールは、RAID コントローラモジュール 1 と RAID コントローラモジュール 2 として識別されます。

詳細に関しては『Getting Started Guide』（はじめに）を参照してください。

各 RAID コントローラモジュールには 4 個の SAS 入力ポートコネクタがあり、このコネクタでホストまたはノードに SAS 接続します。各 RAID コントローラモジュールには、イーサネット管理ポートと SAS 出力ポートコネクタも装備されています。イーサネット管理ポートには、専用の管理ステーション（サーバーまたはスタンドアロンシステム）を取り付けることができます。SAS 出力ポートでストレージレイをオプションの拡張エンクロージャに接続して、ストレージ容量を拡張することができます。詳細に関しては『Getting Started Guide』（はじめに）を参照してください。

各 Dell PowerVault MD3200 シリーズストレージレイは、最大 7 台の PowerVault MD1200 シリーズ拡張エンクロージャを使用することにより、最大 120 台（プレミアム機能の有効化により可能な場合は 192 台）の物理ディスクを使用するよう拡張できます。



メモ: ホストサーバーを SAS 入力ポートコネクタに接続する時は、サーバーのホストバスアダプタ（HBA）の出力ポートのすべてが使用が可能です。

ストレージレイのケーブル接続

ストレージレイとホストサーバーは、次のようにケーブル接続できます。

- シングルパスデータ構成 — シングルパス構成では、最大 8 つのホストを接続することができます。これは非冗長構成です。
- デュアルパスデータ構成 — デュアルパス構成では、最大 4 つのホストを接続することができます。

データ構成は、次の事柄を基本に選択してください。

- 必要なホスト数
- 必要なデータ冗長性レベル

冗長および非冗長構成

非冗長構成は、単一のホストからストレージレイまでのパスをのみを提供する構成です。この種類の構成は、重要でないデータストレージにのみ推奨されます。障害が発生したか取り外されたケーブル、障害が発生した HBA、または障害が発生したか取り外された RAID コントローラモジュールによるパスの障害は、ホストがストレージレイのストレージにアクセスできなくなる原因になります。

冗長性は、個別のデータパスをホストとストレージアレイ間にインストールすることによって確立され、このとき各パスはストレージアレイに設置されている 2 台の RAID コントローラモジュールのうちいずれか 1 つに設定されます。両方の RAID コントローラモジュールがストレージアレイ内のすべてのディスクにアクセスできることから、冗長性により、パスに障害が発生した場合でも、ホストがデータにアクセスできないという事態が回避できます。

シングルコントローラ構成

図 2-1 から図 2-3 は、それぞれ単一の RAID コントローラモジュールのみに接続された 2 台および 4 台のホストを示しています。ホストはストレージ領域を共有できますが、冗長パスがないため、1 つのパスに障害が発生するとそのパスに接続されているサーバーはストレージアレイから切断されます。

図 2-1. 単一のコントローラに接続された 2 台のホスト

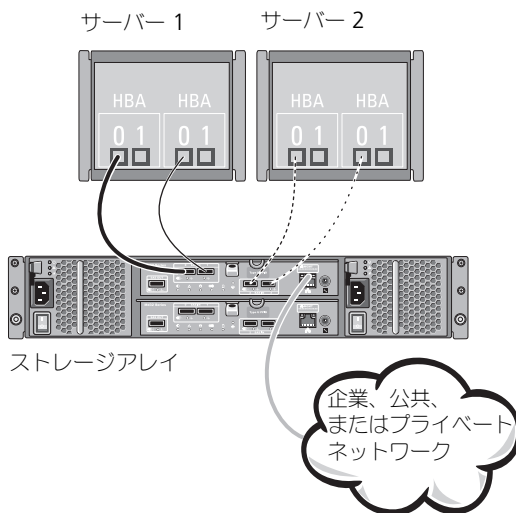


図 2-2. 単一のコントローラに接続された 2 台のホスト

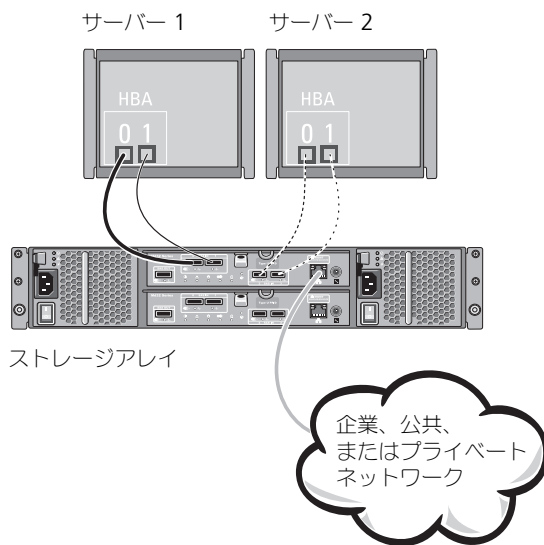
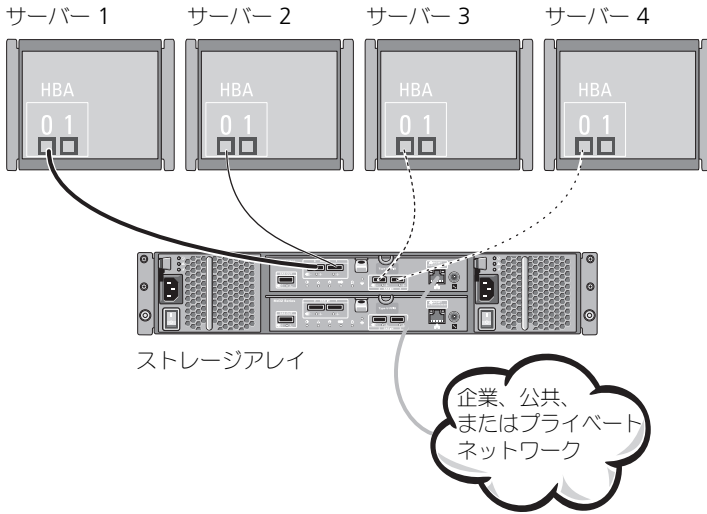


図 2-3. 1つのコントローラに4台のホストを接続



デュアルコントローラ構成

図 2-4 から 図 2-6 は、それぞれ 2 つの RAID コントローラモジュールに接続された 2 台および 4 台のホストを示しています。各ホストには冗長パスがあるため、1 つのパスに障害が発生しても別のパス経由でストレージアレイにアクセスすることができます。

図 2-4. 2 つのコントローラに接続された 2 台のホスト

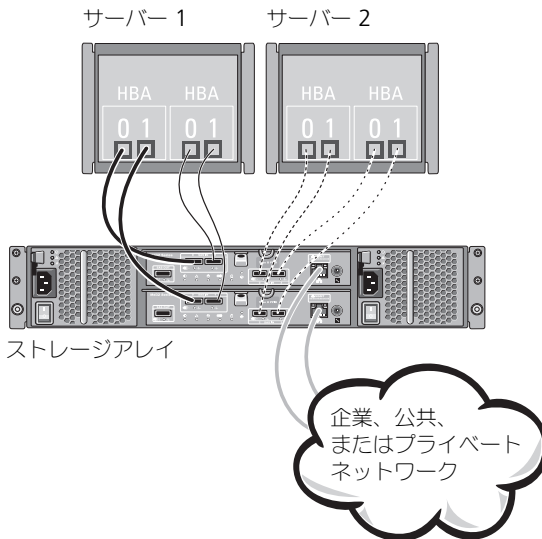


図 2-5. 2つのコントローラに接続された4台のホスト

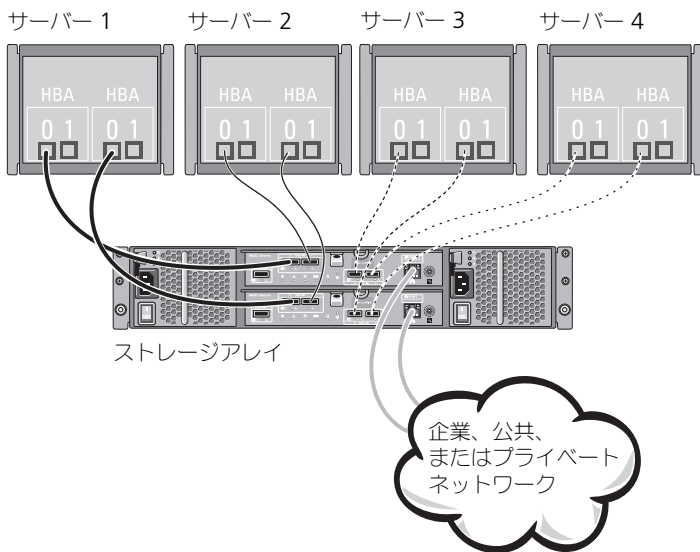


図 2-6. 2つのコントローラに接続された4台のホスト

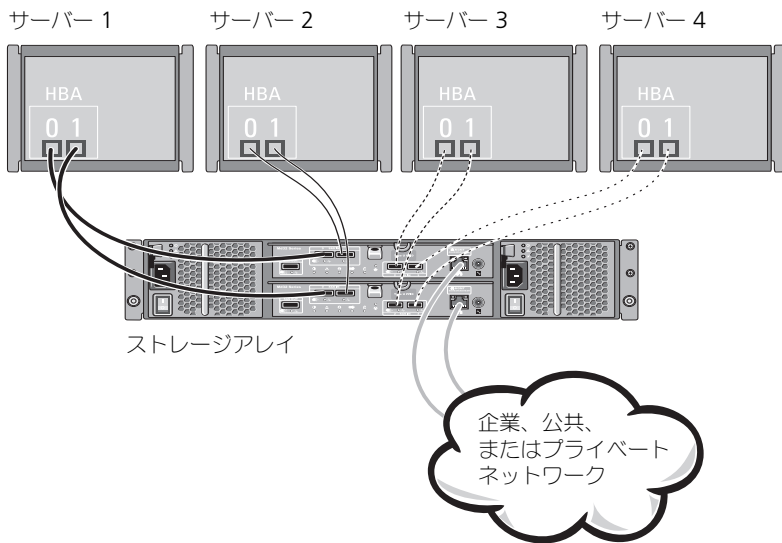


図 2-7 は、それぞれ単一の RAID コントローラモジュールのみに接続された 8 台のホストを示しています。この構成では、接続できる最大数のホストを接続できますが、冗長性はありません。

図 2-7. 2つのコントローラに接続された 8 台のホスト

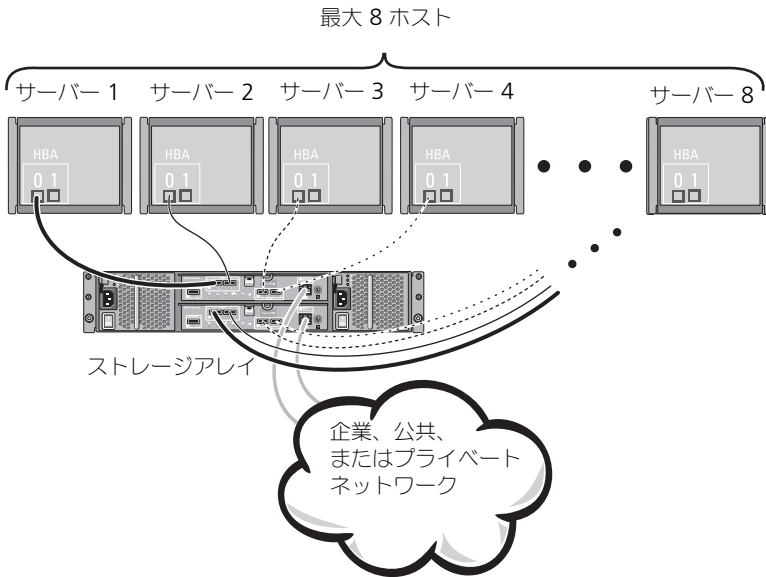


図 2-8 および 図 2-9 は、2 つの RAID コントローラモジュールに接続された、最大 4 つのクラスタノードを示しています。各クラスタノードには冗長パスがあるため、1 つのパスに障害が発生しても別のパス経由でストレージアレイにアクセスすることができます。

