

**Dell PowerVault MD3860i シリーズストレージ
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:** ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。
-  **警告:** 物的損害、けが、または死亡の原因となる可能性があることを示しています。

著作権 © 2014 Dell Inc. 無断転載を禁じます。 この製品は、米国および国際著作権法、ならびに米国および国際知的財産法で保護されています。Dell™、およびデルのロゴは、米国および/またはその他管轄区域における Dell Inc. の商標です。本書で使用されているその他すべての商標および名称は、各社の商標である場合があります。

2015 - 02

Rev. A00

目次

1 はじめに.....	6
システム要件.....	6
管理ステーションの必要条件.....	6
ストレージレイについて.....	6
関連マニュアル.....	7
デルへのお問い合わせ.....	8
マニュアルのフィードバック.....	8
2 ハードウェアの取り付け.....	9
ストレージ構成の計画.....	9
ストレージレイの接続.....	9
ストレージレイのケーブル接続.....	10
冗長および非冗長構成.....	10
直接接続構成.....	10
ネットワーク接続構成.....	13
リモートレプリケーション.....	14
混合環境.....	15
PowerVault MD3060e 拡張エンクロージャのケーブル接続.....	16
MD3060e 拡張のケーブル配線図.....	17
新しい PowerVault MD3060e 拡張エンクロージャでの拡張.....	18
3 MD Storage Manager のインストール.....	20
モジュラディスク設定ユーティリティ.....	21
グラフィカルインストール (推奨).....	21
コンソールインストール.....	22
サイレントインストール.....	22
Windows でのサイレントインストール.....	22
Linux でのサイレントインストール.....	23
プレミアム機能の有効化 (オプション).....	23
PowerVault MD ストレージマネージャのアップグレード.....	23
4 インストール後のタスク.....	24
作業を開始する前に.....	24
iSCSI の設定用語.....	24
iSCSI 設定ワークシート.....	25
ストレージレイの iSCSI の設定.....	25
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.....	26
接続確立後の手順.....	28

5 iSCSI 用のネットワーク設定のガイドライン	29
Microsoft Windows ホストのセットアップ.....	29
DHCP サーバーの使い方.....	29
静的 IP アドレスの使い方.....	29
DNS サーバーの使い方.....	30
WINS サーバーを使用する場合.....	30
Linux ホストのセットアップ.....	30
DHCP の使用.....	30
静的 IP アドレスの使い方.....	31
6 MD Storage Manager のアンインストール	32
Windows からの MD Storage Manager のアンインストール.....	32
Windows Server GUI バージョンからの MD Storage Manager のアンインストール.....	32
Windows Server Core バージョンからの MD Storage Manager のアンインストール.....	32
Linux からの MD Storage Manager のアンインストール.....	33
7 付録 – iSCSI の手動設定	34
手順 1: ストレージアレイを検出する（帯域外管理のみ）.....	34
管理ポートのデフォルト設定.....	34
ストレージアレイの自動検出.....	35
ストレージアレイの手動検出.....	35
アレイのセットアップ.....	35
手順 2: ストレージアレイの iSCSI ポートを設定する.....	36
手順 3 : iSCSI イニシエータからターゲットの検出を行う.....	37
Windows Server GUI バージョンの使用.....	37
Windows Server Core バージョンの使用.....	37
Red Hat Enterprise Linux 6 および SUSE Linux Enterprise Server 11 の場合.....	38
手順 4: ホストアクセスを設定する.....	38
CHAP 認証についての理解.....	39
CHAP について.....	39
ターゲット CHAP.....	39
相互 CHAP.....	39
CHAP の定義.....	39
手順 5: ストレージアレイの CHAP 認証を設定する（オプション）.....	40
ストレージアレイのターゲット CHAP 認証の設定.....	40
'ストレージアレイの相互 CHAP 認証の設定.....	41
手順 6 : ホストサーバーでの CHAP 認証の設定（オプション）.....	41
Windows GUI バージョンを使用したホストサーバーでの CHAP 認証の設定.....	41
Windows Server Core バージョンを使用したホストサーバーでの CHAP 認証の設定.....	42
Linux 6 および SUSE Linux Enterprise Server 11 を使用した CHAP 認証の設定.....	42
SUSE Linux Enterprise Server GUI を使用したホストサーバーでの CHAP 認証の設定.....	43


手順 7: ホストサーバーからターゲットストレージアレイに接続する.....	43
Windows Server GUI を使用したホストサーバーからのターゲットストレージアレイへの 接続.....	43
Windows Server Core バージョンを使用したホストサーバーからのターゲットストレージ アレイへの接続.....	44
Linux Server の場合.....	45
手順 8 : (オプション) 帯域内管理をセットアップする.....	45
8 付録 – インターネット記憶域ネームサービスの使用.....	47
9 負荷分散.....	48
負荷分散ポリシー.....	48
サブセット付きラウンドロビン.....	48
最小キュー深度.....	48
最小パス荷重.....	49
複数の iSCSI セッションによる帯域幅の拡大.....	49
VMware での負荷バランスポリシーの設定.....	49
10 付録 – Linux での iSCSI サービスの停止と開始.....	50
11 IPv4 の設定 – ワークシート.....	51
12 IPv6 の設定 – ワークシート.....	53

はじめに

本ガイドには、Dell PowerVault MD3860i ストレージレイの導入についての情報が記載されています。導入手順には次が含まれます。

- ハードウェアの取り付け
- Modular Disk Storage Manager (MD Storage Manager) 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、「[関連マニュアル](#)」を参照してください。

MD Storage Manager を使用することにより、管理者は最適な可用性のためにストレージレイを設定および監視することができます。PowerVault MD Series シリーズのリソースメディアに収録されている MD Storage Manager のバージョンは、PowerVault MD3860i Series およびその他 PowerVault MD Series ストレージレイ両方の管理に使用することができます。MD Storage Manager は、Microsoft Windows および Linux の両オペレーティングシステムとの互換性があります。

システム要件

PowerVault MD3860i Series ハードウェアの取り付けと設定、およびソフトウェアのインストールと設定を行う前に、対応オペレーティングシステムがインストールされおり、最小システム要件が満たされていることを確認してください。詳細については、dell.com/powervaultmanuals でサポートマトリッ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、ネットワーク全体のストレージレイを設定および管理するために MD Storage Manager を使用します。管理ステーション要件の詳細については、dell.com/powervaultmanuals でサポートマトリックスを参照してください。

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をストレージレイと呼びます。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、および電源装置などの様々なハードウェアコンポーネントが含まれます。

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。

ストレージアレイは、次で実行されている MD Storage Manager 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、MD Storage Manager とストレージアレイは帯域内接続または帯域外接続を使用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、MD Storage Manager はストレージア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アレイと通信します。イーサネット接続はアレイの接続を使って管理ステーションとストレージアレイ間で管理情報をやりとりします。

MD Storage Manager を使用することにより、ストレージアレイ内の物理ディスクをディスクグループおよびダイナミックディスクプール (DDP) と呼ばれる論理コンポーネントに構成し、それらのディスクグループを仮想ディスクに分割することができます。ディスクグループはストレージア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、ディスクグループまたは DDP 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、どの仮想ディスクにも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アレイ内の物理ディスクに書き込まれます。RAID レベルは、物理ディスクにデータが書き込まれる方法を定義します。異なる RAID レベルによって、異なるレベルのアクセス性、冗長性、および容量が提供されます。お使いのストレージアレイにある各ディスクグループと仮想ディスクには、特定の RAID レベルを設定することができます。RAID の使用およびストレージソリューション内でのデータ管理の詳細については、dell.com/powervaultmanuals にある『Dell PowerVault MD Series Storage Arrays Administrator's Guide』（Dell PowerVault MD シリーズストレージアレイ管理者ガイド）を参照してください。

関連マニュアル


-  **メモ:** PowerVault 向けの全マニュアルについては、dell.com/powervaultmanuals にアクセスし、システムのサービスタグを入力してお使いのシステムのマニュアルを入手してください。
-  **メモ:** すべての Dell OpenManage マニュアルは、dell.com/openmanagemanuals にアクセスしてください。
-  **メモ:** ストレージコントローラ向けの全マニュアルについては、dell.com/storagecontrollermanuals にアクセスしてください。

製品のマニュアルには次が含まれます。

- 『Dell PowerVault MD3460/MD3860i/MD3860f Storage Arrays Getting Started Guide』（Dell PowerVault MD3460/MD3860i/MD3860f ストレージアレイ - はじめに） – システム機能、システムのセットアップ、および技術仕様の概要を提供します。このマニュアルはお使いのシステムにも同梱されています。
- 『Dell PowerVault MD3860i Storage Arrays Owner's Manual』（Dell PowerVault MD3460 ストレージアレイオーナーズマニュアル） – システム機能についての情報が記載されており、システムのトラブルシューティング方法、およびシステムコンポーネントの取り付けまたは交換について説明されています。
- ラックの取り付け手順 – ラックへのシステムの取り付け方法が説明されています。この文書は、お使いのラックソリューションにも同梱されています。
- 『Dell PowerVault MD Series Storage Arrays Administrator's Guide』（Dell PowerVault MD Series ストレージアレイ管理者ガイド） – MDSM GUI を使用したシステムの設定および管理についての情報が記載されています。

- 『Dell PowerVault Modular Disk Storage Arrays CLI Guide』(Dell PowerVault Modular Disk ストレージレイ CLI ガイド) – MDSM CLI を使用したシステムの設定および管理についての情報が記載されています。
- 『Dell PowerVault MD3860i Storage Arrays Deployment Guide』(Dell PowerVault MD3460 ストレージアレイ導入ガイド) – SAN アーキテクチャでのストレージシステムの導入に関する情報が記載されています。
- 『Dell PowerVault MD Series Support Matrix』(Dell PowerVault MD Series サポートマトリクス) – ストレージアレイのためのソフトウェアおよびハードウェアの互換性マトリクスに関する情報が記載されています。

デルへのお問い合わせ

 **メモ:** 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。

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。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。デルのセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

dell.com/contactdell にアクセスします。

マニュアルのフィードバック

本マニュアルに対するフィードバックは、documentation_feedback@dell.com まで電子メールを送信してください。または、デルマニュアルページにある **Feedback** (フィードバック) リンクをクリックしてフォームに入力し、**Submit** (送信) をクリックしてフィードバックを送信していただくこともできます。

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。

- 『Dell PowerVault MD3460/MD3860i/MD3860f Storage Arrays Getting Started Guide』（Dell PowerVault MD3460/MD3860i/MD3860f ストレージアレイ - はじめに） - ストレージアレイに同梱の『Getting Started Guide』（はじめに）には、システムの初期セットアップの設定に関する情報が記載されています。
- 『Dell PowerVault MD Series Storage Arrays Administrator's Guide』（Dell PowerVault MD シリーズストレージアレイ管理者ガイド） - 管理者ガイドには、ストレージアレイを設定する前に理解する必要がある重要な概念についての情報が記載されています。詳細については、dell.com/powervaultmanuals を参照してください。
- ラック取り付け手順 - お使いのシステムのラック取り付け方法が説明されています。この文書は、システムに同梱されています。

