

**Dell PowerVault MD3800i および MD3820i 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:** メモでは、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:** 注意では、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:** 警告では、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 © 2016 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 - 10

Rev. A01

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
ストレージアレイについて.....	6
関連マニュアル.....	7
2 ハードウェアの取り付け.....	9
ストレージ構成の計画.....	9
ストレージアレイの接続.....	9
ストレージア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.....	14
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.....	22
新しい PowerVault MD1200 シリーズ拡張エンクロージャでの拡張.....	23
3 PowerVault MD ストレージソフトウェアのインストール.....	25
モジュラディスク設定ユーティリティ.....	26
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
Windows システムでのサイレントインストール.....	27
Linux システムでのサイレントインストール.....	28
プレミアム機能の有効化 (オプション).....	28
MD Storage 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 の設定用語.....	29
iSCSI 設定ワークシート.....	30
ストレージアレイの iSCSI の設定.....	33
Modular Disk Configuration Utility を使用した自動設定.....	33
接続確立後の手順.....	35
iSCSI 用のネットワーク設定のガイドライン.....	36
Microsoft Windows ホストのセットアップ.....	36
DHCP サーバーを使用した Microsoft ホストネットワークのセットアップ.....	36
静的 IP アドレス設定を使用した Microsoft ホストネットワークのセットアップ.....	36

DNS サーバーを使用した Microsoft ホストネットワークのセットアップ.....	37
WINS サーバーを使用した Microsoft ホストネットワークのセットアップ.....	37
Linux ホストのセットアップ.....	37
DHCP を使用した Linux ホストネットワークのセットアップ.....	37
静的 IP アドレスを使用した Linux ホストネットワークのセットアップ.....	38
5 MD ストレージソフトウェアのアンインストール.....	39
Windows からの MD Storage ソフトウェアのアンインストール.....	39
Windows Server GUI バージョンからの MD ストレージソフトウェアのアンインストール.....	39
Windows Server Core バージョンからの MD Storage ソフトウェアのアンインストール.....	39
Linux からの MD Storage ソフトウェアのアンインストール.....	39
6 iSCSI の手動設定.....	41
手順 1 : ストレージアレイの検出 (帯域外管理のみ)	41
IPv4 管理ポートのデフォルト設定.....	41
IPv6 管理ポートのデフォルト設定.....	42
ストレージアレイの自動検出.....	43
ストレージアレイの手動検出.....	43
アレイのセットアップ.....	43
手順 2: ストレージアレイの iSCSI ポートの設定.....	44
手順 3 : iSCSI イニシエータからのターゲット検出の実行.....	45
Windows Server GUI バージョンを使用した iSCSI イニシエータからのターゲット検出の実行.....	45
Windows Server Core バージョンを使用した iSCSI イニシエータからのターゲットの検出の実行.....	46
Linux を使用した iSCSI イニシエータからのターゲット検出の実行.....	46
手順 4: ホストアクセスの設定.....	46
CHAP 認証の理解.....	47
CHAP について.....	47
ターゲット CHAP.....	47
相互 CHAP.....	47
CHAP の定義.....	47
手順 5 : ストレージアレイでの CHAP 認証の設定 (オプション)	48
ストレージアレイのターゲット CHAP 認証の設定.....	48
'ストレージアレイの相互 CHAP 認証の設定.....	49
手順 6 : ホストサーバーでの CHAP 認証の設定 (オプション)	49
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.....	49
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.....	50
Linux を使用した CHAP 認証の設定.....	50
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.....	51
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.....	51

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.....	52
Linux 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	53
手順 8 : 帯域内管理のセットアップ.....	53
7 Internet Storage Naming Service の使用.....	55
8 負荷分散.....	56
負荷分散ポリシー.....	56
サブセット付きラウンドロビン.....	56
最小キュー深度.....	56
最小パス荷重.....	57
Windows Server オペレーティングシステムでの負荷バランスポリシーの変更.....	57
複数の iSCSI セッションによる帯域幅の拡大.....	57
9 Linux での iSCSI サービスの停止.....	59
10 困ったときは.....	60
デルへのお問い合わせ.....	60
Dell システムサービスタグの位置	60

はじめに

本ガイドには、Dell PowerVault MD3800i および MD3820i ストレージア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 (MDSM) ソフトウェアのインストール
- 初期システム設定

システム要件、ストレージアレイの構成、およびユーティリティを含むその他の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。

MDSM 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アレイを設定および監視することができます。MD3820i MD シリーズのリソースメディアに収録されている MDSM のバージョンは、PowerVault MD3800i と MD3820i シリーズの両アレイ、およびそれ以前のストレージアレイの管理に使用することができます。MDSM には、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 MD3800i および MD3820i シリーズのハードウェアとソフトウェアの取り付けとインストール、および設定を行う前に、システムの最小要件を満たしていること、およびサポートされている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を確認してください。詳細については、Dell.com/support/manuals にある『Dell PowerVault MD34xx/38xx Series Support Matrix』(Dell PowerVault MD34xx/38xx シリーズ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、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し、管理します。管理ステーションの要件については、Dell.com/support/powervaultmanuals にある『Dell PowerVault MD34xx/38xx Series Support Matrix』(Dell PowerVault MD34xx/38xx シリーズサポートマトリックス) を参照してください。

ストレージアレイについて

ストレージアレイには、エンクロージャ内に格納された、物理ディスク、RAID コントローラモジュール、ファン、電源装置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います。物理ディスクは、RAID コントローラモジュールを通じてアクセスされます。

ストレージア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が、ストレージアレイ上のデータにアクセスできます。ホストサーバーポートの障害などによるひとつのパスの損失がストレージアレイ上のデー

タへのアクセス損失につながらないように、ホストとストレージア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 MDSM によって管理されます。

- **ホストサーバー** – ホストサーバーシステムでは、MDSM とストレージアレイは、帯域内または帯域外の接続を使用して、管理要求とイベント情報の通信を行います。
- **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、管理ステーションとストレージアレイ接続間で管理情報をやりとりします。




MDSM 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、またはダイナミックディスクグループ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、ディスクグループまたはダイナミック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。

関連マニュアル

-  **メモ:** PowerVault マニュアルについては、Dell.com/support/manuals 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:** 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 MD3800i and MD3820i Storage Arrays Getting Started Guide』（Dell PowerVault MD3800i および MD3820i 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 MD3800i and MD3820i Storage Arrays Owner's Manual』（Dell PowerVault MD3800i および MD3820i 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しています。
- 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 MD34XX/38XX Series Storage Arrays CLI Guide』 (Dell PowerVault MD シリーズストレージアレイ 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 MD3800i and MD3820i Storage Arrays Deployment Guide』 (Dell PowerVault MD3800i および MD3820i 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 MD34/38 Series Support Matrix』 (Dell PowerVault MD34/38 シリーズ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。

ハードウェアの取り付け

本ガイドを使用する前に、マニュアルに記載されている手順を確認するようにしてください。

- 『Getting Started Guide』（はじめに） – お使いのストレージアレイに付属の『Getting Started Guide』（はじめに）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） – 『Owner's Manual』（オーナーズマニュアル）には、お使いのストレージソリューションをセットアップするために重要な概念が記載されています。
Dell.com/support/manualsにある『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、およびエラー状態用の電子メールアラート通知などのストレージアレイ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、またはダイナミック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台のホットスワップ可能な RAID コントローラモジュールで接続されています。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 と認識されます。

 **メモ:** コントローラ上の全部品についての詳しい説明は、オーナーズマニュアルを参照してください。

各コントローラ上のポートの機能は、次のとおりです。

- 10 Gbps iSCSI ホストポート (2) – ストレージアレイへのホストサーバーの接続を可能にします。
- 12 Gbps SAS ホストポート (2) – ストレージアレイへのホストサーバーの接続を可能にします。
- 16 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。

- SAS 拡張ポート (2) – オプションの PowerVault MD1200 シリーズの拡張エンクロージャにストレージアレイの接続して、ストレージ容量を追加することができます。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。

PowerVault MD3800i および MD3820i シリーズストレージアレイは、それぞれ最大 120（プレミアム機能のアクティブ化により有効化されている場合は 192）スロットまで拡張することができます。

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）
- すべてのプロトコルを使用する混在構成

冗長および非冗長構成

非冗長構成では、ホストからストレージアレイへのパスが 1 つしか提供されません。このタイプの構成は、重要ではないデータストレージにのみ推奨されます。ケーブルや RAID コントローラモジュールの故障または取り外しによるパスの障害は、ストレージアレイ上のストレージに対するホストのアクセスが失われる結果となります。

冗長性は、ホストとストレージアレイ間に複数の個別のデータパスを取り付け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 1 台に接続されます。冗長構成では両方の 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、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。

