Veritas ™ Appliance iSCSI ガイド

リリース 3.1.1

VERITAS™

Veritas Appliance iSCSI ガイド

リリース 3.1

法的通知と登録商標

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、NetBackup は Veritas Technologies LLC または同社の米国とその他の国における関連会社の商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この Veritas 製品には、サードパーティ(「サードパーティプログラム」)の所有物であることを示す必要があるサードパーティソフトウェアが含まれている場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。サードパーティプログラムについて詳しくは、この文書のサードパーティの商標登録の付属資料、またはこの Veritas 製品に含まれる TPIP ReadMe File を参照してください。

本書に記載する製品は、使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されています。Veritas Technologies LLC からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供され、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアとみなされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202 以下の「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となり、Veritas による納品が内部設置型またはホスト型のサービスのいずれであるかは問いません。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

テクニカルサポート

テクニカルサポートは、世界中にサポートセンターを有しています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。サポートのサービスおよびテクニカルサポートへのお問い合わせ方法につきましては、当社の Web サイトをご確認ください。

https://www.veritas.com/support/ja_JP

次の URL からベリタスのアカウント情報を管理することができます。

https://my.veritas.com

既存のサポート契約に関してベリタスに問い合わせる場合は、次に示す地域のサポート契約管理チームに電子メールで連絡してください。

世界全域 (日本を除く)	CustomerCare@veritas.com
Japan (日本)	CustomerCare_Japan@veritas.com

マニュアル

最新のマニュアルは、次のベリタス Web サイトで入手できます。

https://sort.veritas.com/documents

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

APPL.docs@veritas.com

次のベリタスコミュニティサイトでマニュアルの情報を参照したり、質問することもできます。

http://www.veritas.com/community/ja

ベリタスの Service and Operations Readiness Tools (SORT) の表示

ベリタスの Service and Operations Readiness Tools (SORT) は、時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供する Web サイトです。製品によって異なりますが、SORT はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。SORT がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目次

第 1 章 概要 6

iSCSI について 6
iSCSI イニシエータとターゲットについて 7
サポートされる iSCSI 機能 7
iSCSI トポロジーの概要 8
iSCSI 修飾名（IQN）について 9

第 2 章 アプライアンスの構成について 10

NetBackup 5240 アプライアンスの I/O 構成 H 10
NetBackup 5340 計算ノードの I/O 構成 11
..... 13

第 3 章 NetBackup for VMware について 15

NetBackup for VMware について 15
VMware バックアップ処理の概要 16
［トランスポートモード (Transport modes)］オプション (VMware) 16

第 4 章 iSCSI の構成 18

アプライアンスでの iSCSI の構成 18
イニシエータの IQN の設定 19
インターフェースプロパティの表示 20
インターフェースプロパティの構成 20
インターフェースプロパティの削除とリセット 22
CHAP 認証について 24
ポータルアドレスを使用したターゲットの検出 24
iSNS について 26
iSNS を使ったターゲットの検出 27
ターゲットへの接続 29
ターゲットとのセッションの切断 30
ターゲットの表示 31

第 5 章 iSCSI の問題のトラブルシューティングとベストプラクティス 33

DataCollect コマンドを使ったデバイスログの収集 33
syslogd メッセージについて 34
iSCSI 警告について 35
ベストプラクティス 36

1

概要

この章では以下の項目について説明しています。

- iSCSI について
- iSCSI イニシエータとターゲットについて
- サポートされる iSCSI 機能
- iSCSI トポロジーの概要
- iSCSI 修飾名 (IQN) について

iSCSI について

iSCSI は、TCP/IP を使用してネットワーク上でストレージデバイスに接続する方法の 1 つです。iSCSI は、既存のインターネットプロトコル (IP) ネットワーク上で TCP/IP プロトコルを使用して SCSI コマンドを転送できるようにするために開発されました。iSCSI は、ファイバーチャネルネットワークを別途設置することなく、メッセージングトラフィックとブロックベースのストレージの両方を IP ネットワーク上で提供します。

このプロトコルを使用すると、クライアント (イニシエータと呼ばれる) がリモートサーバー上の SCSI ストレージデバイス (ターゲット) に SCSI コマンドを送信できます。

ターゲットは iSCSI サーバー上にあるストレージリソースで、通常はそのサーバー上で実行している iSCSI ストレージノードに多数存在する可能性があるインスタンスの 1 つです。相互に通信するために、iSCSI イニシエータとターゲットで iSCSI セッションを確立します。

以下のアプライアンスと構成は、iSCSI をサポートします。

- NetBackup 5240 の構成 H
- NetBackup 5340 の構成 A、B、C、D、E

iSCSI イニシエータとターゲットについて

iSCSI はネットワーク上でストレージを共有する方法の 1 つで、ブロックデバイスレベルで機能します。iSCSI 通信では、次のコンポーネントが相互に通信します。

- イニシエータ
- ターゲット

iSCSI ストレージにアクセスするクライアントは、イニシエータと呼ばれます。この iSCSI イニシエータはサーバー（iSCSI ターゲット）に接続できます。この接続で、iSCSI イニシエータは SCSI コマンドを iSCSI ターゲットに送信します。この場合、SCSI コマンドは IP パケットにパッケージ化されます。

iSCSI ターゲットデバイスは iSCSI コマンドを受信しストレージを共有します。ストレージは物理的なディスク、または複数のディスクをあらわす領域または物理的なディスクの一部である場合があります。storage array は標準的な iSCSI ターゲットです。

サポートされる iSCSI 機能

iSCSI が NetBackup アプライアンスでどのようにサポートされるかを理解するための要点を以下にまとめます。

- iSCSI は 5240 アプライアンスの構成 H と 5340 計算ノードのすべての構成でサポートされます。
- NetBackup 5240 アプライアンスの構成 H は常にイニシエータとして機能します。
  p.10 の「NetBackup 5240 アプライアンスの I/O 構成 H」を参照してください。
- 5340 の構成はイニシエータとして機能します。
  p.11 の「NetBackup 5340 計算ノードの I/O 構成」を参照してください。
- iSCSI は VMware バックアップのみをサポートします。また NetBackup for VMware 機能をサポートします。
  p.15 の「NetBackup for VMware について」を参照してください。
- このリリースでは、iSCSI 機能のコマンドは NetBackup Appliance Shell Menuで利用できます。
- iSCSI は IPV4 アドレスのみをサポートします。IPV6 を介した iSCSI 接続はサポートされません。
  さらに、イニシエータとターゲットは同じレイヤ 2 (L2) ネットワーク上にある必要があります。
- iSCSI は DMP (Dynamic Multi-Pathing) をサポートします。複数のパスを使用して同じターゲットに接続できます。iSCSI 経由のバックアップまたはリストアは、1 つのパスが利用可能であるかぎり続行できます。

