

NetBackup™ SAN クライアントおよびファイバートランスポートガイド

UNIX、Windows および Linux

リリース 11.1

NetBackup™ SAN クライアントおよびファイバートラン サポートガイド

最終更新日: 2026-01-22

法的通知と登録商標

Copyright © 2026 Cohesity, Inc. All rights reserved.

Cohesity、Veritas、Cohesity ロゴ、Veritas ロゴ、Veritas Alta、Cohesity Alta、NetBackup は、Cohesity, Inc. またはその関連会社の米国およびその他の国における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。

この製品には、Cohesity 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア（「サードパーティ製プログラム」）が含まれる場合があります。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。このCohesity製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

<https://www.veritas.com/about/legal/license-agreements>

本書に記載されている製品は、その使用、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ます。Cohesity, Inc. 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、現状のまま提供されるものであり、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。Cohesity, Inc. およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切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。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Cohesityがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19 「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202 「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。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。

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の **Web** サイトにアクセスしてください。

<https://www.veritas.com/support>

次の URL で **Cohesity Account** の情報を管理できます。

<https://my.veritas.com>

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

世界共通 (日本を除く)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が記載されています。最新のマニュアルは、**Cohesity** の **Web** サイトで入手できます。

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity SORT (Service and Operations Readiness Tools) は、特定の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	SAN クライアントとファイバートランスポートの概要	8
	NetBackup SAN クライアントとファイバートランスポートについて	8
	ファイバートランスポートについて	9
	ファイバートランスポートメディアサーバーについて	10
	SAN クライアントについて	10
	ファイバートランスポートサービスマネージャについて	11
	サポート対象のシステムと周辺機器	11
第 2 章	配備の計画	12
	SAN クライアントの配置計画	12
	SAN クライアントの操作上の注意事項	13
	SAN クライアントの宛先ストレージについて	13
	SAN クライアントの宛先ディスクストレージについて	14
	SAN クライアントの宛先テープストレージについて	14
	SAN クライアントとファイバートランスポートのホストを選択する方法	15
	エージェントの NetBackup SAN クライアントサポートについて	15
	クラスタリングのための NetBackup SAN クライアントサポート	16
	NetBackup SAN クライアントの Windows Hyper-V サーバーサポートについて	16
	NetBackup SAN クライアントのサポート外のリストアについて	17
	ファイバートランスポートのスループットについて	17
	SAN クライアントへの SAN メディアサーバーの変換	18
第 3 章	SAN の準備	20
	SAN の準備	20
	ファイバートランスポート用の SAN のゾーン化について	21
	16 gb ターゲットモード HBA をサポートするファイバートランスポート向けの SAN のゾーン化	23
	SAN クライアントおよびファイバートランスポートメディアサーバー用 HBA について	25
	SAN クライアントおよびファイバートランスポートメディアサーバー用 16 gb ターゲットモード HBA について	26
	SAN クライアント用の HBA ポートを選択する場合	27

	SAN クライアントでサポートする SAN 構成について	27
第 4 章	SAN クライアントとファイバートランスポートのライセンス	29
	SAN クライアントのインストールについて	29
	SAN クライアントのライセンスについて	29
	SAN クライアントおよびファイバートランスポートをアップグレードする場合	30
第 5 章	SAN クライアントおよびファイバートランスポートの構成	31
	SAN クライアントおよびファイバートランスポートの構成	31
	ファイバートランスポートメディアサーバーの設定	32
	ターゲットモードドライバについて	33
	nbhba モードと ql2300_stub ドライバについて	34
	FC に接続されるデバイスについて	34
	HBA ポートを識別する方法	35
	Solaris での HBA ポートの検出について	36
	ファイバーのトランスポートのメディアサーバーおよび VLAN について	36
	nbhba モードの開始	37
	ファイバートランスポートメディアサーバー HBA ポートのマーク付け	39
	メディアサーバーのファイバートランスポートサービスの設定	41
	16 gb ターゲットモード HBA サポート向けのメディアサーバーファイバートランスポートサービスの構成	45
	16 gb ターゲットモード HBA をサポートする FTMS の状態の表示	51
	16 gb ターゲットモード HBA をサポートする HBA ポートの識別	51
	SAN クライアントの構成	52
	SAN クライアントのファイアウォールの構成について	52
	SAN クライアントのドライバの要件	53
	SAN クライアントのファイバートランスポートサービスの構成	54
	クラスタ内の SAN クライアントの構成	55
	SAN クライアントのクラスタの仮想名の登録	56
	コマンドラインの使用による NetBackup 構成オプションの設定	57
	ファイバートランスポートのプロパティの構成について	58
	ファイバートランスポートのプロパティの構成	59
	[ファイバートランスポート (Fibre Transport)]プロパティ	60
	Linux 並列 FT 接続について	63
	SAN クライアントの使用設定の構成	64

	SAN クライアントの使用設定	64
第 6 章	SAN クライアントおよびファイバートランスポートの管理	66
	ファイバートランスポートサービスの有効化または無効化	66
	16 gb ターゲットモード HBA サポート向けのファイバートランスポートサービスの有効化および無効化	67
	SAN クライアントからファイバートランスポートデバイスの再スキャン	67
	SAN クライアントのファイバートランスポートジョブの詳細の表示	68
	ファイバートランスポートトラフィックの表示	69
	SAN クライアントの削除	70
第 7 章	SAN クライアントとファイバートランスポートの無効化	71
	SAN クライアントの無効化	71
	ファイバートランスポートメディアサーバーの無効化	72
	16 gb ターゲットモード HBA サポートのファイバートランスポートメディアサーバーの無効化	73
第 8 章	SAN クライアントとファイバートランスポートのトラブルシューティング	75
	SAN クライアントとファイバートランスポートのトラブルシューティングについて	76
	SAN クライアントのトラブルシューティングの TechNote	76
	ファイバートランスポートログの表示	76
	統合ログについて	77
	vxlogview コマンドを使用した統合ログの表示について	78
	vxlogview を使用した統合ログの表示の例	80
	ファイバートランスポートサービスの起動および停止	81
	16 gb ターゲットモード HBA サポート向けのファイバートランスポートサービスの起動および停止	82
	バックアップはファイバートランスポートデバイスが使用可能であっても LAN にフェールオーバーする	83
	Cohesity モジュールのロード時のカーネルの警告メッセージ	84
	SAN クライアントのサービスが起動しない	84
	SAN クライアントファイバートランスポートサービスの検証	84
	SAN クライアントがファイバートランスポートを選択しない	85
	メディアサーバーのファイバートランスポートデバイスが非アクティブ	86
	ファイバートランスポートデバイスの検出なし	87

