

Dell™ PowerVault™ ネットワーク接続
ストレージ (NAS) ソリューション
iSCSI 導入ガイド

メモ、注意、警告



メモ：コンピュータを使いやすくするための重要な情報を説明しています。



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



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

本書の内容は予告なく変更されることがあります。
© 2009 すべての著作権は Dell Inc. にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

本書に使用されている商標：Dell、DELL のロゴ、および PowerVault は Dell Inc. の商標です。
Microsoft、Windows および Windows Server は米国またはその他の国における Microsoft Corporation の商標または登録商標です。

商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。Dell Inc. はデル以外の商標や社名に対する所有権を一切否認します。

目次

1	はじめに	5
	用語と定義	6
	PowerVault ストレージシステム	6
	iSCSI	6
	iSNS	6
	PowerVault ストレージソリューションを iSCSI	
	ターゲットとして設定する前に	6
	iSCSI ストレージエリアネットワーク設定のための	
	ベストプラクティス	7
2	イニシエータ - ターゲット接続の セットアップ手順	11
	前提条件	11
	メソッド 1 (ターゲットポータルを使用した検出)	11
	イニシエータ (ホスト) の設定	12
	PowerVault NAS ストレージシステムとの	
	iSCSI 接続の設定	12
	ターゲットの作成	12
	仮想ディスクの作成	14
	ログオン - イニシエータ (ホスト) からの	
	イニシエータ - ターゲット接続の設定	15
	メソッド 2 (iSNS サーバーを使用した検出)	16
	前提条件	16
	イニシエータからの設定	17
	ログオン - イニシエータ (ホスト) からの	
	イニシエータ - ターゲット接続の設定	18
3	ターゲットの詳細	19
	PowerVault™ NAS ストレージソリューションでの	
	ターゲット IP アドレスのセットアップ	19
	Microsoft® iSCSI ソフトウェアターゲットの	
	設定	19
	iSCSI LUN の設定	24

複数のセッション	25
iSCSI スナップショット	26
iSCSI デバイスの取り外し/クリーンアップ	30
イニシエータから	30
ターゲットから	31
4 チャレンジハンドシェイク認証プロトコルを 使用したセキュアな iSCSI 接続の設定	33
CHAP と IPSec	33
一方向の CHAP 認証	33
iSCSI ターゲットの設定	34
iSCSI イニシエータの設定	34
相互 CHAP 認証	35
イニシエータの設定	35
ターゲットの設定	36
イニシエータの設定の続き	36
A 付録 37	
イニシエータの詳細	37
General (全般) タブ	37
Discovery (検出) タブ	38
Targets (ターゲット) タブ	39
詳細な構成設定	42
イニシエータのマルチパスの有効化	42
詳細オプションの使い方	43
接続されているターゲットのプロパティの 確認	43
iSNS サーバーのインストールと設定	45
iSNS サーバーの設定	46
効率的なストレージ管理のためのベスト プラクティス	48
SAN ストレージマネージャ	48
iSCSI サブシステム用の LUN 管理	48
既知の問題	49

はじめに

本書には、Internet Small Computer System Interface (iSCSI) ソフトウェアターゲットを、ブロックストレージデバイスとして Dell™ PowerVault™ ストレージシステムに設定する方法に関する情報が説明されています。

iSCSI は新しいアプリケーション用のストレージを提供したり、または既存のアプリケーションにストレージのネットワークプールを提供する際に、有用で比較的安価な手段です。デルおよびストレージ部門の提携業者は、実装の容易なストレージソリューションを豊富に提供しています。本書により、管理者と IT マネージャは iSCSI テクノロジーについて調べ、導入の実例を参照することができます。

本書では、次の項目について説明します。

- クイックインストール手順 — iSCSI ターゲットを作成し、Microsoft® iSCSI イニシエータとの間に接続を確立する手順
- エンドツーエンドの iSCSI 設定
 - Microsoft iSCSI イニシエータソフトウェアおよび Microsoft iSCSI ソフトウェアターゲットのインストールと設定に関する詳細手順
 - イニシエータ - ターゲット接続の設定
- セキュリティで保護された iSCSI 接続のセットアップ
- Microsoft iSNS サーバーおよびその他の詳細設定



メモ：本書では、イニシエータは iSCSI イニシエータを、ターゲットは iSCSI ソフトウェアターゲットを指します。

用語と定義

次の項では、本書で使用される用語を説明します。

PowerVault ストレージシステム

本文書内における **PowerVault ストレージシステム** という用語は、個々のストレージユニットを指します。**PowerVault ストレージソリューション** という用語は、ストレージレイとは別になっているサーバー、またはストレージレイを備えたサーバーの構成を意味します。

iSCSI

SCSI コマンドを TCP/IP 経由で送受信する標準。ファイバーチャネルなどの専用ネットワークインフラを必要とせず、ブロックデータを IP ネットワーク経由で送受信することを可能にするプロトコルです。

システムストレージの分野では、iSCSI によって IP ネットワーク上の任意のクライアント/マシン（イニシエータ）が、リモートの専用サーバー（ターゲット）とコンタクトし、ローカルハードディスク上で行うかのようにターゲットでブロック I/O を行うことが可能になります。

iSNS

Microsoft iSCSI インターネット記憶域名前サービス（iSNS）は、iSNS クライアントから TCP/IP 経由で iSNS の登録、登録解除、およびクエリを処理し、これらの登録のデータベースを維持するサービスです（DNS サーバーに類似しています）。Microsoft iSNS サーバーの一般的な使い方は、iSNS クライアント（イニシエータとターゲット）が自らを登録し、登録済みの他の iSNS クライアントを照会できるようにすることです。登録とクエリは、TCP/IP 経由でリモートで処理されます。

Microsoft のサポートサイト www.microsoft.com から iSNS サーバーをダウンロードし、Microsoft iSCSI イニシエータまたはターゲットがインストールされていない別のサーバーにインストールすることができます。



メモ：iSNS サーバーのインストールおよび設定に関する詳細は、37 ページの「付録」を参照してください。

PowerVault ストレージソリューションを iSCSI ターゲットとして設定する前に

お使いのストレージソリューションを iSCSI ターゲットとして設定する前に、本項をよくお読みください。iSCSI ターゲット用のイーサネット設定およびセキュリティ設定といった機能を考慮する必要があります。

iSCSI ストレージエリアネットワーク設定のためのベストプラクティス

表 1-1 には、異なるモデルの iSCSI ネットワークにターゲット上の NIC を設定することに関する情報が記載されています。

- イニシエータ（ホスト）に冗長パスを設定することができます。Microsoft マルチパス I/O (MPIO) は、バージョン 2.06 またはそれ以降のイニシエータでサポートされています。
- PowerVault ストレージソリューションにおける効率的な MPIO 接続のためには、ターゲットおよびイニシエータに 2 つの専用 iSCSI NIC が必要です。
- iSCSI NIC チーミングはサポートされていません。
- 必要に応じて、iSCSI 専用 NIC 1 つ、または 2 つでイニシエータを設定することができます。



メモ: 表 1-1 には、iSCSI ターゲット NIC 構成に関する情報が説明されています。オプションとして、最適な接続情報も提供されています。お使いのネットワーク要件に基づいて iSCSI NIC を設定できます。

表 1-1. ターゲットとしての単一の PowerVault ストレージソリューションの使用

NIC の数	詳細	参照図
4	NIC-1 および NIC-2 - パブリックネットワーク用のチーミングされた NIC NIC-3 - iSCSI 専用トラフィック (サブネット A) NIC-4 - iSCSI 専用トラフィック (サブネット B)	図 1-1
3	NIC-1 - パブリックネットワーク用の NIC NIC-2 - iSCSI 専用トラフィック (サブネット A) NIC-3 - iSCSI 専用トラフィック (サブネット B)	図 1-2

メモ: iSCSI トラフィックの優先度がファイルトラフィックより高い場合は、この構成を使用してください。

- 2 つのポートを iSCSI 専用のポートにすることをお勧めします。各 NIC (マルチポート NIC の場合はポート) を個別のサブネットに設定します。
- チャレンジハンドシェイク認証プロトコル (CHAP) によるセキュアな iSCSI が可能です。CHAP 設定に関する詳細は、33 ページの「チャレンジハンドシェイク認証 プロトコルを使用したセキュアな iSCSI 接続の設定」を参照してください。

表 1-2. ワークシート

	オプション	ホスト IP	ターゲット IP
NIC 1	iSCSI		
	パブリック		
	その他		
NIC 2	iSCSI		
	パブリック		
	その他		
NIC 3	iSCSI		
	パブリック		
	その他		
NIC 4	iSCSI		
	パブリック		
	その他		

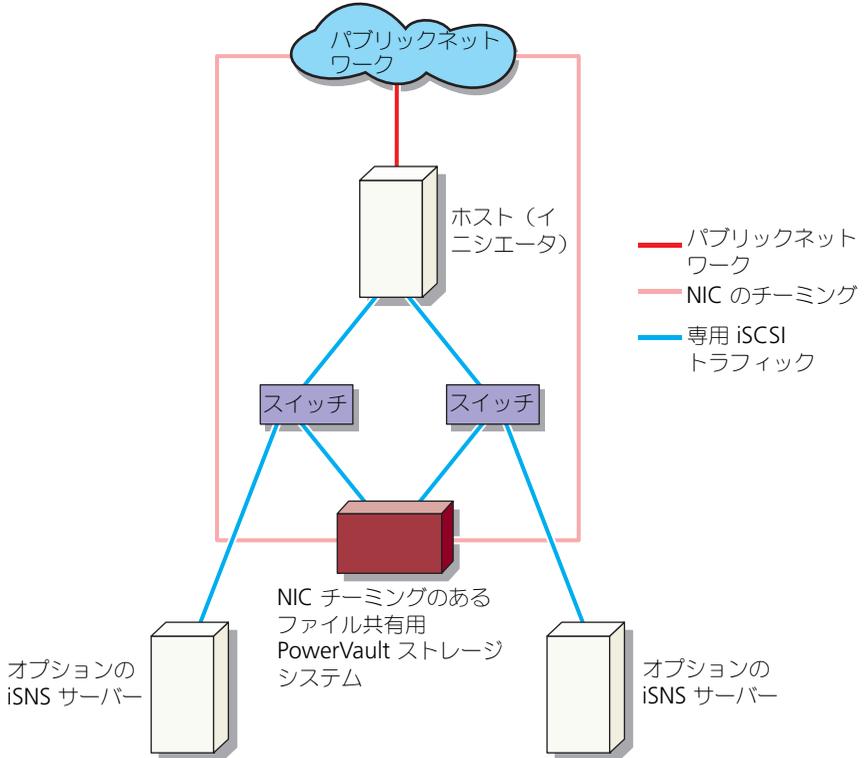


メモ: IQN はターゲットおよびイニシエータを識別するための標準命名規則なので、できる限り IQN を識別子として使用することをお勧めします。



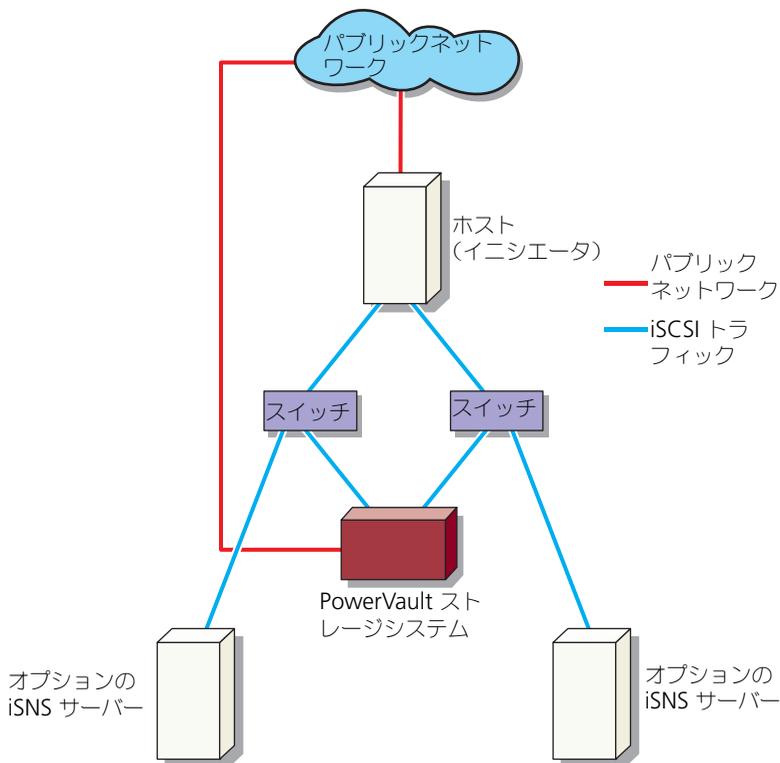
メモ: 専用の iSCSI NIC を、パブリックネットワーク上ではなく、別のサブネット上に設定することをお勧めします。