- ターゲットを検出するための iSNS サーバー (Internet Storage Name Service) の使用がサポートされます。
  p.26 の「iSNS について」を参照してください。
- VLAN は、ネットワークインターフェースまたは iSCSI インターフェースのいずれかで構成できます。VLAN をネットワークと iSCSI インターフェースの両方で構成すると、ネットワークインターフェースの VLAN が両方のインターフェースで有効になります。VLAN が異なるサブネットでネットワークと iSCSI インターフェースの両方で構成されている場合、その構成はサポートされないことに注意してください。

ネットワークインターフェース		iSCSI インターフェース		説明
IP	VLAN	IP	VLAN	
サブネット X	なし	サブネット X	なし	サポート
サブネット X	なし	サブネット Y	VLAN A	サポート
サブネット X	VLAN B	サブネット X	VLAN B	サポート
サブネット X	VLAN B	サブネット Y	VLAN B	サポートしていません

- 10 Gb イーサネット/iSCSI カードでは、QLogic SFP+ (Small Form-Factor Pluggable) モジュールのみがサポートされます。10 Gb イーサネット/iSCSI カードでサポート外の SFP モジュールが検出された場合は、アラートが表示されます (アラートが構成されている場合)。

NetBackup Appliance の互換性に関する最新情報については、次の Web サイトのハードウェア互換性リストを参照してください。

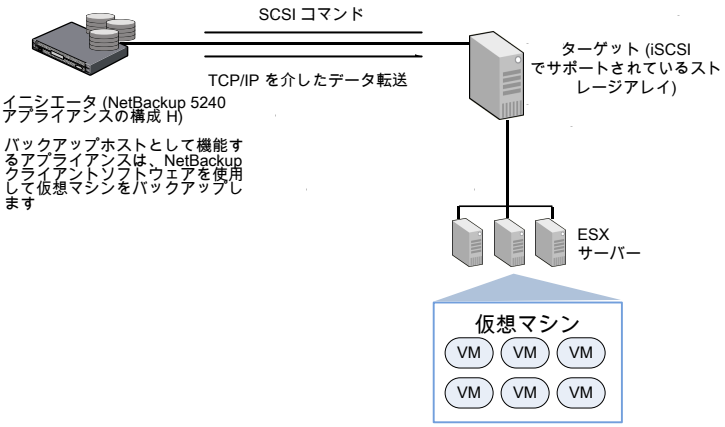
www.netbackup.com/compatibility

iSCSI トポロジーの概要

アプライアンスは VMware バックアップホストとして機能し、iSCSI を使用して VMware のバックアップを作成できます。このトポロジーでは、アプライアンスはイニシエータとして機能し TCP/IP ネットワーク上の storage array (ターゲット) に接続します。storage array は FC/LAN などを経由して ESX ホストに接続できます。

次の図に、例として NetBackup 5240 のトポロジーを示します。

図 1-1 iSCSI トポロジー



仮想マシンのバックアップは iSCSI によりアプライアンス上で作成されます。

iSCSI 修飾名（IQN）について

iSCSI ネットワークでは、ネットワークを使用する各 iSCSI 要素に一意の iSCSI 名があり、iSCSI 要素にアクセス用のアドレスが割り当てられます。各 iSCSI 要素は、イニシエータまたはターゲットを問わず、一意の iSCSI 修飾名（IQN）によって特定されます。この IQN は論理名で、IP アドレスにはリンクされません。

IQN には次のプロパティがあります。

- 一意です。2 つのイニシエータまたはターゲットを同じ名前にすることはできません。
- 最大 255 文字です。
- 数字（0 ～ 9）、文字（A ～ Z、a ～ z）、コロン（:）、ハイフン（-）、ピリオド（.）のみを使用できます。

たとえば IQN は `iqn.yyyy-mm.naming-authority:unique name` のような形式になり、ここで

- `yyyy-mm` はネーミングオーソリティが確立された年と月です。
- naming-authority は、通常、ネーミングオーソリティのインターネットドメイン名のリバース構文です。
- 一意の名前には、任意の名前（ホストの名前など）を使用できます。ネーミングオーソリティにより、コロンに続く名前が一意であることが確認される必要があります。

例: iqn.1999-06.com.veritas:abc

2

アプライアンスの構成について

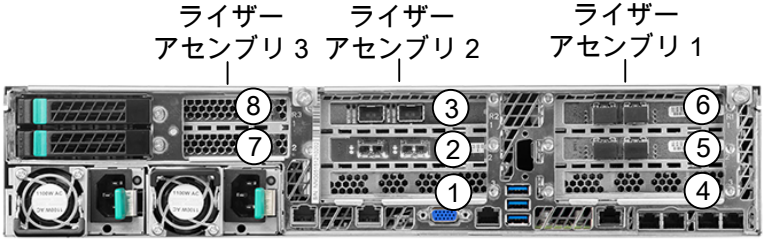
この章では以下の項目について説明しています。

- NetBackup 5240 アプライアンスの I/O 構成 H
- NetBackup 5340 計算ノードの I/O 構成
-

NetBackup 5240 アプライアンスの I/O 構成 H

NetBackup 5240 Appliance の背面パネルには、3 つの PCIe ライザーカードアセンブリがあります。PCIe ライザーカードアセンブリ 1 と 2 には、それぞれ 3 枚の標準 PCIe カードを取り付けることができます。PCIe ライザーカードアセンブリ 3 には、2 枚のロープロファイル PCIe カードを取り付けることができます。スロットには 1 から 8 までのラベルが付いています。次の図に、ライザーアセンブリとスロット番号を示します。

図 2-1 背面パネルのライザーアセンブリの場所と PCIe スロットの割り当て



NetBackup 5240 Appliance は、PCIe ベースの I/O 構成オプションを複数サポートしています。次の表に、スロット 2 に iSCSI カードを含む構成 H を示します。

表 2-1 NetBackup 5240 Appliance の構成 H

I/O 構成オプション	スロット 1 *	スロット 2	スロット 3	スロット 4	スロット 5	スロット 6	スロット 7 **	スロット 8
H	-	10 GbE NIC[1、2] (iSCSI)	10 GbE NIC[1、2]	-	8 Gb FC HBA [2]	8 Gb FC HBA [2]	-	-