図 2-8. 2 台のコントローラに接続された 4 つのクラスタノード

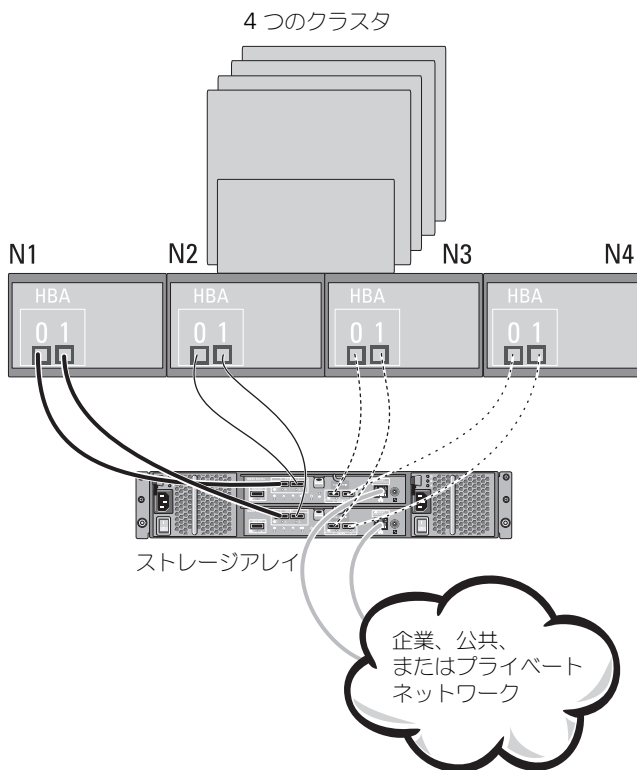
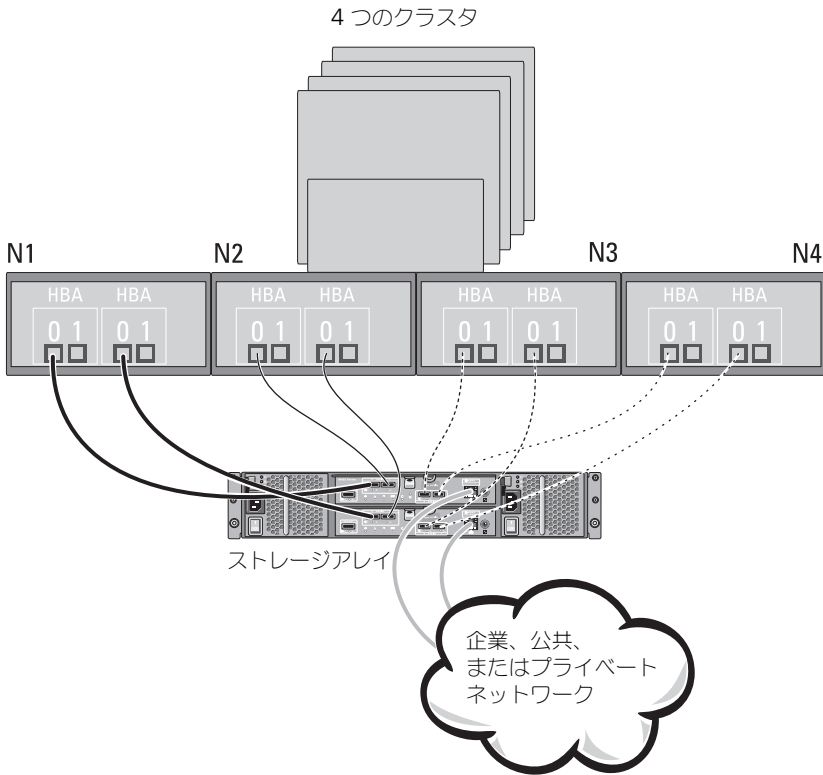


図 2-9. 2 台のコントローラに接続された 4 つのクラスタノード




PowerVault MD1200 シリーズ 拡張エンクロージャのケーブル接続

PowerVault MD1200 シリーズ 拡張エンクロージャを追加して、PowerVault MD3200 シリーズストレージアレイの容量を拡張することができます。物理ディスクプールは、最大 7 台の拡張エンクロージャを使用することにより、最大 120 台（プレミアム機能の有効化により可能な場合は 192 台）の物理ディスクを使用するよう拡張できます。

以前に構成された PowerVault MD1200 シリーズ拡張エンクロージャで拡張する

拡張エンクロージャが Dell PowerEdge RAID Controller (PERC) H800 アダプタに直接接続され、構成されている場合は、この手順を使います。PERC H800 アダプタ上で作成された仮想ディスクからのデータは、PowerVault MD3200 シリーズストレージアレイ、または PowerVault MD3200 シリーズストレージアレイに接続された PowerVault MD1200 シリーズ拡張エンクロージャに直接移行することはできません。

 **注意：**以前 PERC H800 アダプタに接続されていた PowerVault MD1200 シリーズエンクロージャを PowerVault MD3200 シリーズストレージアレイの拡張エンクロージャとして使用した場合、この拡張エンクロージャの物理ディスクは再初期化され、データが失われます。拡張を行う前に、拡張エンクロージャのすべてのデータをバックアップしておく必要があります。

以前に構成済みの PowerVault MD1200 シリーズ拡張エンクロージャを PowerVault MD3200 シリーズストレージアレイに接続するには、次の手順を実行します。

- 1 エンクロージャ上のすべてのデータのバックアップを取ります。
- 2 エンクロージャを PERC H800 コントローラに接続したままの状態、拡張エンクロージャのファームウェアを dell.com/support で入手できる最新バージョンにアップデートします。

Windows システムのユーザーは **DUP.exe** パッケージを参照してください。Linux カーネルについては **DUP.bin** パッケージを参照してください。

- 3 拡張エンクロージャを追加する前に、ストレージレイソフトウェアがインストールされ、最新の状態であることを確認します。

詳細については、dell.com/support/manuals で『Support Matrix』（サポートマトリクス）を参照してください。

- a PowerVault MD シリーズのリソースメディアにあるソフトウェアとドライバのパッケージをインストールします。

ソフトウェアのインストールの詳細については、25 ページの「PowerVault MD ストレージソフトウェアのインストール」を参照してください。

- b PowerVault MDSM を使用して、ストレージレイ RAID コントローラモジュールのファームウェアと NVSRAM を dell.com/support で入手できる最新バージョンにアップデートします。
 - c エンタープライズ管理ウィンドウ (EMW) で、ツール → RAID コントローラモジュールファームウェアのアップグレードとクリックします。
- 4 すべての I/O 処理を停止し、システムおよび接続されている装置の電源を切ります。
- a アレイに対するすべての I/O 処理を停止し、ストレージレイに接続されているホストシステムの電源を切ります。
 - b ストレージシステムの電源を切ります。
 - c 影響を受けるシステム内にある拡張エンクロージャの電源を切ります。
- 5 拡張エンクロージャをストレージレイにケーブルで接続します。
- 6 次の手順で、接続されている装置の電源を入れます。
- a 拡張エンクロージャの電源を入れます。エンクロージャのステータス LED が青色に点灯するまで待ちます。
 - b ストレージレイの電源を入れ、ステータス LED が装置の準備ができたことを示すまで待ちます。
 - ステータス LED が橙色に点灯している場合、ストレージレイはまだオンライン状態になっていません。
 - ステータス LED が橙色に点滅している場合は、エラーが発生しています。エラーは PowerVault MDSM を使用して確認できます。
 - ステータス LED が青色に点灯している場合、ストレージレイは準備ができた状態です。
 - c ストレージレイがオンラインで準備ができた状態になったら、接続されているすべてのホストシステムの電源を入れます。
- 7 PowerVault MD1200 シリーズ拡張エンクロージャがストレージレイの拡張エンクロージャであることが確認されたら、手順 1 でバックアップを行ったデータを復元します。

PowerVault MD1200 シリーズ拡張エンクロージャがオンラインになると、ストレージレイの一部としてアクセスが可能になります。

新しい PowerVault MD1200 シリーズ拡張エンクロージャで拡張する

新しい PowerVault MD1200 シリーズ拡張エンクロージャを PowerVault MD3200 シリーズストレージレイに接続するには、次の手順を実行します。

- 1 拡張エンクロージャを追加する前に、ストレージレイソフトウェアがインストールされ、最新バージョンであることを確認します。詳細については、**dell.com/support/manuals** で『Support Matrix』（サポートマトリクス）を参照してください。
 - a PowerVault MD シリーズのリソースメディアにあるソフトウェアとドライバのパッケージをインストールします。
ソフトウェアのインストールの詳細については、25 ページの「PowerVault MD ストレージソフトウェアのインストール」を参照してください。
 - b PowerVault MD1200 シリーズ拡張エンクロージャを設定します。
PowerVault MD1200 シリーズ拡張エンクロージャの設定の詳細については、**dell.com/support/manuals** で『Owner's Manual』（オーナーズマニュアル）を参照してください。
 - c PowerVault MDSM を使用して、RAID コントローラモジュールのファームウェアと NVSRAM を **dell.com/support** で入手できる最新バージョンにアップデートします。
 - d エンタープライズ管理ウィンドウ（EMW）で、**ツール** → **RAID** コントローラモジュールファームウェアのアップグレードとクリックします。
- 2 I/O 処理を停止し、システムおよび接続されている装置の電源を切ります。
 - a ストレージレイに対するすべての I/O 処理を停止し、ストレージレイに接続されている対象となるホストシステムの電源を切ります。
 - b ストレージシステムの電源を切ります。
 - c 影響を受けるシステム内にある拡張エンクロージャの電源を切ります。
- 3 拡張エンクロージャをストレージレイにケーブルで接続します。
- 4 次の手順で、接続されている装置の電源を入れます。
 - a 拡張エンクロージャの電源を入れます。エンクロージャのステータス LED が青色に点灯するまで待ちます。
 - b ストレージレイの電源を入れ、ステータス LED が装置の準備ができたことを示すまで待ちます。
 - ステータス LED が橙色に点灯している場合、ストレージレイはまだオンライン状態になっていません。
 - ステータス LED が橙色に点滅している場合は、エラーが発生しています。エラーは PowerVault MDSM を使用して確認できます。

- ステータス LED が青色に点灯している場合、ストレージアレイは準備ができた状態です。
 - c ストレージアレイがオンラインで準備ができた状態になったら、接続されているすべてのホストシステムの電源を入れます。
- 5 MDSM を使用し、必要に応じて接続されているすべての拡張エンクロージャファームウェアをアップデートします。
- a エンタープライズ管理ウィンドウで、アップデートしたいエンクロージャを選択して、**アレイ管理ウィンドウ (AMW)** を起動します。
 - b **詳細設定** → **メンテナンス** → **ダウンロード** → **EMM ファームウェア** とクリックします。
 - c **すべて選択** を選択し、接続された拡張エンクロージャすべてを同時にアップデートします。

PowerVault MD ストレージソフトウェアのインストール

Dell PowerVault MD シリーズのリソースメディアには、Linux および Microsoft Windows 両方のオペレーティングシステムのソフトウェアとドライバが含まれています。

メディアのルートには、Linux と Windows の両方に適用されるソフトウェアの変更、アップデート、修正プログラム、バッチ、およびその他の重要なデータが収録されている **readme.txt** ファイルが入っています。**readme.txt** ファイルにはまた、マニュアルを参照するための必要条件が指定されているほか、メディアに収録されているソフトウェアのバージョンに関する情報、ソフトウェアの実行に必要なシステム要件が記載されています。

PowerVault システム用にサポートされているハードウェアとソフトウェアの詳細については、**dell.com/support/manuals** にある『Support Matrix』（サポートマトリクス）を参照してください。



メモ : **dell.com/support** で入手できる最新のアップデートをすべてインストールすることをお勧めします。

PowerVault MD シリーズのリソースメディアストレージソフトウェアインストールには、コアソフトウェア、プロバイダなどの機能が用意されています。コアソフトウェアの機能には、ホストベースのストレージエージェント、マルチパスドライバに加えて、ストレージレイショリユーションの設定、管理、監視に使用する PowerVault MD Storage Manager アプリケーションが含まれます。プロバイダ機能には、Microsoft Virtual Disk Service (VDS) および Microsoft Volume Shadow-Copy Service (VSS) フレームワークのプロバイダが含まれます。



メモ : Microsoft VDS および Microsoft VSS プロバイダの詳細については、**dell.com/support/manuals** で『Owner's Manual』（オーナーズマニュアル）を参照してください。