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。
- データ編成計画に従って、仮想ディスク、ディスクグループ、および DDP 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 つ目を財務および税務情報に、3 つ目を顧客情報に使用します。
- 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。

ストレージアレイの接続

ストレージアレイは、2 個のホットスワップ対応 RAID コントローラモジュールを使用してホストに接続されています。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 0 および RAID コントローラモジュール 1 として識別されます。RAID コントローラモジュールのポートとそれらの機能は次のとおりです。

- 10 Gbps iSCSI 入力ホストポート (2) - イーサネット接続をホストまたはノードに提供します。
- 1 Gbps イーサネット管理 (MGMT) ポート (1) - 管理ポートは、ストレージアレイの帯域外管理を可能にします。
- 予約済みイーサネットポート (1) - 予約済みのポートです。
- 12 Gbps SAS 出力ポート (2) - 追加の SAS ホストポートです。

- SAS 拡張ポート (2) – ストレージ容量を追加するために、オプションの PowerVault MD3060e 拡張エンクロージャへのストレージアレイの接続を可能にします。1 度に使用できる SAS 出力拡張ポートは 1 個に限定されており、推奨される拡張ポートは、ポート 0 です。

各 PowerVault MD3860i Series ストレージアレイは、最大 2 台の PowerVault MD3060e Series 拡張エンクロージャを使用することにより、最大 120 台（プレミアム機能のアクティブ化で有効にする場合は 180 台）の物理スロットに拡張できます。

ストレージアレイのケーブル接続

iSCSI インタフェースによって、異なるホストとコントローラ間の設定が可能になります。本章の図では、以下のカテゴリによってグループ化されています。

- 直接接続構成（イーサネットスイッチ不使用）
- ネットワーク接続（SAN）構成（イーサネットスイッチ使用）

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ア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ア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、各パスはストレージアレイに取り付けられた 2 台の RAID コントローラモジュールのうちいずれか 1 台に設定されます。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、パスの障害イベント時におけるデータへのアクセス喪失からホストを保護します。

直接接続構成

ホストサーバーのイーサネットポートを、ストレージアレイの RAID コントローラモジュールの iSCSI ポートに直接接続することができます。

次の図は、シングルデータパスを持つデュアルコントローラアレイ構成でサポートされる 4 台のスタンドアロンホストを示します。

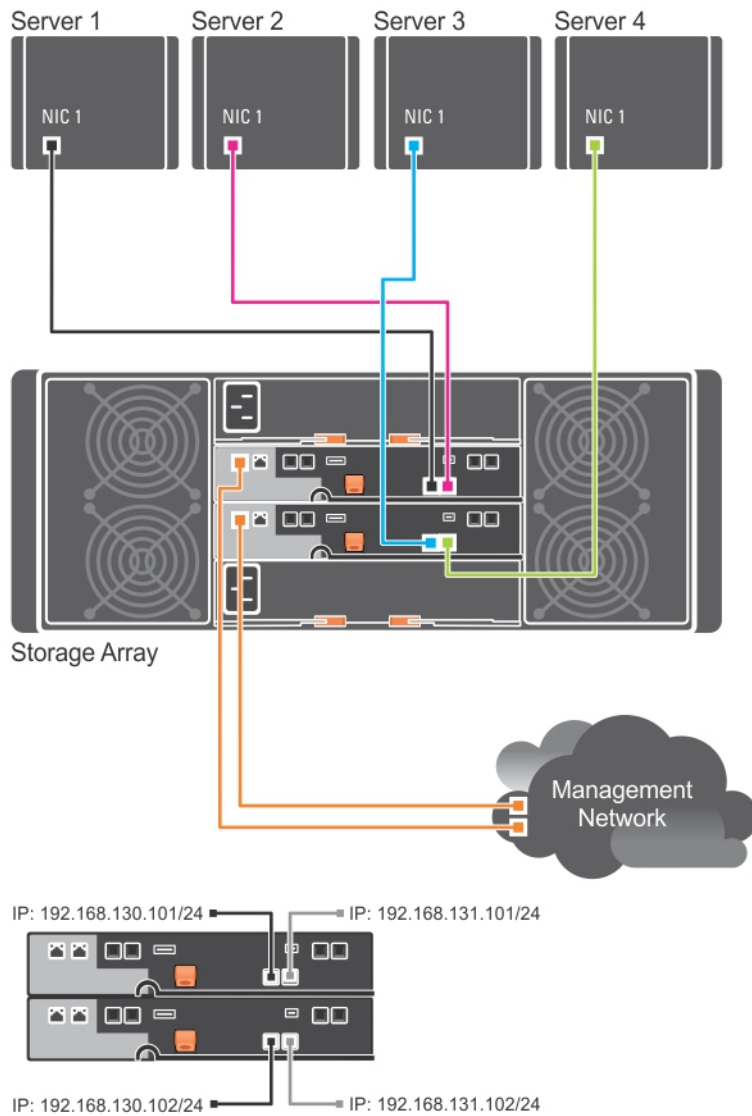


図 1. デュアルコントローラ構成の 4 台のホスト

次の図では、最大 2 台のサーバーが RAID コントローラモジュールに直接接続されています。ホストサーバーにアレイへの 2 つ目のイーサネット接続がある場合は、アレイの 2 番目のコントローラの iSCSI ポートに接続することができます。この構成によって、各ホストが 2 つの独立した物理パスを持つことになり、可用性が向上します。結果として、パスが 1 つ損失した場合でも冗長性を確保することができます。

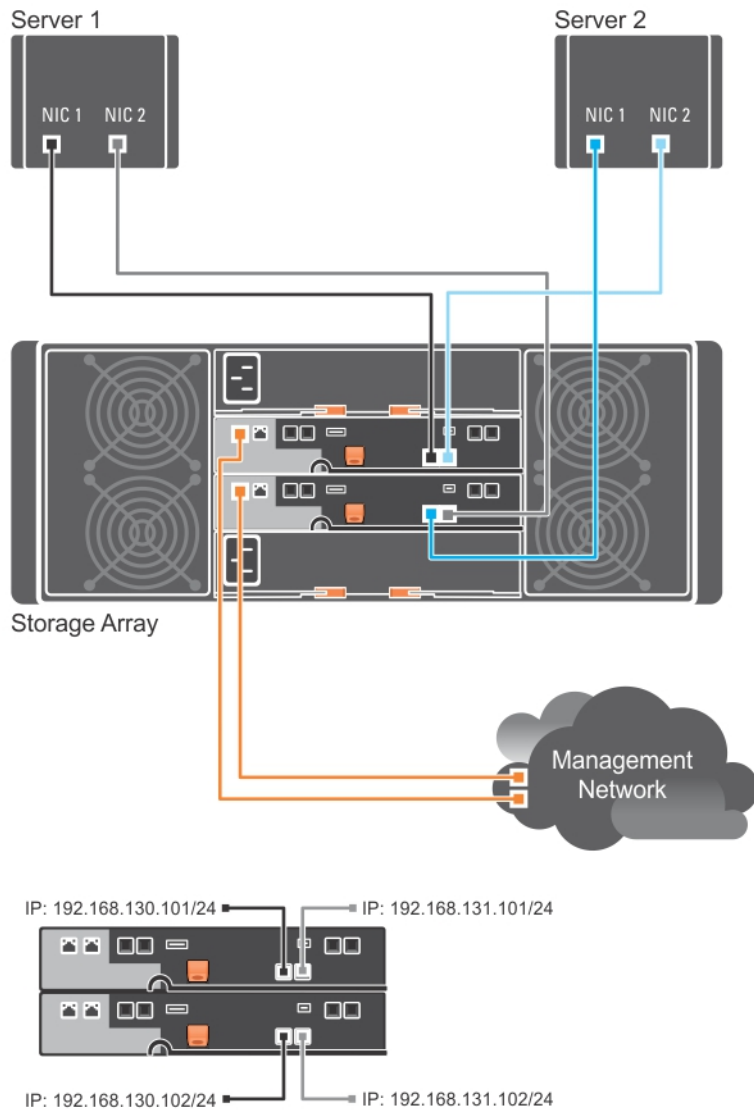


図 2. 2つのコントローラに接続された2台のホスト

次の図では、最大2台のクラスタノードが2台のRAIDコントローラモジュールに直接接続されています。各クラスタノードに冗長パスがあるため、単一のパスを損失しても、代替パス経由でストレージアレイに引き続きアクセスすることができます。

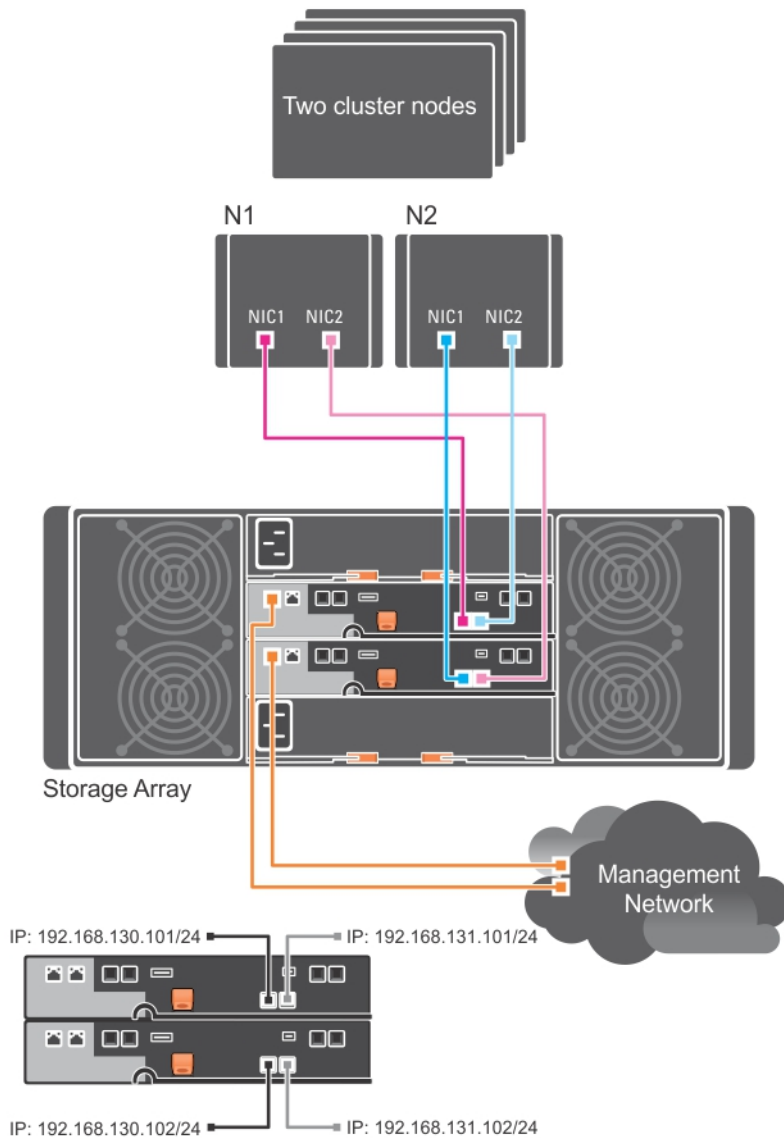


図 3. 2つのコントローラに接続された2つのクラスタノード

ネットワーク接続構成

業界標準の10GBイーサネットスイッチを介してホストサーバーをRAIDコントローラモジュールiSCSIポートにケーブル接続することもできます。イーサネットスイッチを使用するiSCSI設定は、しばしばIP SANと呼ばれます。IP SANを使用することにより、PowerVault MD3860i Seriesストレージレイは最大64個のホストを同時にサポートできるようになります。この設定は、シングルパスまたはデュアルパスのデータ設定のいずれか、およびシングルコントローラモジュールまたはデュアルコントローラモジュールのいずれかをサポートします。