* NetBackup 5240 Appliance とともに 1 台以上の NetBackup 5240 ストレージシェルフを購入している場合、スロット 1 には出荷時に取り付けられている PCIe RAID 6 コントローラがあります。それ以外の場合は、スロット 1 には何も装着されていません。

** スロット 7 には、NetBackup 5240 Appliance の内部 PCIe RAID コントローラが搭載されています。この RAID コントローラを使って、アプライアンスのオペレーティングシステムをインストールしたディスクドライブに RAID 1 アレイを作成します。オペレーシングシステムドライブは、前面パネルのスロット 0 と 1 に配置されています。

PCIe カードケーブル接続の種類:

[1] 直接接続銅線ケーブル (別名、ツインナックスケーブルまたは Twinax)

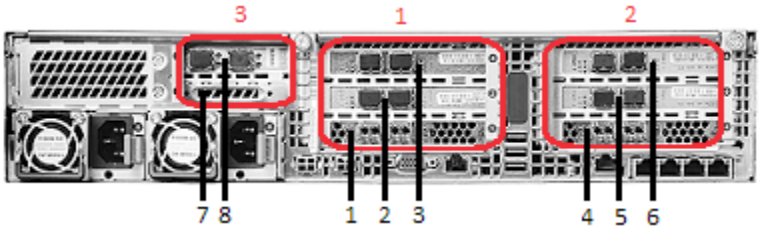
[2] 光ファイバーケーブル

詳しくは、『NetBackup Appliance 製品説明ガイド』を参照してください。

NetBackup 5340 計算ノードの I/O 構成

NetBackup 5340 計算ノードの背面パネルには、3 つの PCIe ライザーカードアセンブリが搭載されています。PCIe ライザーカードアセンブリ 1 と 2 には、それぞれ 3 枚の標準 PCIe カードを取り付けることができます。PCIe ライザーカードアセンブリ 3 には、2 枚のロープロファイル PCIe カードを取り付けることができます。スロットには 1 から 8 までのラベルが付いています。次の図で、ライザーアセンブリは赤色で囲まれています。PCIe スロットも示されています。

図 2-2 背面パネルのライザーアセンブリの場所と PCIe スロットの割り当て



NetBackup 5340 計算ノードは、PCIe ベースの I/O 構成オプションを複数サポートしています。次の表に、構成 A、B、C、D、E を示します。各構成は iSCSI をサポートします。

表 2-2 NetBackup 5340 計算ノードに利用可能な標準の PCIe ベースの I/O 構成

I/O 構成オプション	スロット 1 *	スロット 2	スロット 3	スロット 4*	スロット 5	スロット 6	スロット 7	スロット 8
A	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	予約済み	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)
B	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE2562 8 Gb FC HBA [3]	予約済み	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)
C	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	予約済み	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)
D	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	予約済み	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)
E	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	予約済み	QLogic QLE8442 10 GbE NIC [1、3] (iSCSI 対応)

I/O 構成オプション	スロット 1 *	スロット 2	スロット 3	スロット 4*	スロット 5	スロット 6	スロット 7	スロット 8

* スロット 1 と 4 の 16 Gb ファイバーチャネル HBA ポートを使用して、NetBackup 5340 計算ノードを Veritas 5U84 プライマリストレージシェルフに接続します。そのため、スロット 1 と 4 では、標準的なネットワーク I/O 操作をサポートしません。

PCIe カードケーブル接続の種類:

[1] 直接接続銅線ケーブル (別名、ツインナックスケーブルまたは Twinax)

[2] 標準的な銅

[3] 光ファイバーケーブル

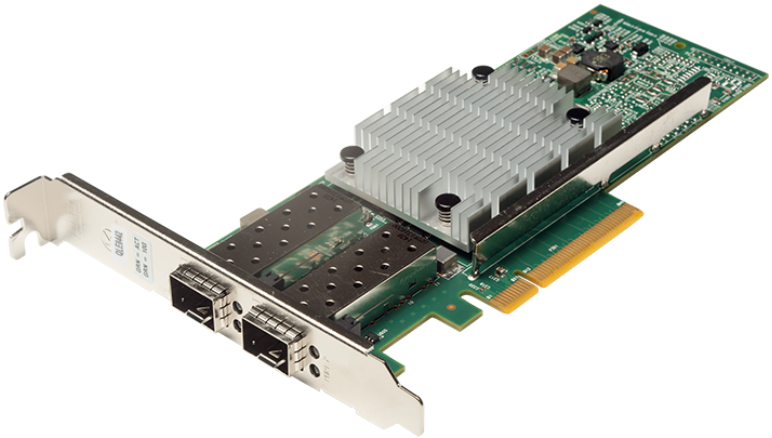


表 **2-3** QLE8442 デュアルポート 10 Gb イーサネットカードの仕様

項目	仕様
ブラケットの高さ	フルハイト
消費電力	9.65 W (公称)
システムインターフェースのタイプ	PCIe v3.0
速度とスロットの幅	8.0 GT/秒、8 レーン

項目	仕様
LED インジケータ	リンク/アクティビティ オフ = リンクなし (ケーブル切断) 点灯 = ラインがオン 点滅 = ネットワークアクティビティ
証明書	FCC A、ICES A、UL、CE、VCCI、CISPR、KCC
動作温度	0 ～ 55°C (32 ～ 131°F)
保管温度	-40 ～ 65°C (-40 ～ 149°F)
動作湿度	7% ～ 93% (55°C)
保管湿度	最大 93% (65°C)
気流	100 LFM (55°C)

アプライアンス用に QLE8442 デュアルポート 10 Gb イーサネットカード (SFP+ モジュール付属) を購入するには、ベリタスの営業担当者またはベリタスパートナー担当者にお問い合わせください。

QLE8442 デュアルポート 10 Gb イーサネットカード (SFP+ モジュール付属)

SKU 番号	説明
18293	

3

NetBackup for VMware について

この章では以下の項目について説明しています。

- NetBackup for VMware について
- VMware バックアップ処理の概要
- ［トランスポートモード (Transport modes)］オプション (VMware)

NetBackup for VMware について

NetBackup for VMware は、VMware ESX Server 上で動作する VMware 仮想マシンのバックアップおよびリストアを実現します。 NetBackup for VMware は、VMware vStorage APIs for Data Protection を利用します。バックアップ処理は、ESX Server から VMware バックアップホストに移行されます。