メモ : Windows または Linux システムにソフトウェアをインストールするには、Administrator または root 権限が必要です。

PowerVault MD シリーズのリソースメディアでは、次の 3 つのインストールオプションが提供されています。

- グラフィカルインストール（推奨） — ほとんどのユーザーに推奨されるオプションです。インストールには、インストールするコンポーネントを選択できるグラフィカルウィザード方式のインターフェースが表示されます。

- コンソールインストール — サポートされている Linux プラットフォームへの X-Window 環境のインストールを希望しない Linux ユーザーには、このオプションをお勧めします。
- サイレントインストール — スクリプトインストールの作成を希望するユーザーには、このオプションをお勧めします。

グラフィカルインストール (推奨)

PowerVault MD Storage Manager アプリケーションは、ストレージレイを設定、管理、および監視します。PowerVault ストレージソフトウェアをインストールするには、次の手順を実行します。

1 PowerVault MD シリーズリソースメディアを挿入します。

お使いのオペレーティングシステムによっては、インストーラが自動的に起動する場合があります。インストーラが自動的に起動しない場合は、インストールメディア（またはダウンロードしたインストーライメージ）のルートディレクトリに移動し、**md_launcher.exe** ファイルを実行してください。Linux ベースのシステムでは、リソースメディアのルートに移動し、**autorun** ファイルを実行します。



メモ：デフォルトで、Red Hat Enterprise Linux はリソースメディアを **-noexec mount** オプションでマウントします。このオプションでは起動可能ファイルを実行できません。この設定を変更するには、インストールメディアのルートディレクトリにある **readme** ファイルを参照してください。

2 MD ストレージソフトウェアのインストール を選択します。

3 ライセンス契約を読み、それに合意します。

4 インストール設定 ドロップダウンメニューから、次のインストールオプションのいずれかを選択します。

- 完全 (推奨) — PowerVault MD Storage Manager (クライアント) ソフトウェア、ホストベースのストレージエージェント、マルチバッドライバ、およびハードウェアプロバイダをインストールします。
- ホストのみ — ホストベースのストレージエージェントおよびマルチバッドライバをインストールします。
- 管理 — 管理ソフトウェアおよびハードウェアプロバイダをインストールします。
- カスタム — 特定のコンポーネントを選択することができます。

5 このホストサーバー用のデータストレージとして機能するようにセットアップしている PowerVault MD ストレージレイのモデルを選択します。

6 イベント監視サービスを、ホストサーバーの再起動時に自動で開始するか、手動で開始するかを選択します。



メモ：このオプションは、Windows クライアントソフトウェアのインストールに限り適用可能です。

- 7 インストール先を確認して、**インストール** をクリックします。
- 8 インストールの完了後、プロンプトが表示されたらホストサーバーを再起動します。
- 9 **MD Storage Manager** を起動してアレイを検出します。
- 10 該当する場合、お使いのストレージアレイと併せてご購入いただいたプレミアム機能をアクティブ化します。

プレミアム機能をご購入いただいた場合は、お使いのストレージアレイに同梱の印刷アクティベーションカードを参照してください。



メモ：**MD Storage Manager** のインストーラは、ストレージアレイの動作に必要なドライバ、ファームウェア、およびオペレーティングシステムのパッチ/ホットフィックスを自動でインストールします。これらのドライバおよびファームウェアは、dell.com/support から入手可能です。お使いの特定のストレージアレイに必要な追加設定および/またはソフトウェアについては、dell.com/support/manuals で『Support Matrix』（ポートマトリックス）を参照してください。

コンソールインストール



メモ：コンソールインストールは、グラフィカル環境を実行していない Linux システムにのみ適用されます。

リソースメディアのルートにある **autorun** スクリプトは、グラフィカル環境が実行されていない場合にこれを検知し、インストーラをテキストベースモードで自動的に開始します。このモードでは、グラフィカルインストールと同じオプションが選択できます。

サイレントインストール

Windows システムでサイレントインストールを実行するには、次の手順に従います。

- 1 インストールメディアまたはイメージの **/windows** フォルダにある **custom_silent.properties** ファイルを、ホストサーバー上の書き込み可能な場所にコピーします。
- 2 **custom_silent.properties** ファイルを修正して、使用する機能、モデル、およびインストールのオプションを反映します。次に、ファイルを保存します。
- 3 **custom_silent.properties** ファイルがお使いの特定のインストールを反映するよう修正されたら、次のコマンドを実行してサイレントインストールを開始します。

```
mdss_install.exe -f <host_server_path>\  
custom_silent.properties
```

Linux システムでサイレントインストールを実行するには、次の手順に従います。



メモ：Red Hat Enterprise Linux 6 オペレーティングシステムで、次のスクリプトをルートディレクトリから実行し、必須パッケージをインストールします。

```
# md_prereq_install.sh
```

- 1 インストールメディアまたはイメージの **/windows** フォルダにある **custom_silent.properties** ファイルを、ホストサーバー上の書き込み可能な場所にコピーします。
- 2 **custom_silent.properties** ファイルを修正して、使用する機能、モデル、およびインストールのオプションを反映します。
- 3 ファイルを保存します。
- 4 **custom_silent.properties** ファイルを修正したら、次のコマンドを実行してインストールを開始します。

```
./mdss_install.bin -f
```

```
<host_server_path>/custom_silent.properties
```

PowerVault MD ストレージソフトウェアのアップグレード

以前のバージョンの PowerVault MD Storage Manager アプリケーションからアップグレードするには、以前のバージョンをアンインストール（41 ページの「Windows からの MD Storage ソフトウェアのアンインストール」を参照）してから、25 ページの「PowerVault MD ストレージソフトウェアのインストール」の手順に従って新バージョンをインストールしてください。

インストール後のタスク

ストレージレイを初めて使用する場合は、使用前に次に示す順序で初期設定タスクを完了してください。これらのタスクは、**MD Storage Manager** を使用して実行します。



メモ：DHCP（ダイナミックホスト設定プロトコル）が使用されていない場合、管理ステーションの初期設定はストレージレイと同じ物理サブネットで行う必要があります。また、初期設定中に、少なくとも1つのネットワークアダプタをストレージレイのデフォルト管理ポート（192.168.128.101 または 192.168.128.102）と同じ IP サブネットで設定する必要があります。初期設定の終了後、管理ポートが MD Storage Manager を使用して設定され、管理ステーションの IP アドレスを元の設定に戻すことができます。

作業を開始する前に



メモ：iSCSI の設定を開始する前に、本書内の IPv4 または IPv6 iSCSI 設定ワークシートへの記入をお勧めします。31 ページの「IPv4 設定 — ワークシート」および 32 ページの「IPv6 設定 — ワークシート」を参照してください。設定の手順を開始する前にネットワークに関するこの種の情報を収集しておくこと、作業をより効率的に完了するために役立ちます。

iSCSI の設定用語

表 4-1. iSCSI の設定で使用される標準的な用語

条件	定義
CHAP（チャレンジハンドシェイク認証プロトコル）	ホストサーバーとストレージレイの両方の iSCSI データポートの使用を制限する方法で iSCSI ストレージシステムへのアクセスを制御するために使用されるオプションのセキュリティプロトコル。サポートされている CHAP 認証の種類の詳細については、55 ページの「CHAP 認証について」を参照してください。
ホストまたはホストサーバー	iSCSI ポートを經由してストレージレイに接続されているサーバー。
ホストサーバーポート	ストレージレイへの接続に使用されるホストサーバーの SCSI ポート。
iSCSI イニシエータ	ホストサーバーとストレージレイの通信を制御する iSCSI 固有のソフトウェア。ホストサーバーにインストールされます。

表 4-1. iSCSI の設定で使用される標準的な用語

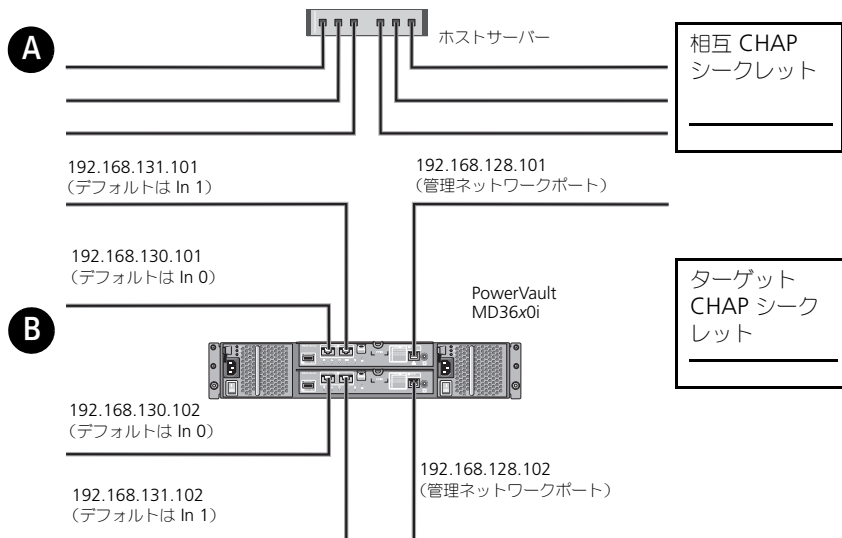
条件	定義
iSCSI ホストポート	ストレージアレイ上の iSCSI ポート (各コントローラに 2 個)。
iSNS (Microsoft Internet Storage Naming Service) 管理ステーション	一部の iSCSI デバイスで使用される自動検出、管理、設定 (記憶域名前サーバー) ツール。 ホストサーバー / ストレージアレイの構成を管理するシステム。
ストレージアレイ	ホストサーバーによってアクセスされるストレージデータが格納されているエンクロージャ。
ターゲット	ホストサーバーにインストールされている iSCSI イニシエータからの要求を受け入れ、それに応答するストレージアレイ上の iSCSI ポート。

iSCSI 設定ワークシート

31 ページの「IPv4 設定 — ワークシート」および 32 ページの「IPv6 設定 — ワークシート」は、設定の計画に役立ちます。ホストサーバーとストレージアレイの IP アドレスを 1 つの場所に記録しておく、セットアップをより短時間で能率的に行うことができます。

37 ページの「iSCSI 用のネットワーク設定のガイドライン」には、Microsoft Windows と Linux の両方の環境に対応するネットワーク設定の一般的なガイドラインが説明されています。ワークシートに記入する前にこれらのガイドラインを参照されることをお勧めします。

IPv4 設定 — ワークシート

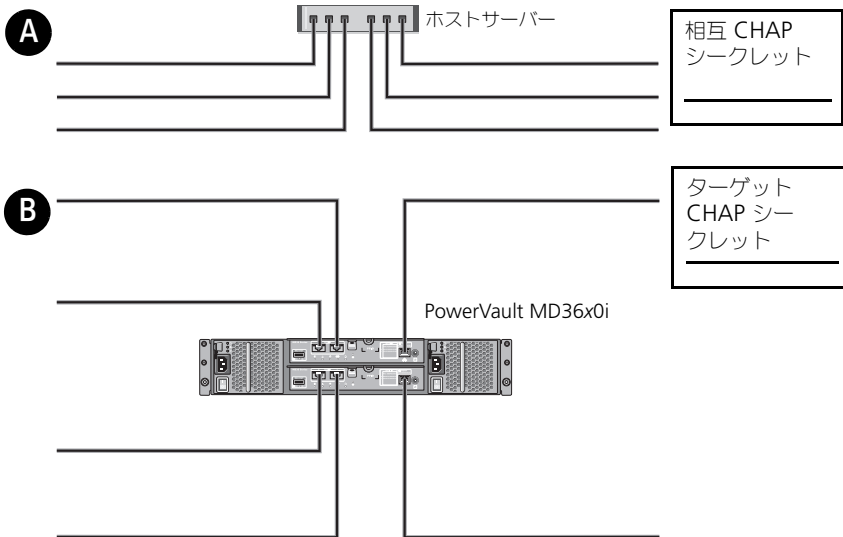


複数のホストサーバーを使用するためにスペースが足りない場合は、複数のシートを使用してください。

A 静的 IP アドレス (ホストサーバー)	サブネット	デフォルトゲートウェイ
iSCSI ポート 1	(NICごとに異なっている必要があります)	
iSCSI ポート 2		
管理ポート		
管理ポート		

B 静的 IP アドレス (ホストサーバー)	サブネット	デフォルトゲートウェイ
iSCSI コントローラ 0, In 0		
iSCSI コントローラ 0, In 1		
管理ポート cntrl 0		
iSCSI コントローラ 1, In 0		
iSCSI コントローラ 1, In 1		
管理ポート cntrl 1		