次の図は、ネットワークを通じてデュアルRAIDコントローラモジュール構成に1 Gbps ~ 10 Gbpsアグリゲーションスキームを使用して接続された（複数のセッションを使用）最大で64台のスタンダードアロンサー

バーを示しています。サーバーの NIC は、1 Gbps の NIC になっており、1 Gbps スイッチのアップリンクポートは、10 Gbps となっています。ホストがネットワークへの 2 つめのイーサネット接続を有することによって、各ホストへ 2 つの独立した物理パスがあることになり、1 つのパスに障害が発生した場合でも、冗長性を確保することができます。多くの冗長性を確保するため、2 つのスイッチの使用が推奨されていますが、1 つのスイッチでの構成もサポートされています。

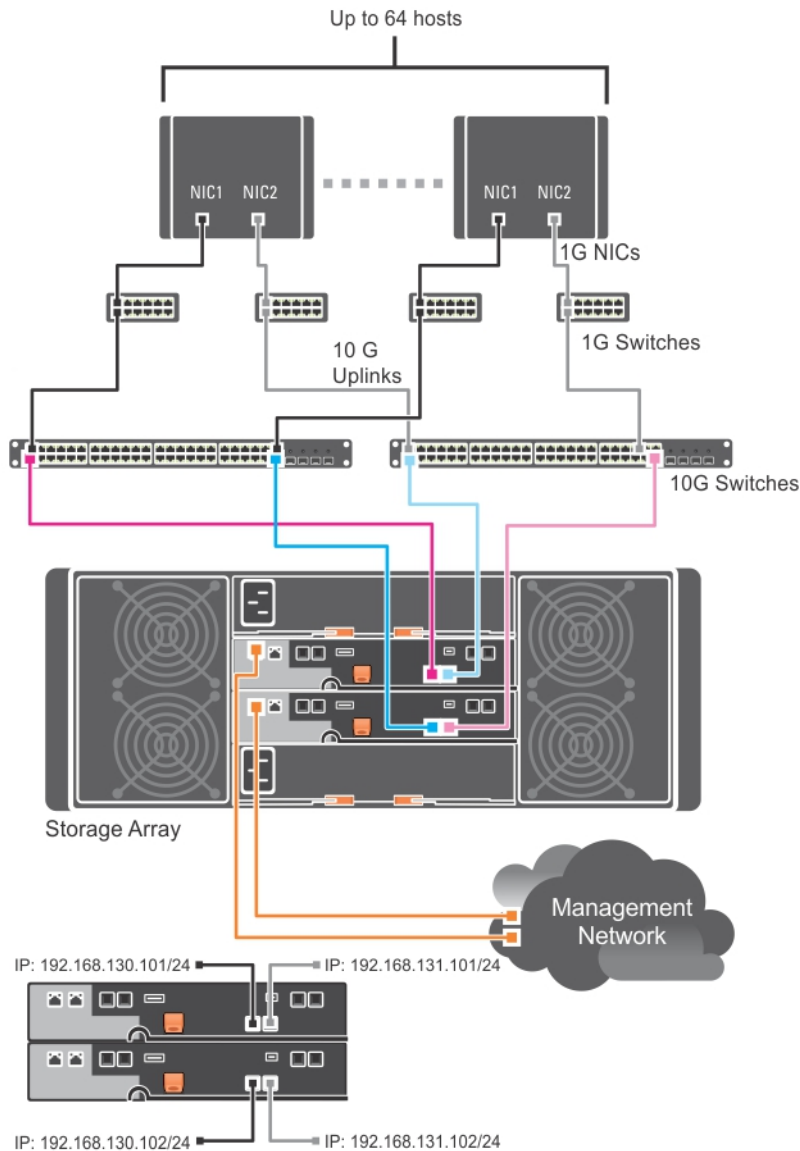


図 4. 2 つの RAID コントローラに接続された 64 台のサーバー

リモートレプリケーション

リモートレプリケーションとは、ストレージレイ間のデータのリアルタイムレプリケーションをオンラインで提供するストレージレイプレミアム機能です。次の図は、リモートレプリケーション環境のセットアップ方法の一例を示しています。リモートレプリケーションの詳細については、dell.com/

powervaultmanuals で、『Dell PowerVault MD Series Administrators Guide』（Dell PowerVault MD シリーズ管理者ガイド）を参照してください。

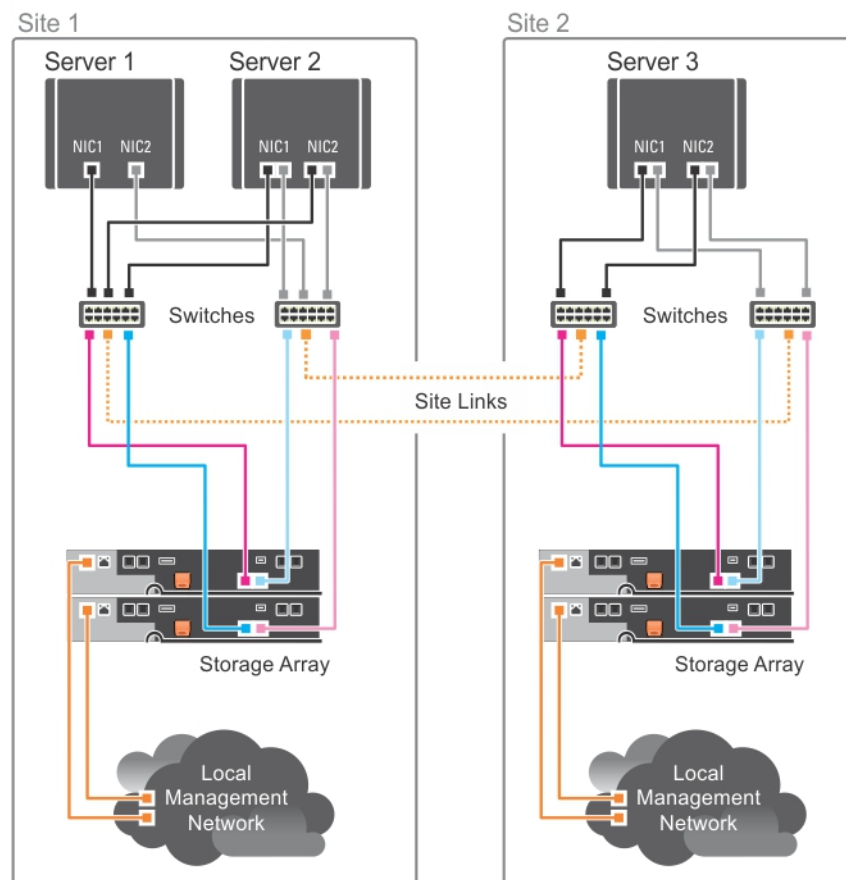
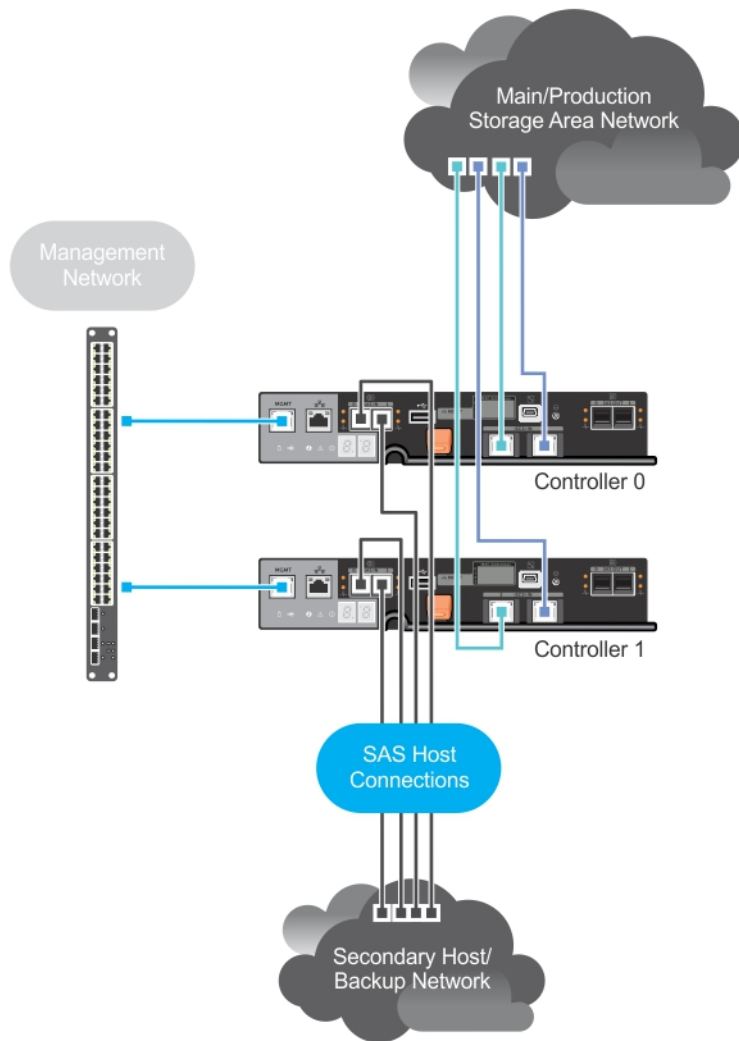


図 5. リモートレプリケーション環境

混合環境

次の図は、ひとつのホストへの SAS 経由の直接接続、直接接続 iSCSI または IP SAN 経由の別のホストへの接続がある混在構成を示しています。

図 6. 混合環境



PowerVault MD3060e 拡張エンクロージャのケーブル接続

PowerVault MD3060e 拡張エンクロージャを追加することにより、PowerVault MD3860i シリーズのストレージアレイの容量を拡張することができます。物理ディスクドライブプールは、最大 2 台の拡張エンクロージャを使用することにより、最大で 120 台（プレミアム機能のアクティブ化で有効にする場合は 180 台）の物理ディスクドライブに拡張することができます。