NetBackup for VMware には、次の機能があります。

- 仮想マシンのオフホストバックアップを実行する (NetBackup クライアントソフトウェアは仮想マシンでは必要がない)。オフホストバックアップによって、VMware ホストでのバックアップ処理の負荷が軽減される。
- 仮想マシンに小さいファイルが多数含まれる場合は、ファイルを順にバックアップする標準的なバックアップ方式よりも高速にデータをバックアップできる。
- VSS を使用して、静止したスナップショットを自動的に作成する (Windows のみ)。Linux ゲスト OS でスナップショットの静止が有効になっている場合、Linux で静止したスナップショットを作成します。
- スナップショットテクノロジを使用して、ユーザーが仮想マシンをいつでも使用できるようにする。
- VMware vSphere と vCloud Director をサポートする。

- 完全バックアップおよび増分バックアップ (Block Level Incremental (BLI) を含む) を実行する。
- 仮想マシン全体をバックアップする。
- 仮想マシンがオフの場合でも仮想マシンをバックアップする。
- バックアップから、選択したファイルをリストアできる。

VMware バックアップ処理の概要

次の表では、NetBackup のバックアップ処理のフェーズについて説明します。

表 3-1 NetBackup のバックアップ処理

フェーズ	説明
フェーズ 1	NetBackup マスターサーバーがバックアップを開始します。
フェーズ 2	VMware バックアップホストの NetBackup クライアントは、仮想マシンの VMware スナップショットを開始します。
フェーズ 3	Windows の場合: VSS が仮想マシン上のファイルシステムを同期化します。 Linux の場合: Linux ゲスト OS でスナップショットの静止が有効になっている場合、ファイルシステムが仮想マシンで同期されます。(スナップショットの静止を有効にする方法について詳しくは、オペレーティングシステムベンダーか VMware にお問い合わせください。)
フェーズ 4	VMware サーバーが、仮想ディスクのデータストア上にスナップショットを作成します。
フェーズ 5	NetBackup クライアントはデータストアからスナップショットを読み込み、NetBackup ストレージユニットにデータを書き込みます。

[トランスポートモード (Transport modes)] オプション (VMware)

トランスポートモードは、スナップショットデータを VMware データストアから VMware バックアップホストに送信する方法を決定します。適切なモードは、VMware データストアを VMware バックアップホストに接続するネットワーク形式によって異なります。

デフォルトでは、すべてのモードが選択されています。NetBackup は、上から下へ順番に各トランスポートモードを試します。最初に成功したモードを、仮想マシンのすべてのディスクに使います。

表 3-2 トランスポートモード (Transport Modes)

モード	説明
SAN	ファイバーチャネル (SAN) または iSCSI を介した、暗号化されていない転送の場合に指定します。 **メモ:** NetBackup アプライアンスでは、iSCSI 経由の VMware のバックアップで san トランスポートモードを使います。 **メモ:** このモードは VMware 仮想ボリューム(VVols)を使う仮想マシンではサポートされません。
hotadd	仮想マシンで VMware バックアップホストを実行できます。 **メモ:** VVols を使用する仮想マシンの場合、仮想マシンとバックアップホスト(hotadd)の仮想マシンは同じ VVol データストアに存在する必要があります。 このトランスポートモードの手順と、バックアップホストの VMware 仮想マシンへのインストール手順に関しては、VMware のマニュアルを参照してください。
nbd	Network Block Device (NBD) ドライバプロトコルを使用する、ローカルネットワークを介した暗号化されていない転送の場合に指定します。この転送モードは、通常、ファイバーチャネルを介した転送よりも低速です。
nbdssl	Network Block Device (NBD) ドライバプロトコルを使用する、ローカルネットワークを介した暗号化転送 (SSL) の場合に指定します。この転送モードは、通常、ファイバーチャネルを介した転送よりも低速です。

4

iSCSI の構成

この章では以下の項目について説明しています。

- アプライアンスでの iSCSI の構成
- イニシエータの IQN の設定
- インターフェースプロパティの表示
- インターフェースプロパティの構成
- インターフェースプロパティの削除とリセット
- CHAP 認証について
- ポータルアドレスを使用したターゲットの検出
- iSNS について
- iSNS を使ったターゲットの検出
- ターゲットへの接続
- ターゲットとのセッションの切断
- ターゲットの表示

アプライアンスでの iSCSI の構成

アプライアンスで iSCSI を構成する前に、ご使用の環境で iSCSI ターゲットが構成されていることを確認してください。詳しくは、ターゲットのベンダーから提供されるマニュアルをチェックしてください。

表 4-1には、アプライアンスで iSCSI を構成、設定する手順が示されています。

表 4-1　アプライアンス上での iSCSI の設定

手順番号	説明	参照先
1.	イニシエータの IQN を設定します。	p.19 の「イニシエータの IQN の設定」を参照してください。
2.	iSCSI インターフェースを設定します。IP アドレスを設定する必要があります。オプションで、ネットマスクやゲートウェイなど他のインターフェースプロパティを設定できます。	p.20 の「インターフェースプロパティの構成」を参照してください。
3.	ポータルアドレスまたは iSNS サーバーを使用してターゲットを検出します。	p.24 の「ポータルアドレスを使用したターゲットの検出」を参照してください。 p.27 の「iSNS を使ったターゲットの検出」を参照してください。
4.	ターゲットに接続します。	p.29 の「ターゲットへの接続」を参照してください。

イニシエータの IQN の設定

この項では、NetBackup アプライアンス(イニシエータ)の IQN を設定する方法について説明します。

IQNを設定するには

1. 管理者として Secure Shell(SSH)セッションを開きアプライアンスにログオンします。
2. Main_Menu >[設定 (Settings)]>[iSCSI]メニューに移動します。
3. Initiator Set IQN コマンドを入力し、IQN をパラメータとして入力します。

   IQN について次の注意点があります。

   - IQN は最大 255 文字です。
   - IQN には、数字(0 ～ 9)、文字(A ～ Z、a ～ z)、コロン(:)、ハイフン(-)、ピリオド(.)のみを使用できます。

   例: iqn.1999-06.com.veritas:abc
4. 次のメッセージが表示されます。

```
iSCSI> Initiator Set IQN iqn.veritas.abc
- [Info] The IQN has been updated to iqn.veritas.abc.
```