IPv6 設定 — ワークシート



複数のホストサーバーを使用するためにスペースが足りない場合は、複数のシートを使用してください。

A	ホスト iSCSI ポート 1	ホスト iSCSI ポート 2
	リンクローカル IP アドレス	リンクローカル IP アドレス
	ルーティング可能な IP アドレス	ルーティング可能な IP アドレス
	サブネットプレフィックス	サブネットプレフィックス
	ゲートウェイ	ゲートウェイ

B	iSCSI コントローラ 0、In 0
	IP アドレス FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____
	ルーティング可能な IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
	ルーティング可能な IP アドレス 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
	ルーター IP アドレス ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
	iSCSI コントローラ 0、In 1
	IP アドレス FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____
	ルーティング可能な IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
	ルーティング可能な IP アドレス 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
	ルーター IP アドレス ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI コントローラ 1、In 0

IP アドレス FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____

ルーティング可能な IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

ルーティング可能な IP アドレス 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

ルーター IP アドレス ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI コントローラ 1、In 1

IP アドレス FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____

ルーティング可能な IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

ルーティング可能な IP アドレス 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

ルーター IP アドレス ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

ストレージアレイの iSCSI の設定

次の項では、ストレージアレイの iSCSI を設定する詳しい手順が説明されています。ただし、作業を開始する前に、お使いのホストサーバー / ストレージアレイ環境と関連して、各手順がどこで行われるのかを理解しておくことが重要です。

次の表は、iSCSI 設定の各手順と、それらが行われる場所を示しています。

表 4-2. ホストサーバーとストレージアレイ

Microsoft または Linux の iSCSI イニシエータを使用してホストサーバーで行う手順	PowerVault MD Storage Manager を使用してストレージアレイで行う手順
	1 ストレージアレイを検知する
	2 ストレージアレイの iSCSI ポートを設定する
3 iSCSI イニシエータからターゲットの検知を行う	
	4 ホストアクセスの設定
	5 (オプション) ストレージアレイの CHAP 認証を設定する
6 (オプション) ホストサーバーの CHAP 認証を設定する	
7 ホストサーバーからストレージアレイに接続する	
	8 (オプション) 帯域内管理をセットアップする



メモ : iSCSI の設定には、PowerVault MD 設定ユーティリティ (MDCU) を使用することをお勧めします。PowerVault MDCU ウィザードに、上記の設定手順が示されます。手動設定を行いたい場合は、47 ページの「付録 — iSCSI の手動設定」を参照してください。

モジュラー型ディスク設定ユーティリティ (MDCU) を使用した自動設定



メモ : MDCU がインストールされていない場合は、MD シリーズのリソースメディアからインストールすることができます。

MDCU はウィザード駆動型のインタフェースを活用し、ホストサーバーおよび iSCSI ベースのストレージアレイによる iSCSI ネットワークの設定に総合的なアプローチを提供します。このユーティリティではこのほか、ベストプラクティスに基づいてホストサーバーの iSCSI セッションを設定し、ストレージアレイ iSCSI ホストポートとの間で経路の負荷分散を達成することができます。ホストソフトウェアのインストール中に **再起動後に MDCU を起動** を選択すると、次にホストサーバーを再起動した後にユーティリティは自動で起動します。このユーティリティは手動で起動することも可能です。

このユーティリティはコンテキスト対応のオンラインヘルプで、ウィザードの各手順を示します。

MDCU は、次を実行します。

- ストレージアレイの設定
- ホストの設定

ストレージレイの設定

ホスト iSCSI イニシエータと iSCSI ベースのストレージレイが通信を確立する前に、それぞれに、使用する IP アドレスや認証方法に関する情報を設定する必要があります。iSCSI イニシエータは、すでに設定済みのストレージレイと通信を確立するため、まず、ストレージレイの iSCSI イニシエータでの利用を可能にする手順を行います。

このユーティリティには、設定したいストレージレイの管理ポートへのネットワークアクセスが必要です。ストレージレイの設定を試みる前に、ネットワークインフラを正しく機能させておく必要があります。ストレージレイを既に設定している場合は、このままホスト設定手順に進みます。

この設定手順は基本的に次の手順で行います。

- 1 設定のための利用可能なストレージレイを検出する。
- 2 設定するストレージレイを選択する。
- 3 ストレージレイ名とパスワードを設定する。
- 4 管理ポートに IP プロトコルおよびアドレスを設定する。
- 5 iSCSI ポートに IP プロトコルおよびアドレスを設定する。
- 6 CHAP 認証方法を指定する。
- 7 サマリを確認した後、設定内容を適用する。
- 8 複数のアレイを設定するには、手順 2 から手順を繰り返してください。

ホスト設定（ホスト接続設定）

iSCSI ベースのストレージレイの設定が済んだら、続いて、ストレージレイへのアクセスが必要なすべてのホストでこのユーティリティを実行します。ネットワーク構成によって、ホストがストレージレイの管理に使用するホストと同じになる場合と、まったく別のネットワーク上のホストになる場合があります。

ユーティリティを実行しているマシンに iSCSI イニシエータがない場合、または必要なドライバコンポーネントがインストールされていない場合、ホスト設定オプションは無効になります。オプションが無効化されると、ユーティリティも情報メッセージを表示します。iSCSI ベースのストレージレイに接続されていない（または、アレイへの接続を希望しない）ホストでユーティリティを実行している場合、この情報は無視してかまいません。

この手順には基本的に次の手順が含まれます。

- 1 接続のための利用可能なストレージレイを検出する。
- 2 ストレージレイを選択する。
- 3 CHAP シークレットを指定する。
- 4 ホストのイニシエータがログインに使用する iSCSI ポートを選択する。
- 5 複数のアレイを接続するには、手順 2 から手順を繰り返してください。
- 6 ストレージレイへのアクセスを必要とする各ホストで、これらの手順を繰り返す。

設定プロセスを開始する前に

ストレージレイの設定またはホストの接続設定を開始する前に、設定計画に役立つ iSCSI 設定ワークシートへの記入をお勧めします。設定内容によって、複数のワークシートの使用が必要になる場合があります。

ストレージレイおよびホストの設定に関して、次のガイドラインにご留意ください。

- 最適なパフォーマンスを得るため、ネットワーク設定を確認してください。
dell.com/support/manuals でストレージレイの『Support Matrix』(サポートマトリクス)を参照してください。
- ホストに複数のネットワークインターフェースがある場合、各ネットワークインターフェースで個別のサブネットを使用することを推奨します。
- デュアルコントローラ(二重)構成における冗長性の確保のため、各ホストネットワークインターフェースが両方のストレージレイコントローラに接続されるように設定されていることを確認します。
- 最適な負荷分散のため、iSCSI トラフィックに使用される各ホストネットワークインターフェースが、各ストレージレイコントローラに接続するように設定されていることを確認します。
- 各ホストネットワークインターフェースが、ストレージレイコントローラごとに iSCSI セッションを 1 つのみ確立することを推奨します。



メモ: ユーティリティは、利用可能なホストネットワークインターフェースおよびストレージレイの iSCSI ホストポートとの接続に基づいて、可能な限りホスト接続のガイドラインに従おうとします。

MDCU を使用してストレージレイを設定する

MDCU を使用して iSCSI ベースのストレージレイを設定するには、次の手順を実行します。

- 1 設定するストレージレイの管理ポートにアクセスしているサーバーから、ユーティリティを起動します(自動的に起動されない場合)。

Windows の場合は、**スタート → すべてのプログラム → Dell → MD Storage ソフトウェア → Modular Disk 設定ユーティリティ** の順にクリックします。

Linux では、デスクトップで MDCU アイコンをクリックするか、ターミナルウィンドウで **/opt/dell/mdstoragesoftware/mdconfigurationutility** ディレクトリに移動し、**PowerVault MDCU** を実行します。

MDCU が利用可能なストレージレイのすべてを自動的に検出します。

- 2 MD アレイの検出ウィンドウで、設定する iSCSI ストレージレイを選択します。

- 3 選択したアレイウィンドウで、現在のポートおよびセッション情報を確認します。
- 4 設定ウィザードをクリックし、iSCSI 設定ウィザードを起動します。
- 5 設定ウィザードの手順を完了して、お使いの iSCSI ストレージアレイを設定します。
- 6 アレイ設定サマリウィンドウで、設定を確認して適用します。
- 7 iSCSI セッションの作成をクリックし、ホスト対ストレージアレイの通信を作成します。
実装するホスト対アレイマッピングのすべてに対してこれを繰り返します。
- 8 ストレージアレイとホストサーバー間で通信が確立されていることを確認します。



メモ: MDCU の詳細については、MDCU オンラインヘルプを参照してください。

接続確立後の手順

ホストサーバーとストレージアレイ間で iSCSI 接続が確立された後、MD Storage Manager を使用してストレージアレイ上で仮想ディスクを作成することができ、ホストサーバーがこれらの仮想ディスクを利用することが可能になります。ストレージ計画、および MD Storage Manager の使用についての詳細は、dell.com/support/manuals で『Administrator's Guide』（管理者ガイド）を参照してください。

iSCSI 用のネットワーク設定のガイドライン

本項では、お使いのホストサーバーおよびストレージアレイの iSCSI ポート用にネットワーク環境と IP アドレスを設定するための一般的なガイドラインを示します。ホストがストレージアレイの管理ポートおよび / または iSCSI ポートと通信を行うためには、IPv4/IPv6 ワークシートにリストされているアドレスとの通信が可能な IP アドレスでローカルの NIC を設定する必要があります。お使いのネットワーク環境では、ここに示すものとは異なる（または追加の）手順が必要になる場合があります。このセットアップを行う前に必ずシステム管理者とご相談ください。

Microsoft Windows ホストのセットアップ

Windows ホストのネットワークをセットアップするには、ストレージアレイに接続する各 iSCSI ポートの IP アドレスとネットマスクを設定する必要があります。具体的な手順は、DHCP サーバー、静的 IP アドレス指定、DNS サーバー、または Windows インターネットネームサービス (WINS) サーバーのいずれかを使用するかによって異なります。



メモ: サーバーの IP アドレスは、ストレージアレイの管理ポート、および iSCSI ポートと同じ IP サブネットへのネットワーク通信用に設定する必要があります。

DHCP サーバーを使用する

- 1 **コントロールパネル** で、**ネットワーク接続** または **ネットワークと共有センター** を選択して、**ネットワーク接続の管理** をクリックします。
- 2 設定するネットワーク接続を右クリックし、次に **プロパティ** を選択します。
- 3 **一般** タブ（ローカルエリア接続の場合）または **ネットワーク** タブ（その他すべての接続の場合）で、**インターネットプロトコル (TCP/IP)** を選択し、**プロパティ** をクリックします。
- 4 **IP アドレスを自動的に取得する** を選択し、**OK** をクリックします。

静的 IP アドレス指定を使用する

- 1 **コントロールパネル** で、**ネットワーク接続** または **ネットワークと共有センター** を選択して、**ネットワーク接続の管理** をクリックします。
- 2 設定するネットワーク接続を右クリックし、次に **プロパティ** をクリックします。
- 3 **一般** タブ（ローカルエリア接続の場合）または **ネットワーク** タブ（その他すべての接続の場合）で、**インターネットプロトコル (TCP/IP)** を選択し、**プロパティ** をクリックします。
- 4 次の **IP アドレスを使用する** を選択し、IP アドレス、サブネットマスクアドレス、およびデフォルトゲートウェイアドレスを入力します。

DNS サーバーを使用する

- 1 **コントロールパネル** で、**ネットワーク接続** または **ネットワークと共有センター** を選択して、**ネットワーク接続の管理** をクリックします。
- 2 設定するネットワーク接続を右クリックし、次に **プロパティ** をクリックします。
- 3 **一般** タブ（ローカルエリア接続の場合）または **ネットワーク** タブ（その他すべての接続の場合）で、**インターネットプロトコル (TCP/IP)** を選択し、**プロパティ** をクリックします。
- 4 **DNS サーバーのアドレスを自動的に取得する** を選択するか、または優先および代替 DNS サーバーの IP アドレスを入力し、**OK** をクリックします。

WINS サーバーを使用する



メモ : DHCP サーバーを使用して WINS サーバーの IP アドレスを割り当てる場合は、WINS サーバーのアドレスをユーザーが追加する必要はありません。

- 1 **コントロールパネル** で **ネットワーク接続** を選択します。
- 2 設定するネットワーク接続を右クリックし、次に **プロパティ** をクリックします。