図 1-1. 4つのNICを使用したデータ共有のための冗長 iSCSI パスおよび NIC チーミング



メモ : iSCSI ターゲットの詳細設定に関しては、19 ページの「ターゲットの詳細」を参照してください。

図 1-2. 3つのNICを使用した冗長 iSCSI バス



メモ: iSCSI ターゲットの詳細設定に関しては、19 ページの「ターゲットの詳細」を参照してください。

イニシエータ - ターゲット接続の セットアップ手順

本項では、iSCSI ターゲットをセットアップし、イニシエータからの接続を確立するための詳しい手順を説明します。これは、ユーザーが次を理解していること前提としています。

- iSCSI プロトコルの操作
- iSCSI イニシエータ - ターゲット接続の情報
- Microsoft® iSCSI イニシエータ、Microsoft ソフトウェア iSCSI ターゲット、および Microsoft iSNS サーバーのインストールおよびセットアップ

前提条件

iSCSI ターゲットをセットアップする前に、必ず次の手順を行ってください。

- 1 Microsoft サポートサイト **support.microsoft.com** から最新の Microsoft iSCSI イニシエータソフトウェアをダウンロードし、イニシエータ（ホスト）をインストールします。
- 2 MS ソフトウェア iSCSI ターゲットを、付属の CD からお使いのストレージシステムにインストールします。
- 3 8 ページの「ワークシート」を使って iSCSI ネットワーク用の IP アドレスを設定し、割り当てます。

iSCSI ターゲットを設定する前に、次のタスクを実行してください。

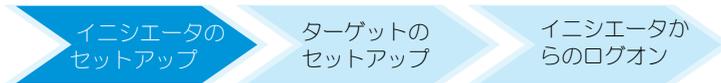
- 1 数個の LUN を作成し、iSCSI ターゲット用の仮想ディスクを作成するためのストレージスペースを確保しておきます。
- 2 **iSCSI Target**（ターゲット）を右クリックし、**Properties**（プロパティ）を選択して iSCSI トラフィック専用の iSCSI NIC を設定します（21 ページの図 3-1 「iSCSI ターゲットの作成」を参照）。

メソッド 1（ターゲットポータルを使用した 検出）

ターゲットの検出を行うには、イニシエータ内で iSCSI トラフィック用に設定された PowerVault ストレージシステムの NIC のいずれかの IP アドレスを入力します。これによってイニシエータは、このターゲットサーバーのすべてのターゲットを検出できるようになります。

次の手順は iSCSI ターゲットを設定し、イニシエータからの接続を確立する方法を説明します。

イニシエータ（ホスト）の設定



ターゲットサーバー情報の IP アドレスを使用して、Microsoft iSCSI イニシエータを設定します。イニシエータを設定するには次を実行します。

- 1 Microsoft iSCSI イニシエータがインストールされているシステムに移動します。
- 2 **Start**（スタート） → **Programs**（プログラム） → **Microsoft iSCSI Initiator**（Microsoft iSCSI イニシエータ） → **iSCSI Initiator Properties**（iSCSI イニシエータプロパティ） → **Discovery**（検出）タブをクリックします。
- 3 **Add portal**（ポータル追加）を選択します。
- 4 iSCSI トラフィック用に設定された PowerVault ストレージシステムの、いずれかの NIC の IP アドレスを追加します（図 1-1 を参照）。
- 5 **OK** をクリックします。

PowerVault NAS ストレージシステムとの iSCSI 接続の設定



ターゲットの作成

- 1 PowerVault NAS アプライアンスから、**Start**（スタート） → **Server Manager**（サーバーマネージャ） → **Storage**（ストレージ） → **MS Software Target**（MS ソフトウェアターゲット）と選択します。
- 2 **Microsoft iSCSI Software Target**（Microsoft iSCSI ソフトウェアターゲット）アイコンを選択します。
iSCSI Target（ターゲット）、**Device**（デバイス）、および **Snapshot**（スナップショット）というオプションが表示されます。
- 3 **iSCSI Target**（ターゲット）を選択し、**Actions**（アクション）タブで、**More Actions**（その他の操作）オプションを右クリックまたは選択します。
- 4 **Create iSCSI Target**（iSCSI ターゲットの作成）オプションを選択します。

- 5 **Welcome to the Create iSCSI Target wizard** (iSCSI ターゲットの作成ウィザードの開始) 画面が表示されます。**Next** (次へ) を選択します。ウィザードの指示に従ってターゲットを作成します。
- 6 **Create iSCSI Target** (iSCSI ターゲットの作成) ウィザードに **iSCSI Target Identification** (iSCSI ターゲット ID) オプションが表示されます。iSCSI ターゲット用の **Name** (名前) と **Description** (説明) (オプション) を入力して、**Next** (次へ) をクリックします。**iSCSI initiators identifiers** (iSCSI イニシエータの識別子) 画面が表示されます。
- 7 **Browse** (参照) をクリックして、ターゲットに接続するホストの **IQN** を選択します。12 ページの「イニシエータ (ホスト) の設定」における手順 1 が正常に完了した場合にのみホストがリスト表示されます。
 **メモ**: IQN 識別子フィールドの入力は必須です。イニシエータ IQN 識別子を追加するには、IQN 識別子を入力するか、または画面の **Browse** (参照) および **Advanced** (詳細) オプションを使用して追加します。Browse (参照) オプションの詳細については、手順 8 を参照してください。Advanced (詳細) オプションについては、手順 9 を参照してください。
- 8 **Browse** (参照) オプションを選択した場合は、次の手順を実行して **IQN 識別子** を選択することができます。
 - a **Browse** (参照) を選択すると、**Add iSCSI Initiator** (iSCSI イニシエータの追加) 画面が表示されます。
 - b iSCSI イニシエータリストの詳細が表示されます。iSCSI イニシエータを入力するか、またはリストから選択し、iSCSI イニシエータ名を入力して **OK** を選択します。**iSCSI Initiators Identifiers** (iSCSI イニシエータの識別子) 画面の **IQN identifier** (IQN 識別子) フィールドには、入力または選択した値が表示されます。**Next** (次へ) を選択します。手順 10 に進みます。
- 9 **Advanced** (詳細) オプションを選択した場合は、次の手順に従って **IQN 識別子** を選択します。
 - a **Advanced** (詳細) オプションを選択した場合、**Advanced Identifiers** (詳細識別子) 画面が表示され、**Add** (追加) オプションを表示します。**Add** (追加) を選択します。
 - b **Add/Edit Identifier** (識別子の追加 / 編集) が表示され、**IQN 識別子** の追加オプションとして、**IQN**、**DNS Domain Name** (DNS ドメインネーム)、**IP address** (IP アドレス)、および **MAC Address** (MAC アドレス) という 4 つのオプションが示されます。4 つのオプションの中から 1 つを選択します。
 - c 値を入力するか、または **Browse** (参照) オプションから値を選択して、**OK** を選択します。

Advanced Identifiers (詳細識別子) 画面に **IQN 識別子**が表示され、**IQN**、**DNS Domain Name** (DNS ドメインネーム)、**IP Address** (IP アドレス)、および **MAC Address** (MAC アドレス) の各フィールドに値が表示されます。

- d 表示されている値を選択し、**OK** をクリックします。
- e **iSCSI Initiator Identifiers** (iSCSI イニシエータの識別子) 画面で、**IQN identifier** (IQN 識別子) フィールドには適切な情報が表示されています。別の識別子を表示するには、**Advanced** (詳細) をクリックします。
- f **Next** (次へ) を選択します。



メモ : IQS は DNS の設定にかかわらず動作します。イニシエータの IP アドレスまたは MAC アドレスも DNS 設定に関係なく指定することができます。DNS ドメイン名を指定するオプションは、iSCSI ソフトウェアターゲットスナップインに組み込まれています。DNS 名を使用する際は、DNS を正しく設定し (前方参照および逆引き参照ゾーンを含む)、イニシエータの完全修飾ドメイン名 (FQDN) を指定する必要があります。イニシエータ FQDN の指定後にターゲットをイニシエータに接続できない場合、ターゲットサーバーで **nslookup InitiatorIP** コマンドを実行し、逆引き参照が正しく有効化されているかを確認します。
nslookup コマンドの失敗は、DNS 逆引き参照が設定されていないことを示します。この場合、ターゲットがイニシエータ IQN、IP アドレス、または MAC アドレスを使用するように再設定します。

- 10 **Completing the Create iSCSI Target** (iSCSI ターゲットの作成の完了) ウィザードが表示されます。**Finish** (終了) をクリックします。

仮想ディスクの作成

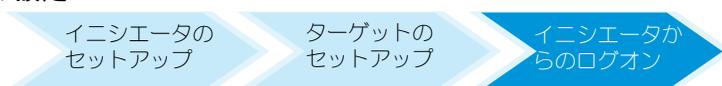
- 1 新しく作成したターゲットを右クリックし、**Create Virtual Disk for iSCSI Target** (iSCSI ターゲット用の仮想ディスクの作成) をクリックします。**Create Virtual Disk** (仮想ディスクの作成) ウィザードが表示されます。**Next** (次へ) を選択します。
- 2 ファイルを作成するには、**Browse** (参照) オプションを選択し、ストレージアレイ上のボリュームを選択して、拡張子 **.vhd** を付けたファイル名を入力します。
例えば、Z がマウントされているストレージアレイのボリュームで、**vol1.vhd** がファイル名である **Z:%vol1.vhd** というファイルを作成します。**Next** (次へ) を選択します。
- 3 **Size** (サイズ) 画面で、**Currently available free space** (現在使用可能な空き領域) から適切なサイズを選択し、**Next** (次へ) を選択します。
- 4 **Description** (説明) 画面が表示される場合もあります。必要に応じて仮想ディスクの説明を入力し、**Next** (次へ) をクリックします。

- 5 **Add** (追加) 画面でターゲット名を選択し、**Next** (次へ) をクリックします。
- 6 **Completing the Create Virtual Disk** (仮想ディスク作成の完了) ウィザードが表示されます。**Finish** (終了) をクリックします。

△ **注意**: 複数のホストが同じターゲットにアクセスすると、データ破損が発生する場合があります。詳細については、42 ページの「イニシエータのマルチパスの有効化」を参照してください。

✍ **メモ**: 同じボリューム上に複数の VHD を作成することができます。

ログオン - イニシエータ (ホスト) からのイニシエータ - ターゲット接続の設定



- 1 iSCSI イニシエータ (ホスト) で、**Start** (スタート) → **Program** (プログラム) → **Microsoft iSCSI Initiator** (Microsoft iSCSI イニシエータ) → **iSCSI Initiator Properties** (iSCSI イニシエータのプロパティ) → **Targets** (ターゲット) タブの順にクリックします。
- 2 画面を更新します。12 ページの「PowerVault NAS ストレージシステムとの iSCSI 接続の設定」で作成した PowerVault ストレージシステムのターゲットデバイスが IQN 名形式で表示されます。
- 3 **Log On to Target** (ターゲットへのログオン) ウィンドウで、**Logon** (ログオン)、**Automatically Restore** (自動復元) と **Enable multipath** (マルチパスの有効化) オプションを選択します。
- 4 **Advanced** (詳細) をクリックします。**Advanced Settings** (詳細設定) ウィンドウで、**General** (全般) タブを選択し、ドロップダウンメニューから次のオプションを選択します。
 - **Local Adapter** (ローカルアダプタ) — Microsoft iSCSI イニシエータ
 - **Source IP** (送信元 IP) — iSCSI トラフィックに使用されるホスト IP アドレスのひとつ
 - **Target Portal** (ターゲットポータル) — PowerVault ストレージソリューションの iSCSI IP アドレス
- 5 **Advanced Settings** (詳細設定) ウィンドウで、**OK** をクリックします。
- 6 **Log On to Target** (ターゲットへログオン) ウィンドウで、**OK** をクリックします。