インターフェースプロパティの表示

このセクションでは、iSCSI インターフェースプロパティを表示する手順を示します。

インターフェースプロパティを表示するには

1. 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2. Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3. Interface Show コマンドを入力して Enter キーを押し、iSCSI インターフェースを表示します。以下のプロパティが表示されます。

```
appliance.iSCSI > Interface Show
Showing the available interfaces...

+--------------+----------+-----------------+-------------+-------+-------+----+----+
|Interface Name|Network   |   MAC Address   | IP Address  |Netmask Gateway|MTU |VLAN
|              |Interface |                 |             |       |       |    |Tag |
+--------------+----------+-----------------+-------------+-------+-------+----|----+
|     iscsi1   |  eth6    |00:0e:1e:53:55:11|10.181.198.62|       |       |1500|    |
+--------------+-----------------+-----------|-------------+-------+-------+----+----+

|     iscsi2   |  eth7     |00:0e:1e:53:55:13|            |       |       |1500|    |
+--------------+-----------------+-----------|-------------+-------+-------+----|----+
```

インターフェースプロパティの構成

このセクションでは、ISCSI インターフェースのゲートウェイ、IPv4 アドレス、ネットマスク、最大転送単位 (MTU)、VLAN タグなどの、インターフェースプロパティを設定する手順を示します。

MTU は、イーサネットフレームの最大伝送単位のサイズを制御します。MTU は必ず 68 から 65535 までの数字になります。iSCSI インターフェースの MTU を設定する場合、iSCSI インターフェースと、iSCSI インターフェースをマッピングするネットワークインターフェースに新しい MTU 値を設定します。

VLAN のタグ付けでは、VLAN ID をパケットヘッダに挿入します。これにより、パケットが属する VLAN を特定できます。具体的には、スイッチは VLAN ID を使ってブロードキャストパケットを送信するポートまたはインターフェースを特定します。

VLAN は、ネットワークインターフェースまたは iSCSI インターフェースのいずれかで構成できます。VLAN をネットワークと iSCSI インターフェースの両方で構成すると、ネットワークインターフェースの VLAN が両方のインターフェースで有効になります。

IP アドレスを設定するには

1 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。

2 Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。

3 Interface IPAddress Set コマンドを入力します。

4 IP アドレスと iSCSI インターフェース名をパラメータとして入力します。Enter キーを押します。

例:

```
 iSCSI> Interface IPAddress Set 10.80.156.88iscsi1

[Info] The IP address has been configured for iscsi1.
```

メモ: 例で使用している値は、サンプルのプレースホルダ値です。

ネットマスクを設定するには

1 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。

2 Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。

3 Interface Netmask Set コマンドを入力します。

4 ネットマスクの値と iSCSI インターフェース名をパラメータとして入力します。Enter キーを押します。

例:

```
 iSCSI> Interface Netmask Set 255.255.255.0iscsi10

[Info] The Netmask has been configured for iscsi10.
```

ゲートウェイを設定するには

1 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。

2 Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。

3 Interface Gateway Set コマンドを入力します。

4 ゲートウェイの値と iSCSI インターフェース名をパラメータとして入力します。Enter キーを押します。

例:

```
 iSCSI> Interface Gateway Set 192.168.4.1iscsi10

[Info] The gateway has been configured for iscsi10.
```

最大伝送単位（MTU）を設定するには

1. 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2. Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3. Interface MTU Set コマンドを入力します。
4. MTU の値と iSCSI インターフェース名を入力します。

   MTU は必ず 68 から 65535 の数字になります。新しい MTU の値は iSCSI インターフェースと、iSCSI インターフェースがマッピングされるネットワークインターフェースに適用されます。

   例:

```
iSCSI> Interface MTU Set 3000iscsi10

The new MTU value applies to both iscsi1 and
also network interface eth6.
Do you want to continue?(yes/no)[no]:yes

[Info] The MTU has been configured for iscsi10.
```

VLAN タグを設定するには

1. 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2. Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3. Interface VLAN Set コマンドを入力します。
4. VLAN ID と iSCSI インターフェース名をパラメータとして入力します。Enter キーを押します。

   VLAN ID は、1 から 4095 までの数字にする必要があります。

   例:

```
 iSCSI> Interface VLAN Set 75iscsi10

[Info] The VLAN tag has been configured for iscsi10.
```

インターフェースプロパティの削除とリセット

このセクションでは、MTU を除くすべてのインターフェースプロパティを削除する手順を示します。また、MTU をデフォルト値（1500）にリセットする手順も説明します。

MTU は削除できず、デフォルト値にのみリセットできます。

インターフェースプロパティを削除するには

1 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。

2 Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。

3 次のコマンドを使用して、特定のプロパティを削除します。

- Interface Gateway Remove コマンドを入力し、iSCSI インターフェース名を入力します。
  このコマンドでは、ゲートウェイが指定のインターフェースから削除されます。
  例:

```
iSCSI> Interface Gateway Remove iscsi1

[Info] The Gateway has been removed from iscsi1.
```

- Interface IPAddress Remove コマンドを入力し、iSCSI インターフェース名を入力します。
  このコマンドでは、IP アドレスが指定のインターフェースから削除されます。
  例:

```
iSCSI> Interface IPAddress Remove iscsi1

[Info] The IP address has been removed from iscsi1.
```

- Interface Netmask Remove コマンドを入力し、iSCSI インターフェース名を入力します。
  このコマンドでは、ネットマスクが指定のインターフェースから削除されます。
  例:

```
iSCSI> Interface Netmask Remove iscsi1

[Info] The Netmask has been removed from iscsi1.
```

- Interface VLAN Remove コマンドを入力し、iSCSI インターフェース名を入力します。
  このコマンドでは、VLAN タグが指定のインターフェースから削除されます。
  例:

```
iSCSI> Interface VLAN Remove iscsi1

[Info] The VLAN tag has been removed from iscsi1.
```

MTU をリセットするには

1. 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2. Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3. Interface MTU Reset コマンドを入力し、iSCSI インターフェース名を入力します。このコマンドでは、iSCSI インターフェースと、iSCSI インターフェースをマッピングするネットワークインターフェースの両方で、MTU がデフォルト値（1500）にリセットされます。

   例:

```
iSCSI > Interface MTU Reset iscsi1
The MTU will be reset to 1500 for both iscsi1 and also
the network interface eth6.
Do you want to continue?(yes/no)[no] :yes

[Info] The MTU has been reset to 1500.
```

CHAP 認証について

アプライアンスに使用する認証方法は、Challenge Handshake Authentication Protocol（または CHAP）と呼ばれます。CHAP 認証は次のコマンドまたは処理に適用できます。