- 3 **一般** タブ（ローカルエリア接続の場合）または **ネットワーク** タブ（その他すべての接続の場合）で、**インターネットプロトコル (TCP/IP)** を選択し、**プロパティ** をクリックします。
- 4 **詳細設定** → **WINS** タブと選択して **追加** をクリックします。
- 5 **TCP/IP WINS サーバー** ウィンドウで、WINS サーバーの IP アドレスを入力し、**追加** をクリックします。
- 6 リモート NetBIOS 名を解決するために Lmhosts ファイルの使用を可能にするには、**LMHOSTS の参照を有効にする** を選択します。
- 7 Lmhosts ファイルにインポートするファイルの場所を指定するには、**LMHOSTS のインポート** を選択し、**開く** ダイアログボックス内のファイルを選択します。
- 8 NetBIOS over TCP/IP を有効または無効にします。

Windows Server 2008 Core バージョンを使用している場合は、netsh インタフェースコマンドを使用してホストサーバーの iSCSI ポートを設定します。

Linux ホストのセットアップ

Linux ホストのネットワークをセットアップするには、ストレージレイに接続する各 iSCSI ポートの IP アドレスとネットマスクを設定する必要があります。具体的な手順は、DHCP を使用して TCP/IP を設定するか、または静的 IP アドレスを使用して TCP/IP を設定するかによって異なります。



メモ: サーバーの IP アドレスは、ストレージレイの管理ポート、および iSCSI ポートと同じ IP サブネットへのネットワーク通信用に設定する必要があります。

DHCP を使用する

DHCP を使用する場合（root ユーザーのみ）

- 1 **/etc/sysconfig/network** ファイルを、次のように編集します。
`NETWORKING=yes HOSTNAME=mymachine.mycompany.com`
- 2 設定したい接続について、設定ファイルを次のように編集します。
/etc/sysconfig/network-scripts/ifcfg-ethX（Red Hat Enterprise Linux の場合）または **/etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX**（SUSE Enterprise Linux の場合）
`BOOTPROTO=dhcp`
また、IP アドレスとネットマスクが定義されていないことを確認します。
- 3 次のコマンドを使用してネットワークサービスを再起動します。
`/etc/init.d/network restart`

静的 IP アドレスを使用する

静的 IP アドレスを使用する場合（root ユーザーのみ）

- 1 **/etc/sysconfig/network** ファイルを次のように編集します。

```
NETWORKING=yes HOSTNAME=mymachine.mycompany.com  
GATEWAY=255.255.255.0
```

- 2 設定したい接続について、設定ファイルを次のように編集します。

/etc/sysconfig/network-scripts/ifcfg-ethX（Red Hat Enterprise Linux の場合）または **/etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX**（SUSE? Enterprise Linux の場合）

```
BOOTPROTO=static BROADCAST=192.168.1.255 IPADDR=  
192.168.1.100 NETMASK=255.255.255.0 NETWORK=192.168.1.0  
ONBOOT=yes TYPE=Ethernet
```

```
HWADDR=XX:XX:XX:XX:XX:XX GATEWAY=192.168.1.1
```

- 3 次のコマンドを使用してネットワークサービスを再起動します。

```
/etc/init.d/network restart
```


PowerVault MD Storage ソフトウェアのアンインストール

Windows からの MD Storage ソフトウェアのアンインストール

プログラムの変更または削除 機能を使って、Microsoft Windows オペレーティングシステム（Windows Server 2008 を除く）から Modular Disk Storage ソフトウェア（MDSS）をアンインストールします。

- 1 コントロールパネル から **プログラムの変更または削除** をダブルクリックします。
- 2 プログラムの一覧から **Dell MD32xxi Storage Software** を選択します。
- 3 **変更と削除** をクリックします。
アンインストール完了 ウィンドウが表示されます。
- 4 画面の指示に従います。
- 5 **はい** を選択してシステムを再起動し、**完了** をクリックします。

Windows Server 2008 GUI バージョンから Modular Disk Storage ソフトウェアをアンインストールするには、次の手順で行います。

- 1 コントロールパネル から **プログラムと機能** をダブルクリックします。
- 2 プログラムの一覧から **MD Storage ソフトウェア** を選択します。
- 3 **アンインストールと変更** をクリックします。
アンインストール完了 ウィンドウが表示されます。
- 4 画面の指示に従います。
- 5 **はい** を選択してシステムを再起動し、**完了** をクリックします。

次の手順に従って、Windows Server 2008 Core バージョンから PowerVault Modular Disk Storage ソフトウェアをアンインストールします。

- 1 **Dell\MD Storage ソフトウェア\Dell Modular Disk 32xxi Storage** ソフトウェアのアンインストール ディレクトリに移動します。



メモ：デフォルトでは、MD Storage Manager は **\Program Files\Dell\MD Storage Manager** ディレクトリにインストールされています。インストール時に別のディレクトリを使用した場合は、アンインストールの手順を開始する前にそのディレクトリに移動してください。

- 2 インストールディレクトリから次のコマンドを入力して <Enter> を押し
ます。
Modular Disk Storage のアンインストール
- 3 アンインストール ウィンドウで **次へ** をクリックし、画面の指示に従います。
- 4 **はい** を選択してシステムを再起動し、**完了** をクリックします。

Linux からの MD Storage ソフトウェアのアンインストール


- 1 デフォルトでは、PowerVault MD Storage Manager は **/opt/dell/mdstoragemanager** ディレクトリにインストールされています。インストール時に別のディレクトリを使用した場合は、アンインストールの手順を開始する前にそのディレクトリに移動してください。
- 2 インストールディレクトリから、**Dell MD Storage ソフトウェアのアンインストール** ディレクトリを開きます。
- 3 **Uninstall Dell MD Storage Software.exe** ファイルを実行します。
- 4 アンインストール ウィンドウで **次へ** をクリックし、画面の指示に従います。ソフトウェアがアンインストールされる間、**アンインストール** ウィンドウが表示されます。アンインストールが完了したら、**アンインストール完了** ウィンドウが表示されます。
- 5 **完了** をクリックします。

困ったときは

システムサービスタグの位置


お使いのシステムは固有のエキスプレスサービスコードとサービスタグ番号で識別されます。エキスプレスサービスコードおよびサービスタグは、システム前面の情報タグを引き出すと、そこに記載されています。この情報は、デルが受けたサポート宛ての電話を、適切な担当者に転送するために使用されます。

デルへのお問い合わせ

 **メモ**：デルでは、オンラインまたは電話によるサポートとサービスのオプションを複数提供しています。お使いのコンピュータがインターネットに接続されていない場合は、購入時の納品書、出荷伝票、請求書、またはデルの製品カタログで連絡先をご確認ください。サポートやサービスの提供状況は国や製品ごとに異なり、国/地域によってはご利用いただけないサービスもございます。

セールス、テクニカルサポート、またはカスタマーサービスの問題については、次の手順でデルにお問い合わせいただけます。

- 1 **dell.com/contactdell** にアクセスします。
- 2 インタラクティブな世界地図からお住まいの国または地域を選択します。
地域を選択すると、選択した地域内の国が表示されます。
- 3 選択した国の下にある適切な言語を選択します。
- 4 該当する事業区分を選択します。
選択した事業区分のメインサポートページが表示されます。
- 5 必要性に応じて、適切なオプションを選択します。

 **メモ**：Dell システムをご購入いただいた場合は、サービスタグを要求される場合があります。

マニュアルに対するフィードバック

本書に関するフィードバックについては、

documentation_feedback@dell.com まで E-メールをご送付ください。

または、任意のデルマニュアルページで **フィードバック** をクリックしてフォームに記入し、**送信** をクリックしてフィードバックを送信することもできます。

付録 — 負荷バランス

Windows 負荷バランスポリシー

マルチパスドライバは、特定の RAID コントローラモジュールを経由して仮想ディスクへの I/O パスを選択します。マルチパスドライバは、新規の I/O を受信すると、仮想ディスクを所有している現在の RAID コントローラモジュールへのパスを検索します。該当するパスが見つからない場合、マルチパスドライバは仮想ディスクの所有権をセカンダリ RAID コントローラモジュールに移行します。仮想ディスクを所有する RAID コントローラモジュールへのパスが複数存在する場合は、負荷バランスポリシーを選択して、I/O の処理に使用するパスを決めることができます。負荷バランスポリシーを設定するいくつかのオプションにより、複数のホストインタフェースが設定されている場合の I/O パフォーマンスを最適化することができます。

次の負荷バランスポリシーのいずれか 1 つを選択して、I/O パフォーマンスを最適化できます。

- サブセット付きラウンドロビン
- サブセット付き最小のキューの深さ

サブセット付きラウンドロビン

サブセット付きラウンドロビン負荷分散ポリシーでは、仮想ディスクを所有する RAID コントローラモジュールへの使用可能な各データバスへ I/O 要求を順に送信します。このポリシーでは、仮想ディスクを所有する RAID コントローラモジュールへのすべてのパスを、I/O 処理が均等になるように扱います。所有権が変更されるまで、セカンダリ RAID コントローラモジュールへのパスは無視されます。ラウンドロビンポリシーでは、基本的にデータバスが同等であると想定しています。複数のホストがサポートされている場合、データバスによって帯域幅またはデータ転送速度が異なることがあります。

サブセット付き最小のキューの深さ

サブセット付き最小のキューの深さポリシーは、最小の I/O、または最小の要求ポリシーとしても知られています。このポリシーは、キューに入っている未処理の I/O 要求が最も少ないデータバスへ、次の I/O 要求を送信します。このポリシーでは、I/O 要求は単にキュー内のコマンドとなります。コマンドの種類またはコマンドに関連するブロックの数は考慮されません。サブセット付き最小のキューの深さポリシーでは、大きいブロック要求と小さいブロック要求が同等に扱われます。選択されるデータバスは、仮想ディスクを所有する RAID コントローラモジュールのパスグループに含まれるパスです。

Windows Server 2008 における負荷バランスポリシーの変更

PowerVault MD3200 シリーズでの負荷バランスは、Windows Server 2008 およびそれ以降のオペレーティングシステムのバージョンでのみ使用できます。次のいずれかを使用して、デフォルトのサブセット付きラウンドロビンから負荷バランスポリシーを変更できます。

- デバイスマネージャオプション
- ディスクの管理オプション

Windows Server 2008 のデバイスマネージャオプションを使用した負荷バランスポリシーの変更

- 1 ホストのデスクトップで **マイコンピュータ** を右クリックして、**管理** を選択し、**コンピュータの管理** ウィンドウを開きます。
- 2 **デバイスマネージャ** をクリックして、ホストに接続されているデバイスの一覧を表示します。
- 3 負荷バランスポリシーを設定するマルチパスディスクデバイスを右クリックして、**プロパティ** を選択します。
- 4 **MPIO** タブから、このディスクデバイスに設定する負荷バランスポリシーを選択します。

Windows Server 2008 ディスクの管理オプションを使用した負荷バランスポリシーの変更

- 1 ホストのデスクトップで **マイコンピュータ** を右クリックして、**管理** を選択し、**コンピュータの管理** ウィンドウを開きます。
- 2 **ディスクの管理** をクリックして、ホストに接続されている仮想ディスクの一覧を表示します。
- 3 負荷バランスポリシーを設定する仮想ディスクを右クリックして、**プロパティ** をクリックします。
- 4 **MPIO** タブから、この仮想ディスクに設定する負荷バランスポリシーを選択します。

Linux での負荷バランスポリシーの設定

Linux では、ラウンドロビンをベースとした負荷バランシングのみがサポートされます。詳細については、45 ページの「サブセット付きラウンドロビン」を参照してください。

付録 — iSCSI の手動設定

次の項では、ストレージレイの iSCSI を設定する詳しい手順が説明されています。ただし、作業を開始する前に、お使いのホストサーバーまたはストレージレイ環境との関係で、各手順をどこで行うのかを理解しておくことが重要です。

表 B-1 に、iSCSI 設定の各手順と、それらをどこで行うのかを示します。

表 B-1. ホストサーバーとストレージレイ

Microsoft または Linux の iSCSI イニシエーターを使用してホストサーバーで行う手順	MD Storage Manager を使用してストレージレイで行う手順
	1 ストレージレイの検知。
	2 ストレージレイの iSCSI ポートを設定します。
3 iSCSI イニシエーターからのターゲットの検出。	
	4 ホストアクセスの設定。
	5 (オプション) ストレージレイにおけるチャレンジハンドシェイク認証プロトコル (CHAP) 認証の設定。
6 (オプション) ホストサーバーにおける CHAP 認証の設定。	
7 ホストサーバーからストレージレイへの接続。	
	8 (オプション) 帯域内管理のセットアップ。