付録 A

AIX に固有の構成の詳細	88
AIX のリファレンス情報	88
NetBackup の構成を開始する前に (AIX)	88
AIX での永続的な名前のサポートについて	89
AIX でのロボット制御デバイスファイルの構成について	89
AIX の SAN クライアントについて	89
AIX での QIC 以外のテープドライブについて	90
AIX の非巻き戻しデバイスファイルについて	90
テープドライブの AIX 非巻き戻しデバイスファイルの作成	91
AIX 動的追跡の無効化	92

SAN クライアントとファイバートランスポートの概要

この章では以下の項目について説明しています。

- [NetBackup SAN クライアントとファイバートランスポートについて](#)
- [ファイバートランスポートについて](#)
- [ファイバートランスポートメディアサーバーについて](#)
- [SAN クライアントについて](#)
- [ファイバートランスポートサービスマネージャについて](#)
- [サポート対象のシステムと周辺機器](#)

NetBackup SAN クライアントとファイバートランスポートについて

SAN クライアントは NetBackup クライアントの高速バックアップとリストアを可能にする NetBackup オプション機能です。

SAN クライアントは特別な NetBackup クライアントです。LAN ではなく SAN 接続で大量のデータのバックアップを迅速に作成できます。たとえば、高速なバックアップとリストアはデータベースホストの役に立ちます。ファイバートランスポートは SAN クライアント機能の一部である NetBackup 高速データトランスポート方式の名前です。

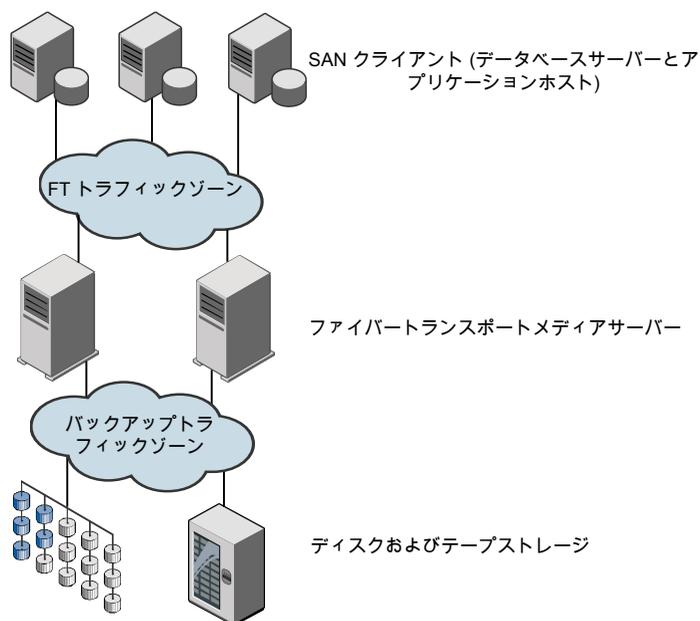
バックアップとリストアのトラフィックはファイバーチャネル (FC) で転送し、NetBackup サーバーとクライアントの管理トラフィックは LAN で転送します。

NetBackup 52xx/53xx Appliance の場合には、ファイバートランスポートはファイバートランスポートをサポートする NetBackup 5000 シリーズのアプライアンスに高速なトラフィック

クを提供します。5000 シリーズアプライアンスは、SAN クライアントバックアップのストレージホストとして機能します。

図 1-1 に SAN クライアントの構成を示します。

図 1-1 SAN クライアントの構成



ファイバートランスポートについて

NetBackup ファイバートランスポートはデータ転送の方式です。これはファイバーチャネルを使用し、LAN を介した TCP/IP ではなく SAN を介したデータ移動用の SCSI コマンドプロトコルの一部を使用します。**NetBackup** クライアントと **NetBackup** メディアサーバー間に高性能なトランスポート機構を提供します。

ファイバートランスポートでは複数の並列論理接続がサポートされます。ファイバートランスポートをサポートする **NetBackup** システムには、FT 通信専用のファイバーチャネル HBA が含まれます。

NetBackup ファイバートランスポートサービスはストレージに接続する **NetBackup** メディアサーバーと SAN クライアントの両方で有効になっています。

このマニュアルでは、**NetBackup** クライアントと **NetBackup** サーバー間におけるファイバートランスポート接続を、FT パイプと呼びます。

ファイバートランスポートメディアサーバーについて

NetBackup FT メディアサーバーは、ファイバートランスポートサービスが有効になっている NetBackup メディアサーバーです。NetBackup FT メディアサーバーは、SAN クライアントからの接続を受け入れ、ディスクストレージにデータを送信します。

SAN クライアントからの接続を受け入れるホストバスアダプタ (HBA) は、特別な NetBackup ターゲットモードドライバを使用して FT 通信を処理します。

メディアサーバーの FT サービスは、データフローの制御、SCSI コマンドの処理、および FT 接続におけるサーバー側のデータバッファの管理を行います。また、ホストバスアダプタのターゲットモードドライバの管理も行います。