- ターゲットの検出
- ターゲットへの接続

iSCSI セッションの最初の手順で、アプライアンス（イニシエータ）はログイン要求をストレージシステムに送信し iSCSI セッションを開始します。ストレージシステムはログイン要求を許可または拒否するか、またはログインが不要なことを判断します。ターゲット上で認証が有効な場合は、サーバーからストレージリソースにアクセスできるようにするために、クレデンシャルの認証を行いセッションを確立する必要があります。サーバーはクライアントからの値を比較し、情報が一致すればセッションを許可します。応答に失敗すると、セッションが拒否され、要求手順をもう一度開始します。

イニシエータは、CHAP ユーザー名とパスワードを使用してログインします。CHAP パスワードを指定するか、またはランダムなパスワードを生成できます。CHAP 認証の設定、構成方法について詳しくは、ターゲットベンダーのマニュアルを参照してください。

ポータルアドレスを使用したターゲットの検出

このセクションでは、ターゲットのポータルアドレスを使用した iSCSI ターゲットの検出手順について説明します。ターゲットのポータルアドレスは、ターゲットに関連付けられたホスト名または IPv4 アドレスです。

ターゲットのポータルアドレスの形式は、<IPv4 Address/hostname>:[<port>] です。

例: 192.116.116.50 または abc:3260（3260 はデフォルトポート）。

ターゲットに接続するには最初にターゲットを検出する必要があります。

ターゲットのポータルアドレスを使用してターゲットを検出するには

1. 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2. Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3. Target Discover Portal コマンドを入力します。
4. パラメータとして設定したターゲットのポータルアドレスと iSCSI インターフェース名を入力します。なお、次の点に注意してください。
   - ターゲットのポータルアドレスには <IPv4 address/hostname>[:port] の形式を使用する必要があります。ホスト名には短いホスト名または完全修飾ドメイン名を使用できます。
     例: 192.116.116.50 または abc:3260

- iSCSI インターフェース名には、数字 (0 から 9)、文字 (A から Z、a から z)、コロン (:)、ハイフン (-)、下線 (_)、ピリオド (.) のみを使用できます。最初の文字は数字 (0 から 9)、文字 (A から Z、a から z)、または下線 (_) に限られます。

5 Target Discover Portal <Portal Address> <Interface Name> コマンドを実行します。ユーザー名とパスワードを入力するように求められます。ターゲットに認証が必要な場合は yes を入力します。指定されたポータルアドレスとインターフェース上で利用可能なターゲットが検出され、次のように表示されます。

```
Does your target require a username and password? (yes,no)[no]:no

Showing the discovered targets...

+-----+-----------------------|--------------------|----------------+
| No. |     Target IQN        |Target Portal Address|
Interfaces   |
+-----+-----------------------|--------------------|----------------|
|  1  |iqn.1996-03.veritas:abc | 10.121.98.22:3260   | iscsi1,
iscsi2 |
+-----+-----------------------|--------------------|----------------|
|  2  |iqn.1996-03.veritas:xyz | 10.121.98.23:3260   | iscsi1,
iscsi2 |
+-----+-----------------------|--------------------|----------------+
|  3  |iqn.1996-03.veritas:host| 10.121.98.24:3260   | iscsi1,
iscsi2 |
------|-----------------------|--------------------|----------------|
```

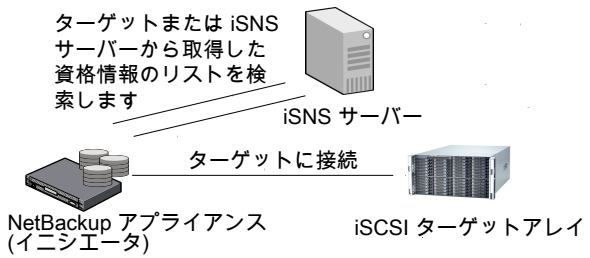
メモ: ターゲットに接続した後、`iSCSI > Target Discover Portal` または `iSCSI > Target Discover iSNS` コマンドを再実行すると、ターゲットのクレデンシャルなどの既存の接続設定が上書きされます。ターゲットに認証が必要な場合は、既存のセッションに再接続したときにターゲットのクレデンシャルを再入力する必要があります。アプライアンスを再起動した場合、アプライアンスの IQN を変更した場合、iSCSI プロセスを再起動した場合などに、既存のセッションに再接続する必要があります。

iSNS について

iSNS サーバーでは、Internet Storage Name Service プロトコルを使用して、ネットワーク上でアクティブな iSCSI デバイスに関する情報を保持します。この情報には、IP アドレス、iSCSI ノード名、ポータルグループが含まれます。iSNS プロトコルは、IP ストレージネットワーク上にある iSCSI デバイスの自動検出と自動管理に対応します。NetBackup アプライアンスに代表される iSCSI イニシエータは、iSNS サーバーに問い合わせて iSCSI ターゲットデバイスを検出できます。

iSNS（Internet Storage Name Service）サーバーを使用してターゲットを検出できます。iSNS サーバーを構成することで、すべてのターゲットごとにすべてのイニシエータを構成する必要がなくなります。ネットワーク上に多数のホストが存在する場合は、iSNS サーバーの構成により時間を節約できます。iSNS サーバーでは、グループボリュームの iSCSI ターゲット名についての最新情報を動的に維持することで、グループの一元的な管理ポイントが可能になります。

iSNS サーバーが存在する場合は、コマンドで特定のターゲット名を使用してターゲットを検出する必要はありません。次の図に、アプライアンスと iSNS サーバーの相互関係を示します。



iSNS を使ったターゲットの検出

このセクションでは、Internet Storage Name Service（iSNS）の手法を使用した iSCSI ターゲットの検出手順について説明します。少なくとも 1 台の iSNS サーバーがネットワーク上にある場合は、この手法を使用します。この手法を使用すると、iSCSI イニシエータで iSNS サーバーに登録されたターゲットを検出できます。この手法の場合、iSNS サーバーのアドレスおよび/またはポートを入力する必要があります。これにより、iSCSI イニシエータは指定された iSNS サーバーに問い合わせてターゲットを検出できます。iSNS サーバーのデフォルトのポートは 3205 です。

ターゲットに接続できるのはそれを検出した後に限られます。次の考慮事項を確認してください。

- ターゲットに接続した後、`iSCSI > Target Discover Portal` または `iSCSI > Target Discover iSNS` コマンドを再実行すると、ターゲットのクレデンシャルなどの既存の接続設定が上書きされます。ターゲットに認証が必要な場合は、既存のセッションを再接続したときに、ターゲットのクレデンシャルを再入力する必要があります。