Targets (ターゲット) タブには、ターゲットのステータスが **Connected** (接続済み) として表示されます。

- 7 マルチパス機能を実行するには、**Microsoft MPIO** を使用してホストから同じターゲットデバイスへのマルチパスセッションを確立することができます。複数のセッションを確立するには次を実行します。
 - a **Targets** (ターゲット) タブをクリックし、**Connected** (接続済み) のターゲットを選択します。
 - b 手順 1 から手順 5 を繰り返します。
 - c **Advanced Setting** (詳細設定) をクリックします。**Target Portal** (ターゲットポータル) アドレスでは、冗長ホスト IP アドレスおよび PowerVault ストレージソリューションの IP アドレスを選択します。



メモ: iSCSI イニシエータソフトウェアのインストール中に、Microsoft MPIO はすでに選択されています。MPIO はバージョン 2.06 またはそれ以降のイニシエータでサポートされています。効率的な MPIO 接続のためには、ターゲットとイニシエータに 2 つの専用 iSCSI NIC が必要です。Multiple connections per session (MC/S) は、PowerVault ストレージソリューションではサポートされていません。

- 8 iSCSI デバイスをローカルドライブとして初期化および設定し、iSCSI I/O 操作を実行するには、**Computer Management** (コンピュータの管理) → **Disk Management** (ディスクの管理) オプションの順に選択します。



注意: 複数のホストが同じターゲットにアクセスすると、データ破損が発生する場合があります。詳細については、42 ページの「イニシエータのマルチパスの有効化」を参照してください。

メソッド 2 (iSNS サーバーを使用した検出)

本項では、iSNS サーバーを使用して iSCSI ターゲットの検出を行う手順を説明します。iSNS サーバーの詳細については、37 ページの「付録」を参照してください。

前提条件

iSCSI ターゲットの検出を行う前に、以下の手順を実行します。

- 1 iSNS サーバーとして動作するシステムを識別します。
- 2 イニシエータおよびターゲットが iSNS サーバーと同じネットワーク上にあることを確認します (図 1-1 および 図 1-2 を参照)。
- 3 Microsoft サポートサイト **support.microsoft.com** から Microsoft iSCSI イニシエータソフトウェアをダウンロードし、イニシエータ (ホスト) をインストールします。

- Microsoft サポートサイト support.microsoft.com から Microsoft iSCSI サーバソフトウェアをダウンロードし、Microsoft® Windows® オペレーティングシステムを実行するクライアント / サーバにソフトウェアをインストールします。

 **メモ:** iSNS サーバソフトウェアをイニシエータ (ホスト) またはターゲット (PowerVault ストレージソリューション) にインストールしないでください。同ソフトウェアは、Windows OS が実行されている別のクライアント / サーバにインストールしてください。

- PowerVault ストレージシステムに電源を入れ、iSCSI ターゲット用の仮想ディスクを作成するためストレージアレイにひとつ、または複数のボリュームを作成します。

イニシエータからの設定



- iSNS サーバの情報を使用して Microsoft iSCSI イニシエータを設定します。**Start** (スタート) → **Programs** (プログラム) → **Administrative Tools** (管理ツール) → **Microsoft iSCSI Initiator** (Microsoft iSCSI イニシエータ) → **Discovery tab** (検出タブ) → **Add iSNS** (iSNS の追加) と進みます。
- iSNS サーバの IP アドレスを追加し、**OK** をクリックします (図 1-1 および図 1-2 を参照)。

ターゲットのセットアップ (PowerVault ストレージシステム)



- PowerVault ストレージシステムから、**Start** (スタート) → **Server Manager** (サーバマネージャ) → **Storage** (ストレージ) → **Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) と進みます。
PowerVault Server Manager Management Console (PowerVault サーバマネージャ管理コンソール) が表示されます。
- ストレージスナップインにある **Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) を選択し、**Properties** (プロパティ) を右クリックします。
- Properties** (プロパティ) ウィンドウで、**iSNS** タブを選択し、iSNS サーバ情報 (DNS 名または IP アドレス) を追加します。

 **メモ:** iSCSI ネットワーク用の NIC のみをチェックすることをお勧めします。

- 4 ターゲットを作成するには、12 ページの「PowerVault NAS ストレージシステムとの iSCSI 接続の設定」の手順に従ってください。



メモ: 手順 7 のターゲットの設定中、**Browse** (参照) オプションを使用して iSNS サーバーに登録されているすべてのイニシエータが **iSCSI Initiator Identifier** (iSCSI イニシエータ識別子) 画面表示されていることを確認します。

- 5 仮想ディスクを作成するには、14 ページの「仮想ディスクの作成」の手順に従ってください。

ログオン - イニシエータ (ホスト) からのイニシエータ - ターゲット接続の設定

イニシエータ - ターゲット接続の設定に関する詳細は、15 ページの「ログオン - イニシエータ (ホスト) からのイニシエータ - ターゲット接続の設定」を参照してください。

ターゲットの詳細

本項では、iSCSI イニシエータ、ターゲット、および接続の確立のための設定を含む、エンドツーエンドの iSCSI のセットアップについて説明します。

PowerVault™ NAS ストレージソリューションでのターゲット IP アドレスのセットアップ

システムの構成（1 つ、または 2 つの専用 iSCSI NIC 装備）に応じて、iSCSI NIC に IP アドレスを割り当てます。イニシエータの **Target Portals**（ターゲットポータル）タブで iSCSI NIC に割り当てた IP アドレスを検索に使用します。

Microsoft® iSCSI ソフトウェアターゲットの設定

iSCSI ターゲットを設定する前に、数個の LUN を作成し、iSCSI ターゲット用の仮想ディスクを作成するためのストレージスペースを確保する必要があります。次の項では、ストレージスペースを作成するための詳しい手順を説明します。

- 1 iSCSI ターゲットデバイス上でのネットワークの設定 — PowerVault NAS ストレージソリューションは、デフォルトで、ネットワーク設定に DHCP を使用するように設定されています。PowerVault NAS ストレージシステムはマルチパス操作用に設計されており、RJ-45 イーサネットコネクタが 2 つ装備されています。オプションの NIC を 1 つ追加することも可能です。**PowerVault NAS Configuration tasks**（PowerVault NAS 設定タスク）ウィンドウで基本設定が表示されます。



メモ：専用の iSCSI NIC を、パブリックネットワーク上ではなく、別のサブネット上に設定することをお勧めします。



メモ：この時点で、ストレージソリューション LUN のサイズを iSCSI ターゲットのサイズと混同しないよう注意することが重要です。iSCSI ターゲットは手順の後半で設定され、ホストサーバー上の特定のアプリケーションに必要なストレージに関連しています。ストレージハードウェアの LUN のサイズは、作成された LUN の下層である物理ディスクの使用を、ストレージサブシステムが最適化できるような大きさにすることをお勧めします。この場合、次に示されているように、このハードウェアに利用可能な最大サイズでの LAN をひとつ作成します。この iSCSI LUN は、ホストアプリケーションの必要に応じて後に作成される iSCSI ターゲットには対応できません。

- 2 LUN 使用のための準備 — PowerVault NAS ストレージソリューションは Microsoft Windows® オペレーティングシステムベースのプラットフォームで実行されます。内蔵サーバー用のドライブ文字の割り当て、ボリュームの命名など、LUN 使用のための準備手順は、Windows オペレーティングシステムのセットアップに沿っています。セットアップウィザードは必要な情報のためのプロンプトを表示し、その後、ストレージ設定に必要なタスクを実行する前にサマリ画面が表示されます。

LUN が作成され、使用可能になりました。手順 3 により iSCSI ターゲットが作成され、新しく作成された LUN と iSCSI ターゲットが関連付けられます。

- 3 PowerVault ストレージソリューションにおける iSCSI トラフィック用 NIC の設定 — まず iSCSI トラフィック用に専用 iSCSI NIC を設定してから、iSCSI ターゲットを作成する必要があります。

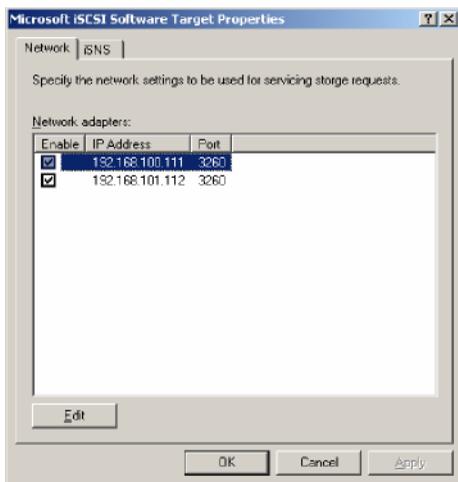
 **メモ** : iSCSI ターゲットの作成は、iSCSI イニシエータの **Discovery** (検出) タブを設定した後でのみ行ってください。

専用 iSCSI NIC を設定するには、次を実行します。

- a **PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) → **iSCSI Target** (iSCSI ターゲット) と進みます。
- b iSCSI Software Target (iSCSI ソフトウェアターゲット) を右クリックし、**Properties** (プロパティ) を選択します。
- c **Microsoft iSCSI Software Target Properties** (プロパティ) ウィンドウで、**Network** (ネットワーク) タブをクリックします。PowerVault NAS ストレージソリューション上のすべての NIC が一覧表示されます。
- d **Edit** (編集) をクリックし、リストからパブリックおよびプライベートネットワーク IP アドレスのチェックを外します。リストからパブリックおよびプライベートネットワーク IP アドレスのチェックを外すことで、専用 iSCSI NIC のみが確実に iSCSI トラフィック用に設定されます。
- e ネットワーク内に iSNS サーバーが設定されている場合は、**iSNS** タブをクリックし、iSNS サーバーの IP アドレスを追加します。**OK** をクリックします。

- 4 iSCSI ターゲットの作成 — iSCSI ターゲットを作成するには次の手順を実行します。

図 3-1. iSCSI ターゲットの作成



- a **PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) で、左ペインの **iSCSI Target (iSCSI ターゲット)** を右クリックして **Create iSCSI Target Wizard** (iSCSI ターゲットの作成ウィザード) を起動します。
Welcome to the Create iSCSI Target wizard (iSCSI ターゲットの作成ウィザードへようこそ) 画面が表示されます。
- b **Next** (次へ) をクリックします。
iSCSI Target identification (iSCSI ターゲット ID) 画面が表示されます。
- c **ターゲット名** と **説明** を入力します。 **Browse** (参照) オプションを使用して、ネットワーク内のサーバー/クライアントを表示および選択します。
iSCSI initiators identifiers (iSCSI イニシエータの識別子) 画面が表示されます。各 iSCSI ターゲットを iSCSI イニシエータと関連付ける必要があります。iSCSI イニシエータは、iSCSI ターゲット名によって表されるストレージに対するアクセスを要求するホストです。
- d **iSCSI Initiators Identifiers** (iSCSI イニシエータの識別子) 画面で、iSCSI イニシエータの iSCSI 修飾名 (IQN) を入力します。IQN を手動で入力するか、または **Browse** (参照) オプションを使用してリストから iSCSI イニシエータを選択します。 **Advanced** (詳細) オプ

ションを使って iSCSI イニシエータを識別することもできます。

Advanced (詳細) をクリックすると、**Advanced Identifiers** (詳細識別子) 画面が表示されます。**Advanced Identifier** (詳細識別子) 画面で、**Add** (追加) をクリックし、識別子の種類と特定の識別情報を入力します。

Advanced Identifier (詳細識別子) → **Add** (追加) → **Add/Edit Identifier** (識別子の追加 / 編集) → **Identifier Type** (識別子の種類) と進み、イニシエータ識別子を追加するため IQN、DNS ドメイン名、IP アドレス、または MAC アドレスのいずれかを選択します。図 A-5 では IP アドレスを使用して iSCSI イニシエータを識別します。**Browse** (参照) オプションを使用して、使用可能なターゲットのリストから値を選択することができます。

 **メモ:** IQN を識別子として使用することをお勧めします。

これで、**PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) に新しく作成された iSCSI ターゲットが表示されます。**PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) には、iSCSI ターゲットに使用できるデバイスも表示されます。iSCSI イニシエータ (アプリケーションホスト) によって使用されるストレージは、後で仮想ディスクの作成時に定義されます。

- 5 仮想ディスクの作成とターゲットへの割り当て — Microsoft ベースの iSCSI ターゲットソリューションのために、iSCSI ターゲット上に仮想ディスクを作成する必要があります。仮想ディスクは、iSCSI イニシエータが使用するストレージボリュームを表します。Microsoft ベースの iSCSI ターゲットソリューション上の特定の iSCSI ターゲットに含まれるすべての仮想ディスクの最大容量は、ターゲットあたり 16 テラバイト (16 TB) です。