お使いの MD シリーズ高密度 RAID ストレージアレイに MD3060e 拡張エンクロージャを接続するには、次の図を参照してください。

MD3060e 拡張のケーブル配線図

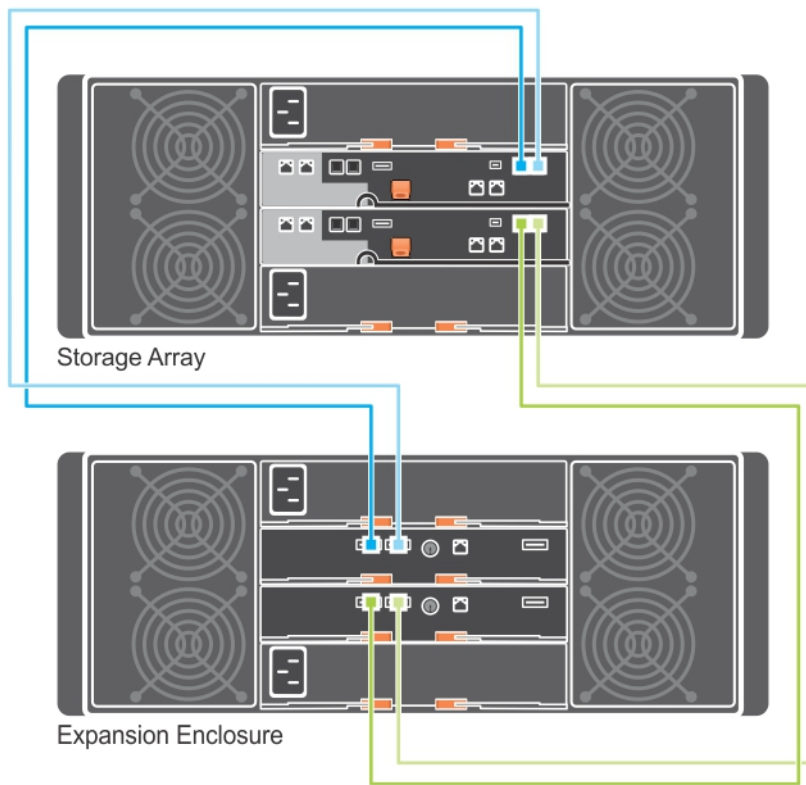


図 7. シングル拡張のダイアグラム

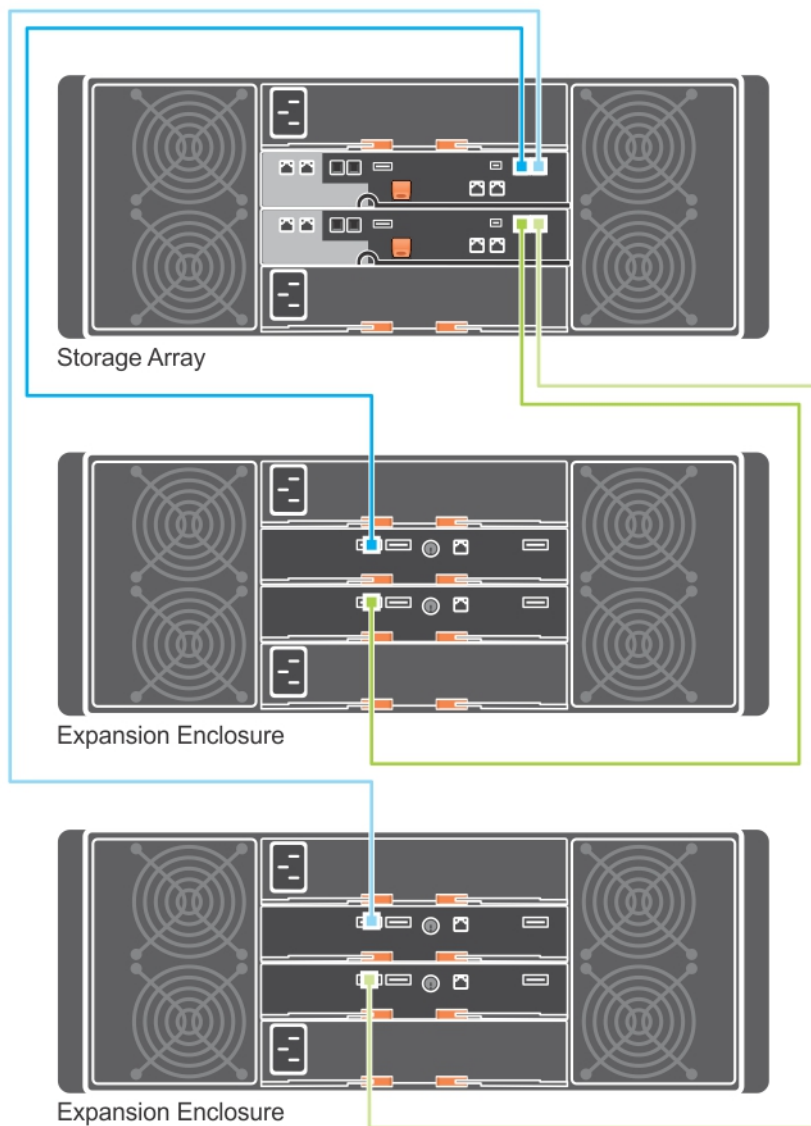


図 8. デュアル拡張のケーブル配線図

新しい PowerVault MD3060e 拡張エンクロージャでの拡張

メモ: MD3060e 拡張エンクロージャのホットプラグは推奨されません。アレイエンクロージャの電源を入れる前に、すべての MD3060e 拡張エンクロージャに電源を入れてください。PowerVault MD Series に役立つビデオ、およびその他のリソースについては、dell.com/PVresources を参照してください。

新しい PowerVault MD3060e 拡張エンクロージャを PowerVault MD3860i シリーズストレージアレイに接続するには、次の手順を実行してください。

1. 拡張エンクロージャを追加する前に、ストレージア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/powervaultmanuals のサポートマトリックスを参照してください。

2. 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に関する詳細は、「[MD Storage Manager のインストール](#)」を参照してください。
3. **MD Storage Manager** を使用して、RAID コントロールモジュールファームウェアおよび NVSRAM を dell.com/support で入手可能な最新バージョンにアップデートします。
4. アップデートするアレイエンクロージャを選択して、**Enterprise Management Window (EMW)** から **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** の順にクリックします。
5. ストレージアレイに対するすべての I/O 処理を停止し、ストレージア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。
6. ストレージアレイの電源を切ります。
7. 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。
8. 拡張エンクロージャをストレージアレイにケーブルで接続します。正しいケーブル配線図については、本ガイド前半にある「PowerVault MD3060e 拡張エンクロージャのケーブル配線」の項を参照してください。
9. 拡張エンクロージャの電源を入れ、エンクロージャのステータス LED が青色になるまで待ちます。
10. ストレージアレイの電源を入れ、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。
 - 電源が入っている場合は、電源インジケータライトが緑色に点灯します。
 - サービスアクション必須インジケータライトが橙色に点灯した場合、PowerVault Modular Disk Storage Manager を使用してエラーを表示することができます。
11. ストレージアレイがオンラインで準備完了状態になったら、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。
12. **PowerVault MD Storage Manager** 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。
13. 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。
14. **アレイ管理ウィンドウ** から、**アップグレード → EMM ファームウェア** の順に選択します。
15. **すべて選択** をクリックし、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。
16. **開始** をクリックします。


MD Storage Manager 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、ソフトウェアへの変更、アップデート、修正、パッチ、および Linux と Windows オペレーティングシステムの両方に適用されるその他の重要なデータが説明されている **readme.txt** ファイルが含まれています。**readme.txt** ファイルには、文書にアクセスするための要件、メディア上にあるソフトウェアバージョンに関する情報、およびソフトウェアを実行するためのシステム要件も記載されています。


 **注意:** MD Storage Manager によってアクティブに管理されている仮想ディスクのみに MD Storage Manager をインストールしないでください。代わりに、SMagent および SMmonitor を実行しているローカルディスクに MD Storage Manager のインスタンスを最低 1 つインストールします。管理ソフトウェアを仮想ディスクにのみインストールすると、複数の物理ディスクやエンクロージャに障害が発生した場合に、リカバリ情報へのアクセスが妨げられる場合があります。


Dell PowerVault システム向け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/powervaultmanuals でサポートマトリックスを参照してください。


 **メモ:** アレイを管理するための第一段階として、MD Storage Manager のアップデートとインストールには常に MD Storage Resource DVD メディアを使用してください。最新アップデートおよびサポートマトリックスについては、dell.com/powervaultmanuals を参照してください。

PowerVault MD3860i Series ストレージファームウェアインストーラは、コアソフトウェアおよびプロバイダを含む機能を提供します。コアソフトウェア機能には、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、およびストレージアレイソリューションの設定、管理、監視に使用する MD Storage Manager アプリケーションが含まれています。プロバイダ機能には、Microsoft Virtual Disk Service (VDS) のプロバイダおよび Microsoft Volume Shadow-Copy Service (VSS) フレームワークがあります。

 **メモ:** Microsoft VDS および Microsoft VSS プロバイダの詳細については、dell.com/powervaultmanuals で管理者ガイド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。

 **メモ:** DHCP (Dynamic Host Configuration Protocol) を使用しない場合、管理ステーションの初期設定は、ストレージアレイと同じ物理サブネット上で行う必要があります。さらに、初期設定中は、少なくとも 1 つのネットワークアダプタをストレージアレイのデフォルト管理ポート (コントローラ 0 MGMT (ポート 0) : 192.168.128.101 またはコントローラ 1 MGMT (ポート 0) : 192.168.128.102) と同じ IP サブネットに設定する必要があります。初期設定の後、管理ポートは MD Storage Manager を使用して設定し、管理ステーションの IP アドレスを以前の設定に戻すことができます。

 **メモ:** 1 つのアレイにつき、2 つの管理ポート (ポート 0) のみがサポートされています。各コントローラの 2 番目のポートは予約済みです。

PowerVault MD シリーズのリソースメディアでは、次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) – 推奨インストール手順です。インストーラには、インストールするコンポーネントのカスタム化を可能にするグラフィカルウィザード駆動のインタフェースが表示されます。
- コンソールインストーラー – 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ラー – 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。

モジュラディスク設定ユーティリティ


PowerVault MD Configuration Utility (MDCU) は、iSCSI モジュラディスクストレージレイの管理ポートと iSCSI ホストポートの設定、およびセッション作成に対する統合されたアプローチを提供します。ストレージレイに接続されている各ホストサーバーでの iSCSI の設定には PowerVault MDCU の使用をお勧めします。

グラフィカルインストール (推奨)

MD Storage Manager で、ストレージレイを設定、管理、監視します。MD Storage Manager をインストールするには、次の手順に従います。