シングルパスデータ構成

シングルパス構成では、単一の物理イーサネットポート経由で、異種ホストのグループをストレージアレイに接続することができます。ポートが 1 つしかないため、各 iSCSI ポータルが複数の接続をサポートしていても、冗長性はありません。この構成はシングルコントローラモードとデュアルコントローラモードの両方でサポートされています。

次の図は、シングルパスデータ構成を使用した RAID コントローラモジュールへ非冗長ケーブル配線構成を示しています。

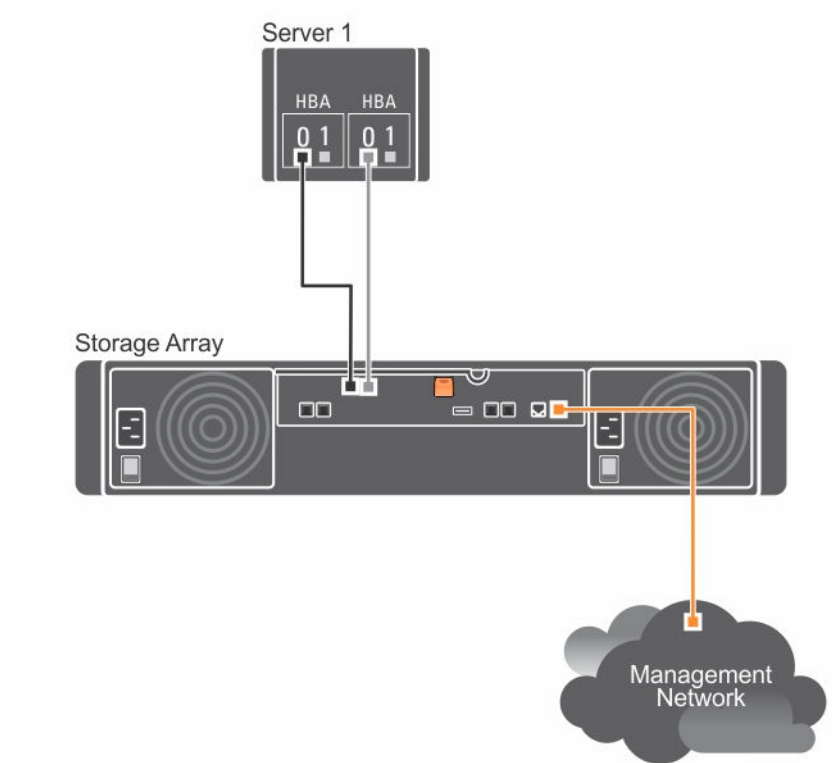


図 1. 単一のコントローラに接続された 1 台のホスト

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。

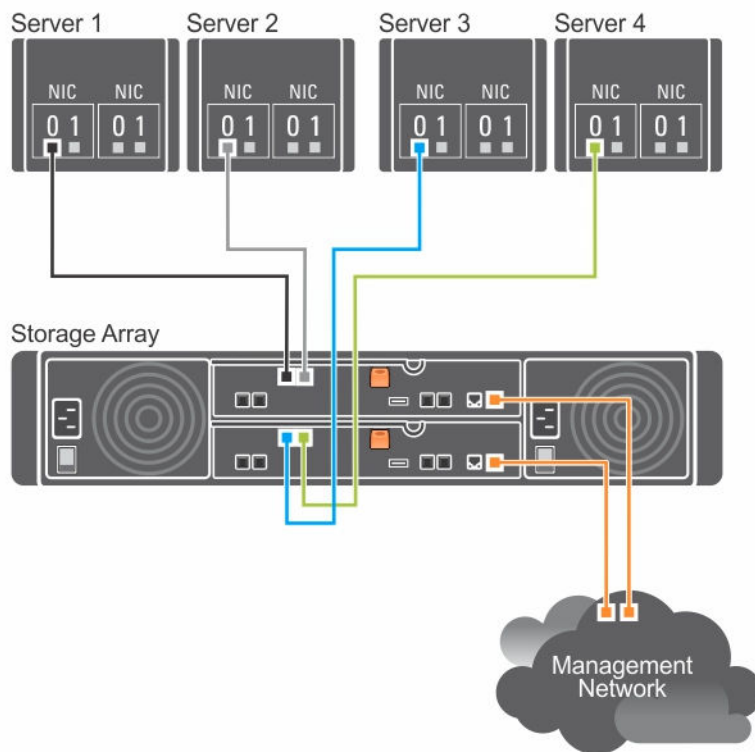


図 2. HBA を 1 つずつ使用したデュアルコントローラ構成内のホスト 4 台

デュアルパスデータ構成

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にある 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、パスの 1 つが損失された場合でも完全な冗長性を確保することができます。

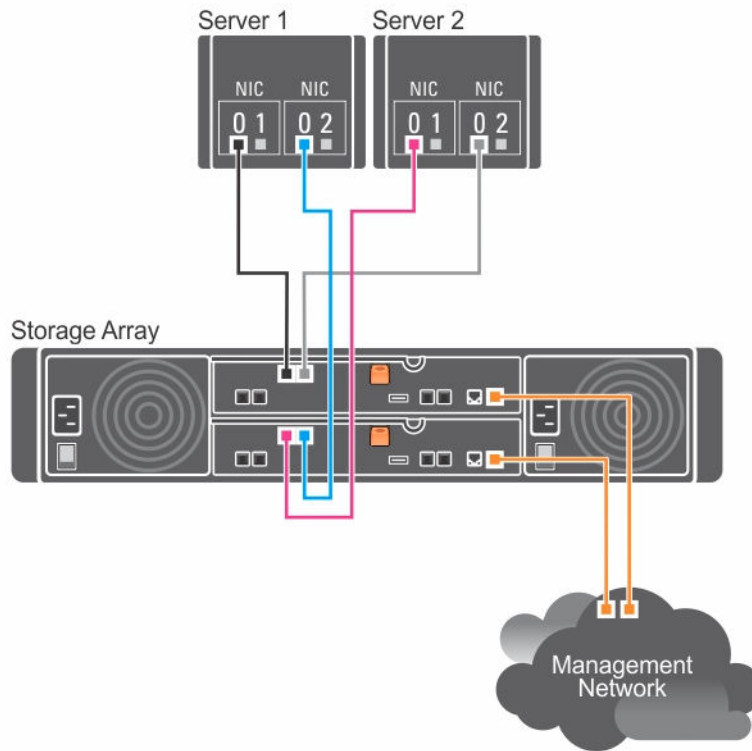


図 3. 2 つのコントローラに接続された 2 台のホスト

次の図では、最大 2 つのクラスタノードが 2 つの 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、1 つのパスが損失しても、もう 1 つのパスでストレージアレイへのアクセスを確保することができます。

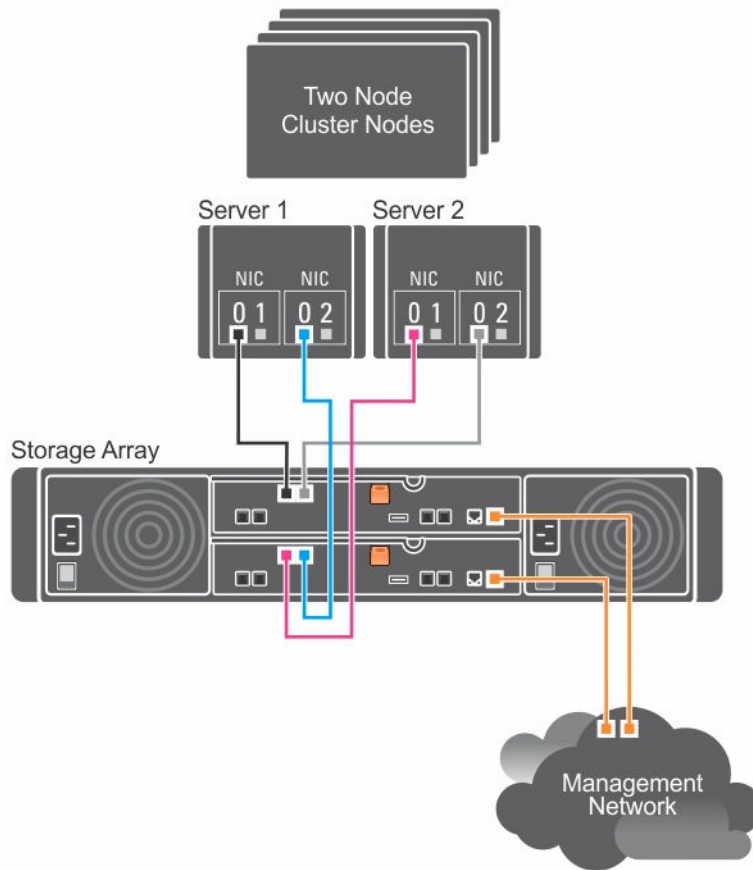


図 4. デュアルコントローラ構成で接続された 2 台のホスト

ネットワーク接続構成

業界標準の 10G 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 MD3800i および MD3820i シリーズストレージアレイは最大 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 RAID コントローラモジュールまたはデュアル RAID 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、ネットワーク経由で単一の RAID コントローラモジュールに接続された（複数のセッションを使用）最大 64 台のスタンダオンサーバーを示しています。ネットワークへの 2 番目のイーサネット接続を持つホストによって、各ホストに対する 2 つの独立した物理パスが可能になり、1 つのパスに障害が発生した場合でも、完全な冗長性が確保されます。さらに優れた冗長性のため、2 つのスイッチの使用が推奨されていますが、単一スイッチでの構成もサポートされます。