次の手順では仮想ディスクの作成方法を説明します。この例では、100 GB の仮想ディスクと 200 GB の仮想ディスクが iSCSI ターゲット上に作成されます。iSCSI イニシエータは、これら 2 つの仮想ディスクを TCP/IP ネットワーク上のボリュームとして識別します。

- a ターゲット名を右クリックして、**Create Virtual Disk Wizard** (仮想ディスクの作成ウィザード) を起動します。
- b **Next** (次へ) をクリックします。**File** (ファイル) 画面が表示されます。iSCSI ターゲットで使用できる内蔵ディスクボリューム (接続されているストレージアレイから利用可能な RAID ボリューム) 上に仮想ディスクを作成します。

 **メモ:** **File** (ファイル) 画面で、**Browse** (参照) オプションを使用して内蔵ディスクボリュームを選択し、拡張子 **.vhd** を持つ仮想ディスクファイルの名前を入力します。

- c **Next** (次へ) をクリックします。**Size** (サイズ) 画面が表示されます。仮想ディスクのサイズは、ホストサーバー上のアプリケーションの必要性によって左右されます。

- d 仮想ディスクのサイズを選択し、**Next**（次へ）をクリックします。この例では、このボリューム上で使用可能な **501 GB** から **100 GB** のサイズを選択します。
Description（説明）画面が表示されます。
- e **Description**（説明）フィールドの入力は任意です。ただし、管理上、入力しておくことをお勧めします。
- f **Next**（次へ）をクリックします。**Access**（アクセス）画面が表示されます。
- g **Add**（追加）をクリックし、iSCSI ターゲット情報を入力します。
アプリケーションホストが仮想ディスクを iSCSI ストレージボリュームとして使用するには、仮想ディスクを iSCSI ターゲットと関連付ける必要があります。
- h **Next**（次へ）をクリックします。**Completing the Create Virtual Disk Wizard**（仮想ディスクの作成の完了ウィザード）が表示され、仮想ディスクが正常に作成されたことが示されます。
- i 追加の仮想ディスクを作成するには、手順 a ～ 手順 h を繰り返します。
仮想ディスクの設定が完了すると、**PowerVault NAS Management Console**（PowerVault NAS 管理コンソール）に iSCSI ターゲットと関連付けられた仮想ディスクが表示されます。

iSCSI Target device（iSCSI ターゲットのデバイス）ビューには、合計ボリュームサイズと、iSCSI ターゲット用に使用できるデバイス（RAID ボリューム）上の空き領域が表示されます。

iSCSI ターゲットの設定は、これで完了です。

デバイスの設定

仮想ディスク（デバイス）に関連するすべての操作は、**PowerVault NAS Management Console**（PowerVault NAS 管理コンソール）にある次のオプションを使用して実行できます。

- **Create/Delete Virtual Disk**（仮想ディスクの作成 / 削除）— 仮想ディスクには拡張子 **.vhd** で示されます。このオプションを使用して仮想ディスクを作成または削除できます。
- **Extend Virtual Disk**（仮想ディスクの拡張）— データを失ったり iSCSI ターゲットを再起動することなく、iSCSI 仮想ディスクのサイズを動的に増やすことができます。
- **Import**（インポート）— 同じサーバー、または異なるサーバーで以前に作成された古い仮想ディスク、および既存の仮想ディスクをインポートできます。この機能はソフトウェアアップグレードの最中に便利です。

- **Disable**（無効化） — 仮想ディスクを一時的にオフラインにし、**Enable**（有効化）オプションを使ってオンラインに戻すことができます。
- **Assign/Remove Target**（ターゲットの割り当て / 削除） — ひとつ、または複数のターゲットと仮想ディスクを関連付けたり、既存の関連を削除します。
- **Create Snapshot**（スナップショットの作成） — 仮想ディスクの内容のスナップショットを常時作成できます。
- **Disk Access**（ディスクアクセス） — 読み取り / 書き込みをマウントします（PowerVault NAS ストレージシステムのボリュームとしてマウントすることによる仮想ディスクの読み取り / 書き込みアクセス設定で、マウントされた仮想ディスクはローカルディスクとして表示されます）。



注意：仮想ディスクをマウントする前に、同じ仮想ディスクを使用するすべての **iSCSI ターゲット** を切断します。切断しなかった場合、データ破損の原因となる可能性があります。



メモ：負荷分散とフェイルオーバーの設定は、Microsoft MPIO サポートまたは MC/S（Multiple Connections per Session）を使用して行うことが可能です。現在、3.2 iSCSI ターゲットおよび Microsoft iSCSI イニシエータのバージョン 2.06 またはそれ以降で設定されている PowerVault NAS ストレージソリューションでは MPIO オプションのみがサポートされています。MC/S オプションは、PowerVault NAS ストレージシステムではサポートされていません。

iSCSI LUN の設定

- 1 ディスクの管理から、iSCSI ターゲットデバイスを設定します。iSCSI イニシエータホストに移動して、**Start**（スタート） → **Control Panel**（コントロールパネル） → **Administrative Tools**（管理ツール） → **Computer Management**（コンピュータの管理） → **Disk Management**（ディスクの管理）の順にクリックします。

右ペインに、iSCSI ディスクが **Unknown Not Initialized**（不明、未初期化）および **Unallocated**（未割り当て）として表示されます。

- 2 **Welcome to the Initialize and Convert Disk Wizard**（ディスクの初期化と変換ウィザードへようこそ）オプションが表示されます。**Initialize and Convert Disk Wizard**（ディスクの初期化と変換ウィザード）を実行します。

- a すべての画面で、デフォルト設定をそのままにして **Next**（次へ）を選択します。
- b **Completing the Initialize and Convert Disk Wizard**（ディスクの初期化と変換ウィザードの完了）画面が表示されます。**Finish**（完了）をクリックします。



メモ：動的ディスクは iSCSI 設定ではサポートされていません。

- 3 **Disk Management** (ディスクの管理) に進みます。 **Unallocated** (未割り当て) の iSCSI ディスクが、 **Basic** (基本) および **Unallocated** (未割り当て) として識別されています。 iSCSI ディスクを右クリックし、 **New Partition...** (新しいパーティション) を選択します。
- a **New Partition Wizard** (新しいパーティションウィザード) が起動します。 **Next** (次へ) をクリックします。
 - b **Select Partition Type** (パーティションの種類を選択) 画面で、 **Partition Type** (パーティションの種類) として **Primary Partition** (プライマリパーティション) を選択します。 **Next** (次へ) をクリックします。
 - c **Specify Partition size** (パーティションサイズの指定) 画面で、パーティションのサイズを指定します。 **Next** (次へ) をクリックします。
 - d **Assign Drive Letter or Path** (ドライブ文字またはパスの割り当て) 画面で、ドロップダウンメニューからドライブ文字を割り当てます。 **Next** (次へ) をクリックします。
 - e **Format Partition** (パーティションのフォーマット) 画面で、デフォルトのオプションを使用してパーティションをフォーマットします。ボリュームラベルを入力し、 **Next** (次へ) をクリックします。
-  **メモ** : 短時間でフォーマットするには、 **Perform quick format** (クイックフォーマットする) チェックボックスを選択します。
- f **Completing the New Partition Wizard** (新しいパーティションウィザードの完了) 画面で、 **Finish** (完了) をクリックします。新しいパーティションが正常に作成されます。
- 4 **Disk Management** (ディスクの管理) に進みます。 iSCSI ディスクが、ユーザーの入力したボリュームラベルで識別されます。
-  **メモ** : 動的ディスクは iSCSI ではサポートされていません。

複数のセッション

異なるデバイス内の異なるイニシエータ - ターゲットの組み合わせで、複数のセッションを作成することが可能です。

- 複数の PowerVault NAS ストレージ システムの異なる iSCSI ターゲットにアクセスするようにひとつのイニシエータを設定できます。
- 同じ、または異なる PowerVault NAS ストレージ システムの異なる iSCSI ターゲットにアクセスするように、複数のイニシエータを設定できます。
- PowerVault NAS ストレージ ソリューションの同じ iSCSI ターゲットに複数のイニシエータがアクセスするようには設定できません。

△ 注意：必須のホストクラスタリングがサポートされていないため、3.2 iSCSI ターゲットのある複数の iSCSI イニシエータを使って同じターゲットデバイスにアクセスすることはできません。3.2 iSCSI ターゲットのある複数の iSCSI イニシエータを使って同じターゲットデバイスにアクセスしようとすると、データ破損が発生する恐れがあります。

iSCSI スナップショット

Microsoft iSCSI ソフトウェアターゲットを使用して、スナップショットを包括的なバックアップおよびリカバリシステムの一環として作成および管理することができます。スナップショットは、VSS（ボリュームシャドウコピーサービス）テクノロジを使用して構築されるシャドウコピーです。

スナップショットの作成および定期的バックアップのための iSCSI 仮想ディスクのマウントの自動化には、**スナップショットのスケジュール設定ウィザード** が使用できます。NTFS ファイルシステムボリュームに存在する仮想ディスクのスナップショットは永続的です。これはシステムが再起動しても残るという意味です。

iSCSI ターゲットサーバーで作成されるスナップショットはクラッシュコンシステントです。iSCSI スナップショットは VSS および VSS を使用するように設計されているハードウェアを備えたストレージレイを使用して作成されます。

Microsoft iSCSI ソフトウェアターゲットで一貫したスナップショットを有効化するには、Microsoft iSCSI ソフトウェアターゲット VSS ハードウェアプロバイダが必要です。Microsoft iSCSI ソフトウェアターゲット VSS ハードウェアプロバイダは、iSCSI ソフトウェアターゲットのインストールオプションとして利用可能です。ハードウェアプロバイダはローカル VSS と連携し、中央バックアップサーバーにトランスポートできる一貫したボリュームのイメージを作成します。

PowerVault ストレージシステムでは、2 つの方法で iSCSI スナップショットを作成することができます。

- Microsoft iSCSI ソフトウェアターゲットコンソール内の単一の仮想ディスクのスナップショットを手動で作成。
- **スナップショットのスケジュール設定ウィザード** を使用して、スナップショットを単一で、または定期的に自動作成するようにスケジュールをセットアップ。

スナップショットを作成する前に

仮想ディスクのスナップショットを作成する前に、次の手順を実行してください。



メモ：Windows エクスプローラを使用して、スナップショットを作成する仮想ディスクを含むボリュームへ進みます。

- 1 **Volume** (ボリューム) → **Properties** (プロパティ) → **Shadow Copies** (シャドウコピー) → **Settings** (設定) と進みます。 **Storage Area** (ストレージ領域) タブの **Located on this volume** (このボリュームに存在) オプションにボリュームと同じドライブ文字が表示されていることを確認します。

- 2 **Details** (詳細) をクリックしてボリュームの使用を確認します。デフォルトの設定は次の通りです。

- **最大サイズ**

- **使用限度** — MB 単位のサイズ、または **無制限**

サイズは仮想ディスク / スナップショットのサイズに応じて変更するか、設定を **無制限** にします。

△ **注意**: 仮想ディスクスナップショットを保存するために十分な容量がボリュームにあることを確認してください。容量が足りないと、スナップショットは失われます。

- 3 必要な変更を行った後、**OK** をクリックします。

△ **注意**: デフォルトの設定を変更しない場合も、**Volume (ボリューム)** → **Properties (プロパティ)** → **Shadow Copies (シャドウコピー)** → **Settings (設定)** と進んで **OK** をクリックします。このアクションを実行して、ノード障害が発生した場合に適切なスナップショットリカバリが行われることを確実にしてください。スナップショットのサイズがストレージ領域の最大サイズを超えると、最も古いスナップショットが削除されます。



メモ: ボリュームで作成された仮想ディスクの数にかかわらず、各ボリュームは iSCSI 仮想ディスク用に最高 512 のスナップショットを格納することができます。スナップショットは差分コピーなので余分なスペースをとりません。

スナップショットのスケジュール

iSCSI 仮想ディスク用のスナップショットをスケジュールするには、次を実行します。

- 1 **PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) → **Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) と進みます。
- 2 **Snapshots** (スナップショット) タブで、**Schedules** (スケジュール) を右クリックし、**Create Schedule** (スケジュールの作成) を選択します。
Welcome to the Schedule Snapshot Wizard (スナップショットのスケジュール設定ウィザードへようこそ) 画面が表示されます。
- 3 **Next** (次へ) をクリックします。
- 4 **Schedule Actions** (アクションのスケジュール) 画面が表示され、次のオプションが利用可能になります。