1. PowerVault MD シリーズリソースメディアを挿入します。

オペレーティングシステムによって異なりますが、インストーラは自動的に起動することがあります。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のルートディレクトリ (またはダウンロードしたインストーライメージ) に移動し、**md_launcher.exe** ファイルを実行します。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:** Red Hat Enterprise の Linux は、デフォルトではリソースメディアを **-noexec** のマウントオプションでマウントするため実行可能ファイルを実行することができません。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で **Readme** ファイルを参照します。

2. MD Storage 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)** – MD Storage Manager (クライアント) ソフトウェア、MD Configuration Utility (MDCU) ホストベースストレージエージェント、マルチパスドライバ、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パスドライバをインストールします。「MD Storage Manager のインストール」を参照してください。
- **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。


 **メモ:** MD Storage Manager をネットワークやサーバーに接続されていない管理ステーションにインストールすると、**管理ステーション** オプションのみが使用可能になります。

5. ホストサーバーの再起動時にイベント監視サービスを手動で開始するか自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。

6. 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。
7. インストールの完了後、プロンプト表示に従ってホストサーバーを再起動します。
8. 再起動の完了時に MDCU が自動的に開始されない場合は、手動で開始します。
 - a. Windows ベースのオペレーティングシステムでは、**スタート → Dell → Modular Disk Configuration Utility** の順にクリックします。
 - b. Linux ベースのオペレーティングシステムでは、デスクトップの **Modular Disk Configuration Utility** アイコンをダブルクリックします。
9. iSCSI イニシエータを確立します。
10. **MD Storage Manager** を起動してアレイを検出します。


 **メモ:** PowerVault MD ストレージアレイの管理ポートが接続されているネットワークで Dynamic Host Configuration Protocol (DHCP) が使用されていない場合、ストレージアレイを検出するために管理ステーションで IPv6 を有効にすることをお勧めします。

 **メモ:** 自動検出によって新しいアレイが検出されない場合、手動オプションを使用して、同じサブネット、または同じ VLAN を使って MD Storage Manager 管理ステーション用にデフォルト管理ポート IP アドレス、Controller 0 MGMT (port 0) : 192.168.128.101 または Controller 1 MGMT (port 0) : 192.168.128.102、を入力します。

11. 必要に応じて、ストレージアレイと同時に購入したプレミアム機能を有効にします。プレミアム機能を購入した場合は、ストレージアレイに同梱されている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** インストーラは、お使いのストレージアレイを動作させるために必要なドライバ、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的に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。これに加えて、ユーザー固有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、dell.com/powervaultmanuals でサ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 での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、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た後、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.bin -f <host_server_path>/custom_silent.properties
```

Linux でのサイレントインストール

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 **/linux** ディレクトリにある **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、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た後、ファイルを保存します。
3. **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
```

プレミアム機能の有効化（オプション）


プレミアム機能をご注文いただいた場合、プレミアム機能カードの手順に従って追加の機能をインストールします。

PowerVault MD ストレージマネージャのアップグレード


以前のバージョンの PowerVault MD Storage Manager からのアップグレードには、古いバージョンをアンインストール（[Windows からの MD Storage Manager のアンインストール](#)を参照）してから、[MD Storage Manager のインストール](#)」の指示に従って新しいバージョンをインストールします。

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一連の初期設定タスクを完了してください。以下のタスクは、MD Storage Manager を使用して実行します。

-  **メモ:** DHCP (Dynamic Host Configuration Protocol) を使用しない場合、ストレージレイと同じ物理サブネット上で管理ステーションを使用した初期設定を行う必要があります。さらに、初期設定中、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 (Controller 0 MGMT (port 0) : 192.168.128.101, Controller 1 MGMT (port 0) : 192.168.128.102) と同じ IP サブネット上で設定する必要があります。初期設定後、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 を設定する前に、本文書にある IPv4 または IPv6 iSCSI 設定ワークシートに記入することをお勧めします。設定作業を開始する前に、お使いのネットワークのこれらの情報を収集することによって、作業をより効率的に完了させることができます。

iSCSI の設定用語

表 1. iSCSI の設定で使用される標準的な用語

用語	定義
チャレンジハンドシェイク認証プロトコル (CHAP)	ホストサーバーとストレージレイ両方の iSCSI データポートの使用を制限することにより、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です。サポートされる CHAP 認証の種類については、 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 ポートを経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	ストレージレイ上の iSCSI ポート (各コントローラに 2 個)。
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。
iSCSI ホストポート	ストレージレイ上の iSCSI ポート (各コントローラに 2 個)。
iSNS (Microsoft Internet Storage Naming Service)	一部の iSCSI デバイスで使用される、検出、管理、設定を自動化するストレージネームサービスツール。

用語	定義
管理ステーション	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。
フロー制御	データの転送を一時的に停止するメカニズム。

iSCSI 設定ワークシート

[IPv4 設定 – ワークシート](#) および [IPv6 設定 – ワークシート](#) は、設定作業に役立ちます。ホストサーバーおよびストレージアレイの IP アドレスを一箇所に記録しておくことにより、その後の設定をよく早く効率的に行うことができます。

「[iSCSI 用ネットワーク設定のガイドライン](#)」には、Windows および Linux 環境での一般的なネットワーク設定に関するガイドラインが記載されています。ワークシートに記入する前に、ガイドラインの内容を確認するようお勧めします。


ストレージアレイの iSCSI の設定

次の項では、ストレージアレイ上での iSCSI の設定が順番に説明されています。作業を始める前に、お使いのホストサーバーまたはストレージアレイの環境では各手順をどこで行うかを理解することが重要です。


以下の表には、iSCSI 設定の具体的な各手順とそれをどこで行うのかが示されています。

表 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
	手順 1: ストレージアレイを検出する
	手順 2: ストレージアレイの iSCSI ポートを設定する
手順 3: iSCSI イニシエータからターゲットの検出を行う	
	手順 4: ホストアクセスを設定する
	手順 5: (オプション) ストレージアレイの CHAP 認証を設定する
手順 6: (オプション) ホストサーバーの CHAP 認証を設定する	
手順 7: ホストサーバーからストレージアレイに接続する	
	手順 8: (オプション) 帯域内管理をセットアップする

-  **メモ:** iSCSI の設定では、MDCU (PowerVault Modular Disk Configuration Utility) の使用が推奨されています。PowerVault MDCU ウィザードが、上で説明された設定手順のガイドとなります。手動での設定を行う場合は、「[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:** PowerVault MDCU がインストールされていない場合は、PowerVault 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。

PowerVault MDCU は、ウィザード方式のインタフェースを使用して、ホストサーバーの iSCSI ネットワークおよび iSCSI ベースのストレージレイの設定に対する総合的なアプローチを提供します。また、このユーティリティによって、ユーザーはホストサーバーの iSCSI セッションをベストプラクティスに基づいて設定し、ストレージレイの iSCSI ホストポートで、負荷バランスの取れたパスを確保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 の起動** を選択した場合は、ユーティリティは次のホストサーバーの再起動後に自動的に起動します。または、このユーティリティを手動で起動させることもできます。

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。

PowerVault MDCU の機能は次のとおりです。

- ストレージレイの設定
- 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間で通信するためには、IP アドレスや認証方法などの情報を使用して設定を行う必要があります。iSCSI イニシエータは、設定済みのストレージレイとの接続を行うため、最初にストレージレイを iSCSI イニシエータが使用できるよう設定する必要があります。このユーティリティでは、設定する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。的確に機能しているネットワークのインフラを確保してから、ストレージレイの設定を行います。ストレージレイの設定が既に完了している場合は、手順を省略して直接ホスト設定に進むことができます。

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. 2以降の手順を繰り返して追加レイを設定する。

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完了したら、次のタスクは、このユーティリティをストレージアクセスへのアクセスが必要なすべてのホストで実行します。ネットワークの設定により異なりますが、お使いのホストは、ストレージレイを管理するのに使用するのと同じマシンであるか、全く別のネットワーク上にあるマシンである場合があります。

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、ホストを設定できるオプションは無効になっています。オプションが

無効になっていることを告げるメッセージもユーティリティで表示されます。iSCSI ベースのストレージアレイに接続されていないホストでユーティリティを実行している場合 (またはアレイに接続したくない場合) は、メッセージを無視してください。

このタスクには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アレイを検出する。
2. ストレージアレイを選択する。
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 からの手順を繰り返す。
6. ストレージア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

ストレージアレイやホスト接続の設定を開始する前に、設定の計画に役立つ iSCSI 設定ワークシートを作成することをお勧めします。お使いの設定により、ワークシートを複数使用することもできます。

ストレージア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のため、ネットワーク設定が有効であることを確認します。 dell.com/powervaultmanuals でストレージアレイのサポートマトリッ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フェースがある場合、各ネットワークインタ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フェースが両方のストレージア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。
- 最適な負荷分散を行うため、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フェースが、各ストレージア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フェースが、ストレージアレイコントローラ 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フェースおよびストレージアレイの 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。

PowerVault MDCU を使用したストレージアレイの設定

PowerVault MDCU を使用して iSCSI ベースのストレージア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ア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 では、**スタート → すべてのプログラム → Dell → MD Storage ソフトウェア → モジュール ディスク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て **PowerVault MDCU** を実行します。

MDCU は、利用可能なすべてのストレージアレイ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 ストレージアレイを選択します。
3. **選択されたアレイ** ウィンドウで、現在のポートおよびセッションの情報を確認します。
4. **設定ウィザード** をクリックして、iSCSI 設定ウィザードを開始します。
5. **設定ウィザード** の手順を実行して 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、設定内容を確認し、適用します。

7. **iSCSI セッションの確立** をクリックして、ホストとストレージアレイ間の通信を確立します。
実行するすべてのホストとアレイ間のマッピングで同じ手順を繰り返します。
8. ストレージアレイとホストサーバー間の通信が確立されているのを確認します。


 **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。ストレージ計画と MD Storage Manager の使用の詳細については、dell.com/powervaultmanuals で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

本項には、ネットワーク環境の構築およびホストサーバーとストレージアレイの iSCSI ポートで使用する IP アドレスの設定に必要なガイドラインが記載されています。特定のネットワーク環境には、ここに示される手順とは異なる手順や追加の手順が必要なことがあるため、システム管理者の指示を受けてからこのセットアップを実行してください。

 **メモ:** お使いのネットワークコンポーネントすべてでフロー制御が有効になっていることを確認してください。

Microsoft Windows ホストのセットアップ

Windows ホスト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されている各 iSCSI ポートの IP アドレスおよび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 (Dynamic Host Configuration Protocol) サーバー、静的 IP アドレス方式、DNS (Domain Name System) サーバーまたは WINS (Windows Internet Name Service) サーバーのいずれを使用しているかにより異なります。

 **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 サーバーの使い方

DHCP サーバーを使用する場合：

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 アドレスの使い方

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. **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 サーバーの使い方

静的 IP アドレス指定を使用する場合：

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. **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場合


静的 IP アドレス指定を使用する場合：

 **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. **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。

Linux ホストのセットアップ

Linux のホストネットワークを設定するには、ストレージアレイに接続されている各 iSCSI ポートの IP アドレスおよび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 で TCP/IP を設定するか、静的 IP アドレスで TCP/IP を設定するかにより異なります。