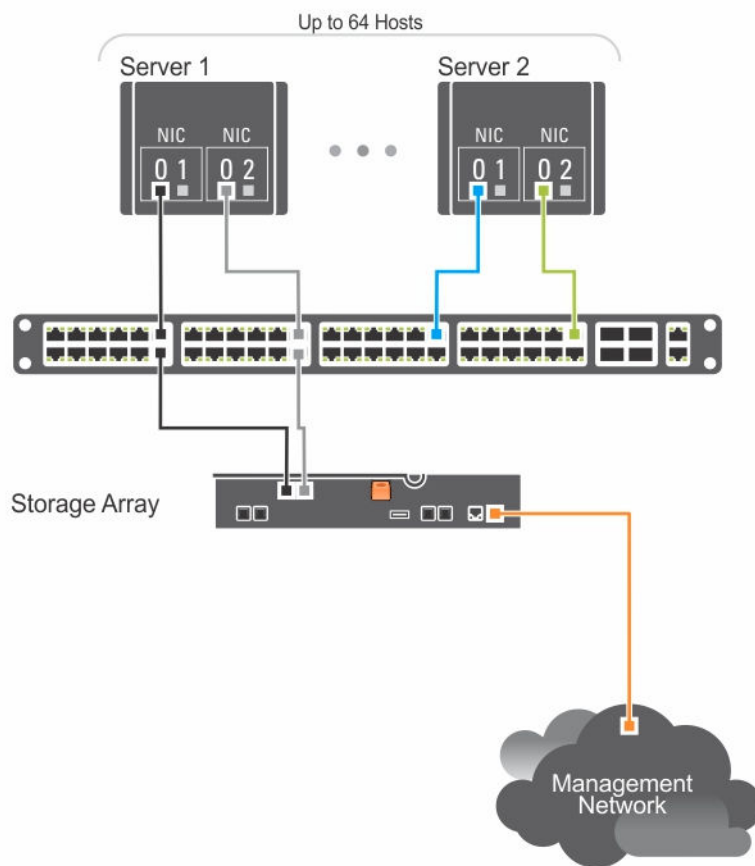


図 5. 単一のコントローラに接続された 64 台のサーバー

次の図は、デュアル RAID コントローラモジュール構成に対し、同じ数のホストを同様に接続する方法を示しています。

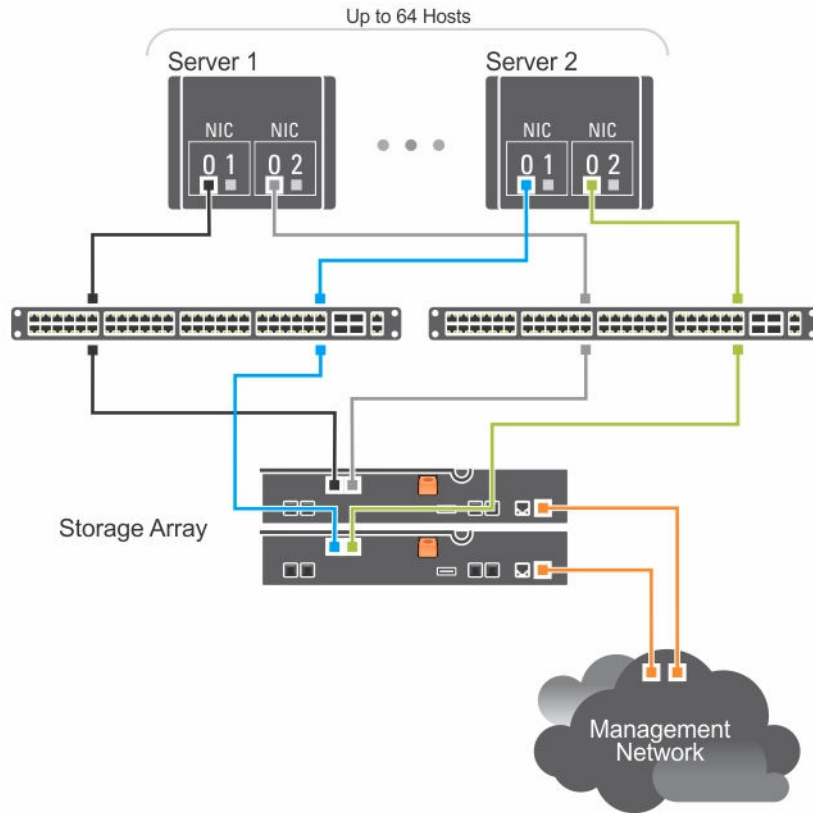


図 6. 2つの RAID コントローラに接続された 64 台のサーバー

次の図は、10G アグリゲーションスキームを使用して、ネットワーク経由で単一の RAID コントローラモジュールに接続された（複数のセッションを使用）最大で 64 台のスタンドアロンサーバーを示しています。サーバーの NIC は、0 G NIC で、アップリンクポートは 10G です。ネットワークへの 2 番目のイーサネット接続を持つホストによって、各ホストに対する 2 つの独立した物理パスが可能になり、1 つのパスに障害が発生した場合でも、完全な冗長性が確保されます。さらに優れた冗長性のため、2 つのスイッチの使用が推奨されていますが、単一スイッチでの構成もサポートされます。

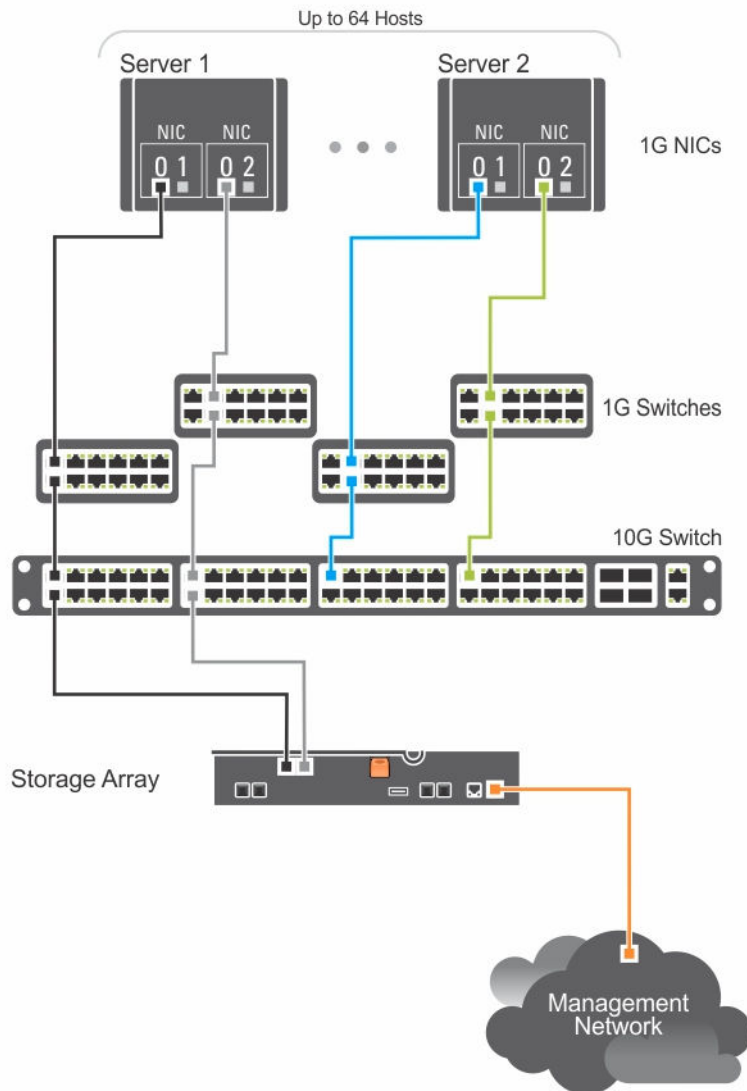


図 7. 単一のコントローラに接続された 64 台のサーバー

次の図は、デュアル RAID コントローラモジュール構成に対し、同じ数のホストを同様に接続する方法を示しています。この構成では、スイッチ障害発生時におけるハードウェアの冗長性が達成されます。