Take snapshots of the Virtual Disks (default) (仮想ディスクのスナップショットを撮る (デフォルト))

Take snapshots of the Virtual Disks and mount the

snapshots locally (仮想ディスクのスナップショットを撮り、スナップショットをローカルマウントする)

オプションをひとつ選択し、**Next** (次へ) をクリックします。

- Name** (名前) 画面で、スケジュールの名前を入力し、**Next** (次へ) をクリックします。
- Virtual Disks** (仮想) 画面が表示され、次のオプションが表示されます。
Include all Virtual Disks (default) (すべての仮想ディスクを含む (デフォルト))

Include only the selected Virtual Disks (選択した仮想ディスクのみを含む)

スナップショット用にすべての仮想ディスク、または選択した仮想ディスクを選択することができます。
 **メモ** : PowerVault NAS ストレージソリューションでは、すべての仮想ディスクが **Virtual Disks** (仮想ディスク) 画面にリスト表示されます。
- Frequency** (頻度) 画面が表示され、**Daily** (毎日)、**Weekly** (毎週)、**Monthly** (毎月) および **On-time only** (一度のみ) といった異なるオプションがリスト表示されます。オプションを選択して、**Next** (次へ) をクリックします。
- 手順 7 で選択した頻度に応じて、**開始時間**、**日**、**月**、**開始日**、およびその他の時間パラメータを設定する必要があります。これらのパラメータを希望する時間に編集します。**Next** (次へ) をクリックします。
 **メモ** : スナップショットのスケジュールは後で変更できます。
- Completing the Schedule Snapshot Wizard** (スナップショットのスケジュール設定ウィザードの完了) 画面が表示されます。**Finish** (終了) をクリックします。

スナップショットのスケジュールの確認 (オプション)

スナップショット作成のスケジュールを組んだ後、**PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) → **Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) → **Snapshots** (スナップショット) → **Schedules** (スケジュール) と進み、タイムスタンプと共に中央ペインに表示されているスケジュール名、今回の実行、次回の実行を確認してください。

アクティブなスナップショット

スナップショット作成のスケジュールを組んだ後、**Active Snapshots** (アクティブなスナップショット) タブへ進みます。ソース仮想ディスク、タイムスタンプ、およびエクスポートステータスを含むスナップショット詳細のすべてが中央ペインにリスト表示されます。

Active Snapshots (アクティブなスナップショット) タブを使って、アクティブなスナップショットをローカルディスクのようにエクスポート、削除、ロールバック、およびマウントすることができます。

- スナップショットのエクスポート — このオプションを使ってスナップショットをリモートシステムで利用できるようにしたり、スナップショットの冗長コピーを撮ることができます。**Export Snapshot**（スナップショットのエクスポート）ウィザードを使用して、ひとつ、または複数の iSCSI ターゲットへスナップショットをエクスポートします。こうすることで、エクスポートされたスナップショットへのイニシエータからのアクセスが可能になります（読み取りアクセスのみ）。スナップショットをエクスポートするには、次を実行します。
 - Active Snapshots**（アクティブなスナップショット）タブで、中央ペインからエクスポートするスナップショットを選択し、右クリックして **Export Snapshot**（スナップショットのエクスポート）を選択します。
 - Welcome to the Export Snapshot Wizard**（スナップショットのエクスポートウィザードへようこそ）画面が表示されます。**Next**（次へ）をクリックします。
 - Snapshot Access**（スナップショットアクセス）画面で、このスナップショットへの読み取り専用のアクセスを許可するターゲットを追加します。**Next**（次へ）をクリックします。
 - Finish**（終了）をクリックします。
 - ターゲットへ進み、このスナップショットが仮想ディスクとして追加されていることを確認します。
- スナップショットの削除 — 削除するスナップショットを選択し、そのスナップショットを右クリックして **Delete**（削除）をクリックします。

 **メモ**：マウントされたスナップショットは削除できません。削除する前にスナップショットのマウントを解除する必要があります。
- ディスクアクセス — PowerVault NAS ストレージ システムから iSCSI 仮想ディスクのスナップショット、を読み取り専用モードとしてマウントすることができ、そのスナップショットはローカルディスクとして表示されます。

 **注意**：スナップショット / 仮想ディスクをマウント解除する際は、ディスクが使用されていないことを確認してください。使用中に解除するとデータが破壊される恐れがあります。

 **メモ**：マウントできるのは iSCSI 仮想ディスク（読み取り / 書き込み、または読み取り専用）、またはそのスナップショットのいずれかで、両方はマウントできません。仮想ディスクをマウントした後でスナップショットのマウント操作を行うと、その前に前回のインスタンスがマウント解除されます。
- ロールバック — このオプションを使用して iSCSI 仮想ディスクを前回のスナップショットにロールバックします。この操作は **C:\¥Windows¥Temp** にある **temp** ディレクトリを使用します。**temp** ディレクトリに差分データを格納するために十分なスペースがあることを確認してください。十分なスペースがない場合は、ロールバックが失敗します。

- a スナップショットを右クリックし、**Rollback to snapshot** (スナップショットへロールバック) を選択します。ポップアップメッセージで、**Yes** (はい) を選択します。
- b ロールバックのステータスをチェックするには、**Devices** (デバイス) タブに移動します。ロールバックの進行状態は、中央ペインの仮想ディスクセクションに % (パーセント) で表示されます。
- c ロールバック操作を中断することも可能です。別のスナップショットにロールバックできる場合は、ロールバックを中断します。できない場合は、ロールバックを完了することを強くお勧めします。



メモ: ロールバックを実行すると、現在仮想ディスクにあるデータはすべて失われます。この仮想ディスクを使用するイニシエータからすべての iSCSI ターゲットを切断します。仮想ディスクが読み取り / 書き込みディスクとしてマウントされている場合は、ロールバックの前にその仮想ディスクのマウントを解除してください。

iSCSI デバイスの取り外し / クリーンアップ

本項では、iSCSI デバイスで実行されるクリーンアップ操作の手順を説明します。このクリーンアップ操作は iSCSI ターゲットと iSCSI イニシエータの両方で実行する必要があります。

イニシエータから

次の手順を行って、ターゲットデバイスで実行されている iSCSI I/O 動作を停止することにより、ターゲットとのアクティブな接続を切断します。

- 1 **Start** (スタート) → **All Programs** (すべてのプログラム) → **Microsoft iSCSI Initiator** (Microsoft iSCSI イニシエータ) → **iSCSI Initiator Properties** (iSCSI イニシエータのプロパティ) → **Targets** (ターゲット) タブをクリックします。
- 2 **Connected** (接続済み) のターゲットを選択し、**Details** (詳細) をクリックします。
- 3 **Target Properties** (ターゲットのプロパティ) 画面が表示されます。**Sessions** (セッション) タブで、識別子の横にあるチェックボックスを選択し、**Logoff** (ログオフ) をクリックします。これで接続が切断されました。
- 4 **iSCSI Initiator Properties** (iSCSI イニシエータのプロパティ) 画面で、**Persistent Targets** (固定ターゲット) タブをクリックし、固定ターゲットの項目を削除します。

- 5 ターゲット IQN 名の項目を削除する場合、**Discovery** (検出) タブに移動し、**Target Portals** (ターゲットポータル) の項にある **PowerVault NAS ストレージ システムの IP アドレス /DNS 名** を削除、または **iSNS サーバーの IP アドレス /DNS 名** を削除します。
- 6 **Targets** (ターゲット) タブで、**Refresh** (リフレッシュ) をクリックします。ターゲット IQN 名はリストから削除されています。

ターゲットから

iSCSI ターゲットから仮想ディスクを削除するには、次の手順を実行します。

- 1 **PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) → **Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) → **iSCSI Targets** (iSCSI ターゲット) と進みます。削除するターゲット、およびそれに関連する仮想ディスクを選択します。
 - a 中央ペインにはすべての仮想ディスクがリストされます。削除する仮想ディスクを右クリックし、**Remove Virtual Disk From iSCSI Target** (iSCSI ターゲットから仮想ディスクを削除) オプションを選択します。
 - b そのターゲットに関連している仮想ディスクすべてに対して手順 a を繰り返します。
- 2 ターゲットを削除するには、ターゲットを右クリックし、**Delete iSCSI Target** (iSCSI ターゲットを削除) オプションを選択します。ターゲットと関連付けられている **.vhd** ファイルを手動で参照し、削除します。
- 3 仮想ディスクを削除するには、**Devices** (デバイス) オプションを選択し、中央ペインから仮想ディスクを右クリックして **Delete Virtual Disk** (仮想ディスクの削除) を選択します。

 **メモ:** 手順 3 は iSCSI ターゲットソフトウェアへの関連付けを削除するのみで、ボリュームのディスク容量はクリアされません。ディスク容量をクリアするには、ボリュームを手動で参照し、**.vhd** ファイルを削除する必要があります。
- 4 iSNS サーバーの項目を削除するには、**Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) を右クリックし、→ **Properties** (プロパティ) → **iSNS** タブ → **Remove the DNS name or IP address entry** (DNS 名または IP アドレスの項目を削除) を選択します。

チャレンジハンドシェイク認証 プロトコルを使用したセキュアな iSCSI 接続の設定

TCP/IP およびイーサネットの下層にあるセキュリティ層を除いて、iSCSI 層そのものに含まれている iSCSI プロトコル用のセキュリティ機能はわずかです。iSCSI セキュリティ機能は、必要に応じて有効と無効を切り替えることができます。

Microsoft® iSCSI イニシエータでは、チャレンジハンドシェイク認証プロトコル (CHAP) を使用して、iSCSI ターゲットへのアクセスを試みている iSCSI ホストシステムを識別します。iSCSI イニシエータと iSCSI ターゲットは CHAP を使用し、定義済みのシークレットを共有します。イニシエータは、シークレットと他の情報と組み合わせて 1 つの値とし、MD5 (Message Digest 5) 機能を使用して、一方向のハッシュを計算します。ハッシュの値はターゲットに送信されます。ターゲットは、その共有シークレットと他の情報から一方向のハッシュを計算します。ハッシュの値が一致すれば、イニシエータは認証されます。もう一方のセキュリティ情報には ID 値が含まれており、リプレイ攻撃から守るために、CHAP ダイアログが行われるたびに値が増えるようになっています。

Dell™ PowerVault™ NAS ストレージソリューションは相互 CHAP もサポートします。

CHAP は一般にパスワード認証プロトコル (PAP) よりも安全とされています。

CHAP と IPSec

CHAP は接続のピアを認証するもので、シークレット (パスワードに似たセキュリティキー) を共有するピアに基づいています。IP セキュリティ (IPSec) は、IP パケット層で認証とデータ暗号化を強制し、セキュリティをより強固にするプロトコルです。

一方向の CHAP 認証

一方向の CHAP 認証では、iSCSI ターゲットの側からのみイニシエータの認証が行われます。シークレットはターゲットにのみ設定され、ターゲットにアクセスするすべてのイニシエータは、ターゲットとのログオンセッションの開始に同じシークレットを使用する必要があります。一方向の CHAP 認証を設定するには、ターゲットとイニシエータに以下の項で説明する設定を行います。

iSCSI ターゲットの設定

本項で説明されている設定を行う前に、少数の iSCSI ターゲットと仮想ディスクが作成済みであることと、仮想ディスクがターゲットに割り当てられていることを確認します。

- 1 iSCSI ターゲットで、**PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) → **Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) → **iSCSI Targets** (iSCSI ターゲット) → <ターゲット名> と進み、右クリックで **Properties** (プロパティ) を選択するか、**Actions** (アクション) ペイン → **More Actions** (その他のアクション) → **Properties** (プロパティ) と移動します。
<ターゲット名> **Properties** (プロパティ) ウィンドウが表示されます。
ターゲット名は、現在 iSCSI 設定を行っている iSCSI ターゲットの名前です。
- 2 **Authentication** (認証) タブで、**Enable CHAP** (CHAP の有効化) のチェックボックスを選択し、ユーザー名 (イニシエータの IQN 名) を入力します。IQN を手動で入力するか、または **Browse** (参照) オプションを使用してリストから IQN を選択します。
- 3 **Secret** (シークレット) を入力し、**Confirm Secret** (シークレットの確認) に同じ値を再入力し、**OK** をクリックします。シークレットに使用できる文字数は 12 ~ 16 です。