SAN クライアント機能をアクティブ化するライセンスが必要です。

p.32 の「ファイバートランスポートメディアサーバーの設定」を参照してください。

p.60 の「[ファイバートランスポート (Fibre Transport)] プロパティ」を参照してください。

p.8 の「NetBackup SAN クライアントとファイバートランスポートについて」を参照してください。

SAN クライアントについて

NetBackup SAN クライアントは、ファイバートランスポートサービスが有効になっている NetBackup クライアントです。SAN クライアントは、Shared Storage Option に使用される NetBackup SAN メディアサーバーと類似しており、自身のデータをバックアップします。ただし、SAN クライアントは小さいクライアントのインストールパッケージに基づいているため、管理の要件および使用されるシステムリソースはより小規模になります。

NetBackup

通常、SAN クライアントにはバックアップのために高帯域幅が必要な重要なデータが含まれています。それはファイバーチャネルを介して NetBackup メディアサーバーに接続します。

NetBackup SAN クライアントのファイバートランスポートサービスは、SAN クライアントの FT パイプの接続性とデータ転送を管理します。また、SAN クライアントの FT サービスは、NetBackup メディアサーバー上の FT ターゲットモードデバイスを検出し、それを FT Service Manager に通知します。

<http://www.veritas.com/docs/DOC5332>

p.52 の「SAN クライアントの構成」を参照してください。

p.52 の「SAN クライアントのファイアウォールの構成について」を参照してください。

p.53 の「SAN クライアントのドライバの要件」を参照してください。

p.54 の「SAN クライアントのファイバートランスポートサービスの構成」を参照してください。

ファイバートランスポートサービスマネージャについて

FT Service Manager (FSM) は、NetBackup Enterprise Media Manager サービスをホスティングする NetBackup サーバーに存在します。FSM は、SAN クライアントおよび FT メディアサーバーで実行される FT サービスと相互作用します。FSM は、FT のリソースおよびイベントを検出、構成および監視します。FSM の実行は、EMM と同じプロセスで行われます。

サポート対象のシステムと周辺機器

制限事項と操作上の注意事項については、『[NetBackup リリースノート](#)』を参照してください。サポート対象のシステムと周辺機器については、[Services and Operations Readiness Tools \(SORT\)](#) のサイトを参照してください。

配備の計画

この章では以下の項目について説明しています。

- [SAN クライアントの配置計画](#)
- [SAN クライアントの操作上の注意事項](#)
- [SAN クライアントの宛先ストレージについて](#)
- [SAN クライアントとファイバートランスポートのホストを選択する方法](#)
- [エージェントの NetBackup SAN クライアントサポートについて](#)
- [クラスタリングのための NetBackup SAN クライアントサポート](#)
- [NetBackup SAN クライアントの Windows Hyper-V サーバーサポートについて](#)
- [NetBackup SAN クライアントのサポート外のリストアについて](#)
- [ファイバートランスポートのスループットについて](#)
- [SAN クライアントへの SAN メディアサーバーの変換](#)

SAN クライアントの配置計画

表 2-1 に、SAN クライアントとファイバートランスポートの配置計画の概要を示します。

表 2-1 SAN クライアントの配置の概要

手順	配置タスク	セクション
手順 1	操作上の注意事項について	p.13 の「 SAN クライアントの操作上の注意事項 」を参照してください。
手順 2	宛先ストレージの決定	p.13 の「 SAN クライアントの宛先ストレージについて 」を参照してください。

手順	配置タスク	セクション
手順 3	使うホストの決定	p.15 の「 SAN クライアントとファイバートランスポートのホストを選択する方法 」を参照してください。
手順 4	SAN の準備	p.20 の「 SAN の準備 」を参照してください。
手順 5	SAN クライアントのライセンスの取得	p.29 の「 SAN クライアントのライセンスについて 」を参照してください。
手順 6	NetBackup エージェントについて読む	p.15 の「 エージェントの NetBackup SAN クライアントサポートについて 」を参照してください。
手順 7	SAN クライアントおよび Hyper-V についての確認	p.16 の「 NetBackup SAN クライアントの Windows Hyper-V サーバーサポートについて 」を参照してください。
手順 8	SAN クライアントとファイバートランスポートの構成	p.31 の「 SAN クライアントおよびファイバートランスポートの構成 」を参照してください。
手順 9	SAN クライアントへの SAN メディアサーバーの変換	p.18 の「 SAN クライアントへの SAN メディアサーバーの変換 」を参照してください。

SAN クライアントの操作上の注意事項

次に、留意すべき操作上の注意事項のいくつかについて説明します。

- NetBackup クライアントの暗号化オプションは、UNIX と Linux の SAN クライアントではサポートされません。
- データ圧縮または暗号化により、バックアップとリストアのためのファイバートランスポートのパフォーマンスが低下する場合があります。
バックアップでデータの圧縮または暗号化を使うと、バックアップとリストアの両方で、ファイバートランスポートパイプのパフォーマンスが大幅に低下する場合があります。構成によっては、圧縮を使用すると、圧縮を使用しなかった場合に比べてパフォーマンスが最大 95 % 低下する場合があります。

SAN クライアントの宛先ストレージについて

SAN クライアントとファイバートランスポート機能のための宛先ストレージとしてディスクかテープを使うことができます。

NetBackup はあらゆる手段を用いてストレージデバイスによる FT メディアサーバーへの接続を可能にします。

SAN クライアントの宛先ディスクストレージについて

ディスクストレージの場合、NetBackup OpenStorage の実装は高パフォーマンスのバックアップとリストアに対する絶好の機会を提供します。それらのソリューションは、NetBackup ファイバートランスポート機構が提供する大量のデータを受け入れるのに十分な帯域幅と読み込みおよび書き込み速度を提供することができます。

NetBackup メディアサーバーの重複排除は OpenStorage の実装です。NetBackup クライアント側の重複排除はサポートされません。

SAN クライアントの宛先テープストレージについて

SAN クライアントは宛先ストレージユニットとしてテープを使うことができます。一部のテープドライブは、NetBackup ファイバートランスポート機構が提供する大量のデータの読み込み、書き込みを行うのに十分な速度を備えています。