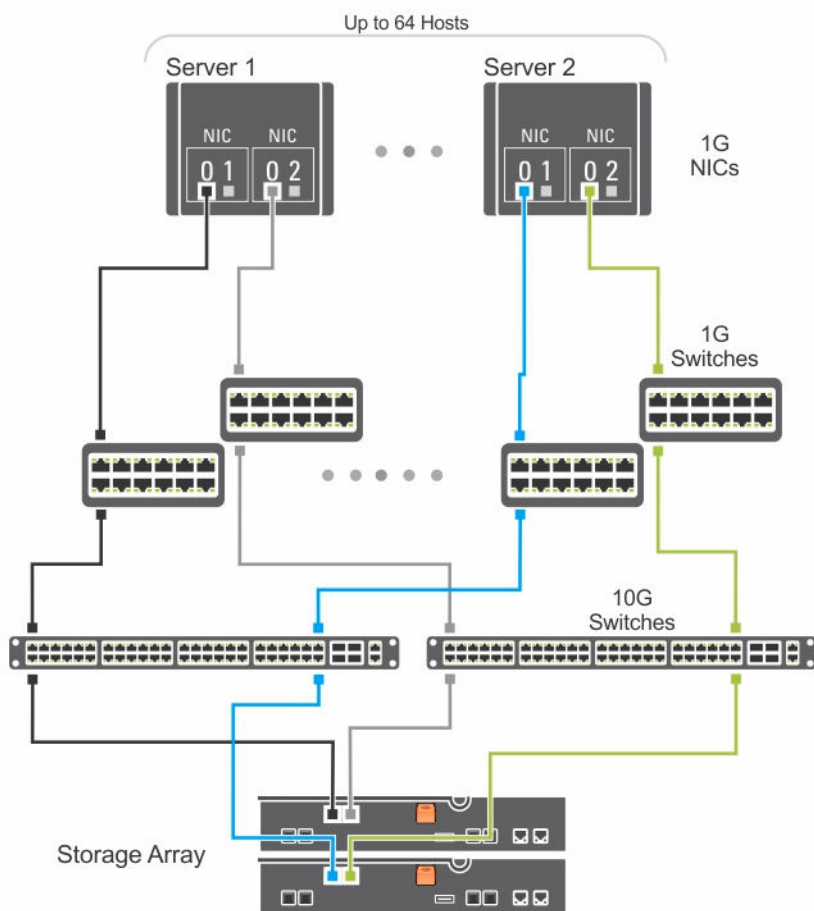


図 8. 2つの RAID コントローラに接続された 64 台のサーバー

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合環境を示しています。

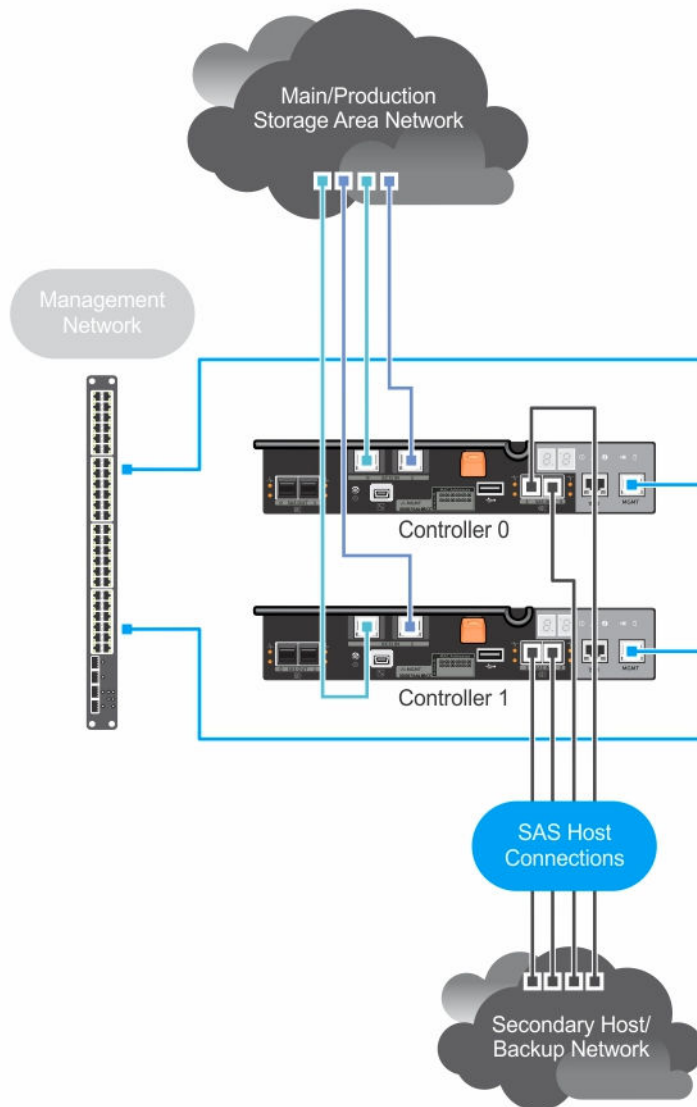



図 9.2 台の RAID コントローラ用の混合環境ケーブル配線

 **メモ:** PowerVault MD 3800i ストレージアレイおよび MD 3820i ストレージアレイの SAS ホストポートは、セカンダリホストまたはバックアップネットワークに接続しておくことをお勧めします。

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/support で『MD Administrators Guide』（MD 管理者ガイド）を参照してください。

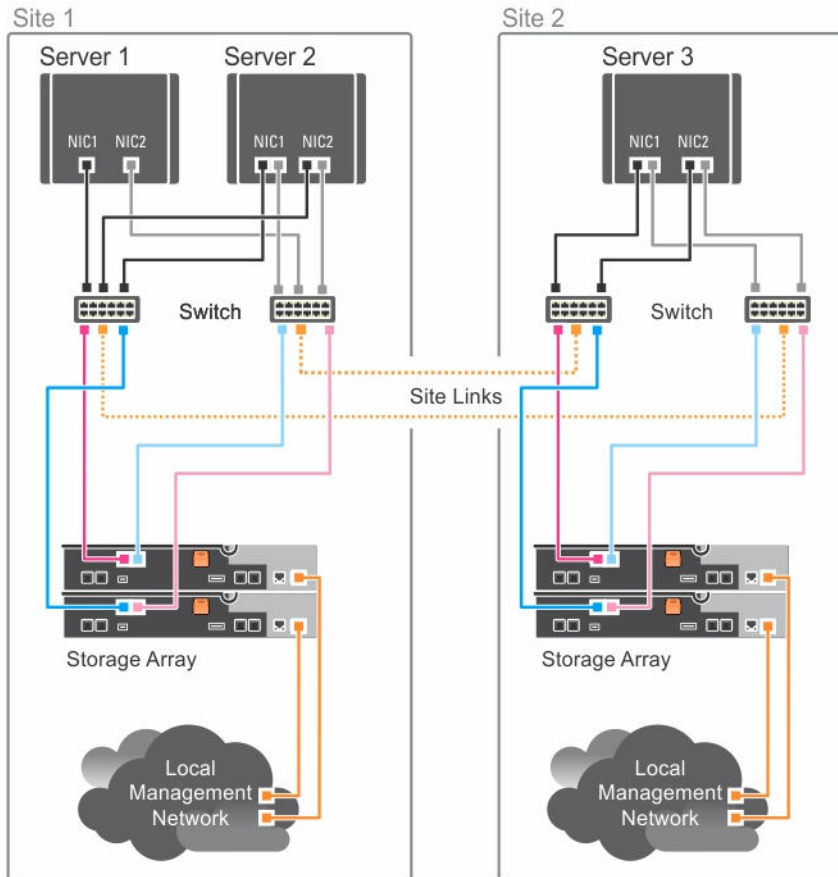


図 10. リモートレプリケーションのケーブル配線例

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することにより、お使いの PowerVault MD3800i および MD3820i シリーズストレージレイの容量を拡張することができます。拡張エンクロージャを最大 7 台使用することにより、物理ディスクのプールを最大 120 台（プレミアム機能のアクティブ化で有効になっている場合は、192 台）の物理ディスクに拡張できます。

メモ: お使いの MD シリーズ RAID ストレージレイに MD1200 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。