 **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 の使用

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. 設定ファイルを目的の接続に合わせて編集します（Red Hat Enterprise Linux の場合は **/etc/sysconfig/network-scripts/ifcfg-ethX**、SUSE Enterprise Linux の場合は **/etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX**）。

BOOTPROTO=dhcpm

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 アドレスの使い方

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. 設定ファイルを目的の接続に合わせて編集します (Red Hat Enterprise Linux の場合は **/etc/sysconfig/network-scripts/ifcfg-ethX**、SUSE Enterprise Linux の場合は **/etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX**)。

```
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
```

MD Storage Manager のアンインストール

Windows からの MD Storage Manager のアンインストール

Microsoft Windows Server から Modular Disk Storage Manager をアンインストールするには、次の手順を実行します。

1. コントロールパネル から **プログラムの追加または削除** をダブルクリックします。
2. プログラムの一覧から **Dell MD Storage ソフトウェア** 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 GUI バージョンからの MD Storage Manager のアンインストール

Windows Server GUI バージョンから Modular Disk Storage Manager をアンインストールするには、次の手順を実行します。

1. コントロールパネル から **プログラム** → **プログラムと機能** をダブルクリックします。
プログラムのアンインストールまたは変更 ウィンドウが表示されます。
2. プログラムの一覧から、**MD Storage ソフトウェア** を選択し、右クリックします。
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。

Windows Server Core バージョンからの MD Storage Manager のアンインストール

Windows Server Core バージョンから PowerVault Modular Disk Storage Manager をアンインストールするには、次の手順を実行します。

1. **Dell\MD Storage Software\Uninstall Dell MD Storage Software** ディレクトリに移動します。
 **メモ:** デフォルトで、MD Storage Manager は **\Program Files(x86)\Dell\MD Storage Software** ディレクトリにインストールされています。インストール中に別のディレクトリを使用した場合は、そのディレクトリに移動してからアンインストールを開始します。
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。
`Uninstall Modular Disk Storage`

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 Manager のアンインストール

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。インストール中に別のディレクトリを使用した場合は、そのディレクトリに移動してからアンインストールを開始します。

1. 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。
2. **Uninstall Dell MD Storage Software.exe** ファイルを実行します。
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。
ソフトウェアのアンインストール中に、**アンインストール ウィンドウ**が表示されます。アンインストール作業が完了すると、**アンインストール完了** ウィンドウが表示されます。
4. **完了** をクリックします。

付録 – iSCSI の手動設定

次の項では、ストレージレイ上での iSCSI の設定が順番に説明されています。作業を始める前に、お使いのホストサーバーまたはストレージレイの環境では各手順をどこで行うかを理解することが重要です。

以下の表には、iSCSI 設定の具体的な各手順とそれをどこで行うのかが示されています。


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レイで行う手順
	手順 1: ストレージレイを検出する
	手順 2: ストレージレイの iSCSI ポートを設定する
手順 3: iSCSI イニシエータからターゲットの検出を行う	
	手順 4: ホストアクセスを設定する
	手順 5: (オプション) ストレージレイの CHAP 認証を設定する
手順 6: (オプション) ホストサーバーの CHAP 認証を設定する	
手順 7: ホストサーバーからストレージレイに接続する	
	手順 8: (オプション) 帯域内管理をセットアップする


手順 1: ストレージレイを検出する (帯域外管理のみ)


管理ポートのデフォルト設定

ストレージレイの管理ポートは、デフォルトで DHCP (Dynamic Host Configuration Protocol) に設定されています。お使いのストレージレイ上のコントローラが、DHCP サーバーから IP 設定を取得できない場合は、10 秒後にタイムアウトし、デフォルトの静的 IP アドレスにフォールバックします。デフォルトの IP 設定は次の通りです。

```
Controller 0, MGMT (port 0): IP:192.168.128.101 Subnet Mask: 255.255.255.0
Controller 1, MGMT (port 0): IP:192.168.128.101 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 を使用しない場合、ストレージアレイと同じ物理サブネット上で管理ステーションを使用した初期設定を行う必要があります。さらに、初期設定中、少なくとも1つのネットワークアダプタをストレージアレイのデフォルト管理ポート (Controller 0 MGMT (port 0) : 192.168.128.101 または Controller 1 MGMT (port 0) : 192.168.128.102) と同じ IP サブネット上で設定する必要があります。管理ステーションの IP アドレスは、初期設定後 (管理ポートが PowerVault MD Storage Manager を使用して設定されます) 以前の設定に戻すことができます。

 **メモ:** この手順は、帯域外管理にのみ適用されます。帯域内管理の設定を選択する場合は、この手順を完了してから「[手順 8: 帯域内管理の設定 \(オプション\)](#)」を参照してください。

ストレージアレイの検出は自動でも手動でも可能です。

ストレージアレイの自動検出


1. **MD Storage Manager** を起動します。

これが最初にセットアップする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。

検出が完了したら、確認画面が表示されます。検出プロセスが完了するまで数分かかる場合があります。検出プロセスが完了する前に、検出の状態ウィンドウを閉じると、検出プロセスがキャンセルされます。

3. **閉じる** をクリックして、画面を閉じます。

 **メモ:** ファイアウォールのポート 3260 が、アレイ検出用に開いていることを確認します。

ストレージアレイの手動検出

1. **MD Storage Manager** を起動します。

これが最初にセットアップする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. **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 ストレージア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。

5. 検出が完了した後、確認画面が表示されます。**閉じる** をクリックして画面を閉じます。

 **メモ:** ファイアウォールのポート 3260 が、アレイ検出用に開いていることを確認します。

アレイのセットアップ

 **メモ:** ストレージア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、ストレージアレイ内のエンクロージャが **最適状態** 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/powervaultmanuals で管理者ガイドを参照してください。

1. 検出が完了すると、検出された最初のストレージアレイの名前が MD Storage Manager 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アレイのデフォルト名は、**名前なし** となっています。別の名前が表示された場合は、名前の横にある下矢印ボタンをクリックして、ドロップダウンリストから **名前なし** 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、残っているインストール後タスクへのリンクを表示します。各タスクの詳細については、dell.com/powervaultmanuals で管理者ガイドを参照してください。これらのタスクは、次の表に示される順序で実行します。

タスク	目的
ストレージレイの名前を変更します。	ソフトウェアによって割り当てられた名前なし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を設定します。	不正なアクセスを防ぐために、MD Storage Manager は、設定を変更する前、または破壊的な操作を行う前にパスワードを求めます。
アラート通知をセットアップします。 電子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 ポートを設定する


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)。

コントローラ 0、ポート 0: IP: 192.168.130.101 サブネットマスク: 255.255.255.0 ポート: 3260
 コントローラ 0、ポート 1: IP: 192.168.131.101 サブネットマスク: 255.255.255.0 ポート: 3260
 コントローラ 1、ポート 0: IP: 192.168.130.102 サブネットマスク: 255.255.255.0
 ポート: 3260
 コントローラ 1、ポート 1: IP: 192.168.131.102 サブネットマスク: 255.255.255.0
 ポート: 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. MD Storage Manager から、AMW の **セットアップ** タブに移動します。イーサネット管理ポートの設定をクリックして、**iSCSI ホストポートの設定** を選択します。
2. ストレージレイの 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) サポート – VLAN は、それぞれが同じローカルエリアネットワーク (LAN) のセグメントに接続されているかのように機能する異なるシステムのネットワークで、同じスイッチおよびルーターでサポートされています。VLAN として設定されると、デバイスは、再設定をすることなく別の場所に動かすことができます。ストレージレイで、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、ここに入力します。
- 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

 **メモ:** iSNS サーバーの TCP リスニングポートは、ストレージレイコントローラが iSNS サーバーに接続するのに使用するポート番号です。これにより iSNS サーバーが iSCSI ターゲットおよびストレージレイのポータルを登録し、ホストサーバーのイニシエータが認識できるようになります。


- ジャンボフレーム – 最大送信単位 (MTU) が 1 フレームにつき 1500 バイトを超えると、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できます。
3. 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。
 4. すべての iSCSI ストレージレイポートの設定が完了したら、**OK** をクリックします。
 5. 各 iSCSI ストレージレイポートの接続をテストします。

手順 3 : iSCSI イニシエータからターゲットの検出を行う

この手順では、ホストサーバーへのストレージレイ上で、iSCSI ポートを識別します。以下のセクション (Microsoft Windows または Linux) からお使いのオペレーティングシステムに合った手順を選択します。

Windows Server GUI バージョンの使用

1. **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** の順にクリックします。
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** – 接続元となるホストサーバーのソース 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ため、転送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 がすでに設定されている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き、この時点ではこのオプションを未選択のままにしておき、CHAP 情報は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 認証を設定する予定の場合は、この時点で複数の iSCSI ポートで検出を行わないでください。「ホストアクセスの設定」を参照してください。
 - 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 ~ 6 を繰り返します。

Windows Server Core バージョンの使用

1. `sc\< server_name >config msiscsi start=auto` を使用して、iSCSI イニシエータサービスが自動的に開始されるように設定します。
2. `sc start msiscsi` を使用して iSCSI サービスを開始します。

3. `iscsictl QAddTargetPortal <IP_address_of_iSCSI_port_on_storage_array>` を使用して、ターゲットポータルを追加します。

Red Hat Enterprise Linux 6 および SUSE Linux Enterprise Server 11 の場合

Red Hat Enterprise Linux 6 および SUSE Linux Enterprise Server 11 ディストリビューション向けの iSCSI イニシエータの設定は、MD Storage Manager のインストール時にデフォルトでインストールされる `/etc/iscsi/iscsid.conf` ファイルを変更することによって行います。ファイルディレクトリの編集、またはデフォルトファイルの PowerVault MD Series リソースメディアに含まれているサンプルファイルへの置き換えを行うことができます。

リソース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` ファイルに任意の別名を付けて保存します。
2. 適切なサンプルファイルをメディアの `/linux/etc` から `/etc/iscsi/iscsid.conf` にコピーします。
3. サンプルファイルの名前を `iscsid.conf` に変更します。
4. `/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` の行を変更するか、無効になっていることを確認します。
 - b. `node.startup = automatic` の行を変更するか、有効になっていることを確認します。
これで、起動時にサービスが自動的に開始します。
 - c. 次のコマンドを実行して、タイムアウト値が 30 に設定されているか確認します。
`node.session.timeo.replacement_timeout = 30`
 - d. `/etc/iscsi/iscsid.conf` ファイルを保存して閉じます。
5. コンソールから、次のコマンドを実行して iSCSI サービスを再開します。
`service iscsi start`
6. 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`
7. 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>`
8. 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。
9. 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: ホストアクセスを設定する

この手順では、ストレージレイの仮想ディスクにアクセスするホストサーバーを特定します。次の状態でこの手順を実行します。

- 仮想ディスクをホストサーバーにマップする前
 - ストレージレイに新しいホストサーバーを接続した際に毎回
1. MD Storage Manager 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. 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かを選択します。ホストが Microsoft クラスタの一部である場合のみ、**はい** を選択します。
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かどうかを指定します。
9. **終了** をクリックします。

CHAP 認証についての理解

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、CHAP シークレットを使用してホストサーバーの iSCSI イニシエータからのすべてのアクセス要求を認証します。ターゲット CHAP 認証を設定するには、ストレージアレイで CHAP シークレットを入力してから、ホストサーバーの各 iSCSI イニシエータが、ストレージへのアクセスがある度に入力したシークレットを送信するよう設定します。

相互 CHAP

ターゲット CHAP の設定に加えて、ストレージアレイと iSCSI イニシエータの両方が相互認証する相互 CHAP を設定することができます。相互 CHAP を設定するには、iSCSI イニシエータを、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 CHAP シークレットで設定します。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両方が情報を送信し、接続が許可される前にお互いが認証する必要があります。

CHAP はオプションの機能で、iSCSI を使用するために必須ではありません。しかしながら、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たすべてのホストサーバーから、ストレージアレイへの読み書きが可能となってしまいます。

 **メモ:** CHAP 認証を使用する際は、仮想ディスクがデータを受信できるようにする前に、ストレージアレイ (MD Storage Manager を使用) とホストサーバー (iSCSI イニシエータ使用) の両方で、CHAP 認証を設定する必要があります。CHAP 認証を設定する前にデータ受信のディスクを準備すると、CHAP が設定された後はディスクが見えなくなってしまいます。


CHAP の定義

ターゲット CHAP 認証と相互 CHAP 認証の違いを以下の表に要約します。

CHAPの種類	説明
ターゲット CHAP	iSCSI イニシエータがターゲットストレージアレイに接続する際に使用するアカウントを設定します。その後、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	相互 CHAP は、ターゲット CHAP に追加して適用され、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際に使用するアカウントを設定します。その後、iSCSI イニシエータは、ターゲットを認証します。

手順 5: ストレージアレイの CHAP 認証を設定する (オプション)

いずれの CHAP も設定しない場合は、この手順は省略し、「[手順 7: ホストサーバーからターゲットストレージアレイへの接続](#)」に進みます。

 **メモ:** 相互 CHAP 認証を設定する場合は、最初にターゲット CHAP を設定する必要があります。

iSCSI 設定において、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. **MD Storage Manager** 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。

次の表に示される CHAP 設定のいずれかを選択します。

CHAP 設定	説明
なし	これがデフォルトになっています。 なし 以外に選択肢がない場合、ストレージアレイは CHAP 認証の種類を示すことなく、iSCSI イニシエータにログインを許可します。
なしと CHAP	CHAP 認証の有無に関係なく、ストレージアレイは iSCSI イニシエータにログインを許可します。
CHAP	CHAP が選択され、 なし の選択が解除されると、ストレージアレイはアクセスを許可する前に CHAP 認証を求めます。

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 (または **ランダムシークレットを生成**) し、**ターゲット CHAP シークレットの確認** に再度入力してから、**OK** をクリックします。

ストレージアレイでは 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 シークレットは一度入力すると、再度表示することができないため、シークレットは記録し、手の届く場所に保管してください。ランダムなシークレットの生成を使用する場合、シークレットをまた将来使用できるようにテキストファイルにコピー、ペーストします。ストレージアレイに新たに追加するホストサーバーには、同じ CHAP シークレットを認証に使用します。CHAP シークレットを忘れた場合は、ストレージアレイに接続されたすべてのホストを切り離し、この章にある手順を繰り返して再度追加する必要があります。


4. **OK** をクリックします。

‘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 で、イニシエータの認証設定を変更します。以下のオプションを使用して設定を変更します。

- **なし** – イニシエータ認証をしない場合は、**なし** を選択します。**なし** を選択した場合は、どのイニシエータからもこのターゲットにアクセスできます。セキュアなデータが必要でない場合のみ、このオプションを使用します。ただし、**なし** および **CHAP** を同時に選択することもできます。
- **CHAP** – ターゲットへのアクセスを試みるイニシエータに CHAP を使用して認証させるようにする場合は、**CHAP** を選択します。CHAP シークレットは、相互 CHAP 認証を使用する場合にのみ定義します。**CHAP** が選択されていても CHAP ターゲットシークレットは定義されていないという場合は、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用して、CHAP シークレットを定義します。

 **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: ホストサーバーでの CHAP 認証の設定 (オプション)


[手順 5: ストレージレイでの CHAP 認証の設定 \(オプション\)](#) で CHAP 認証を設定した場合は、次の手順を完了します。設定しなかった場合は、[手順 7: ホストサーバーからのターゲット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 GUI バージョンを使用したホストサーバーでの CHAP 認証の設定

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 → プログラム → **管理ツール** → **iSCSI イニシエータ** の順にクリックします。
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。
ターゲット検出中にストレージレイで設定された 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、ストレージレイ上の iSCSI ポートの IP アドレスまたは DNS 名 (上記の手順で削除済み) を再入力します。
7. **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 ヘッドダイジェスト – 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 – ストレージレイで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。

検出セッションフェイルオーバーが必要な場合は、ストレージレイ上のすべての iSCSI ポートでこの手順順序の手順 5~6 を繰り返します。必要ない場合は、シングルホストポートの設定で十分です。

 **メモ:** 接続に失敗する場合は、すべての IP アドレスが正しく入力されているかを確認します。IP アドレスの入力を間違えると、接続失敗の原因となります。

8. **OK** をクリックします。

Windows Server Core バージョンを使用したホストサーバーでの CHAP 認証の設定

1. iSCSI イニシエータサービスが自動的に開始されるように設定する (未設定の場合) : `sc \\
 \<server_name> config msiscsi start=auto`
2. iSCSI サービスを開始する (必要に応じて) : `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する : `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する : `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する : `iscsicli QAddTargetPortal
 <IP_address_of_iSCSI_port_on_storage_array> [CHAP_username] [CHAP_password]`
ここで、[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。

検出セッションフェイルオーバーが必要な場合は、ストレージレイのすべての iSCSI ポートで手順 5 を繰り返します。必要でない場合は、シングルホストポートの設定で十分です。

Linux 6 および SUSE Linux Enterprise Server 11 を使用した CHAP 認証の設定

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>`

- 相互 CHAP の場合に、イニシエータによるターゲット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_target_username>
discovery.sendtargets.auth.password_in = <CHAP_target_password>
```