宛先としてテープを使用する場合は、複数ストリームを使用できます。複数ストリームは、クライアントの自動バックアップを複数のジョブに分割します。ジョブは個別のデータストリームにあるので、並列実行できます。データストリームは FT メディアサーバーに 1つ以上の FT パイプを介して送信できます。メディアサーバーはそれらを一緒に 1つ以上のテープメディアボリューム上に多重化します。たとえば、複数のデータストリームを提供するデータベースサーバーがあれば、FT メディアサーバーへのそれらのデータベースバックアップを複数ストリームで実行できます。FT メディアサーバーはデータストリームをメディア上に多重化し、パフォーマンス全体を向上させます。

NetBackup の SAN メディアサーバーを SAN クライアントに置き換えて、テープにバックアップし続けることができます。SAN クライアントでは、ディスク領域と CPU 両方のシステムリソースの使用量は SAN メディアサーバーよりも少なくなります。

マルチストリームを構成するには、『NetBackup 管理者ガイド Vol.1』を参照してください。

<http://www.veritas.com/docs/DOC5332>

SAN クライアントのテープストレージの制限事項

次の制限事項は SAN クライアントの宛先ストレージとしてのテープのためのものです。

- 同じクライアントからの FT のバックアップのみが特定の MPX グループで多重化されます。
- 異なるクライアントからの FT のバックアップは同じ MPX グループで一緒に多重化されません。
- 同じテープに異なる SAN クライアントを多重化できません。異なるクライアントは同じ FT メディアサーバーに引き続きバックアップされますが、異なる MPX グループの異なるテープドライブに書き込まれます。
- (同じクライアントまたは異なるクライアントからの) FT と LAN のバックアップは同じ MPX グループで一緒に多重化されません。

- SAN クライアントはファイバートランスポート上のインラインテープコピーをサポートしません。インラインテープコピージョブは LAN を介して行われます。SAN クライアント機能は非常に高速なバックアップとリストア操作のために設計されています。したがって、SAN クライアントは、処理および管理するのにさらに多くのリソースが必要な (インラインテープコピーのような) バックアップオプションを除外します。

SAN クライアントとファイバートランスポートのホストを選択する方法

NetBackup ファイバートランスポートに使用するシステムを選択する場合は、次の点に注意してください。

- NetBackup SAN クライアントを、NetBackup サーバーとして使用することはできません。したがって、NetBackup クライアントソフトウェアのみがインストールされているシステムにのみ、NetBackup クライアントを SAN クライアントとして構成します。
- NetBackup プライマリサーバーを FT メディアサーバーとして使用しないでください。データ転送によってシステムリソースが消費されるため、NetBackup の管理パフォーマンスが著しく低下します。

エージェントの NetBackup SAN クライアントサポートについて

SAN クライアント機能はデータ転送に共有メモリを使います。SAN クライアントで NetBackup エージェントを使う場合、エージェントはその共有メモリから読み書きする権限が必要です。

次のように、エージェントに適切な権限があることを確認します。

- UNIX システムでは、NetBackup がインストールされた同じユーザーアカウントを使って、NetBackup エージェントをインストールします。
- Windows SAN クライアントで、NetBackup エージェントと SAN Client Fibre Transport Service が同じアカウント (つまり、[ログオン (Log On As)]) を使います。アカウントには有効状態の [オペレーティング システムの一部として機能 (Act as a part of the operating system) 権限が必要です。デフォルトでは、[ローカルシステム (Local System)] アカウントだけが [オペレーティング システムの一部として機能 (Act as a part of the operating system) 権限が有効になっています。

SAN クライアントは次の種類のエージェントバックアップをサポートしません。

- Microsoft SharePoint
- Enterprise Vault
- Microsoft Exchange データベース可用性グループ (DAG)

クラスタリングのための NetBackup SAN クライアントサポート

NetBackup は、アプリケーションクラスタで SAN クライアントをサポートします。アプリケーションクラスタ内の SAN クライアントの要件は以下のとおりです。

- SAN クライアントはクラスタのすべてのフェールオーバーノードにインストールする必要があります。
- FT クライアントサービスおよび PBX サービスは、すべてのフェールオーバーノードで実行する必要があります。
- 各ノード上の各 SAN クライアントのホストコンピュータオペレーティングシステムが FT メディアサーバーのターゲットモードドライバを検出する必要があります。
- NetBackup LOCAL_CACHE 値は各 SAN クライアントで NO でなければなりません。デフォルトでは値は指定されていないため、値を設定する必要があります。

警告: FT メディアサーバーまたはプライマリサーバーの LOCAL_CACHE 値は変更しないでください。

p.55 の「[クラスタ内の SAN クライアントの構成](#)」を参照してください。

バックアップポリシーで、SAN クライアントコンピュータへの参照のエイリアスまたは動的アプリケーションクラスタ名を使用できます。NetBackup は、5 分ごとに SAN クライアントクラスタ情報を更新します。

NetBackup SAN クライアントの Windows Hyper-V サーバーサポートについて

NetBackup SAN クライアントは Windows Hyper-V サーバーのためのファイバートランSPORT上のバックアップをサポートします。Hyper-V サーバーの NetBackup クライアントソフトウェアをインストールし、Hyper-V Server の SAN クライアントを構成します。Hyper-V 仮想マシン内のオペレーティングシステムに NetBackup クライアントソフトウェアをインストールすることや SAN クライアントを構成することは行わないでください。

p.52 の「[SAN クライアントの構成](#)」を参照してください。

バックアップを実行する場合、『NetBackup™ for Hyper-V 管理者ガイド』に従って、Hyper-V ポリシーを作成して、Hyper-V サーバーとその仮想マシンをバックアップします。

<http://www.veritas.com/docs/DOC5332>

SAN クライアントおよびファイバートランスポートが正しく構成されると、ファイバーのトランスポート上でバックアップが行われます。

NetBackup は Windows Hyper-V サーバーへのファイバートランスポートのリストアをサポートしません。リストアは LAN を介して行います。

p.17 の「[NetBackup SAN クライアントのサポート外のリストアについて](#)」を参照してください。

NetBackup SAN クライアントのサポート外のリストアについて

ほとんどの場合、バックアップが NetBackup ファイバートランスポートのデータ転送方式を使う場合は、リストアもファイバートランスポートの方式によって実行されます。