手順 1：ストレージレイの検出 (帯域外管理のみ)

IPv4 管理ポートのデフォルト設定

デフォルトで、ストレージレイ管理ポートは DHCP（ダイナミックホスト設定プロトコル）に設定されています。ストレージレイのコントローラが DHCP サーバーから IP 設定を取得できない場合、約 3 分後にタイムアウトになり、デフォルトの静的 IP アドレスに戻ります。デフォルトの IP 設定は次のとおりです。

Controller 0: IP: 192.168.128.101 Subnet Mask: 255.255.255.0

Controller 1: IP: 192.168.128.102 Subnet Mask: 255.255.255.0



メモ：デフォルトゲートウェイは設定されていません。

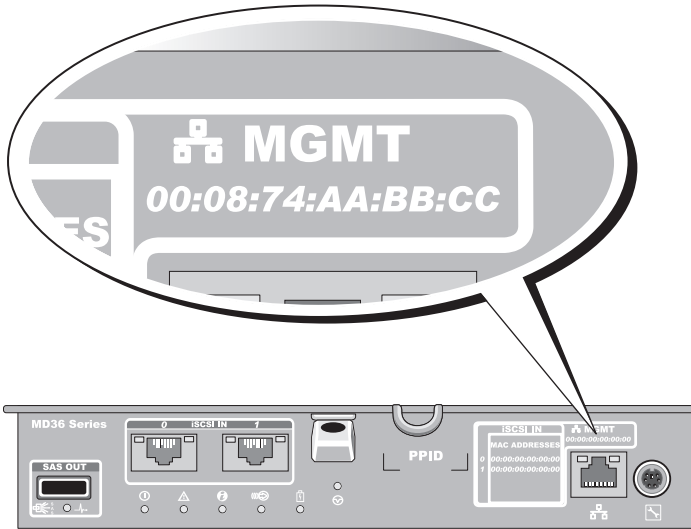


メモ：DHCP が使用されていない場合、ストレージレイと同じ物理サブネット上にある管理ステーションを利用して初期設定を行います。また、初期設定中に、少なくとも 1 つのネットワークアダプタをストレージレイのデフォルト管理ポート（192.168.128.101 または 192.168.128.102）と同じ IP サブネットで設定します。初期設定が終われば（管理ポートは MD Storage Manager を使用して設定）、管理ステーションの IP アドレスを元の設定に戻すことができます。

IPv6 管理ポートのデフォルト設定

デフォルトでは、ストレージレイの管理ポートは IPv6 のステートレス自動設定が有効になっています。設定済みの IPv6 ルーターがネットワーク上に存在する場合、これらのポートはそのリンクローカルアドレスおよびルータブルアドレスに응答するよう自動的に設定されます。管理ポートのリンクローカルアドレスを調べるには、コントローラにある管理ポートの MAC ラベルを確認してください。たとえば、次のとおりです。

- 1 MAC アドレスが 00:08:74:AA:BB:CC である場合、リンクローカルアドレスは FE80::02 で始まります。
- 2 プレフィックスに MAC アドレスの 2 番目と 3 番目のバイト、08:74 を付加して FE80::0208:744 にします。
- 3 さらに FF:FE を付加して FE80::0200:08FF:FE を得ます。
- 4 最後に、MAC アドレスの末尾 3 バイトを付加して、FE80::0200:08FF:FEAA:BBCC となります。



メモ：この手順は帯域外管理のみに適用されます。帯域内管理をセットアップする場合は、この手順を実行してから、65 ページの「手順 8：帯域内管理のセットアップ（オプション）」に進む必要があります。

ストレージアレイの検出は自動でも手動でも可能です。どちらかを選択し、次の手順を完了してください。

ストレージアレイの自動検知

1 MDSM を起動します。

これが管理用にセットアップする最初のストレージアレイである場合は、**新規ストレージアレイの追加** ウィンドウが表示されます。

2 自動 を選択し、OK をクリックします。

検知が完了するのに数分かかることがあります。検出処理が完了する前に検出のステータスウィンドウを閉じると、検出処理がキャンセルされます。

検知が完了すると、確認画面が表示されます。

3 閉じる をクリックして、画面を閉じます。

ストレージレイの手動検出

- 1 **MDSM** を起動します。
これが管理用にセットアップする最初のストレージレイである場合は、**新規ストレージレイの追加** ウィンドウが表示されます。
- 2 **手動** を選択し、**OK** をクリックします。
- 3 **帯域外管理** を選択し、iSCSI ストレージレイコントローラのホストサーバー名または IP アドレスを入力します。
- 4 **追加** をクリックします。
これで帯域外管理が正常に設定されました。
検知が完了すると、確認画面が表示されます。
- 5 **閉じる** をクリックして、画面を閉じます。

レイのセットアップ

- 1 検出が完了すると、検出された最初のストレージレイの名前が **MDSM** の **サマリ** タブの下に表示されます。
- 2 新しく検出されたストレージレイのデフォルト名は、**無題** です。別の名前が表示された場合は、名前の隣の下矢印をクリックし、ドロップダウンリスト内の **無題** を選択します。
- 3 **初期セットアップタスク** オプションをクリックして、残りのインストール後のタスクへのリンクを確認します。各タスクの詳細については、『**Owner's Manual**』（オーナーズマニュアル）を参照してください。表 B-2 に示す順序でこれらのタスクを実行してください。



メモ：ストレージレイを設定する前に、**サマリ** タブのステータスアイコンをチェックして、ストレージレイ内のエンクロージャが最適ステータスであることを確認します。ステータスアイコンの詳細については、dell.com/support/manuals で『**Owner's Manual**』（オーナーズマニュアル）を参照してください。

表 B-2. 初期セットアップタスクダイアログボックス

タスク	目的
ストレージレイの名前の変更	ソフトウェアによって割り当てられた 無題 というラベルよりも意味のある名前を付ける。
ストレージレイのパスワード設定	不正なアクセスを制限する。設定を変更する前、または破壊的な操作を行う前に MDSM からパスワードを求められる場合があります。
アラート通知のセットアップ E- メールアラートのセットアップ SNMP アラートのセットアップ	ストレージレイのコンポーネントに劣化や障害が生じた場合、または環境が悪化した場合に、個人および / または Dell Management Console (SNMP 経由) 等のストレージのエンタープライズ管理コンソールに (E- メールで) 通知する。
ストレージレイの設定	仮想ディスクを作成し、これをホストにマッピングする。

手順 2 : ストレージレイの iSCSI ポートの設定

デフォルトでは、ストレージレイの iSCSI ポートは次のように設定されています (IPv4 設定)。

Controller 0, Port 0: IP: 192.168.130.101 Subnet Mask: 255.255.255.0 Port: 3260

Controller 1, Port 0: IP: 192.168.130.101 Subnet Mask: 255.255.255.0 Port: 3260

Controller 0, Port 2: IP: 192.168.132.101 Subnet Mask: 255.255.255.0 Port: 3260

Controller 0, Port 3: IP: 192.168.133.101 Subnet Mask: 255.255.255.0 Port: 3260

Controller 1, Port 0: IP: 192.168.130.101 Subnet Mask: 255.255.255.0 Port: 3260

Controller 1, Port 1: IP: 192.168.130.101 Subnet Mask: 255.255.255.0 Port: 3260

Controller 1, Port 2: IP: 192.168.132.101 Subnet Mask: 255.255.255.0 Port: 3260

Controller 1, Port 3: IP: 192.168.133.102 Subnet Mask: 255.255.255.0 Port: 3260



メモ : デフォルトゲートウェイは設定されていません。

ストレージアレイの iSCSI ポートを設定するには、次の手順を実行します。

- 1 MDSM から、**AMW** の **セットアップ** タブに移動します。
- 2 **イーサネット管理ポートの設定** をクリックし、**iSCSI ホストポートを設定する** を選択します。
- 3 ストレージアレイの iSCSI ポートを設定します。



メモ：DHCP はサポートされていますが、静的 IPv4 アドレスの割り当てをお勧めします。

詳細設定 ボタンをクリックすると、（構成に応じて）次の設定が使用できます。

- 仮想 LAN (VLAN) のサポート — VLAN とは、LAN の同じセグメントに接続されて同じスイッチとルーターによってサポートされているかのように動作する複数のシステムから成るネットワークのことです。VLAN として設定すると、デバイスを別の場所に移動しても再設定の必要がありません。ストレージアレイで VLAN を使用するには、ネットワーク管理者から VLAN ID を取得してください。
- イーサネットの優先度 — このパラメータは、ネットワークアクセスの優先度を定めるために設定します。
- TCP リスニングポート — ストレージアレイがホストサーバーの iSCSI イニシエータからの iSCSI ログインをリッスンするポート番号です。




メモ：iSNS サーバー用の TCP リスニングポートは、ストレージアレイコントローラが iSNS サーバーに接続するために使用するポート番号です。これにより、iSNS サーバーは iSCSI ターゲットとストレージアレイのポータルを登録することができ、その結果、ホストサーバーイニシエータがそれらを識別できます。

- ジャンボフレーム — 最大転送単位 (MTU) が 1500 バイト / フレームよりも大きい場合、ジャンボイーサネットフレームが作成されます。この設定はポートごとに調整可能です。
- 4 すべてのポートについて **ICMP PING 応答を有効にするには、ICMP PING 応答を有効にします** を選択します。
 - 5 すべての iSCSI ストレージアレイポートの設定が完了したら、**OK** をクリックします。
 - 6 iSCSI ストレージアレイの各ポートで ping コマンドを実行することで、接続をテストします。

手順 3：iSCSI イニシエータからのターゲットの検出

この手順により、ホストサーバーに接続されているストレージレイの iSCSI ポートが識別されます。お使いのオペレーティングシステムに（Windows または Linux）に対応する手順一連を次の項から選んでください。

Microsoft Windows Server 2003 または Windows Server 2008 GUI バージョン を使用している場合

- 1 **スタート** → **プログラム** → **Microsoft iSCSI イニシエータ** または **スタート** → **すべてのプログラム** → **管理ツール** → **iSCSI イニシエータ** の順に選択します。
 - 2 **検出** タブをクリックします。
 - 3 **ターゲットポータル** で、**追加** をクリックし、ストレージレイの iSCSI ポートの IP アドレスまたは DNS 名を入力します。
 - 4 iSCSI ストレージレイがカスタム TCP ポートを使用している場合には、**ポート** 番号を変更します。デフォルトは **3260** です。
 - 5 **詳細設定** をクリックし、**一般** タブで次の値を設定します。
 - **ローカルアダプタ** — Microsoft iSCSI イニシエータ に設定する必要があります。
 - **ソース IP** — 接続したいホストのソース IP アドレスです。
 - **データダイジェストとヘッダダイジェスト** — オプションとして、トラブルシューティングに役立つように、送信中にデータまたはヘッダ情報のダイジェストがコンパイルされるように指定できます。
 - **CHAP ログオン情報** — ターゲット CHAP が設定済みのストレージエリアネットワーク（SAN）にストレージレイを追加する場合を除いて、この時点ではこのオプションは選択せず、CHAP 情報を入力しないでください。
-  **メモ**：IPSec はサポートされていません。
- 6 **OK** をクリックして **詳細設定** メニューを終了し、再度 **OK** をクリックして **ターゲットポータルの追加** 画面を終了します。
 - 7 **検出** タブを終了するには、**OK** をクリックします。
 - **CHAP 認証を設定する場合は**、この時点で複数の iSCSI ポートで検出を実行しないでください。55 ページの「**手順 4：ホストアクセスの設定**」に進みます。
 - **CHAP 認証を設定しない場合は**、ストレージレイのすべての iSCSI ポートで手順 1 ～ 手順 6 を繰り返します。

Windows Server 2008 Core バージョンを使用している場合

- 1 iSCSI イニシエータサービスを自動開始するように設定します。
`sc \\<サーバー名> config msiscsi start=auto`
- 2 iSCSI サービスを開始：`sc start msiscsi`
- 3 ターゲットポータルを追加します。
`iscsicli QAddTargetPortal <ストレージアレイの iSCSI ポートの IP アドレス>`