- `/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.123456discovery.sendtargets.auth.password_in =
test1234567890
```

SUSE Linux Enterprise Server GUI を使用したホストサーバーでの CHAP 認証の設定


- デスクトップ → YaST → iSCSI イニシエータ の順にクリックします。
- サービスの開始 をクリックし、次に 起動時 を選択します。
- 検出されたターゲット を選択し、検出 を選択します。
- ポートの IP アドレスを入力します。
- 次へ をクリックします。
- 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。
- 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** を選択して、手順 8 に進みます。
または
 - CHAP 認証を使用する場合は、CHAP ユーザー名およびパスワードを入力します。相互 CHAP を有効にするには、**相互 CHAP** を選択して、ユーザー名およびパスワードを入力します。
- 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。
- 接続済みのターゲット に移動します。
- ターゲットが接続されていること、およびステータスが、**接続済み** 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ターゲットストレージレイに接続する

Windows Server GUI を使用したホストサーバーからのターゲットストレージレイへの接続


- 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 の順にクリックします。
- 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正常に行われた場合、ストレージレイの IQN がターゲットの下に表示されます。
- ログオン をクリックします。
- 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。
- 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** – 接続元となるホストサーバーのソース IP アドレスです。
 - **ターゲットポータル** – 接続先となるストレージア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てるため、転送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。

ストレージア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 iSCSI ポートに最低 1 つ接続し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確立するストレージアレイの各 iSCSI ポートで、手順 3 から手順 8 を繰り返します。ターゲットポータルアドレスは、接続した各ポートで異なります。

 **メモ:** より優れたマルチパス I/O スループットを有効にするには、ホストサーバーを、できれば個別のホスト側 NIC から、各コントローラの iSCSI ポート両方に接続する必要があります。各コントローラの各 iSCSI ポートで、手順 3~7 を繰り返します。デュプレックス構成を使用する場合は、LUN もコントローラ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、**接続中** が表示されるようになります。

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

 **メモ:** システムはラウンドロビン負荷分散ポリシーのみをサポートします。

Windows Server Core バージョンを使用したホストサーバーからのターゲットストレージアレイへの接続

1. iSCSI イニシエータサービスが自動的に開始されるように設定する (未設定の場合) : `sc \\
\`
2. iSCSI サービスを開始する (必要に応じて) : `sc start msiscsi`
3. ターゲットへにログオンする : `scsicli PersistentLoginTarget <Target_Name>
<Report_To_PNP> <Target_Portal_Address TCP_Port_Number_Of_Target_Portal> * *
* <Login_Flags> * * * * * <Username> <Password> <Authtype> * <Mapping_Count>`
 - <Target_Name> は、ターゲットリストに表示されるターゲット名です。 `scsicli ListTargets` コマンドを使用して、ターゲットリストを表示します。
 - <Report_To_PNP> は T にします。これで、LUN がオペレーティングシステムにストレージデバイスとして公開されます。
 - <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、イニシエータ上のターゲットのマルチパスを有効にするため 0x2 です。この値により、複数のセッションが一度にターゲットに記録されます。
 - <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 が使用されていない場合は、アスタリスク (*) に置き換えることができます。

- Mapping_Count は 0 にします。これは、マッピングが指定されておらず、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示します。たとえば、コマンドのログが次のようになる場合があります。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、コマンド iscsicli SessionList を実行します。

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、ホストサーバーが各コントローラの少なくとも 1 つの iSCSI 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確立するストレージレイの各 iSCSI ポートで手順 3 を繰り返します。Target_Portal_Address は、接続する各ポートごとに異なります。PersistentLoginTarget は、システムが再起動されるまで、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確立するには、LoginTarget の代わりに PersistentLoginTarget を使用します。

 **メモ:** 前の手順で使用されるコマンドの詳細については、『Microsoft iSCSI Software Initiator 2.x User's Guide』（Microsoft iSCSI ソフトウェアイニシエータ 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 で Microsoft Developers Network (MSDN) を参照してください。

Linux Server の場合

MD Storage Manager では、**iSCSI ホストポートの設定** に、接続しようとしている各 iSCSI ポートの状態およびすべての IP アドレスの設定状態が表示されます。どちらかに、**未接続** または **未設定** が表示される場合、以下の内容を確認し、iSCSI 設定の手順をやり直します。

- 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セットアップと構成設定を確認するには、「iSCSI 用ネットワークの構成ガイドライン」を参照してください。

手順 8 : (オプション) 帯域内管理をセットアップする

帯域外管理（「手順 1 : ストレージレイの検出（帯域外管理のみ）」を参照）が、ストレージレイの管理に推奨される方法ですが、オプションとして帯域内管理を設定する場合は、次に示す手順に従います。

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

 **メモ:** 使用している管理ステーションは、PowerVault MD3860i ホストポートと同じ IP サブネットに対するネットワーク通信のために設定する必要があります。

1. PowerVault MD3860i 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. MD Storage Manager 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。そうでない場合は、**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、PowerVault MD Storage Manager 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。

付録 – インターネット記憶域ネームサービスの使用


Microsoft Windows iSCSI 環境でのみサポートされているインターネット記憶域ネームサービス (iSNS) サーバーによって、各個別のストレージレイを手動で特定のイニシエータおよびターゲット IP アドレスで設定する必要がなくなります。その代わりに、iSNS が自動的に環境内にあるすべての iSCSI デバイスを検出、管理、設定します。

インストールと設定を含む iSNS の詳細については、[microsoft.com](https://www.microsoft.com) を参照してください。

負荷分散

負荷分散ポリシー

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経由の仮想ディスクへの I/O パスを選択します。処理する新たな I/O をマルチパスドライバが受信すると、ドライバは、仮想ディスクを所有する現在の RAID コントローラモジュールへのパスを見つけようとします。仮想ディスクを所有する現在の RAID コントローラモジュールへのパスを見つけられない場合、マルチパスドライバは、仮想ディスクの所有権を 2 番目の RAID コントローラモジュールへ移行させます。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ある場合は、負荷分散ポリシーを選択して、どのパスが I/O をプロセスするかを決定することができます。複数の負荷分散ポリシー設定用オプションにより、混在ホストインタフェースの設定時における I/O パフォーマンスの最適化が可能になります。

 **メモ:** 負荷分散ポリシーについての詳細は、お使いのオペレーティングシステムのマニュアルとアップデートを参照してください。

次の負荷分散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します。

- ラウンドロビン
- 最小キュー深度
- 最小パス荷重 (Microsoft Windows オペレーティングシステムのみ)

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の I/O 負荷分散ポリシーは、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各使用可能な各データパスに、I/O 要求を順番にルーティングします。このポリシーは、I/O アクティビティにおいて、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同等に扱います。セカンダリ RAID コントローラモジュールへのパスは所有権が変更されるまで無視されます。ラウンドロビンポリシーの基本的な前提は、データパスが同等であることです。混在ホストがサポートされることから、データパスの帯域幅またはデータ転送速度が異なる場合があります。

最小キュー深度

最小キュー深度ポリシーは、最小 I/O、または最小要求ポリシーとも呼ばれています。このポリシーは、次の I/O 要求を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パスにルーティングします。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、またはそのコマンドに関連付けられているブロックの数は考慮されません。

最小キュー深度ポリシーでは、大型のブロック要求と小型のブロック要求が同等に扱われます。選択されるデータパスは、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の 1 つです。

最小パス荷重

最小パス荷重ポリシーは、仮想ディスクへのデータパスそれぞれに荷重係数を割り当てます。I/O 要求は、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荷重値が最も低いパスにルーティングされます。同じ荷重値を持つ仮想ディスクへのデータパスが複数ある場合、サブセット付きラウンドロビンのパス選択ポリシーが同じ荷重値を持つパス間での I/O 要求のルーティングに使用されます。最小パス荷重負荷分散ポリシーは、Linux オペレーティングシステムではサポートされていません。

複数の iSCSI セッションによる帯域幅の拡大

デュプレックス構成の PowerVault MD3860i シリーズストレージアレイは、2つのアクティブ / アクティブ非対称冗長コントローラをサポートします。各コントローラには、iSCSI をサポートする 4 つの 1 Gbps イーサネットポートがあります。同じコントローラ上の 4 つのポートの帯域幅は、最適なパフォーマンスを実現するために集約させることができます。ホストは、コントローラの両ポートの帯域幅を同時に使用してコントローラが所有する仮想ディスクにアクセスするように設定することができます。すべてのポートが I/O の同時アクセスに使用されるようにストレージアレイを設定するには、デルが MD3860i シリーズストレージアレイ用に提供するマルチパスフェイルオーバードライバを使用することができます。マルチパスドライバが、同じ仮想ディスクに対する同じコントローラ上のポート経由のパスを複数検知した場合、ドライバはコントローラ上のポート全体でホストからの I/O アクセスの負荷分散を行います。

VMware での負荷バランスポリシーの設定

VMware は非対称論理ユニットアクセス (ALUA) に対応しています。Most Recently Used (MRU) およびラウンドロビン (RR) 負荷バランスポリシーの詳細については、VMware マニュアルを参照してください。

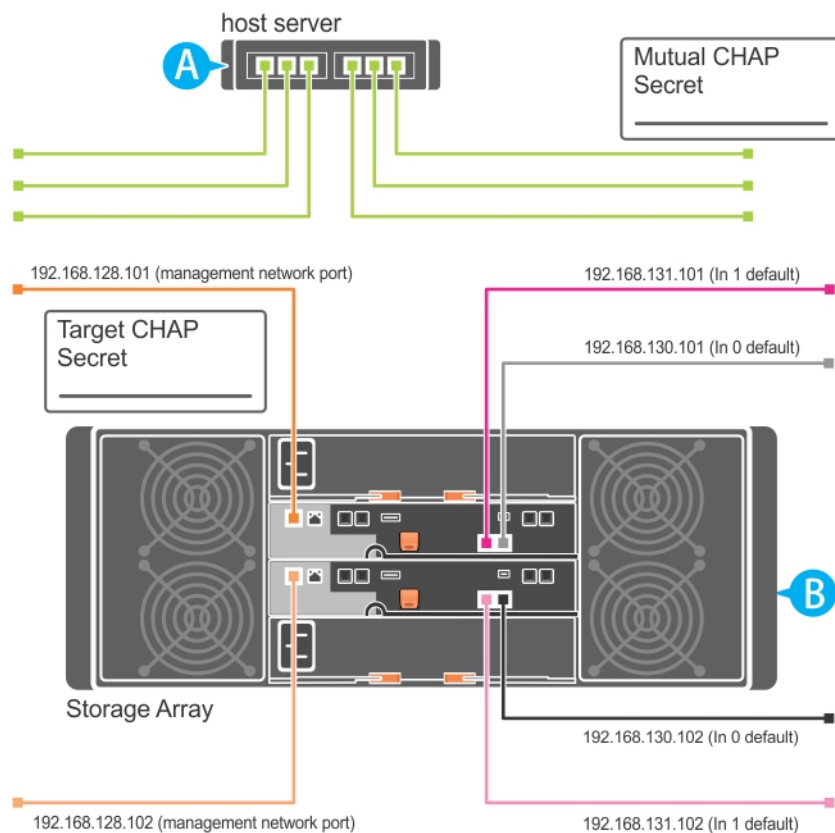
付録 — Linux での iSCSI サービスの停止と開始

Linux 環境で、iSCSI サービスを手動で停止するには、ストレージレイとホストサーバーの間の並行処理を維持するために特定の手順を実行する必要があります。

1. すべての I/O 処理を停止します。
2. 関連付けられたすべてのファイルシステムをマウント解除します。
3. 次のコマンドを実行して、iSCSI サービスを停止します。