ただし、NetBackup は一部の NetBackup のオプションや他の製品のファイバートランスポートリストアをサポートしないことがあります。

NetBackup では、次のオプションについてファイバートランスポートリストアをサポートしません。

FlashBackup リストア SAN クライアントは FlashBackup バックアップをサポートしますが、リストアは LAN 経由で行われます。

Windows Hyper-V のリストア SAN クライアントは Fibre Transport 経由のバックアップをサポートしますが、リストアは LAN 経由で行われます。

バックアップポリシーの設定のタイミングを選択するオプションによっては、仮想マシンと仮想マシン内の個々のファイルをリストアすることもできます。

p.16 の「[NetBackup SAN クライアントの Windows Hyper-V サーバーサポートについて](#)」を参照してください。

ファイバートランスポートのスループットについて

次のコンポーネントの最低速度はファイバートランスポートのスループット率を制限することがあります。

- SAN クライアントの速度性能。
クライアントがファイルシステムかデータベースに読み込み、書き込みを行う速度はパフォーマンスに影響します。
- ストレージユニットの読み込みおよび書き込み速度。
- コンピュータ PCI の I/O メモリの帯域幅。

SAN クライアントで、HBA の PCI-X バスの非 PCI X カードは制御バスの速度を下げます。NetBackup FT メディアサーバーほどは影響されませんが、パフォーマンスは許容できないレベルにまで低下することがあります。

- データを転送するファイバーチャネルパイプの速度。
- ファイバーチャネルのトポロジー。
ボトルネックは、複数のデータストリームがトランクまたはスイッチ間のリンクのような共有要素を通して送信されるときに起きることがあります。

SAN クライアントへの SAN メディアサーバーの変換

表 2-2 に、SAN メディアサーバーを SAN クライアントに変換する方法の概要を示します。コンピュータのホスト名は変わりません。この手順はすべての NetBackup サーバーが SAN クライアント機能をサポートするリリースを実行していることを想定しています。

表 2-2 SAN メディアサーバーから SAN クライアントに変換する方法

手順	作業	手順の詳細
手順 1	SAN メディアサーバーの削除	次を実行します。 <ul style="list-style-type: none"> ■ NetBackup Web UI で、[ストレージ (Storage)]、[メディアサーバー (Media servers)]の順に選択します。 ■ ホストを選択します。 ■ [デバイスホストの削除 (Delete device host)]を選択します。
手順 2	SAN メディアサーバーソフトウェアのアンインストール	『NetBackup インストールガイド』を参照してください。
手順 3	ファイバートランスポートに対する準備	ファイバートランスポート用に SAN を準備し、ファイバートランスポートのホストと SAN クライアントのホストに HBA をインストールします。 p.20 の「SAN の準備」を参照してください。
手順 4	FT メディアサーバーのホストへのストレージの接続	新しい SAN クライアントの FT メディアサーバーに SAN メディアサーバーのストレージデバイスを接続します。ディスクストレージの場合は、必要に応じてストレージをマウントします。 p.20 の「SAN の準備」を参照してください。

手順	作業	手順の詳細
手順 5	NetBackup メディアサーバーソフトウェアのインストール	ファイバートランスポートメディアサーバーとして機能するホストにメディアサーバーソフトウェアをインストールします。 『NetBackup インストールガイド』を参照してください。
手順 6	FT メディアサーバーの構成	p.31 の「SAN クライアントおよびファイバートランスポートの構成」を参照してください。
手順 7	NetBackup クライアントソフトウェアのインストール	SAN メディアサーバーとして機能していたホストにクライアントソフトウェアをインストールします。 『NetBackup インストールガイド』を参照してください。
手順 8	SAN クライアントの構成	p.31 の「SAN クライアントおよびファイバートランスポートの構成」を参照してください。
手順 9	代替サーバーのリストアの構成	現在のホストはメディアサーバーではないため、代替サーバーのリストアを構成し、[リストアサーバー (Restore server)] に FT メディアサーバーを指定します。その後、NetBackup は、SAN メディアサーバーに関連付けられたイメージをリストアするために FT メディアサーバーを使用します。 プライマリサーバーの[ホストプロパティ (Host properties)]の[一般的なサーバー (General server)]プロパティで[メディアホストの上書き (Media host override)]の設定を参照してください。 SAN メディアサーバーに関連付けられたイメージすべてが期限切れになった後、代替サーバーのリストアを構成解除できます。

SAN の準備

この章では以下の項目について説明しています。

- [SAN の準備](#)
- [ファイバートランスポート用の SAN のゾーン化について](#)
- [16 gb ターゲットモード HBA をサポートするファイバートランスポート向けの SAN のゾーン化](#)
- [SAN クライアントおよびファイバートランスポートメディアサーバー用 HBA について](#)
- [SAN クライアントおよびファイバートランスポートメディアサーバー用 16 gb ターゲットモード HBA について](#)
- [SAN クライアント用の HBA ポートを選択する場合](#)
- [SAN クライアントでサポートする SAN 構成について](#)

SAN の準備

表 3-1 に準備の手順とそれらを実行する順序を示します。

表 3-1 SAN の準備の概要

手順	手順	項
手順 1	SAN のゾーン化	p.21 の「 ファイバートランスポート用の SAN のゾーン化について 」を参照してください。
手順 2	HBA のインストール	p.25 の「 SAN クライアントおよびファイバートランスポートメディアサーバー用 HBA について 」を参照してください。
手順 3	HBA ポートの選択	p.27 の「 SAN クライアント用の HBA ポートを選択する場合 」を参照してください。