Red Hat Enterprise Linux 5、Red Hat Enterprise Linux 6、SUSE Linux Enterprise Server 10、または SUSE Linux Enterprise Server 11 を使用している場合

Red Hat Enterprise Linux 5 および SUSE Linux Enterprise Server 10 SP1 ディストリビューション用の iSCSI イニシエータの設定は、**/etc/iscsi/iscsid.conf** ファイルの変更によって行います。このファイルは、MDSM のインストール時にデフォルトでインストールされています。ファイルを直接編集するか、またはデフォルトファイルを PowerVault MD3600i シリーズのリソースメディアに収録されているサンプルファイルと置き換えます。メディアに収録されているサンプルファイルを使用する場合は、次の手順に従います。

- 1 デフォルトの **/etc/iscsi/iscsid.conf** ファイルを任意の別ディレクトリに保存することによってコピーを作成します。
- 2 **/etc/iscsi/iscsid.conf** ファイルで以下のエントリを編集します。
 - a `node.startup = manual` 行を無効にします。
 - b `node.startup = automatic` 行を有効にします。これで、起動時にサービスが自動的に開始します。
 - c 次のタイムアウト値が 30 に設定されていることを確認します。
`node.session.timeo.replacement_timeout = 30`
 - d **/etc/iscsi/iscsid.conf** ファイルを保存して閉じます。
- 3 コンソールから、コマンド `service iscsi start` を実行して iSCSI サービスを再開します。
- 4 コンソールから次のコマンドを実行して、起動中に iSCSI サービスが実行されていることを確認します。
`chkconfig iscsi on`
- 5 指定された IP アドレスで使用可能な iSCSI ターゲットを表示するには、次のコマンドを実行します。
`iscsiadm -m discovery -t st -p <IP_address_of_iSCSI_port>`

- 6 ターゲットの検出後に、次のコマンドを使用して手動でログインします。
`iscsiadm -m node -l`

このログインは、自動開始が有効になっている場合には、起動時に自動的に行われます。

- 7 次のコマンドを実行して、セッションから手動でログアウトします。
`iscsiadm -m node -T <initiator_username> -p
<target_ip> -u`

手順 4：ホストアクセスの設定

この手順では、どのホストサーバーがストレージアレイの仮想ディスクにアクセスするかを指定します。仮想ディスクをホストサーバーにマップする前、または、新しいホストサーバーをストレージアレイに接続するたびに、この手順を実行するようにしてください。

- 1 MDSM を起動します。
- 2 アレイ管理ウィンドウに移動し、**ホストの手動定義** をクリックします。
- 3 **ホスト名の入力** で、仮想ディスクのマッピング用のホストサーバーを入力します。
これは、必ずしも、ネットワークに対してホストサーバーの ID を示すために使われる名前ではなく、非公式の名前でかまいません。
- 4 ホストポート識別子を追加する方法を選択します。
- 5 ホストのタイプを選択します。
- 6 そのホストサーバーを、他のホストサーバーと同じ仮想ディスクへのアクセスを共有するホストサーバーグループの一部とすることを決めます。ホストが Microsoft クラスタの一部である場合にのみ、**はい** を選択してください。
- 7 **次へ** をクリックします。
- 8 このホストをホストグループの一部とすることを指定し、**完了** をクリックします。

CHAP 認証について

CHAP について

チャレンジハンドシェイク認証プロトコル (CHAP) は、ストレージアレイ (ターゲット) がホストサーバーの iSCSI イニシエータを認証するという、オプションの iSCSI 認証方法です。2 種類の CHAP がサポートされています。

- ターゲット CHAP
- 相互 CHAP

ターゲット CHAP

ターゲット CHAP では、ストレージアレイは、ホストサーバー上で CHAP シークレット経由で iSCSI イニシエータによって発行されたすべてのアクセス要求を認証します。ターゲット CHAP 認証をセットアップするには、ストレージアレイに CHAP シークレットを入力し、次に、ホストサーバーがストレージアレイへのアクセスを試みるときに毎回そのシークレットを送信するように、ホストサーバー上の各 iSCSI イニシエータを設定します。

相互 CHAP

ターゲット CHAP に加えて、相互 CHAP もセットアップできます。後者では、ストレージアレイと iSCSI イニシエータの両方が互いに認証します。相互 CHAP をセットアップするには、接続を確立するためにストレージアレイがホストサーバーに送信する必要がある CHAP シークレットを使用して、iSCSI イニシエータを設定します。この双方向の認証プロセスでは、ホストサーバーとストレージアレイの両方が、接続が許可される前に相手方の認証を受けなければならない情報を送信します。

CHAP はオプション機能であり、iSCSI を使用するのに必須な機能ではありません。ただし、CHAP 認証を設定しないと、ストレージアレイと同じ IP ネットワークに接続されているどのホストサーバーにも、ストレージアレイへの読み書きが許可されます。



メモ： CHAP 認証の使用時、仮想ディスクでデータ受信の準備をする前に、ストレージアレイ（MD Storate Manager を使用）とホストサーバー（iSCSI イニシエータを使用）の両方を構成する必要があります。CHAP 認証を設定する前に、データを受け取るディスクの準備を行うと、CHAP が設定された時点でディスクが確認できなくなります。

CHAP の定義

ターゲット CHAP 認証と相互 CHAP 認証の違いを表 B-3 に要約します。

表 B-3. CHAP の種類の定義

CHAP の種類	説明
ターゲット CHAP	ターゲットストレージアレイに接続するために iSCSI イニシエータが使用するアカウントがセットアップされます。セットアップされると、ターゲットストレージアレイは iSCSI イニシエータを認証します。
相互 CHAP	CHAP に 加えて 適用されるもので、相互 CHAP はターゲットストレージアレイが iSCSI イニシエータに接続するために使用するアカウントをセットします。セットアップされると、iSCSI イニシエータはターゲットを認証します。

手順 5：ストレージアレイにおける CHAP 認証の設定（オプション）

どの種類の CHAP 認証を設定する場合も（ターゲットのみ、またはターゲットと相互の両方）、この手順と 57 ページの「手順 5：ストレージアレイにおける CHAP 認証の設定（オプション）」を完了する必要があります。

どの種類の CHAP も設定しない場合は、これらの手順を省略して 62 ページの「手順 7：ホストサーバーからストレージアレイへの接続」に進んでください。




メモ：相互 CHAP 認証を設定する場合は、最初にターゲット CHAP を設定してください。

iSCSI 設定においては、ターゲットという語は常にストレージアレイを指します。

ストレージアレイのターゲット CHAP 認証の設定

- 1 MDSM で **iSCSI** タブをクリックし、**ターゲット認証の変更** をクリックします。
表 B-4 で説明する CHAP 設定のうちいずれか 1 つを選択します。
- 2 CHAP シークレットを設定するには、**CHAP** を選択し、**CHAP シークレット** を選択します。
- 3 ターゲットの CHAP シークレットを入力します（または、ランダムシークレットを生成します）。**ターゲット CHAP シークレットの確認** で確認して **OK** をクリックします。

ストレージレイでは 12 ～ 57 文字まで使用できますが、多くのイニシエータでは CHAP シークレットが 16 文字 (128 ビット) までに制限されています。

 **メモ** : CHAP はいったん入力すると、表示して確認することができません。シークレットはユーザー自身が確認できるところに必ずメモしておいてください。ランダムシークレットの生成を使用した場合は、後で参照できるようにシークレットをテキストファイルにコピーペーストしてください。ストレージレイに追加する新しいホストサーバーを認証する際に、同じ CHAP シークレットが使用されます。この CHAP シークレットを忘れた場合は、ストレージレイに接続されている既存のホストをすべて取り外し、本章の手順を繰り返してホストを追加しなおす必要があります。

4 OK をクリックします。

表 B-4. CHAP 設定


オプション	説明
なし	これがデフォルトの選択です。なし以外に選択肢がない場合、ストレージレイは CHAP 認証の種類を示すことなく、iSCSI イニシエータにログオンを許可します。
なしおよび CHAP	CHAP 認証の有無に関係なく、ストレージレイは iSCSI イニシエータにログオンを許可します。
CHAP	CHAP が選択され、なしの選択が解除されると、ストレージレイはアクセスを許可する前に CHAP 認証を求めます。

ストレージレイの相互 CHAP 認証の設定

イニシエータのシークレットは、ストレージレイに接続するホストサーバーごとに一意である必要があります。また、ターゲット CHAP シークレットと同一のシークレットは使用できません。

ターゲット認証の変更 ウィンドウで、イニシエータ認証設定を変更します。設定内容を変更するには、次の手順を実行します。

- **なし** — イニシエータ認証を許可しない場合は、**なし** を選択します。**なし** を選択した場合は、どのイニシエータもこのターゲットにアクセスできません。このオプションは、データのセキュリティ保護を必要としない場合にのみ使用してください。ただし、**なし** と **CHAP** は同時に選択することができます。
- **CHAP** — 認証のために CHAP を使ってターゲットへのアクセスを試行するイニシエータを有効にしたい場合は、**CHAP** を選択します。相互 CHAP 認証を使用したい場合のみ、CHAP シークレットを定義してください。**CHAP** を選択し、CHAP ターゲットのシークレットが定義されていない場合、エラーメッセージが表示されます。**CHAP シークレット** をクリックして **CHAP シークレットの入力** ウィンドウを表示します。このウィンドウを使って、CHAP シークレットを定義してください。

 **メモ** : CHAP シークレットを削除するには、ホストイニシエータを削除し、追加しなおす必要があります。

手順 6：ホストサーバーにおける CHAP 認証の設定（オプション）

57 ページの「手順 5：ストレージレイにおける CHAP 認証の設定（オプション）」で CHAP 認証を設定した場合は、以下の手順を実行してください。上記の手順で CHAP 認証を設定していない場合は、62 ページの「手順 7：ホストサーバーからストレージレイへの接続」に進みます。

お使いの OS（Windows または Linux）に対応する手順を以下から選んでください。

Windows Server 2008 GUI バージョンを使用している場合

- 1 **スタート** → **プログラム** → **Microsoft iSCSI イニシエータ** または **スタート** → **すべてのプログラム** → **管理ツール** → **iSCSI イニシエータ** の順に選択します。
- 2 相互 CHAP 認証を使用しない場合は、手順 4 に進みます。
- 3 相互 CHAP 認証を使用する場合は、**一般** タブをクリックして **シークレット** を選択します。**セキュアシークレットの入力** で、ストレージレイ用に入力した相互 CHAP シークレットを入力します。
- 4 **検出** タブをクリックします。
- 5 **ターゲットポータル** で、ストレージレイの iSCSI ポートの IP アドレスを選択し、**削除** をクリックします。
ターゲットの検出中にストレージレイに設定した iSCSI ポートが表示されなくなります。
- 6 **ターゲットポータル** で **追加** をクリックし、ストレージレイの iSCSI ポートの IP アドレスまたは DNS 名（上記の手順で削除）を再入力します。
- 7 **詳細** をクリックし、**全般** タブで次の値を設定します。
 - ローカルアダプタ — Microsoft iSCSI イニシエータ に常時設定するようにします。
 - ソース IP — 接続したいホストのソース IP アドレスです。
 - データダイジェストとヘッダダイジェスト — オプションとして、トラブルシューティングに役立つように、送信中にデータまたはヘッダ情報のダイジェストがコンパイルされるように指定できます。
 - CHAP ログオン情報 — ストレージレイのホストサーバー用に入力したターゲット CHAP 認証のユーザー名とシークレットを入力します。
 - 相互認証の実行 — 相互 CHAP 認証が設定されている場合、このオプションを選択します。



メモ：IPSec はサポートされていません。

8 OK をクリックします。

検出セッションのフェイルオーバーを必要とする場合は、ストレージレイのすべての iSCSI ポートを対象に本手順の 手順 5 と 手順 6 を繰り返します。フェイルオーバーを設定しない場合は、シングルホストポートの構成で十分です。



メモ：接続が失敗する場合は、すべての IP アドレスが正しく入力されていることを確認します。誤った IP アドレスを入力すると、接続の問題が生じます。

Windows Server 2008 Core バージョンを使用している場合

- 1 iSCSI イニシエータサービスを、自動で起動するよう設定（未設定の場合）：
`sc \\<server_name> config msiscsi start= auto`
- 2 必要に応じて iSCSI サービスを開始：`sc start msiscsi.`
- 3 相互 CHAP 認証を使用しない場合は、手順 5 に進みます。
- 4 ストレージレイ用に入力した相互 CHAP シークレットを入力：
`iscsicli CHAPSecret <secret>`
- 5 ターゲットの検出中にストレージレイに設定したターゲットポータルを削除します。

```
iscsicli RemoveTargetPortal <IP_address>  
<TCP_listening_port>
```