アプライアンスを再起動した場合は、既存のセッションに再接続する必要があります。アプライアンスの IQN を変更した場合、または iSCSI プロセスを再起動した場合、既存のセッションに再接続する必要があります。

- 2 つの iSCSI インターフェース上で iSNS を使用してターゲットを検出する場合は、最初に `Target Discover iSNS` コマンドを *iscsi1* に実行してから *iscsi2* に実行します。`Target Show All` コマンドでは、最近のレコードのみ表示されます。たとえば、一部のターゲットに対しては、`Target Show All` コマンドの［インターフェース (Interfaces)］列に両方のインターフェース (*iscsi1*、*iscsi2*) が表示されないことがあります。一部のターゲットに対しては、直近のコマンドからのインターフェースのみが表示されます (この場合は *iscsi2*)。

iSNS サーバーを使って iSCSI ターゲットを検出する方法

メモ: 次の手順を行うには、iSNS サーバーを事前に設定してネットワークで利用可能にしておく必要があります。

---

1. 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2. Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3. Target Discover iSNS コマンドを入力します。
4. パラメータとして設定した iSNS サーバーのアドレスと iSCSI インターフェース名を入力します。
   - iSNS アドレスには <IPv4 address or hostname>[:port] の形式を使用する必要があります。ホスト名には短いホスト名または完全修飾ドメイン名を使用できます。デフォルトのポートは 3205 です。
     例: 192.116.50.50 または abc:3205

- iSCSI インターフェース名には、数字 (0 から 9)、文字 (A から Z、a から z)、コロン (:)、ハイフン (-)、下線 (_)、ピリオド (.) のみを使用できます。最初の文字は数字 (0 から 9)、文字 (A から Z、a から z)、または下線 (_) に限られます。

5 Target Discover iSNS <*iSNS address*> <*Interface name*> コマンドを実行して、特定インターフェース上の iSNS サーバーに登録されているすべての iSCSI ターゲットを検出します。

ユーザー名とパスワードを入力するように求められます。ターゲットに認証が必要な場合は yes を入力します。

メモ: ターゲットデバイスで CHAP 認証を有効にして、iSNS を使用してターゲットを検出するとき、`iSCSI > Target Discover` コマンドを使用してもターゲットの資格情報の入力が求められない場合もあります。

```
Does your target require a username and password? (yes,no)[no]:no

Showing the discovered targets...

+-----+-------------------------|---------------------|----------------+
| No. |          Target IQN      |Target Portal Address|
Interfaces   |
+-----+-------------------------|---------------------|----------------|
|  1  | iqn.1996-03.veritas:abc  | 10.121.98.22:3260   | iscsi1,
 iscsi2 |
+-----+-------------------------|---------------------|----------------|
|  2  | iqn.1996-03.veritas:xyz  | 10.121.98.23:3260   | iscsi1,
 iscsi2 |
+-----+-------------------------|---------------------|----------------+
|  3  | iqn.1996-03.veritas:host | 10.121.98.24:3260   | iscsi1,
 iscsi2 |
------|-------------------------|---------------------|----------------|
```

ターゲットへの接続

イニシエータとターゲットの接続が検出されたら、iSCSI イニシエータからターゲットにログオンし、接続を確立して iSCSI 上でデータを転送する必要があります。ログオンは固定され、サーバーが再起動すると(ユーザーがターゲットからログオフしない限り)接続は自動的に復元されます。

イニシエータを単一のターゲットに接続するには、ポータルの IP アドレスとターゲット IQN を指定します。

ターゲットに接続するには

1 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。

2 Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。

3 Target Connect コマンドを入力します。

4 検出されたターゲットの IQN とポータルアドレスを入力します。ターゲットで認証が有効な場合は、ユーザー名を入力する必要があります。

なお、IQN、ポータルアドレス、ユーザー名について、次の点に注意してください。

- IQN には、数字 (0 から 9)、文字 (A から Z、a から z)、コロン (:)、ハイフン (-)、下線 (_)、ピリオド (.) のみを使用できます。
  例: iqn.1999-06.com.veritas:storage.lun1
- ターゲットのポータルアドレスには <IP address/hostname>[:port] の形式を使用する必要があります。IPv4 アドレスのみがサポートされます。ホスト名には短いホスト名または完全修飾ドメイン名を使用できます。
  例: 192.116.116.50 または abc:3260
- ユーザー名には、数字 (0 から 9)、文字 (A から Z、a から z)、ハイフン (-)、下線 (_)、ピリオド (.) のみを使用できます。最初の文字は数字（0 ～ 9）、文字（A ～ Z、a ～ z）、または下線（_）に限られます。
  例: john.smith

5 コマンドを実行してターゲットに接続します。一度に 1 つの検出されたターゲットに接続できます。

ターゲットとのセッションの切断

iSCSI > Target Disconnect コマンドを使用して、特定の IQN とポータルアドレスを持つターゲットとのセッションを切断できます。このコマンドを実行すると、このターゲットに接続されているすべてのセッションが切断されます。

一度に 1 つのターゲットとのセッションを切断できます。

メモ: iSCSI インターフェース上でワークロードが稼働中の場合は、コマンドの完了までの時間が長くなります。

ターゲットとのセッションを切断するには

1 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。

2 Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。

3 Target Disconnect コマンドを入力します。

4 切断するターゲットの IQN とポータルアドレスを入力します。

IQN とポータルアドレスについて、次の注意点があります。

- IQN には、数字（0 ～ 9）、文字（A ～ Z、a ～ z）、コロン（:）、ハイフン（-）、下線（_）、ピリオド（.）のみを使用できます。
  例: iqn.1999-06.com.veritas:storage.lun1
- ターゲットのポータルアドレスには <IPv4 address/hostname>[:port] の形式を使用する必要があります。ホスト名には短いホスト名または完全修飾ドメイン名を使用できます。
  例: 192.116.116.50 または abc:3260

5 コマンドを実行して特定のターゲットとのセッションを切断します。次のプロンプトが表示されたら、yes を入力します。

```
Do you want to disconnect the target session?[yes, no](no):yes

[Info] The target session has been disconnected.
```

ターゲットの表示

このセクションでは、ターゲットを表示する手順について説明します。iSCSI > Target Show コマンドを使用して、すべての検出済みターゲットまたは接続済みターゲットを表示できます。