手順	手順	項
手順 4	ファイバーの接続	p.27 の「SAN クライアントでサポートする SAN 構成について」を参照してください。

ファイバートランスポート用の SAN のゾーン化について

NetBackup ファイバートランスポート (FT) メカニズムを設定して使うには、まず SAN を設定して動作可能な状態にする必要があります。

p.27 の「SAN クライアントでサポートする SAN 構成について」を参照してください。

SAN スイッチ構成の場合、適切なゾーン化を行うことで、他の SAN アクティビティで必要になる可能性がある帯域幅がファイバートランスポート通信によって使われることがなくなります。また、適切なゾーン化によりホストバスアダプタ (HBA) ポートが検出するデバイスが限定されます。ポートは他のポートのゾーン内でのみそれらのポートを検出します。ゾーン化しない場合、各 HBA ポートは SAN のすべてのホストからすべての HBA ポートを検出します。デバイス数が多いと、オペレーティングシステムがサポートするデバイス数を超える場合があります。

SAN の設定と管理方法については、NetBackup マニュアルでは説明していません。ただし、次の推奨事項は SAN の通信を最適化するのに役立つことがあります。

表 3-2 では、NetBackup Appliance の SAN をゾーン化するためのベストプラクティスについて説明します。

表 3-2 NetBackup Appliance の SAN をゾーン化するためのベストプラクティス

ガイドライン	説明
ゾーンごとに 1 つのイニシエータ、複数のターゲットを受け入れ可能。	<p>Cohesity はゾーンごとに 1 つのイニシエータのみを持つゾーンを作成することをお勧めします。すべてのターゲットが類似している場合にのみ、1 つのゾーンに複数のターゲットを受け入れ可能です。</p> <p>イニシエータに関係なく、テープターゲットリソースはディスクターゲットリソースとは別のゾーンにしてください。ただし、両方のリソースのセットで同じイニシエータを共有することはできません。</p>
1 つのポートを複数のゾーンに対して構成するときは、パフォーマンスの低下に注意してください。	<p>1 つのポートを複数のゾーンのイニシエータまたはターゲットとして使用すると、そのポートがシステム全体のパフォーマンスのボトルネックとなる場合があります。システムのすべての部分で必要となるスループットの合計を分析し、必要に応じてトラフィックフローを最適化する必要があります。</p>

ガイドライン	説明
耐障害性のために、接続はポートではなく HBA カードに分散します。	システム接続の可用性を確保するために、共通リソースに対してマルチパスアプローチを組み込む場合には、ゾーン化のように別のカード上のポートをペアにします。この構成は、カード障害が発生した場合にリソースへのパスがすべて失われることを防ぐために役立ちます。
WWN を基に SAN をゾーン化し、デバイスがポートを変更した場合のゾーン移行を容易にします。	WWN に基づいて SAN をゾーン化することを推奨します。スイッチポート構成またはケーブル構成に変更が必要な場合、ゾーンを再作成する必要はありません。

表 3-3 は、SAN トラフィックに使用する必要があるゾーンを説明します。

メモ: NetBackup ファイバートランスポートメディアサーバーで HBA ポートを指定する場合は、物理ポート ID またはワールドワイドポート名 (WWPN) を使う必要があります。

p.35 の「[HBA ポートを識別する方法](#)」を参照してください。

表 3-3 ファイバーチャネルゾーン

ゾーン	説明
ファイバートランスポートゾーン	<p>ファイバートランスポートゾーン (またはバックアップゾーン) には、次のようにファイバートランスポートを使うホストの特定の HBA ポートのみを含めてください。</p> <ul style="list-style-type: none"> ■ SAN クライアントに接続する FT メディアサーバー HBA 上のポート。これらのポートは Cohesity ターゲットモードドライバを使います。 p.33 の「ターゲットモードドライバについて」を参照してください。 ■ ターゲットモードにあるメディアサーバーポートに接続する SAN クライアント HBA 上のポート。SAN クライアント上のポートは標準イニシエータモードドライバを使用します。 物理ポート ID またはワールドワイドポート名 (World Wide Port Name) で FT メディアサーバーのターゲットポートを定義する必要があります。ターゲットモードドライバの WWPN は、ファイバーチャネル HBA の WWPN から導出されるため一意ではありません。 NetBackup SAN クライアントは、NetBackup メディアサーバーのターゲットモードである HBA ポートのみを検出します。NetBackup メディアサーバーのイニシエータモードの HBA ポートは検出されません。他のホストの FC HBA は検出されません。 複数ストリームのスループットを向上させるには、各 SAN クライアントで、ゾーンのメディアサーバー HBA ポートのすべてのターゲットモードデバイスが検出される必要があります。
外部ストレージのゾーン	<p>ストレージが SAN にある場合、外部ストレージのゾーンを作成します。ゾーンはストレージの HBA ポートとストレージに接続する FT メディアサーバー HBA ポートを含む必要があります。ストレージゾーン内のすべてのポートが標準イニシエータモードの HBA ドライバを使用します。</p>

16 gb ターゲットモード HBA をサポートするファイバートランスポート向けの SAN のゾーン化

NetBackup ファイバートランスポート (FT) メカニズムを設定して使うには、まず SAN を設定して動作可能な状態にする必要があります。

p.27 の「[SAN クライアントでサポートする SAN 構成について](#)」を参照してください。

SAN スイッチ構成の場合、適切なゾーン化を行うことで、他の SAN アクティビティで必要になる可能性がある帯域幅がファイバートランスポート通信によって使われることがなくなります。また、適切なゾーン化によりホストバスアダプタ (HBA) ポートが検出するデバイスが限定されます。ポートは他のポートのゾーン内でのみそれらのポートを検出します。ゾーン化しない場合、各 HBA ポートは SAN のすべてのホストからすべての HBA ポートを検出します。デバイス数が多いと、オペレーティングシステムがサポートするデバイス数を超える場合があります。

SAN の設定と管理方法については、NetBackup マニュアルでは説明していません。ただし、次の推奨事項は SAN の通信を最適化するのに役立つことがあります。