- 6 CHAP が定義されているターゲットポータルを追加します。

```
iscsicli QAddTargetPortal  
<IP_address_of_iSCSI_port_on_storage_array>  
[CHAP_username]  
[CHAP_password]
```

[CHAP_username] はイニシエータ名、[CHAP_password] はターゲット CHAP シークレットです。

検出セッションのフェイルオーバーを設定する場合は、ストレージレイのすべての iSCSI ポートを対象に手順 5 を繰り返します。フェイルオーバーを設定しない場合は、シングルホストポートの構成で十分です。

Red Hat Enterprise Linux 5、Red Hat Enterprise Linux 6、SUSE Linux Enterprise Server 10、または SUSE Linux Enterprise Server 11 を使用している場合

- 1 CHAP（オプション）を有効にするには、**/etc/iscsi/iscsid.conf** ファイル内で次の行を有効にする必要があります。

```
node.session.auth.authmethod = CHAP
```

- 2 ターゲットによるイニシエータの CHAP 認証に使用するユーザー名とパスワードを設定するには、次の行を次のように編集します。


```
node.session.auth.username = <iscsi_initiator_username>
node.session.auth.password = <CHAP_initiator_password>
```
- 3 相互 CHAP 認証を使用している場合、イニシエータによるターゲットの CHAP 認証に使用するユーザー名とパスワードを設定するには、次の行を編集します。


```
node.session.auth.username_in= <iscsi_target_username>
node.session.auth.password_in = <CHAP_target_password>
```
- 4 検出セッションの CHAP 認証をセットアップするには、最初に次の行からコメントを削除します。


```
discovery.sendtargets.auth.authmethod = CHAP
```
- 5 ターゲットによるイニシエータの検出セッションの CHAP 認証に使用するユーザー名とパスワードを設定するには、次の行を編集します。


```
discovery.sendtargets.auth.username =
<iscsi_initiator_username>

discovery.sendtargets.auth.password =
<CHAP_initiator_password>
```
- 6 相互 CHAP のイニシエータによってターゲットの検出セッション CHAP 認用に使用するユーザー名とパスワードを設定するには、次の行を編集します。


```
discovery.sendtargets.auth.username =
<iscsi_target_username>

discovery.sendtargets.auth.password_in =
<CHAP_target_password>
```
- 7 **/etc/iscsi/iscsid.conf** ファイル内の最終的な構成内容は、次のように表示されます。


```
node.session.auth.authmethod = CHAP

node.session.auth.username = iqn.2005-
03.com.redhat01.78b1b8cad821

node.session.auth.password = password_1

node.session.auth.username_in= iqn.1984-
05.com.dell:powervault.123456

node.session.auth.password_in = test1234567890
```

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = iqn.2005-
03.com.redhat01.78b1b8cad821
discovery.sendtargets.auth.password = password_1
discovery.sendtargets.auth.username = iqn.1984-
05.com.dell:powervault.123456
discovery.sendtargets.auth.password_in = test1234567890
```

SUSE Linux Enterprise Server SP3 using the GUI を使用している場合

- 1 **デスクトップ** → **YaST** → **iSCSI イニシエータ** とクリックします。
- 2 **サービスの開始** をクリックし、次に **起動時** を選択します。
- 3 **検出されたターゲット** を選択し、**検出** を選択します。
- 4 ポートの IP アドレスを入力します。
- 5 **次へ** をクリックします。
- 6 ログインされていない任意のターゲットを選択し、**ログイン** をクリックします。
- 7 次のいずれか 1 つを選択します。
 - CHAP 認証を使用しない場合は、**認証なし** を選択します。手順 8 に進みます。
または
 - CHAP 認証を使用する場合は、CHAP のユーザー名とパスワードを入力します。相互 CHAP を有効にする場合は、相互 CHAP のユーザー名とパスワードを選択し、入力します。
- 8 各コントローラにつき、少なくとも 1 つの接続がログインされた状態になるまで、各ターゲットに手順 7 を繰り返します。
- 9 **接続済みのターゲット** に移動します。
- 10 ターゲットが接続され、ステータスが **true** になっていることを確認します。

手順 7：ホストサーバーからストレージレイ への接続

Windows Server 2008 GUI を使用している場合

- 1 **スタート** → **プログラム** → **Microsoft iSCSI イニシエータ** または **スタート** → **すべてのプログラム** → **管理ツール** → **iSCSI イニシエータ** の順に選択します。

2 **ターゲット** タブをクリックします。

前回のターゲット検出が成功していた場合、ストレージレイの **iqn** がターゲットの下に表示されています。


3 **ログオン** をクリックします。

4 **システムの起動時にこの接続を自動的に回復する** を選択します。

5 **マルチパスの有効化** を選択します。


6 **詳細** をクリックし、**全般** タブで次の設定を行います。

- **ローカルアダプタ** — **Microsoft iSCSI イニシエータ** に設定する必要があります。
- **ソース IP** — 接続元にしたがってホストサーバーのソース IP アドレスを入力します。
- **ターゲットポータル** — 接続先とするストレージレイコントローラの iSCSI ポートを選択します。
- **データダイジェストとヘッダダイジェスト** — オプションとして、トラブルシューティングに役立つように、送信中にデータまたはヘッダ情報のダイジェストがコンパイルされるように指定できます。
- **CHAP ログオン情報** — CHAP 認証が必要な場合は、このオプションを選択してターゲットのシークレットを入力します。
- **相互認証の実行** — 相互 CHAP 認証が設定されている場合、このオプションを選択します。

 **メモ** : IPsec はサポートされていません。


7 **OK** をクリックします。

ストレージレイコントローラのフェイルオーバーをサポートするには、ホストサーバーは各コントローラの少なくとも 1 つの iSCSI ポートに接続されている必要があります。フェイルオーバーターゲットとして構築するストレージレイの各 iSCSI ポートに対して、手順 3 ~ 手順 8 を繰り返します。**ターゲットポータル** アドレスは、接続するポート 1 つ 1 つで異なります。

 **メモ** : マルチパス I/O の、より高いスループットを有効にするためには、ホストサーバーは、理想的にはホスト側の別々の NIC から、各コントローラの両方の iSCSI ポートに接続する必要があります。各コントローラの各 iSCSI ポートに対して手順 3 ~ 手順 7 を繰り返します。MD36x0i 二重構成を使用している場合には、LUN もコントロール間で分散させる必要があります。

ターゲット タブの **ステータス** フィールドには、**接続中** で表示されます。

8 **OK** をクリックして **Microsoft iSCSI イニシエータ** を閉じます。

 **メモ** : PowerVault MD36x0i はラウンドロビン方式の負荷分散ポリシーのみをサポートします。

Windows Server 2008 Core バージョンを使用している場合

- 1 iSCSI イニシエータサービスを、自動で起動するよう設定（未設定の場合）:

```
sc \\<server_name> config msiscsi start= auto
```

- 2 必要に応じて iSCSI サービスを開始: `sc start msiscsi`

- 3 ターゲットにログオンします。

```
iscsicli PersistentLoginTarget <Target_Name>  
<Report_To_PNP> <Target_Portal_Address>  
<TCP_Port_Number_Of_Target_Portal> * * *  
  
<Login_Flags> * * * * * <Username> <Password>  
<Authtype> * <Mapping_Count>
```

ここで、

- <Target_Name> は、ターゲットリストに表示されているターゲット名です。 `scsicli ListTargets` コマンドを使用すると、ターゲットリストを表示できます。
- <Report_To_PNP> は T にします。これで、LUN が OS に対してストレージアレイとして提供されます。
- <Target_Portal_Address> は、ログインするコントローラの iSCSI ポートの IP アドレスです。
- <TCP_Port_Number_Of_Target_Portal> は 3260 にします。
- <Login_Flags> は 0x2 で、イニシエータでターゲットに対してマルチパスを有効にします。これにより、1 度に複数のセットが 1 つのターゲットにログインすることを許可します。
- <Username> はイニシエータ名です。
- <Password> はターゲット CHAP シークレットです。
- <Authtype> は、認証なしの場合は 0 に、ターゲット CHAP の場合は 1 に、相互 CHAP の場合は 2 にします。



メモ: <Username>、<Password>、および <Authtype> はオプションのパラメータです。CHAP を使用しない場合には、アスタリスク (*) に置き換えられます。

- < マップ数 > は 0 にします。これは、マッピングの指定がなく、これ以上のパラメータの指定は必要ないことを示します。

*** アスタリスク (*) は、パラメータのデフォルト値を表します。

たとえば、ログオンコマンドは次のようになります。

```
iscsicli PersistentLoginTarget iqn.1984-  
05.com.dell:powervault.6001372000ffe3332xx0000046 72edf2 3260  
T 192.168.130.101 * * * 0x2 * * * * *  
* * * * * 0
```


ターゲットに対するアクティブなセッションを表示するには、次のコマンドを使用します。

```
iscsicli SessionList
```

ストレージレイコントローラのフェイルオーバーをサポートするには、ホストサーバーは各コントローラの少なくとも 1 つの iSCSI ポートに接続されている必要があります。フェイルオーバーターゲットとして構築するストレージレイの各 iSCSI ポートに対して、手順 3 を繰り返します。ターゲットポータルアドレスは、接続する各ポートごとに異なります。

PersistentLoginTarget は、システムが再起動するまでターゲットへのログインを開始しません。ターゲットへの即時ログインを行うには、**PersistentLoginTarget** の代わりに **LoginTarget** を使用します。



メモ：ここで使用したコマンドの詳細については、『Microsoft iSCSI Software Initiator 2.x User's Guide』（Microsoft iSCSI Software Initiator 2.x ユーザーズガイド）を参照してください。Windows Server 2008 Server Core の詳細については、microsoft.com の Microsoft Developers Network (MSDN) を参照してください。

Linux Server を使用する場合は

MDSM の iSCSI ホストポートの設定 に、接続する各 iSCSI ポートのステータスおよびすべての IP アドレスの設定状態が表示されます。ステータスに **接続の切断** または **未設定** と表示されている場合は、以下の事柄をチェックし、iSCSI の設定手順を繰り返します。

- ホストサーバーとストレージレイの各ポートにすべてのケーブルがしっかり接続されているか。
- すべてのターゲットホストポートで TCP/IP が正しく設定されているか。
- ホストサーバーとストレージレイの両方で CHAP が正しくセットアップされているか。

最適なネットワークのセットアップと構成の設定については、33 ページの「ストレージレイの iSCSI の設定」を参照してください。

手順 8：帯域内管理のセットアップ (オプション)

ストレージレイの管理には、帯域外管理（48 ページの「手順 1：ストレージレイの検出（帯域外管理のみ）」を参照）が推奨されます。ただし、オプションとして帯域内管理のセットアップを行う場合には、次の手順に従ってください。

(参考のためにデフォルト iSCSI ホストポートの IPv4 アドレスを示します。)

Controller 0, Port 0: IP: 192.168.130.101 Controller 0, Port 1: IP: 192.168.131.101

Controller 0, Port 0: IP: 192.168.132.101 Controller 0, Port 1: IP:
192.168.133.101

Controller 1, Port 0: IP: 192.168.130.102 Controller 1, Port 1: IP:
192.168.131.102

Controller 1, Port 0: IP: 192.168.132.102 Controller 1, Port 1: IP:
192.168.133.102



メモ：ネットワーク通信に使用する管理ステーションは、PowerVault MD36x0i
ホストポートと同じ IP サブネットに設定します。

- 1 PowerVault MD3600i RAID ストレージアレイに対する iSCSI セッション
を確立します。
- 2 **SMagent** サービスを再起動します。
- 3 MDSM を起動します。
これが管理用にセットアップする最初のストレージアレイである場合は、
新規ストレージアレイの追加 ウィンドウが表示されます。表示されなかつ
た場合は、**新規** をクリックします。
- 4 **手動** を選択し、**OK** をクリックします。
- 5 帯域内管理を選択し、**MD Storage Manager** ソフトウェアが実行されて
いるホストサーバーのホストサーバー名または IP アドレスを入力します。
- 6 **追加** をクリックします。
これで帯域内管理が正常に設定されました。