メモ: IPsec を使用しない場合、イニシエータとターゲットの CHAP シークレットはどちらも 12 バイト以上 16 バイト以下にしてください。IPsec を使用する場合、イニシエータとターゲットのシークレットは 2 バイト以上 16 バイト以下にしてください。

iSCSI イニシエータの設定

- 1 **Discovery** (検出) タブに進みます。
- 2 **iSCSI Initiator Properties** (iSCSI イニシエータのプロパティ) → **Targets** (ターゲット) タブ → **Log On...** (ログオン ...) の順にクリックして、CHAP を有効にしたターゲットにログインします (34 ページの「iSCSI ターゲットの設定」を参照してください)。
- 3 **Log On to Target** (ターゲットへログオン) ウィンドウで、**Advanced** (詳細) を選択します。
- 4 **Advanced Settings** (詳細設定) ウィンドウで、**CHAP logon information** (CHAP ログオン情報) のチェックボックスを選択します。
User name (ユーザー名) フィールドにイニシエータの IQN が自動的に表示されます。

- 5 **Target secret** (ターゲットのシークレット) フィールドに iSCSI ターゲット内で設定したターゲットのシークレットと同じ値を入力し、**OK** をクリックします。

ターゲットのシークレットの値が正しい場合は、ターゲットにログオンできます。正しくない場合は、認証エラーとともにログオンが失敗します。

相互 CHAP 認証

相互 CHAP 認証を使用すると、ターゲットとイニシエータが互いに認証し合います。ストレージエリアネットワーク (SAN) 内の各ターゲットと各イニシエータに対して、個別のシークレットが設定されます。

イニシエータの設定

- 1 iSCSI イニシエータで、**iSCSI Initiator Properties** (iSCSI イニシエータのプロパティ) → **General** (全般) タブ → **Secret** (シークレット) ボタンの順にクリックします。
- 2 **CHAP Secret Setup** (CHAP シークレットのセットアップ) 画面が表示されます。**Enter a secure secret** (セキュアシークレットの入力) フィールドに、12 ~ 16 文字から成るシークレットコードを入力し、**OK** をクリックします。
 **メモ:** このイニシエータ CHAP シークレットとターゲット CHAP シークレットは異なっている必要があります。
- 3 ターゲットにログオンする前に、ターゲット内でイニシエータ CHAP シークレットを設定する必要があります。したがって、ターゲットの設定を完了してから iSCSI イニシエータにログオンしてください。

ターゲットの設定

34 ページの「iSCSI ターゲットの設定」の説明に従って CHAP のターゲット設定を行い、次の手順を実行します。

- 1 <ターゲット名> **Properties** (プロパティ) ウィンドウで、**Authentication** (認証) タブを選択します。
- 2 **Enable reverse CHAP authentication** (逆 CHAP 認証を有効にする) のチェックボックスを選択します。**User name** (ユーザー名) フィールドにイニシエータの IQN を入力します。
- 3 **Reverse secret** (逆シークレット) フィールドに、イニシエータで設定した **Secret** (シークレット) 値を入力します。



メモ: 逆シークレットが CHAP シークレットと同じでないことを確認します。逆シークレットには 12 ~ 16 文字が含まれている必要があります。

イニシエータの設定の続き

- 1 34 ページの「iSCSI イニシエータの設定」の説明に従って CHAP のイニシエータの設定を行います。
- 2 **Advanced Settings** (詳細設定) ウィンドウで、**CHAP logon information** (CHAP のログオン情報) を選択し、**User name** (ユーザー名) と **Target secret** (ターゲットのシークレット) を入力します。**Perform mutual authentication** (相互認証の実行) のチェックボックスを選択し、**OK** をクリックします。

ターゲット用とイニシエータ用に入力した資格情報を持っている場合に限り、ログインが可能となります。

付録

本書の前章までには、基本的な iSCSI セッション / 接続の手順が説明されています。本章では、詳細な構成設定の手順のいくつかについて簡単に説明します。

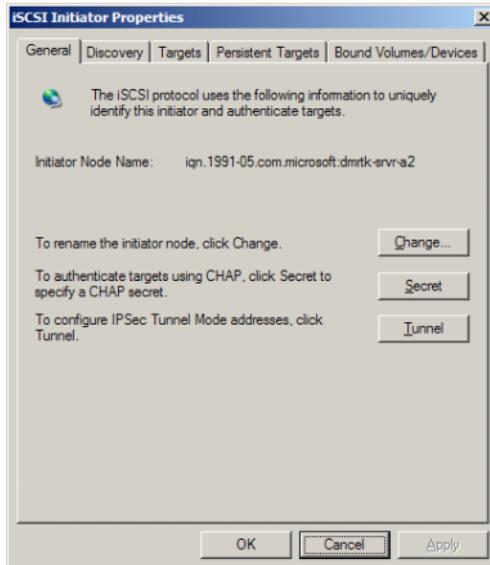
イニシエータの詳細

この項では、**iSCSI Initiator Properties** (iSCSI イニシエータプロパティ) ウィンドウに含まれている様々な機能について説明します。

General (全般) タブ

イニシエータの iSCSI 修飾名 (IQN) であるイニシエータノード名が表示されません。

図 A-1. iSCSI Initiator Properties (iSCSI イニシエータプロパティ) ウィンドウの General (全般) タブ



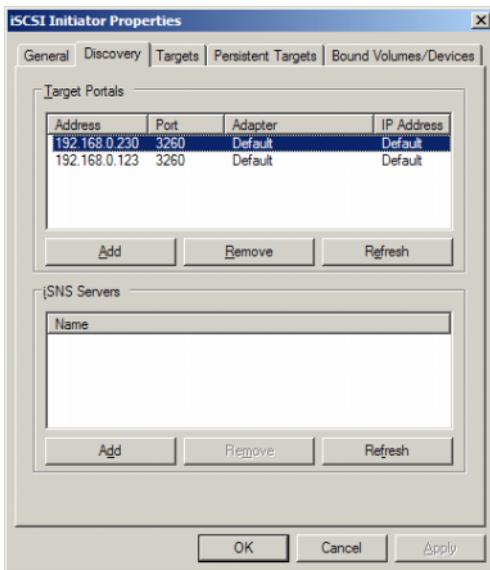
General (全般) タブには、**Change** (変更)、**Secret** (シークレット)、および **Tunnel** (トンネル) という 3 つのオプションがあります。

- **Change** (変更) — 表示されているイニシエータノード名を変更できます。
- **Secret** (シークレット) — iSCSI セキュリティが提供されている **CHAP**。詳細については、「チャレンジハンドシェイク認証 プロトコルを使用したセキュアな iSCSI 接続の設定」ページの 33 を参照してください。
- **Tunnel** (トンネル) — IPsec を使った詳細設定にはこのオプションを使用できます。

Discovery (検出) タブ

Target Portals (ターゲットポータル) — **Discovery** (検出) タブでは、検出されたイニシエータで利用できる iSCSI ターゲットポータルのリストが表示されます。ターゲットポータルは iSCSI ターゲットソリューションのプライマリ IP アドレスで、PowerVault NAS ストレージソリューション用の専用 iSCSI NIC IP アドレスを提供します。ターゲットポータルがリストにない場合は、ターゲットサーバーの IP アドレスまたは DNS 名を使用して加えることができます。次の例では、2 つの iSCSI ターゲットポータルがすでに加えられています。

図 A-2. iSCSI Initiator Properties Window (iSCSI イニシエータプロパティ) ウィンドウの Discovery (検索) タブ



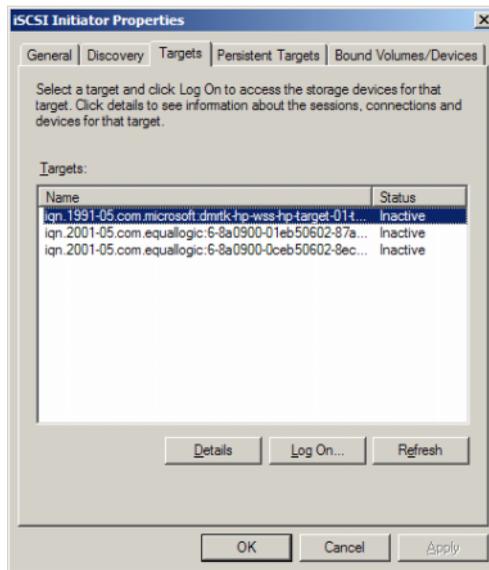
iSNS Servers (iSNS サーバー) — iSNS サーバーを使用してターゲットの検出を行うことも可能です。

iSNS サーバーの IP アドレスまたは DNS 名を加えます。サーバー上で iSNS サービスが起動している場合には、iSNS サーバーに登録されているすべてのクライアント (イニシエータとターゲット) が **Registered Clients** (登録済みクライアント) 画面に一覧表示されます。iSNS サーバー上のこの情報を取得するには、**Microsoft iSNS Properties** (Microsoft iSNS のプロパティ) → **Registered Clients** (登録済みクライアント) と進みます。

Targets (ターゲット) タブ

Targets (ターゲット) タブには、iSCSI イニシエータで使用可能な個々のターゲットのリストが表示されます。次の例では、iSCSI イニシエータで 3 つのターゲットが使用できるようになっています。

図 A-3. iSCSI Initiator Properties Window (iSCSI イニシエータプロパティ) ウィンドウの Target (ターゲット) タブ



メモ: 上の図は **Targets** (ターゲット) タブにおける検出の例を示しています。実際には、PowerVault NAS ストレージシステムをターゲットとして設定した後でのみ、ターゲットが検出されます。

Log On (ログオン) — ターゲットにアクセスするには、イニシエータがターゲットにログオンする必要があります。ターゲットへのパスが 1 つしかない場合、ログインの手順は 1 ステップだけで済みます。**Log On...** (ログオン) をクリックし、**Target Name** (ターゲット名) を指定して、**OK** をクリックします。

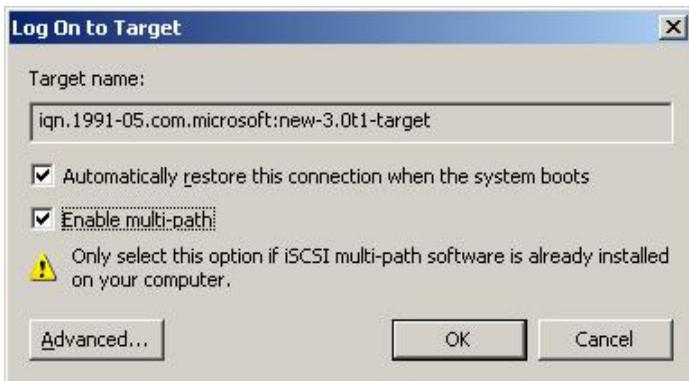
ターゲットへのパスが複数ある場合は、iSCSI イニシエータに各パスの説明を入力する必要があります。イニシエータに複数のパスの説明を入力するには、次の手順に従います。

- 1 **Log On to Target** (ターゲットへのログオン) ウィンドウで **Enable multi-path** (マルチパスの有効化) を選択し、**Advanced** (詳細) をクリックします。

Advanced (詳細) オプションには、可能なすべての送信元 (イニシエータ) IP アドレスが含まれたドロップダウンメニューと、可能なすべてのターゲットポータルアドレス用の別のドロップダウンメニューがあります。この場合、ターゲットソリューションは実際のパスと IP アドレスを内部で管理します。他のターゲットソリューションでは、マルチパス操作に使用できる利用可能な各 IP アドレスが表示されます。

- 2 同一のターゲットデバイスに複数のセッションを持たせるには、送信元 IP アドレスとターゲット IP アドレスの希望の各組み合わせを選択し、別々にログインします。
- 3 出カスパイクまたはシステムの再起動中に連続的な接続を確保し、ターゲット - イニシエータの関連付けの確立を避けるには、**Automatically restore this connection when the system boots** (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。
- 4 各 iSCSI NIC について **ログオン** 手順を繰り返します。