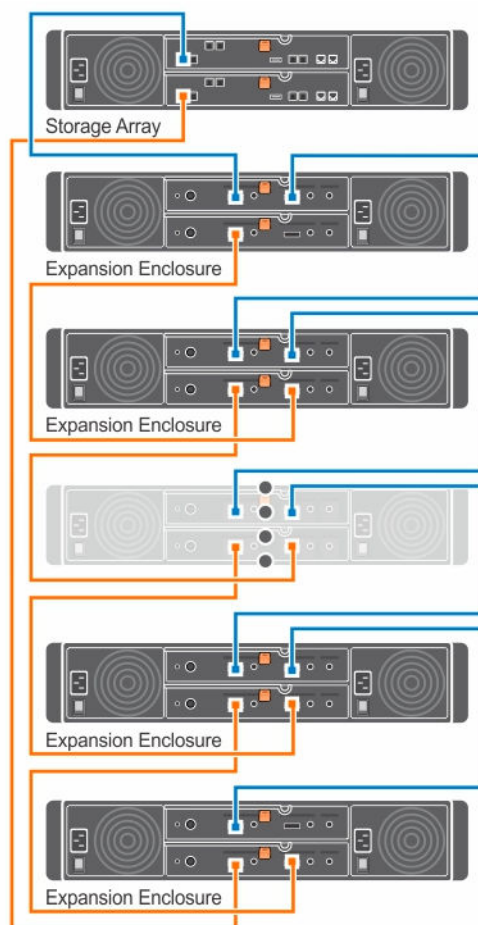


図 11. シングル拡張のケーブル配線図

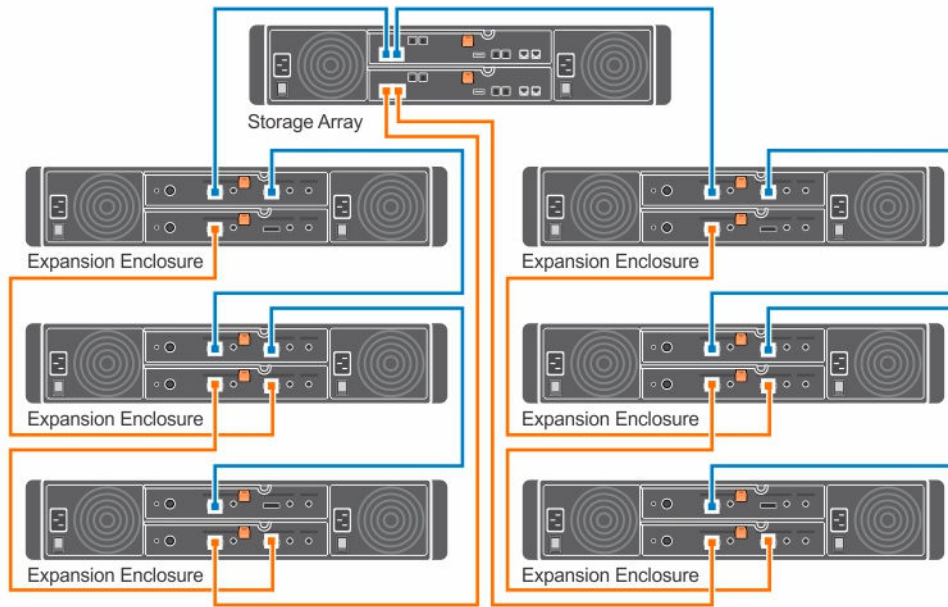


図 12. デュアル拡張のケーブル配線図

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

お使いの拡張エンクロージャが Dell PowerEdge RAID Controller (PERC) 800 アダプタに直接接続され、設定されている場合は、この手順を使用してください。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 MD シリーズストレージレイや PowerVault MD シリーズストレージレイに接続されている 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:** 以前に PERC H800 アダプタに接続されていた PowerVault MD1200 シリーズ拡張エンクロージャが PowerVault MD34xx/MD38xx シリーズストレージレイの拡張エンクロージャとして使用される場合は、拡張エンクロージャの物理ディスクは再度初期化され、データは損失します。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する必要があります。

1. 拡張エンクロージャ上のすべての全データをバックアップします。
2. エンクロージャが PERC H800 コントローラに接続されたままの状態、拡張エンクロージャのファームウェアを Dell.com/support で入手可能な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ており、最新状態であることを確認します。詳細については、Dell.com/support/manuals にある、『Dell PowerVault MD34xx/38xx Support Matrix』(Dell PowerVault MD34xx/38xx 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収録されてい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詳細については、トピック「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. 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 で入手可能な最新バージョンにアップデートします。
 - c. MDSM を使用して、ツール → RAID コントロールモジュールファームウェアのアップグレード → エンタープライズ管理ウィンドウ (EMW) の順にクリックします。
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. 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ホストシステムの電源を切ります。
- b. ストレージアレイの電源を切ります。
- 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アレイにケーブル接続します。
 - a. サポートされている SAS ケーブルの MiniSAS HD 側を、MD1200 シリーズ拡張エンクロージャの SAS 出力ポート 0 に接続します。
 - b. SAS ケーブルのもう一方の端を MD1200 シリーズ拡張エンクロージャの入力ポートに接続します。
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、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。
 - ステータス LED が橙色に点灯している場合、ストレージア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 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は、ストレージアレイの準備が整っています。
 - c. 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。
7. PowerVault MD1200 シリーズ拡張エンクロージャをストレージアレイの拡張エンクロージャとして設定した後、手順 1 でバックアップしたデータを復元します。
 拡張エンクロージャがオンラインになったら、ストレージアレイの一部としてエンクロージャにアクセスすることができます。

新しい PowerVault MD1200 シリーズ拡張エンクロージャでの拡張

次の手順を実行して、PowerVault MD34xx/38xx シリーズストレージアレイに新しい PowerVault MD1200 シリーズ拡張エンクロージャを接続します。

1. 拡張エンクロージャを追加する前に、ストレージアレイソフトウェアがインストールされており、最新状態であることを確認します。詳細については、Dell.com/support/manuals にある『Dell PowerVault MD34xx/38xx Support Matrix』（Dell PowerVault MD34xx/38xx 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収録されてい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詳細については、トピック「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セットアップします。PowerVault MD1200 シリーズ拡張エンクロージャのセットアップの詳細については、Dell.com/support/manuals にある『Owner's Manual』（オーナーズマニュアル）を参照してください。
 - c. 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/manuals で入手可能な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の順にクリックします。
2. 次の手順で I/O 処理を停止し、すべてのシステムの電源を切ります。
 - a. 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。
 - b. ストレージアレイの電源を切ります。
 - c. 影響を受けるシステム内にある拡張エンクロージャすべての電源を切ります。
3. 拡張エンクロージャをストレージアレイにケーブル接続します。
 - a. サポートされている SAS ケーブルの MiniSAS HD 側を、MD1200 シリーズ拡張エンクロージャの SAS 出力ポート 0 に接続します。


- b. SAS ケーブルのもう一方の端を MD1200 シリーズ拡張エンクロージャの入力ポートに接続します。
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、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。
 - ステータス LED が橙色に点灯している場合、ストレージア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 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は、ストレージアレイの準備が整っています。
 - c. 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。
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. EMW でアップデートするエンクロージャを選択し、**アレイ管理ウィンドウ (AMW)** を起動します。
 - b. **詳細** → **メンテナンス** → **ダウンロード** → **EMM ファームウェア** の順にクリックします。
 - 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、ソフトウェアへの変更、アップデート、修正、パッチおよびその他 Linux および Windows オペレーティングシステムに重要なデータに関する **readme.txt** ファイルが入っています。また、**readme.txt** ファイルには、文書アクセスへの要件、メディアの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が記載されています。


Dell PowerVault システムで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関しては、**Dell.com/support/manuals** で『Dell PowerVault MD34xx/38xx Series Support Matrix』（Dell PowerVault MD34xx/38xx シリーズサポートマトリクス）を参照してください。


 **メモ:** **Dell.com/support/manuals** で入手可能な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は、コアソフトウェア、プロバイダ、およびユーティリティを含む機能を提供します。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、およびストレージレイソリューションの設定、管理、監視に使用される Modular Disk Storage Manager (MDSM) 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) フレームワークがのプロバイダが含まれます。

 **メモ:** デルでは、VSS および VDS ハードウェアプロバイダのサポートを廃止することになりました。この廃止についての詳細は、『Dell MD Series Storage Arrays Information Update』（Dell MD シリーズストレージレイ情報アップデート）を参照してください。サポートされるソフトウェアについては、**Dell.com/powervaultmanuals** で『Dell™ PowerVault™ MD Series Support Matrix』（Dell™ PowerVault™ MD シリーズサポートマトリクス）の「サポートされる管理ソフトウェア」の項を参照してください。

DHCP (Dynamic Host Configuration Protocol) を使用していない場合、管理ステーションの初期設定中、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 (コントローラ 0 管理 (ポート 1) : 192.168.129.101 または コントローラ 1 管理 (ポート 1) : 192.168.129.102) と同じ IP サブネットに設定する必要があります。初期設定完了後、管理ポートは MDSM を使用して設定され、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アレイにつき、2個の管理ポートのみがサポートされます。各コントローラの2番目のポートは予約済みです。

 **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)** – 多くのユーザーに推奨される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を選択できるグラフィカルウィザード方式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を作成するユーザーには、このオプションが有効です。

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するユーティリティです。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)