接続済みターゲットを表示するには

1 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2 Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3 Target Show Connected コマンドを入力し、Enter キーを押します。
4 接続済みターゲットのリストが次のように表示されます。

```
Showing the connected targets...

+-----+------------+-----------------------+----------------------+--------+
| No. | Session ID |      Target IQN       | Target Portal Address| Status |
+-----+------------+-----------------------+----------------------|--------+
|  1  |     5      |iqn.1996-03.veritas:abc|   10.121.37.51:3260  | Online 1     |
+-----+------------+-----------------------+----------------------+--------+
```

セッションの［状態（Status）］は、［オンライン（Online）］または［オフライン（Offline）］のいずれかです。［状態（Status）］は、ケーブルが引き抜かれるか、またはネットワーク接続性の問題がある場合に［オフライン（Offline）］になることがあります。

利用可能なすべてのターゲットを表示するには

1. 管理者として Secure Shell（SSH）セッションを開きアプライアンスにログオンします。
2. Main_Menu >［設定 (Settings)］>［iSCSI］メニューに移動します。
3. Target Show All コマンドを入力し、Enter キーを押します。
4. 検出済みのすべてのターゲットのリストが次のように表示されます。

```
Showing all the targets...

+-----+------------------------|---------------------|-----------+
| No. |      Target IQN        |Target Portal Address|Interfaces |
+-----+------------------------|---------------------|-----------|
|  1  |iqn.1996-03.veritas:abc | 10.121.98.22:3260   | iscsi1    |
+-----+------------------------|---------------------|-----------|
|  2  |iqn.1996-03.veritas:xyz | 10.121.98.23:3260   | iscsi1    |
+-----+------------------------|---------------------|-----------+
|  3  |iqn.1996-03.veritas:host| 10.121.98.24:3260   | iscsi1    |
------|------------------------|---------------------|-----------|
```

メモ: 2 つの iSCSI インターフェースで iSNS を使用してターゲットが検出された場合、`Target Show All` コマンドで表示されるのは最新レコードのみです。たとえば、`Target Discover iSNS` コマンドを *iscsi1* に実行した後に *iscsi2* にコマンドを実行した場合、［インターフェース (Interfaces)］列は `Target Show All` コマンドの出力で一部のターゲットに両方のインターフェース (*iscsi1*、*iscsi2*) は表示されない場合があります。一部のターゲットに対しては、直近のコマンドからのインターフェースのみが表示されます (この場合は *iscsi2*)。

5

iSCSI の問題のトラブルシューティングとベストプラクティス

この章では以下の項目について説明しています。

- DataCollect コマンドを使ったデバイスログの収集
- syslogd メッセージについて
- iSCSI 警告について
- ベストプラクティス

DataCollect コマンドを使ったデバイスログの収集

`Main > Support` シェルメニューから `DataCollect` コマンドを使ってデバイスログを収集できます。これらのデバイスログを ベリタスのサポートチームと共有することで、デバイス関連の問題を解決できます。

DataCollect コマンドは次のログを収集します。

- リリース情報
- ディスクパフォーマンスのログ
- コマンド出力ログ
- iSCSI ログ

メモ: iSCSI ログは /var/log/messages and /var/log/iscsiuio.log にあります。

- CPU 情報
- メモリ情報
- オペレーティングシステムのログ
- Patch ログ
- ストレージログ
- ファイルシステムログ
- Test hardware のログ
- AutoSupport ログ
- ハードウェア情報
- Sysinfo ログ

DataCollect コマンドを使ってデバイスログを収集する方法

1. NetBackup Appliance Shell Menuにログオンします。
2. `Main > Support` ビューから次のコマンドを入力して、デバイスログを収集します。

   ```
   DataCollect
   ```

   アプライアンスは `/tmp/DataCollect.zip` ファイルにデバイスログを生成します。
3. `Main > Support > Logs > Share Open` コマンドを使って、`DataCollect.zip` をローカルフォルダにコピーします。
4. 問題を解決するために、ベリタスのサポートチームに `DataCollect.zip` ファイルを送信できます。

syslogd メッセージについて

NetBackup Appliance Shell Menuには次のようなメッセージが表示される場合があります。

```
Message from syslogd@host at Sep 12 10:09:14 ...
iscsid:

Message from syslogd@host at Sep 12 10:13:27 ...
iscsid:

Message from syslogd@host at Sep 12 10:17:53 ...
iscsid:
```

これらのメッセージは、NetBackup Appliance Shell Menuに異なるタイミングで表示されます。これらは、iSCSIコマンドを実行しているとき、コマンド出力の途中、またはコンソールがアイドル状態のときにも表示されます。これらのメッセージは無害で無視できます。

iSCSI 警告について

特定のアプライアンスに警告を構成している場合は、iSCSI 警告も受け取ることができます (該当する場合)。iSCSI 警告は、次の状況で生成されます。

- iSCSI セッションでターゲットが切断された場合 (V-475-108-1000)
- iSCSI セッションでターゲットストレージサーバーがオフラインの場合 (V-475-108-1001)
- 10Gb イーサネット/iSCSI カードで、サポートされていない Small Form-Factor Pluggable (SFP+) モジュールが検出された場合 (V-475-107-1000)

次に、iSCSI 警告の例を示します。

```
An iSCSI session with the target has been disconnected.
Time of event: 2016-09-09 21:34:13 (-07:00)
UMI Event code: V-475-108-1000
Component Type: Connections
Component: <Target IQN> <Portal address> <Interface name>
Status: Disconnected
State: ERROR
Additional information about this error is available at following
link: V-475-108-1000

An iSCSI session with the target storage server is offline.
Time of event: 2016-10-13 21:34:13 (-07:00)
UMI Event code: V-475-108-1001
Component Type: Connections
Component: <Target IQN> <Portal address> <Interface name>
Status: Offline
State: ERROR
Additional information about this error is available at following
link: V-475-108-1001

The SFP+ module that is currently installed in the 10Gb Ethernet/iSCSI

card is not supported.
Time of event: 2016-10-06 18:31:42 (-07:00)
UMI Event code: V-475-107-1000
Component Type: Ethernet
Component: PCIe slot 6, port 1 SFP
Status: Unsupported
```

```
State: ERROR
Additional information about this error is available at following
link: V-475-500-1000
```

ベストプラクティス

次に、iSCSI の推奨事項とベストプラクティスをいくつか示します。

- デフォルト値と異なる IQN を構成します。
  p.19 の「イニシエータの IQN の設定」を参照してください。
- iSCSI 関連の警告を受け取ることができるように警告を構成します。
  アラートの構成については、『NetBackup Appliance 管理者ガイド』を参照してください。