図 A-4. Log On to Target (ターゲットへのログオン) ウィンドウ

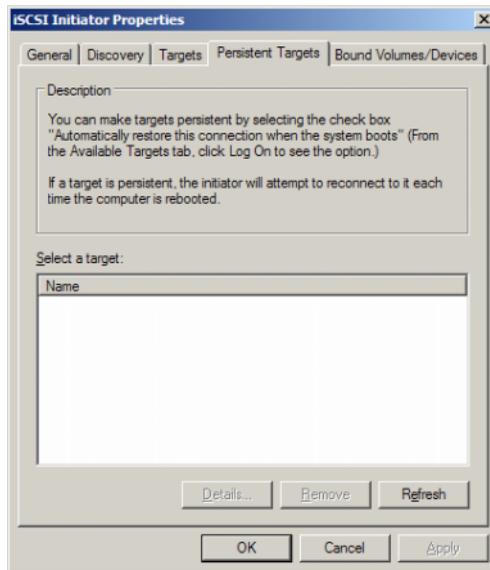


MPIO 接続のためには、ステータスが **Connected**（接続済み）と表示されているターゲットを選択し、**Log On**（ログオン）を選択する必要があります。**Log On to Target**（ターゲットへのログオン）ウィンドウで、**Advanced**（詳細）を選択し、冗長 iSCSI ターゲットの IP アドレスを設定します。

Persistent Targets（固定ターゲット）タブ

システムの再起動時にターゲットへの接続が自動的に回復するように、Persistent Targets（固定ターゲット）を設定できます。ターゲットを固定に設定すると、この **Persistent Targets**（固定ターゲット）タブに表示されます。

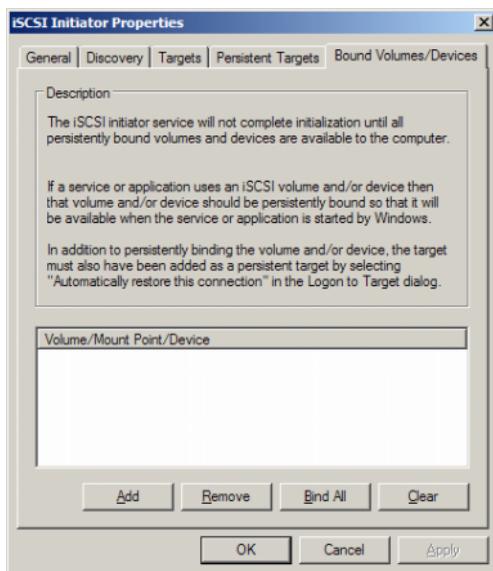
図 A-5. iSCSI Initiator Properties（iSCSI イニシエータプロパティ）ウィンドウの Persistent Targets（固定ターゲット）タブ



Bound Volumes/Devices（バインドされたボリューム / デバイス）タブ

ホストサービスまたはアプリケーションが iSCSI ボリュームの可用性に依存している場合は、バインドされた各ボリュームが iSCSI サービスに初期化の一部として含まれるように、そのホストサービスまたはアプリケーションをバインドされたものとして設定する必要があります。

図 A-6. iSCSI Initiator Properties (iSCSI イニシエータプロパティ) ウィンドウの Bound Volumes/Devices (バインドされたボリューム/デバイス) タブ



詳細な構成設定

イニシエータのマルチパスの有効化

iSCSI イニシエータ - ターゲットの接続を確立した後で、次の手順を実行してマルチパス操作を有効にします。

- 1 イニシエータ上で、**iSCSI Initiator Properties** (iSCSI イニシエータのプロパティ) → **Targets** (ターゲット) タブ → **Log On...** (ログオン) → **Log On to Target** (ターゲットへログオン) ウィンドウの順にクリックし、**Enable multi-path** (マルチパスの有効化) オプションのチェックボックスを選択します。
- 2 効率的なブロック (iSCSI) I/O 操作とリンクフェイルオーバーの準備のために、iSCSI 操作に複数の NIC ポートを設定する必要があります。また、マルチパスオプションにより、異なる IP アドレスを使用して、同一の iSCSI ターゲットに対して複数の接続が可能になります。

詳細オプションの使い方

詳細オプションを使用して、以下のことが行えます。

- **iSCSI Initiator Properties** (iSCSI イニシエータのプロパティ) → **Targets** (ターゲット) タブ → **LogOn...** (ログオン) → **Log On to Target** (ターゲットへログオン) ウィンドウ → **Advanced** (詳細) オプションの順にクリックします。**Advanced Settings** (詳細設定) 画面が表示されます。この画面は **Advanced** (詳細) および **IPSec** の 2 つのタブで構成されています。**General** (全般) タブでは、**CRC/ チェックサム**、**CHAP** を設定し、発信元 IP アドレスとターゲットポータル (iSCSI ターゲットの IP アドレス) を選択できます。また、マルチパスオプションを使用して、負荷分散とフェイルオーバーの設定を行うことができます。
- **Advanced Settings** (詳細設定) ウィンドウでは、**Advanced** (詳細) タブにすべての発信元 (イニシエータ) IP アドレス用のドロップダウンメニューと、すべてのターゲットポータルアドレス用のドロップダウンメニューがあります。iSCSI イニシエータ-ターゲット接続では、ターゲットソリューションは実際のパスと IP アドレスを内部で管理します。複数の異なるターゲットソリューションを使用している場合は、リストからマルチパス操作の IP アドレスを選択できます。
 - a ログオンして、発信元 IP アドレスとターゲット IP アドレスの組み合わせを選択します。
 - b 別々にログインして、同じターゲットデバイスの複数の接続を設定します。
- **Advanced Settings** (詳細設定) ウィンドウでは、**IPSec** タブを使用して **IPSec** を設定できます。**IPSec** を有効にすると、データ転送中に送信されたすべての IP パケットが暗号化・認証されます。すべての IP ポータルに共通のキーが設定されるため、すべてのピアが相互に認証し、パケットの暗号化をネゴシエートできます。

接続されているターゲットのプロパティの確認

iSCSI Initiator Properties (iSCSI イニシエータのプロパティ) → **Targets** (ターゲット) の順にクリックし、**Connected** (接続状態) のターゲットをハイライト表示し、**Details** (詳細) をクリックします。→ **Target properties** (ターゲットのプロパティ) 画面が表示されます。画面は、**Sessions** (セッション)、**Devices** (デバイス)、**Properties** (プロパティ) という 3 つのタブで構成されています。以下の項では、これらのタブの詳細について説明します。

Sessions (セッション) タブ

Sessions (セッション) タブには、**Session Identifier** (セッション識別子)、**Session properties** (セッションプロパティ)、および **Sessions Connections** (セッション接続) に関する情報が表示されます。このタブを使用して、セッションからログオフできます。

Devices (デバイス) タブ

Target Properties (ターゲットのプロパティ) 画面の **Devices** (デバイス) タブには、ターゲットと関連している仮想ディスクなど、汎用デバイスの詳細が表示されます。

Advanced (詳細) をクリックして **MPIO** に関する情報を表示し、**Device Details** (デバイスの詳細) 画面を表示します。

MPIO タブを使って **MPIO** 設定を変更できます。このタブで、適切な負荷分散ポリシー設定を選択することができます。使用可能なさまざまな **Load Balance Policy** (負荷分散ポリシー) オプションから、各接続の負荷分散を設定します。

MPIO タブの **Load Balance Policy** (負荷分散ポリシー) フィールドで各ポリシーを選択する際に、画面に次の説明が表示されます。

- **Fail Over Policy** (フェイルオーバーポリシー) — フェイルオーバーポリシーは、1 つのアクティブパスを使用し、その他すべてのパスをスタンバイに指定します。アクティブパスに障害が発生すると、使用可能なパスが見つかるまで、スタンバイパスはラウンドロビンアプローチに対して試行されます。
- **Round Robin** (ラウンドロビン) — ラウンドロビンポリシーは、着信要求をすべての可能なパスに均等に配分するように試みます。
- **Round Robin With Subset** (サブセット付きラウンドロビン) — ラウンドロビンサブセットポリシーは、アクティブに指定してあるパスのみに対してラウンドロビンポリシーを実行します。すべてのアクティブパスに障害が発生すると、スタンバイパスがラウンドロビンアプローチに対して試行されます。
- **Least Queue Depth** (最小のキューの深さ) — 最小のキューの深さポリシーは、負荷の軽いプロセッシングパスへの I/O 要求の配分を負荷に応じて増やすことで、不均等な負荷を補正します。
- **Weighted Paths** (加重パス) — 加重パスポリシーを使用すると、各パスの処理負担の割合を指定できます。大きい数字は、パスの優先度が低いことを意味します。

デフォルトのオプションは **Round Robin** (ラウンドロビン) です。 **Load Balance Policy** (負荷分散ポリシー) ドロップダウンメニューから必要なオプションを選択して負荷分散ポリシーを設定し、**Apply** (適用) をクリックして設定を確認します。

Properties (プロパティ) タブ

Target Properties (ターゲットのプロパティ) 画面の **Properties** (プロパティ) タブには、**Target Alias** (ターゲットエイリアス)、**Authentication** (認証)、**Associated Network** (関連ネットワーク) ポータル、およびターゲットのその他のその他の詳細に関する情報が表示されます。

iSNS サーバーのインストールと設定

Microsoft iSNS Server は Microsoft のウェブサイト www.microsoft.com から無償でダウンロードでき、2 つのバージョン (x86 と IA64) が利用できます。iSCSI ネットワーク上でターゲットを検出するために、iSNS Server を使用できます。

iSNS サーバーは、Microsoft Windows 2000 Server Service Pack 4 および Microsoft Windows Server 2003 オペレーティングシステムでサポートされています。iSNS サーバーのインストールは、次の手順で行います。



メモ : iSNS サーバーを Microsoft iSCSI Initiator が実行されているのと同じサーバーにインストールしないでください。

- 1 **Microsoft iSNS Server** バージョン 3.0 またはそれ以降をインストールします。インストールはウィザードを使用して簡単に実行できます。**Welcome to the Microsoft iSNS Server Setup Wizard** (Microsoft iSNS Server セットアップウィザードへようこそ) 画面で、**Next** (次へ) をクリックします。
- 2 **License Agreement** (使用許諾契約書) 画面が表示されます。情報を読み、**Next** (次へ) をクリックします。
- 3 **Select Installation Folder** (インストールフォルダの選択) が表示されます。フォルダのパスを入力するか、または **Browse** (参照) オプションを使用してローカルドライブ上の場所を選択し、**Next** (次へ) をクリックします。
- 4 **Confirm Installation** (インストールの確認) 画面で、**Next** (次へ) をクリックします。
- 5 **Installing Microsoft iSNS Server** (Microsoft iSNS Server をインストール中) 画面にインストールの進行状況が表示されます。**Microsoft iSNS Installation Program** (Microsoft iSNS インストールプログラム) で、**iSNS Installation Options** (iSNS インストールオプション) から選択するように指示されます。**Install iSNS Service** (iSNS サービスのインストール) を選択し、**OK** をクリックします。
- 6 **End User License Agreement** (エンドユーザー使用許諾契約書) 画面が表示されます。契約内容を読み、**Agree** (同意します) をクリックしてプログラムをインストールします。
- 7 **Microsoft iSNS Service Setup Program** (Microsoft iSNS Service セットアッププログラム) ウィンドウに、プログラムが正常にインストールされたことが示されます。
- 8 **Microsoft iSNS Server Information** (Microsoft iSNS Server 情報) 画面が表示されます。情報を読み、**Next** (次へ) をクリックします。
- 9 **Installation Complete** (インストールの完了) 画面が表示され、プログラムのインストールが完了したことが示されます。**閉じる** をクリックします。

iSNS サーバーの設定

iSCSI イニシエータとターゲットを iSNS サーバーに登録すると、iSNS サーバーはそれらを自動的に検出します。

- iSNS サーバーに登録されたイニシエータでは、iSNS に登録されたすべてのターゲットデバイスが **Targets** (ターゲット) タブ内に表示され、ターゲットにログオンできます。**Target Portals** (ターゲットポータル) 内の個々のターゲットサーバーの IP アドレスまたは DNS 名を使用してイニシエータを設定する必要はありません。iSNS サーバーがターゲットの検出を行います。
- 同様に、PowerVault NAS ストレージ システム (ターゲット) は、関連付けのために iSNS サーバーから使用可能なイニシエータを照会できます。

iSNS サーバーの設定には、次の手順を実行してください。

- 1 iSNS Server 3.0 またはそれ以降のバージョンをインストールしたサーバーにログオンし、**Start** (スタート) → **Program** (プログラム) → **Microsoft iSNS Server** → **Configure iSNS server (iSNS サーバーの設定)** の順に進みます。

iSNS サーバーの画面は、**General** (全般)、**Discovery Domains** (検出ドメイン)、および **Discovery Domain Sets** (検出ドメインセット) の 3 つのタブで構成されています。**General** (全般) タブには、iSNS サーバーに登録されているすべてのデバイス (iSCSI イニシエータとターゲット) が一覧表示されます。次の手順に従って iSNS サーバーにターゲットとイニシエータを追加します。