PowerVault MD Storage Manager は、ストレージレイを構成、管理、および監視するソフトウェアです。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するユーティリティで、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。MD 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。

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. **インストールセット** 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)** – MD Storage Manager (クライアント) ソフトウェア、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。
 - **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. 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。


6. インストール先を確認して、**インストール** を選択します。
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. 再起動の完了後、インストール中に自動起動を選択しなかった場合は、MDCU を手動で起動します。起動は、次のどちらかの方法で行うことができます。
 - 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。
 - 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. MDCU を使用して 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。
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、ユーザー特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/support/manuals で『Dell PowerVault MD34xx/38xx Series Support Matrix』（Dell PowerVault MD34xx/38xx シリーズサポートマトリクス）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、MDCU 固有のオプションを除いて、グラフィカルインストールと同じオプションが提供されます。MDCU の動作には、グラフィカル環境が必要です。

 **メモ:** コンソールモードのインストーラは MDCU をインストールするオプションを提供します。ただし、MDCU を使用するにはグラフィカル環境が必要です。

サイレントインストール

Windows システム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** ファイルが希望する特定のインストールを反映するよう修正されたら、コマンド **mdss_install.exe -f <host_server_path>\ custom_silent.properties** を実行してサイレントインストールを開始します。

Linux システムでのサイレントインストール

 **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、前提条件のパッケージ **# md_prereq_install.sh** をインストールします。

1. インストールメディアまたはイメージの **/linux** 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た後、ファイルを保存します。
3. **custom_silent.properties** ファイルがユーザー固有のインストールを反映するように修正されたら、コマンド **mdss_install.bin -f <host_server_path>/ custom_silent.properties** を実行してサイレントインストールを開始します。

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。

MD Storage ソフトウェアのアップグレード


古いバージョンの MDSM アプリケーションからアップグレードするには、旧バージョンをアンインストール（「MD ストレージソフトウェアのアンインストール」の項を参照）してから、本章の手順に従って新しい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

ストレージア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 (Dynamic Host Configuration Protocol) 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 Port 0:192.168.129.101 または Controller 1 Port 1:192.168.129.102) 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 設定ワークシートへの記入をお勧めします。「[iSCSI 設定ワークシート](#)」を参照してください。設定手順を開始する前に、お使いのネットワークについてこのタイプの情報を収集しておくこと、作業をより効率的に完了させるために役立ちます。

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アレイ両方の 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アレイに接続されているサーバー。
ホストサーバーポート	ストレージアレイ上の 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ア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)	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、設定を計画するために役立ちます。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、セットアップの設定をより素早く効率的に行うことができます。

「[iSCSI 用のネットワーク設定ガイドライン](#)」には、Microsoft Windows および Linux 両環境のための一般的なネットワークセットアップ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ことをお勧めします。

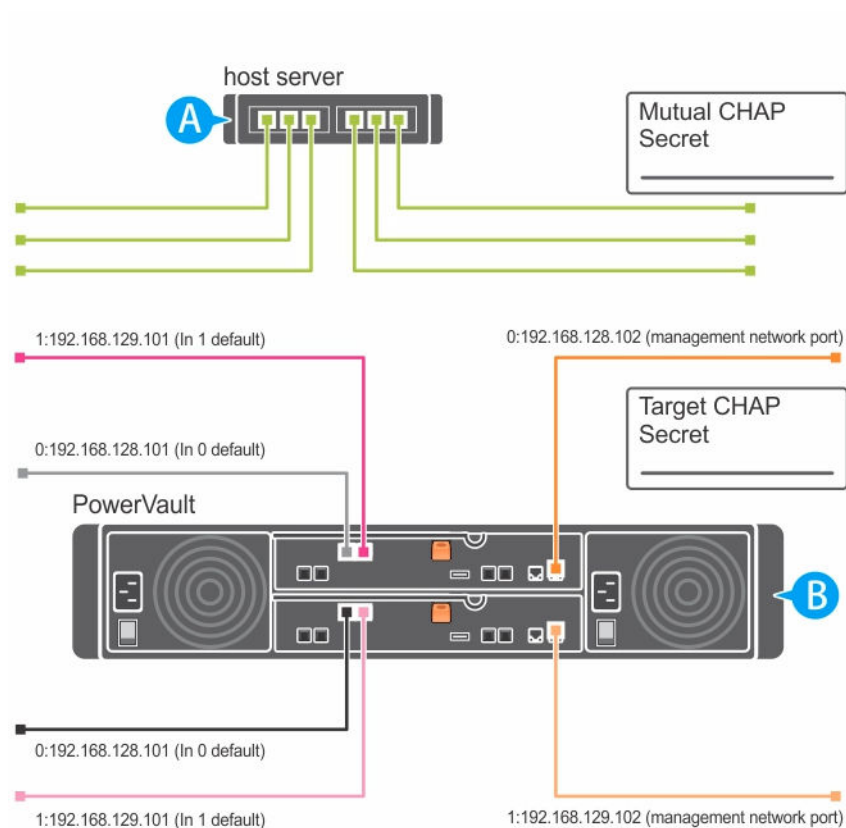


図 13. IPv4 設定 – ワークシート

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。

表 2. A 静的 IP アドレスの設定

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	-----	-----

表 3. B 静的 IP アドレスの設定

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、入力 0	-----	-----
iSCSI コントローラ 0、入力 1	-----	-----
管理ポート cntrl 0	-----	-----
iSCSI コントローラ 1、入力 0	-----	-----
iSCSI コントローラ 1、入力 1	-----	-----
管理ポート cntrl 1	-----	-----

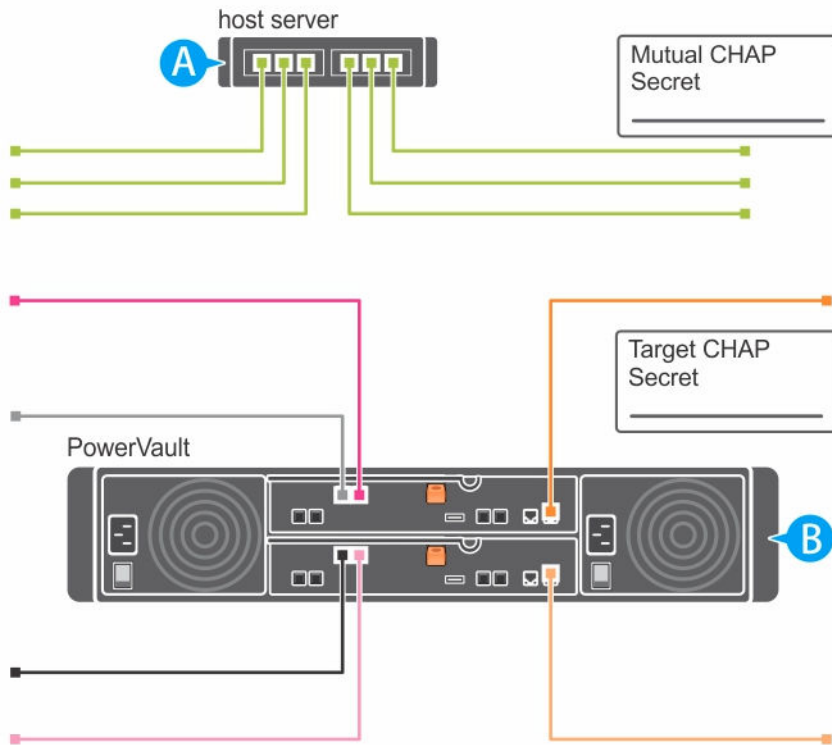


図 14. IPv6 設定 – ワークシート

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。

表 4. ホスト iSCSI ポート 1 と 2 の設定

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

表 5. ワークシートの設定

B ゲートウェイ	Gateway (ゲートウェイ)
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 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

ストレージアレイの iSCSI の設定


次の項では、お使いの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。ただし、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において、これらの手順をそれぞれどこで行うのかを理解することが重要です。次の表には、各 iSCSI 設定手順、およびそれらを行う箇所が説明されています。

表 6. 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: ストレージアレイの検出
	2: ストレージアレイでの iSCSI ポートの設定
3: iSCSI イニシエータからのターゲット検出の実行	4: ホストアクセスの設定
	5: (オプション) ストレージアレイでの CHAP 認証の設定
6: (オプション) ホストサーバーでの CHAP 認証の設定	
7: ホストサーバーからストレージアレイへの接続	8: (オプション) 帯域内管理のセットアップ

 **メモ:** iSCSI の設定には、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、上で説明した設定手順のガイドとなります。手動で設定を行う場合は、「[iSCSI の手動設定](#)」を参照してください。

Modular Disk Configuration Utility 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アレイを設定に対する統合された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 ホストポートとの負荷バランスの取れたパスを実現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** を選択した場合は、次回のホストサーバー再起動後にユーティリティが自動的に起動します。ユーティリティは手動で起動させることも可能です。