```
/etc/init.d/open-iscsi stop
```

IPv4 の設定 – ワークシート



メモ: 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。

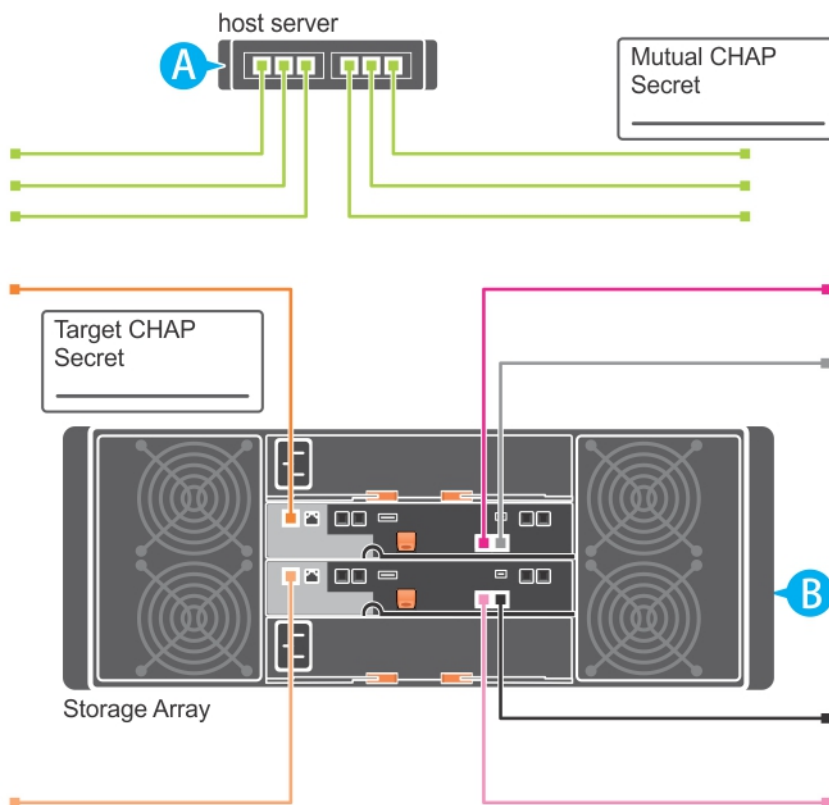
A	静的 IP アドレス (ホストサーバー)	サブネット (NIC ごとに異なっている必要があります)	デフォルトゲートウェイ
iSCSI ポート 1
iSCSI ポート 2
管理ポート
管理ポート

B静的 IP アドレス (ホストサブネット
オーバー)

デフォルトゲートウェイ

iSCSI ポート 0、 入力 0	-----	-----	-----
iSCSI ポート 0、 入力 1	-----	-----	-----
管理ポート cntrl 0	-----	-----	-----
iSCSI ポート 1、 入力 0	-----	-----	-----
iSCSI ポート 1、 入力 1	-----	-----	-----
管理ポート cntrl 1	-----	-----	-----

IPv6 の設定 – ワークシート



メモ: 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
ルータブル IP アドレス	ルータブル 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、入力 0

IP アドレス FE80: 0000: 0000 : 0000: ____ : ____ : ____ : ____
ルータブル IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
ルータブル IP アドレス 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
ルーター IP アドレス ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI コントローラ 0、入力 1

IP アドレス FE80: 0000: 0000 : 0000: ____ : ____ : ____ : ____
ルータブル IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
ルータブル 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: ____ : ____ : ____ : ____
ルータブル IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
ルータブル IP アドレス 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
ルーター IP アドレス ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI コントローラ 1、入力 1

IP アドレス FE80: 0000: 0000 : 0000: ____ : ____ : ____ : ____
ルータブル IP アドレス 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
ルータブル IP アドレス 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
ルーター IP アドレス ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____