- a **iSCSI Initiator properties** (iSCSI イニシエータのプロパティ) → **Discovery** (検出) → **iSNS Servers** (iSNS サーバー) → **Add** (追加) の順にクリックして、イニシエータの IP アドレスまたは DNS 名を追加し、このイニシエータを iSNS サーバーに登録します。
- b iSNS サーバーにログインし、**Start** (スタート) → **Program** (プログラム) → **Microsoft iSNS Server** (Microsoft iSNS サーバー) → **Configure iSNS Server** (iSNS サーバーの設定) → **General** (全般) タブの順にクリックします。ステップ a で iSNS サーバーに登録したイニシエータがリストに表示されています。同様に、iSNS サーバーに登録するすべての iSCSI イニシエータが **General** (全般) タブに表示されます。
- c ターゲットとして設定した PowerVault NAS ストレージ ソリューションにログインし、**PowerVault NAS Management Console** (PowerVault NAS 管理コンソール) → **Microsoft iSCSI Software Target** (Microsoft iSCSI ソフトウェアターゲット) → 右クリックして **Properties** (プロパティ) を選択 → **iSNS** タブの順に進み、iSNS サーバーの IP アドレスまたは DNS 名を追加します。

- d 確認するには、iSNS サーバーにログインし、**General**（全般）タブをチェックして、**PowerVault** ストレージソリューションのすべてのターゲットがリストに表示されていることを確認します。

iSNS サーバーに複数の **PowerVault NAF** ストレージシステムが登録されている場合は、**PowerVault** ストレージシステム内で作成されたすべてのターゲットデバイスが iSNS サーバー内に一覧表示されます。

- 2 **Discovery Domains**（検出ドメイン）機能を使用して、特定のイニシエータを特定のアクセスを持つターゲットとグループにまとめることができます。
 - a **iSNS Server Properties**（iSNS サーバーのプロパティ） → **Discovery Domains**（検出ドメイン）タブの順にクリックし → **Create**（作成）をクリックし、検出ドメインの名前を入力し → **Add**（追加）を選択してください。
 - b **Add registered Initiator or Target to Discovery Domain**（登録済みのイニシエータまたはターゲットを検出ドメインに追加する）画面が表示されます。設定する特定のイニシエータとターゲットを選択し、**OK** をクリックします。
- 3 iSCSI ネットワーク内に複数の検出ドメインを設定することが可能です。ドメインは **Discovery Domain Sets**（検出ドメインセット）タブ内に一覧表示されます。**Discovery Domain Sets**（検出ドメインセット）タブには、デフォルト **DD** オプションとデフォルト **DDS** オプションが表示されます。グループは必要に応じていくつでも作成できます。

効率的なストレージ管理のためのベストプラクティス

SAN ストレージマネージャ

SAN ストレージマネージャは Microsoft Management Console のスナップインです。システム管理者は、このスナップインを使用して、ファイバーチャネルと iSCSI の両方の環境でストレージアレイ上のスペースの割り当てに使用する LUN を作成・管理できます。SAN ストレージマネージャはコンベンショナルなスナップインを介して導入され、ハードウェア VDS（仮想ディスクサーバー）プロバイダを使用して VDS をサポートする SAN ベースのストレージアレイ上で使用できます。ハードウェア、プロトコル、トランスポート層、およびセキュリティの違いのために、サポートされている 2 種類の環境（iSCSI とファイバーチャネル）で、設定と LUN の管理が異なります。この機能は、SAN 上のどの種類のホストバスアダプタ（HBA）またはスイッチでも使用できます。ハードウェア互換性テスト（HCT）に合格済みの VDS プロバイダのリストは、Microsoft Storage のウェブサイト www.microsoft.com/storage を参照してください。

iSCSI サブシステム用の LUN 管理

iSCSI では、LUN はターゲット（1 つまたは複数の LUN を含む論理エンティティ）に割り当てられます。サーバーは、自らの iSCSI イニシエータを使用してターゲットにログオンすることで、LUN にアクセスします。ターゲットにログオンするために、イニシエータはターゲット上のポータルに接続します。サブシステムには 1 つまたは複数のポータルがあり、それがターゲットと関連付けられています。サーバーのイニシエータがターゲットにログオンしており、新しい LUN がターゲットに割り当てられている場合、サーバーはすぐに LUN にアクセスできます。

iSCSI SAN 上のデータの保護 — サーバーとサブシステム間のデータ転送を保護するには、イニシエータとターゲットの間にログインセッション用のセキュリティを設定します。SAN のストレージマネージャを使用して、イニシエータとターゲットの間に一方向または相互のチャレンジハンドシェイク認証プロトコル（CHAP）認証を設定することができ、また、インターネットプロトコルセキュリティ（IPsec）のデータ暗号化を設定することも可能です。



メモ : iSCSI トラフィックがパブリックネットワークを使用する場合、CHAP を使用することをお勧めします。

既知の問題

- 仮想ディスクのマウント解除中にイベントが生成される — ローカルでマウントされている仮想ディスクをマウント解除すると、次のイベントがシステムログに生成される場合があります。

Plugplaymanager 12 event :

The device 'MSFT 00000000F852A09D SCSI Disk Device'

(SCSI\Disk&Ven_MSFT&Prod_00000000F852A09D\1&2afd7d61&3&000003) disappeared from the system without first being prepared for removal.

It is safe to ignore these events for normal Microsoft iSCSI Software Target dismount operations イベント 12、PlugPlayManager: デバイス「MSFT 00000000F852A09D SCSI Disk Device」

(SCSI\Disk&Ven_MSFT&Prod_00000000F852A09D\1&2afd7d61&3&000003) が、取り外し準備なしにシステムから消失しました。これらのイベントを無視して、通常通り Microsoft iSCSI ソフトウェアターゲットのマウント解除操作を行っても安全です。)

- ローカルマウントされている仮想ディスクのロールバック操作 — 仮想ディスクを読み取り / 書き込みモードでローカルマウントすると、その仮想ディスクでのロールバック操作完了に長い時間がかかります。
- ロールバックの中止 — ロールバックの最中に仮想ディスクを無効にすると、警告無しでロールバック操作が中止されます。ロールバックが終了したとイベントにログ記録されます。
- ローカルマウントの仮想ディスクが利用可能なドライブラストに表示される — 新規の仮想ディスクを作成すると、ローカルマウントの仮想ディスクが新規仮想ディスクをホストできるボリュームとしてリストに表示されます。ローカルマウントの仮想ディスクは仮想ディスクの保存をサポートしません。新規仮想ディスクのストレージ場所としてローカルマウントの仮想ディスクを選択すると、次のエラーメッセージが表示されます。
The wizard was unable to import one or more virtual disks (ウィザードはひとつ、または複数の仮想ディスクをインポートできませんでした)。Make sure that the files are not in use, and then run the wizard again (ファイルが使用されていないことを確認し、ウィザードを再度実行してください)。

- イニシエータが DNS ドメイン名を使用するターゲットを検出しない — iSCSI ターゲットへのイニシエータのアクセスを設定する際は IQN が推奨方法で、DSN 設定にかかわらず動作します。DNS ドメイン名を指定するオプションは Microsoft iSCSI ソフトウェアターゲットスナップインに組み込まれています。DNS 名を使用する場合、DNS が正しく設定されていること（前方参照ゾーンおよび逆引き参照ゾーンを含む）を確認し、イニシエータの完全修飾ドメイン名（FQDN）を指定してください。イニシエータの FQDN を指定した後、ターゲットをイニシエータに接続しづらい場合は、次のコマンドをターゲットサーバーで実行し、DNS 逆引き参照ゾーンが正しく有効化されているかを確認してください。
nslookup <InitiatorIP> (<InitiatorIP> は iSCSI イニシエータの IP アドレスです)。
nslookup コマンドの失敗は、DNS 逆引き参照が設定されていないことを示します。イニシエータ IQN、IP アドレス、または MAC アドレスを使用するようにターゲットを再設定します。または、NetBIOS 名を使用してイニシエータに接続し、次の状況を満たすことができます。
 - ターゲットによって使用されるサブネットに DNS 逆引き参照ゾーンが設定されていない。
 - ネットワーク検出、またはファイル共有がイニシエータおよびターゲットサーバーで有効化されている。
- ローカルマウントのボリュームのシャドウコピー — ローカルマウントのボリュームのシャドウコピーは作成しないことをお勧めします。仮想ディスクをローカルマウントしてから Windows Explorer を使ってボリュームのシャドウコピーを作成しようとすると、ストレージアプライアンスがハングアップしているかようになります。これはシャドウコピーが作成される方法に起因するものです。ローカルマウントされた仮想ディスクのシャドウコピーを作成すると、ローカルマウントのドライバは仮想ディスクをホストしている下層ボリュームに書き込みを行います。これは、ホストボリュームの差分領域への追加書き込みの原因となります。その結果巡回書き込みとなり、最終的にストレージアプライアンスの無応答を引き起こします。このシナリオが発生した場合は、ストレージアプライアンスを再起動します。
- イニシエータが切断された接続を復元しない — 不良 IP アドレスが原因でイニシエータが切断された接続を復元しない場合があります。iSCSI イニシエータが Microsoft iSCSI ソフトウェアターゲットとの通信を損失する場合の一部では、接続中にイニシエータがハングアップしているように見えることがあります。この問題は、Microsoft iSCSI ソフトウェアターゲットを実行しているサーバーがイニシエータとの通信に使用されない IP アドレスを持っている場合に発生します。イニシエータは設定された IP アドレスそれぞれに接続を試行し、応答を最高 100 秒間待ちます。この問題はブライ

バート IP アドレスの自動割り当て（169.x.x.x）が原因で発生する場合もあります。この問題を防ぐには、DHCP が利用できない時に静的 IP アドレスを使用します。

次のオプションは、この問題の回避法です。

- IP アドレスでソースおよびターゲットポータルを指定します。
- IPv4 アドレスまたは IPv6 アドレスのみを使用します。アドレスの種類を混同しないようにします。
- ネットワークに接続されていないネットワークカードを無効化します。
- イベントビューアのエラー — Microsoft iSCSI ソフトウェアターゲット 3.2 をアンインストールしてから再インストールしようとする、イベントビューアのエラーが発生する場合があります。回避法として、ソフトウェアをアンインストールする前に Microsoft iSCSI ソフトウェアターゲットサービスを停止します。ソフトウェアがすでにアンインストールされている場合、Microsoft iSCSI ソフトウェアターゲットを再インストールする前にコンピュータを再起動してください。
- iSCSI イニシエータに対する追加のファイアウォールルール — Windows Storage Server 2008 上で iSCSI イニシエータを Microsoft iSCSI ソフトウェアターゲットに接続するには、追加のルールを有効にする必要がある場合があります。次の Windows ファイアウォールルールが必要です。
 - Windows Management Instrumentation (WMI 受信)
[TCP/ すべてのポート]
 - Windows Management Instrumentation (DCOM 受信)
[TCP/ ポート 135]
 - Windows Management Instrumentation (ASync 受信)
[TCP/ すべてのポート]
 - Windows Management Instrumentation (WMI 送信)
[TCP/ すべてのポート]
 - リモートボリューム管理 (RPC-EPMAP) [TCP/RPC エンドポイント マッパー]
 - リモートボリューム管理 - 仮想ディスクサービスローダ (RPC)
[TCP/ 動的 RPC]
 - リモートボリューム管理 - 仮想ディスクサービス (RPC)
[TCP/ 動的 RPC]

索引

C

CHAP, 33
一方向, 33
相互, 35

I

iSCSI, 6
iSCSI スナップショット, 26
iSNS, 6

P

PowerVault ストレージシステム,
6

き

既知の問題, 49

せ

切断 / クリーニング
iSCSI デバイス, 30
設定
iSCSI LUN, 19
PowerVault ストレージシステム
との iSCSI 接続, 12
イニシエータ, 17
イニシエータからのセットアップ,
17
イニシエータ (ホスト), 12
イニシエータ (ホスト) からの
イニシエータ - ターゲット
接続, 15
セットアップ
ターゲット, 17

へ

ベストプラクティス
iSCSI ストレージエリア
ネットワークのセットアップ,
7

わ

ワークシート, 8