このユーティリティには文脈依存のオンラインヘルプがあり、ウィザードの各手順の指針となります。MDCU は次の設定を実行します。

- 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. 手順 2 以降を作業を繰り返して追加のレイを設定する。

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、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、ホストの設定オプションは無効になっています。また、オプションが無効化されていると、ユーティリティによって情報メッセージが表示されます。iSCSI ベースのストレージレイに接続されていないホスト（またはレイに接続したくないホスト）でユーティリティを実行している場合は、メッセージを無視してください。このタスクでは、通常次の手順を実行します。


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. 手順 2 以降を作業を繰り返して追加のレイに接続する。
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。

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

- 最適なパフォーマンスのため、ネットワーク設定を確認します。 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 (デュプレックス) 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。
- 最適な負荷バランシングを行うため、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 を使用したストレージレイの設定

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。

 **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。

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 ストレージソフトウェア** とクリックします。
 - 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 は、利用可能なすべてのストレージ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/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 ポートで使用するネットワーク環境および IP アドレス設定のための全般的なガイドラインを説明します。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 ポートと通信するには、ローカル NIC が IPv4 または 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 アドレスで設定されている必要があります。お使いの特定のネットワーク環境によっては、異なる手順、または追加手順が必要となる場合があるため、このセットアップを実行する前にシステム管理者に問い合わせるようにしてください。

 **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化され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 サーバーを使用した Microsoft ホストネットワークのセットアップ

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 アドレス設定を使用した Microsoft ホストネットワークのセットアップ

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 サーバーを使用した Microsoft ホストネットワークのセットアップ

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 サーバーを使用した Microsoft ホストネットワークのセットアップ

 **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で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 を使用した Linux ホストネットワークのセットアップ

DHCP を使用する場合（root ユーザーのみ）

1. **/etc/sysconfig/network** ファイルを、次を使って編集します。
`NETWORKING=yes HOSTNAME=mymachine.mycompany.com`
2. 設定ファイルを設定する接続用に編集します。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** です。
`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. `/etc/init.d/network restart` を使用して、ネットワークサービスを再起動します。