表 3-4 では、16Gb および 32Gb HBA 対応の NetBackup Appliance と NBU FTMS の SAN をゾーン化するためのベストプラクティスについて説明します。

表 3-4 NetBackup Appliance の SAN をゾーン化するためのベストプラクティス

ガイドライン	説明
ゾーンごとに 1 つのイニシエータ、複数のターゲットを受け入れ可能。	<p>Cohesity はゾーンごとに 1 つのイニシエータのみを持つゾーンを作成することをお勧めします。すべてのターゲットが類似している場合にのみ、1 つのゾーンに複数のターゲットを受け入れ可能です。</p> <p>イニシエータに関係なく、テープターゲットリソースはディスクターゲットリソースとは別のゾーンにしてください。ただし、両方のリソースのセットで同じイニシエータを共有することはできません。</p>
1 つのポートを複数のゾーンに対して構成するときは、パフォーマンスの低下に注意してください。	<p>1 つのポートを複数のゾーンのイニシエータまたはターゲットとして使用すると、そのポートがシステム全体のパフォーマンスのボトルネックとなる場合があります。システムのすべての部分で必要となるスループットの合計を分析し、必要に応じてトラフィックフローを最適化する必要があります。</p>

16 gb ターゲットモード HBA をサポートするファイバートランスポート向けの SAN のゾーン化

ガイドライン	説明
耐障害性のために、接続はポートではなく HBA カードに分散します。	システム接続の可用性を確保するために、共通リソースに対してマルチパスアプローチを組み込む場合には、ゾーン化のように別のカード上のポートをペアにします。この構成は、カード障害が発生した場合にリソースへのパスがすべて失われることを防ぐために役立ちます。
WWN を基に SAN をゾーン化し、デバイスがポートを変更した場合のゾーン移行を容易にします。	WWN に基づいて SAN をゾーン化することを推奨します。スイッチポート構成またはケーブル構造に変更が必要な場合、ゾーンを再作成する必要はありません。

メモ: HBA ポート用の SAN クライアント 16 GB ターゲットモードドライバサポートを有効にするには、1 つのイニシエータのみのゾーンを作成し、1 ゾーンのターゲットモードを 1 つにする必要があります。

表 3-5 は、SAN トラフィックに使用する必要があるゾーンを説明します。

メモ: NetBackup ファイバートランスポートメディアサーバーで HBA ポートを指定する場合は、物理ポート ID またはワールドワイドポート名 (WWPN) を使う必要があります。

p.35 の「HBA ポートを識別する方法」を参照してください。

表 3-5 ファイバーチャネルゾーン

ゾーン	説明
ファイバートランスポートゾーン	<p>ファイバートランスポートゾーン (またはバックアップゾーン) には、次のようにファイバートランスポートを使うホストの特定の HBA ポートのみを含めてください。</p> <ul style="list-style-type: none"> ■ SAN クライアントに接続する FT メディアサーバー HBA 上のポート。これらのポートは Cohesity ターゲットモードドライバを使います。 p.33 の「ターゲットモードドライバについて」を参照してください。 ■ ターゲットモードにあるメディアサーバーポートに接続する SAN クライアント HBA 上のポート。SAN クライアント上のポートは標準イニシエータモードドライバを使います。 物理ポート ID またはワールドワイドポート名前 (World Wide Port Name) で FT メディアサーバーのターゲットポートを定義する必要があります。ターゲットモードドライバの WWPN は、ファイバーチャネル HBA の WWPN から導出されるため一意ではありません。 NetBackup SAN クライアントは、NetBackup メディアサーバーのターゲットモードである HBA ポートのみを検出します。NetBackup メディアサーバーのイニシエータモードの HBA ポートは検出されません。他のホストの FC HBA は検出されません。 複数ストリームのスループットを向上させるには、各 SAN クライアントで、ゾーンのメディアサーバー HBA ポートのすべてのターゲットモードデバイスが検出される必要があります。

ゾーン	説明
外部ストレージのゾーン	ストレージが SAN にある場合、外部ストレージのゾーンを作成します。ゾーンはストレージの HBA ポートとストレージに接続する FT メディアサーバー HBA ポートを含む必要があります。ストレージゾーン内のすべてのポートが標準イニシエータモードの HBA ドライバを使用します。

SAN クライアントおよびファイバートランスポートメディアサーバー用 HBA について

次のように、ファイバーチャネルのホストバスアダプタ (HBA) およびドライバの要件は、SAN クライアントと NetBackup FT メディアサーバーとで異なります。

SAN クライアントの HBA

SAN クライアントの HBA には、サポートされているすべてのファイバーチャネル HBA を使用することができます。HBA ポートはデフォルトのイニシエータモードで動作する必要があります。

SAN クライアントシステムの HBA の場合、次の作業を行います。

- HBA のドライバをインストールします。
- HBA のユーティリティをインストールします。NetBackup の操作には必要ありませんが、ユーティリティは接続の問題のトラブルシューティングに役立つ場合があります。

NetBackup FT メディアサーバーの HBA

ファイバートランスポートをホストする NetBackup メディアサーバーには、次のものがが必要です。

- SAN クライアントに接続する場合は、NetBackup がファイバートランスポートのためにサポートする QLogic HBA または Emulex HBA を使用します。これらの HBA は、NetBackup ターゲットモードドライバを使用するように構成する必要があります。
p.34 の「nbhba モードと ql2300_stub ドライバについて」を参照してください。
- SAN 接続されたストレージを使用する場合、サポートされているファイバーチャネル HBA を使用して、ストレージに接続することができます。この HBA の場合、QLogic ドライバおよびユーティリティをインストールします。ストレージに接続する HBA ポートは、デフォルトのイニシエータモードのままにしておく必要があります。
- HBA とドライバはデータ転送に 256K サイズのバッファをサポートする必要があります。

メモ: HBA ポート用の SAN クライアント 16 GB ターゲットモードドライバサポートを有効にするには、1 つのイニシエータのみのゾーンを作成し、1 ゾーンのターゲットモードを 1 つにする必要があります。各 NetBackup クライアントは、ファイバートランスポートメディアサーバーを 1 つだけ備えたゾーンを 1 つ持つことができます。