静的 IP アドレスを使用した Linux ホストネットワークのセットアップ

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. 設定ファイルを設定する接続用に編集します。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` です。

```
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. `/etc/init.d/network restart` を使用して、ネットワークサービスを再起動します。

MD ストレージ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

1. コントロールパネル から、プログラムの追加と削除 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. **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 ストレージソフトウェアのアンインストール

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。

Windows Server Core バージョンからの MD Storage ソフトウェアのアンインストール

1. `\Program Files\Dell\MD Storage Software\Uninstall Dell MD Storage Software` ディレクトリに移動します。
 **メモ:** MD Storage Manager はデフォルトで `\Program Files\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、**Uninstall Dell MD Storage Software** と入力し、<Enter> を押します。
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。
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. MD Storage Manager は、デフォルトで `/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、**Uninstall Dell MD Storage Software** ディレクトリを開き、**Uninstall Dell MD Storage Software.exe** ファイルを実行します。

アンインストールが完了すると、ルートプロンプトに戻ります。

iSCSI の手動設定

次の項では、お使いの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。ただし、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において、これらの手順をそれぞれどこで行うのかを理解することが重要です。次の表には、各 iSCSI 設定手順、およびそれらを行う箇所が説明されています。

表 7. 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
3. iSCSI イニシエータからのターゲットの検出。	1. ストレージレイを検出します。
6. (オプション) ホストサーバーでの CHAP 認証の設定。	2. ストレージレイの iSCSI ポートを設定します。
7. ホストサーバーからストレージレイへの接続。	4. ホストアクセスの設定。
	5. (オプション) ストレージレイでの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。
	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)

この手順は、IPv4 と IPv6 で異なります。

IPv4 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、約 3 分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。


コントローラ 0 のデフォルトの IP 設定は次のとおりです。

Port 0:192.168.129.101

コントローラ 1 のデフォルトの IP 設定は次のとおりです。

Port 0:192.168.129.102

 **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は、ストレージア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使用して初期設定を実行します。さらに、初期設定中、ストレージアレイのデフォルト管理ポートと同じ IP サブネット上で、少なくとも 1 つのネットワークアダプタを設定してください。初期設定後（管理ポートが MD Storage Manager を使用して設定済み）、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。

IPv6 管理ポートのデフォルト設定

ストレージアレイ管理ポートは、デフォルトで IPv6 ステートレス自動設定用に有効化されています。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、ポートはそれら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応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

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。

 **メモ:** この手順は、帯域外管理にのみ適用されます。帯域内管理のセットアップを選択する場合は、この手順を完了してから「手順 8: (オプション) 帯域内管理のセットアップ」に進んでください。

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 バイトを付加すると、FE80::0200:08FF:FEAA:BBCC になります。

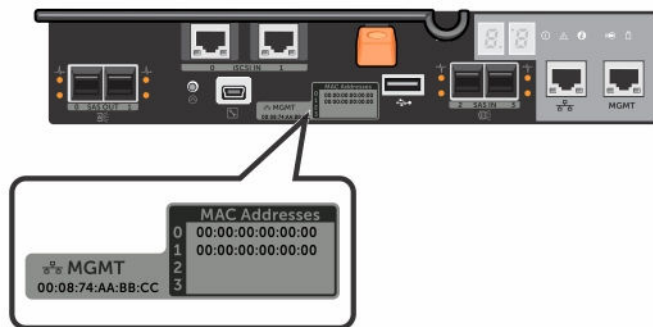




図 15. 管理ポート MAC アドレス

 **メモ:** この手順は、帯域外管理にのみ適用されます。帯域内管理のセットアップを選択する場合は、この手順を完了してから「[帯域内管理のセットアップ](#)」に進んでください。

ストレージアレイの検出は自動でも手動でも行うことができます。どちらかを選択し、次の手順を完了します。


ストレージアレイの自動検出

 **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。

1. MD Strage Manager (MDSM) 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。
検出プロセスの完了には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ステータス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。

検出が完了すると、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。

ストレージアレイの手動検出

 **メモ:** ポート番号がアレイの手動検出用に開いていることを確認します。

1. MDSM 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。
帯域外管理が正常に設定されました。検出の完了後、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。

ア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アレイの名前が MDSM の **サマリ** タブ下に表示されません。
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、残りの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、『Owner's Manual』（オーナーズマニュアル）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。


 **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 8. 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。	不正アクセスを防ぎます。MDSM は、設定の変更前、または破壊的な操作を行う前にパスワードを求める場合があります。
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（電子メール経由）および / または Dell Management Console などのストレージエンタープライズ管理コンソール（SNMP 経由）に通知します。
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 0, Port 1: IP: 192.168.131.101 Subnet Mask: 255.255.255.0 Port: 3260


Controller 1, Port 0: IP: 192.168.130.102 Subnet Mask: 255.255.255.0 Port: 3260

Controller 1, Port 1: IP: 192.168.131.102 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. **iSCSI ホストポートの設定** を選択します。
3. 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ます。VLAN として設定されているデバイスは、再設定することなく別の場所に移動させることができます。お使いのストレージレイで 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 – ホストサーバー iSCSI イニシエータからの iSCSI ログインをリッスンする、ストレージレイ上のポート番号です。

 **メモ:** iSNS サーバーの 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ア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。
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. 各 iSCSI ストレージアレイポートで ping コマンドを実行して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検出の実行

この手順では、ホストサーバーへのストレージアレイ上で、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 バージョンを使用した iSCSI イニシエータからのターゲット検出の実行

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、ストレージアレイの iSCSI ポートの IP アドレスまたは DNS 名を入力します。
4. iSCSI ストレージアレイがカスタム 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** – 接続するホストのソース 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) にストレージア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」に進んでください。
 - CHAP 認証を設定しない場合は、ストレージアレイのすべての iSCSI ポートで手順 1 ~ 6 を繰り返します。

Windows Server Core バージョンを使用した iSCSI イニシエータからのターゲットの検出の実行

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. `iscscli 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。

Linux を使用した iSCSI イニシエータからのターゲット検出の実行

Red Hat Enterprise Linux および SUSE Linux Enterprise Server 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、MDSM 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。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` line 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` line を変更するか、有効になっていることを確認します。これにより、起動時におけるサービスの自動的な起動が可能になります。
 - 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 サービスを再起動します。
4. コンソールからコマンド `chkconfig iscsi on` 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。
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、`scsiadm -m discovery -t st -p <IP_address_of_iSCSI_port>` を使用します。
6. ターゲットの検出後、`iscsiadm -m node -l` コマンドを使用して手動でログインします。このログインは、自動起動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. セッションから手動でログアウトするには、次のコマンド、`iscsiadm -m node -T <initiator_username> -p <target_ip> -u` を使用します。

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レイ上の仮想ディスクにアクセスするかを指定します。この手順は、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レイに接続するときに行う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. 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、**終了** をクリックします。

CHAP 認証の理解

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 認証を使用するときは、仮想ディスクをデータ受信用に準備する前に、ストレージアレイ (MDSM 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 認証の設定前にディスクをデータ受信用に準備すると、CHAP 設定後にディスクを認識できなくなります。

CHAP の定義

ターゲット CHAP 認証と相互 CHAP 認証の違いを要約するには、次の表を参照してください。


表 9. CHAP の種類の定義

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 : ストレージアレイでの CHAP 認証の設定 (オプション)

認証の種類 (ターゲットのみ、またはターゲットと相互) に関わらず、CHAP 認証を設定する場合は、この手順を完了する必要があります。


どの CHAP も設定しない場合は、この手順を省略して「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」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 を設定してください。

iSCSI 設定では、ターゲットという用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。
表で説明する CHAP 設定の 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 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**) します。**ターゲット CHAP シークレットの確認** で確認してから **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 シークレットは入力後、読み出すことができなくなります。シークレットは記録して、アクセス可能な場所に保管してください。ランダムシークレットの生成を使用した場合、ストレージアレイに追加する新規ホストサーバーの認証には同じ CHAP シークレットが使用されることから、今後の参照のため、シークレットをコピーしてテキストファイルにコピーします。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。この CHAP シークレットを忘れた場合は、ストレージアレイに連結されたすべてのホストを切断し、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。

表 10. CHAP 設定


オプション	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オンを許可します。
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、ストレージアレイはアクセスを許可する前に CHAP 認証を求めます。

‘ストレージアレイの相互 CHAP 認証の設定

イニシエータのシークレットは、ストレージア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一切許可しない場合は、**なし** を選択します。**なし** を選択した場合、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。このオプションは、セキュアなデータが必要ない場合に限り、使用してください。ただし、**なし** および **CHAP** を同時に選択することも可能です。
- **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)

「ストレージアレイでの 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。そうでない場合は、「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」に進みます。次にある、お使いのオペレーティングシステムに対応する項 (Windows または Linux) どちらかの手順一連を選択します。


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、ストレージア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、ストレージアレイの 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アレイで設定された 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、ストレージアレイ上の 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 – ストレージア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、ストレージアレイ上のすべての 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 \\
\`
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. ストレージア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ア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、ストレージアレイのすべての 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 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` ファイルの `node.session.auth.authmethod=CHAP` 行を有効にする必要があります。
2. ターゲットによるイニシエータの CHAP 認証用のユーザー名とパスワードを設定するには、次の行、`node.session.auth.username = <iscsi_initiator_username>`
`node.session.auth.password = <CHAP_initiator_password>` を編集します。
3. 相互 CHAP 認証を使用している場合は、次の行、`node.session.auth.username_in =
<iscsi_target_username> node.session.auth.password_in =
<CHAP_target_password>` を編集して、イニシエータによるターゲットの CHAP 認証用のユーザー名とパスワードを設定できます。

4. 検出セッションの CHAP 認証をセットアップするには、
discovery.sendtargets.auth.authmethod = CHAP 行からコメントを削除します。
5. 次の行、discovery.sendtargets.auth.username = <iscsi_initiator_username>
discovery.sendtargets.auth.password = <CHAP_initiator_password> を編集して、ターゲットによるイニシエータの検出セッション CHAP 認証用のユーザー名とパスワードを設定します。
6. 相互 CHAP のために、イニシエータによるターゲットの検出セッション CHAP 認証用のユーザー名とパスワードを設定するには、次の行、discovery.sendtargets.auth.username = <iscsi_target_username> discovery.sendtargets.auth.password_in = <CHAP_target_password> を編集します。
7. **/etc/iscsi/iscsid.conf** ファイル内に含まれる最終的な設定は、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 となります。


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

1. 開始 → YaST → iSCSI イニシエータをクリックします。
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。
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、各ターゲットで手順 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。

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


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. 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。
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 RAID 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 RAID 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 RAID 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 RAID 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 RAID 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 RAID 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 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

MDSM 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。どちらかに未接続または未設定が表示される場合、以下を確認し、iSCSI 設定の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セットアップと構成設定を確認するには、「ストレージレイでの 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

タスクの簡単な説明をここに入力してください (オプション)。帯域外管理 (「ストレージレイの検出 (帯域外管理のみ)」を参照) は、ストレージレイを管理するための推奨方法です。ただし、任意で帯域内管理をセットアップするには、次の手順に従ってください。参照用のデフォルト iSCSI ホストポート IPv 4 アドレスは次のとおりです。

- 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:** ネットワーク通信用に使用している管理ステーションを、PowerVault システムホストポートと同じ IP サブネットに設定します。

1. PowerVault 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。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、MD Storage Manager ソフトウェアを実行し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。


Internet Storage Naming Service の使用

Microsoft Windows iSCSI 環境でのみサポートされる Internet Storage Naming Service (iSNS) サーバーは、個々のストレージレイを、特定のイニシエータおよびターゲット IP アドレスのリストで手動設定する必要をなくします。iSNS は、その代わりにお使いの環境内にあるすべての iSCSI デバイスを自動で検出、管理、設定します。インストールおよび設定を含む iSCSI の詳細に関しては、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。

Windows Server オペレーティングシステムでの負荷バランスポリシーの変更

PowerVault MD シリーズストレージアレイとの負荷バランスは、次のいずれかを使用することによって、サブセット付きラウンドロビン（デフォルト）で実現できます。

- デバイスマネージャ
- ディスク管理

Windows Server デバイスマネージャを使用した負荷バランスポリシーの変更

Windows Server のデバイスマネージャを使用して負荷バランスポリシーを変更するには、次の手順を実行します。

1. **マイコンピュータ** を右クリックし、**管理** を選択して **コンピュータの管理** ダイアログボックスを開きます。
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** タブで、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 ディスク管理を使用した負荷バランスポリシーの変更

ディスク管理を使用して負荷バランスポリシーを変更するには、次の手順を実行します。

1. **マイコンピュータ** を右クリックし、**管理** をクリックして **コンピュータの管理** ダイアログボックスを開きます。
2. **ディスク管理** 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。

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 MD 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 2 つの 10G イーサネットポートがあります。同じコントローラ上の 2 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 PowerVault MD 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。

1つのTCP接続での2つのセッションは、ホストから各コントローラに設定されます（1つのポートにつき1セッション、合計2つのセッション）。マルチパスフェイルオーバードライバは、同じコントローラ上のポートに対するセッション全体のI/Oアクセスを分散します。各コントローラに仮想ディスクがあるデュプレックス構成では、両コントローラの各iSCSIデータポートを使用してセッションを作成することにより、帯域幅を増加させ、負荷分散を提供します。

Linux での iSCSI サービスの停止

次の手順に従って、Linux で iSCSI サービスを手動で停止します。iSCSI サービスをシャットダウンするには、次の手順を実行します。

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アンマウントします。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
```

。

困ったときは

デルへのお問い合わせ

デルでは、オンラインおよび電話によるサポートとサービスオプションをいくつかご用意しています。アクティブなインターネット接続がない場合は、ご購入時の納品書、出荷伝票、請求書、またはデル製品カタログで連絡先をご確認いただけます。これらのサービスは国および製品によって異なり、お住まいの地域では一部のサービスがご利用いただけない場合があります。販売、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関するデルへのお問い合わせは、

1. **Dell.com/support** にアクセスしてください。
2. お住まいの国を、ページ右下隅のドロップダウンメニューから選択します。
3. カスタマイズされたサポートを利用するには、次の手順に従います。
 - a. **Enter your Service Tag** (サービスタグの入力) フィールドに、お使いのシステムのサービスタグを入力します。
 - b. **Submit** (送信) をクリックします。
さまざまなサポートのカテゴリのリストが掲載されているサポートページが表示されます。
4. 一般的なサポートを利用するには、次の手順に従います。
 - a. 製品カテゴリを選択します。
 - b. 製品セグメントを選択します。
 - c. お使いの製品を選択します。
さまざまなサポートのカテゴリのリストが掲載されているサポートページが表示されます。
5. Dell グローバルテクニカルサポートへのお問い合わせ先詳細：
 - a. [Global Technical Support](#) (グローバルテクニカルサポート) をクリックしてください。
 - b. **テクニカルサポート** ページには、Dell グローバルテクニカルサポートチームへの電話、チャット、または電子メール送信のための詳細が記載されています。

Dell システムサービスタグの位置

ハードウェアは、一意のエクスプレスサービスコードとサービスタグ番号によって識別されます。エクスプレスサービスコードとサービスタグは、システム前面で情報タグを引き出して確認できます。

また、この情報はシステムのシャーシに貼られたシール上でも確認できます。この情報は、サポートへの電話問い合わせを適切な担当者に転送するためにデルによって使用されます。