サポートされている HBA については、[ハードウェア互換性リスト](#)を参照してください。

p.20 の「[SAN の準備](#)」を参照してください。

SAN クライアントおよびファイバートランスポートメディアサーバー用 16 gb ターゲットモード HBA について

次のように、ファイバーチャネルのホストバスアダプタ (HBA) およびドライバの要件は、SAN クライアントと NetBackup FT メディアサーバーとで異なります。

SAN クライアントの HBA

SAN クライアントの HBA には、サポートされているすべてのファイバーチャネル HBA を使用することができます。HBA ポートはデフォルトのイニシエータモードで動作する必要があります。

SAN クライアントシステムの HBA の場合、次の作業を行います。

- HBA のドライバをインストールします。
- HBA のユーティリティをインストールします。NetBackup の操作には必要ありませんが、ユーティリティは接続の問題のトラブルシューティングに役立つ場合があります。

NetBackup FT メディアサーバーの HBA

ファイバートランスポートをホストする NetBackup メディアサーバーには、次のものがが必要です。

- SAN クライアントに接続する場合は、NetBackup がファイバートランスポートのためにサポートする QLogic HBA または Emulex HBA を使用します。これらの HBA は、NetBackup ターゲットモードドライバを使用するように構成する必要があります。
- QLogic HBA と Emulex HBA をターゲットモードとして同時に使用することはできません。ターゲットモードとしてそれらのいずれかを選択する必要があります。
- QLogic HBA をターゲットとして使用し、イニシエータ HBA が必要な場合は、Emulex HBA を使用してイニシエータとして機能させることができます。

サポートされている HBA については、次の URL のハードウェア互換性リストを参照してください。

<http://www.netbackup.com/compatibility>

p.20 の「[SAN の準備](#)」を参照してください。

SAN クライアント用の HBA ポートを選択する場合

SAN クライアントで FT パイプをサポートするには、FT メディアサーバーに十分な HBA ポートが必要です。SAN 接続されたストレージも使用する場合、メディアサーバーには、共有ストレージに接続するのに十分な HBA ポートが必要です。

NetBackup メディアサーバーと SAN クライアント間の FT 接続に使用するポートを次のように決定する必要があります。

- NetBackup メディアサーバーがインストールされているシステムの FT 接続に使用するファイバーチャネル HBA を決定します。
- 各 SAN クライアントの FT 接続に使用するファイバーチャネルポートを決定します。

QLogic HBA のすべてのポートを、ターゲットモードまたはイニシエータモードのいずれかにする必要があります。HBA 上の 1 つのポートを SAN クライアントに接続して、別のポートをストレージに接続することはできません。

SAN クライアントでサポートする SAN 構成について

NetBackup によるファイバートランスポートには、次の SAN 構成がサポートされています。

ノードポート (N_Port) スイッチ 構成 次の通り、SAN スイッチに NetBackup メディアサーバーと SAN クライアントを接続します。

- NetBackup FT メディアサーバーの HBA ポートをファイバーチャネルスイッチポートに接続します。
- 各 SAN クライアントの HBA ポートを同じファイバーチャネルスイッチのポートに接続します。
- クライアントおよびサーバーが同じゾーンになるようにスイッチのゾーンを定義します。次の点に注意します。
 - 物理ポート ID またはワールドワイドポートネーム (World Wide Port Name) で NetBackup FT メディアサーバーのターゲットポートを定義する必要があります。ターゲットモードドライバの WWPN は、ファイバーチャネル HBA の WWPN に基づくため一意ではありません。
 - ポート ID または WWPN のいずれかで SAN クライアントポートを定義できます。ただし、1 つの方法のみを使用した場合、ゾーンの定義および管理がより容易になります。

ファイバーチャネルアービトレートッドループ (FC-AL) 構成 ファイバーチャネルアービトレートッドループ (FC-AL) を使用して、NetBackup FT メディアサーバーの HBA ポートを NetBackup SAN クライアントの HBA ポートに直接接続します。

メモ: FC-AL ハブはサポートされません。

SAN クライアントとファイバートランスポートのライセンス

この章では以下の項目について説明しています。

- [SAN クライアントのインストールについて](#)
- [SAN クライアントのライセンスについて](#)
- [SAN クライアントおよびファイバートランスポートをアップグレードする場合](#)

SAN クライアントのインストールについて

NetBackup のファイバートランスポートのコアコンポーネントには、特別なインストールは必要ありません。ただし、機能のライセンスを入力して、機能をアクティブ化する必要があります。

p.29 の「[SAN クライアントのライセンスについて](#)」を参照してください。

SAN クライアントのライセンスについて

NetBackup プライマリサーバーで、SAN クライアント機能をアクティブ化するライセンスを入力します。

SAN クライアントおよびファイバートランスポートをアップグレードする場合

NetBackup をアップグレードすると、SAN クライアントとファイバートランスポートコンポーネントを含む、すべてのコンポーネントがアップグレードされます。

NetBackup アップグレードのインストール手順については、『NetBackup インストールガイド UNIX および Windows』を参照してください。

<http://www.veritas.com/docs/DOC5332>

SAN クライアントおよびファイバートランスポートの構成

この章では以下の項目について説明しています。

- [SAN クライアントおよびファイバートランスポートの構成](#)
- [ファイバートランスポートメディアサーバーの設定](#)
- [SAN クライアントの構成](#)
- [クラスタ内の SAN クライアントの構成](#)
- [ファイバートランスポートのプロパティの構成について](#)
- [ファイバートランスポートのプロパティの構成](#)
- [\[ファイバートランスポート \(Fibre Transport\)\] プロパティ](#)
- [SAN クライアントの使用設定の構成](#)
- [SAN クライアントの使用設定](#)

SAN クライアントおよびファイバートランスポートの構成

SAN クライアントとファイバートランスポートを構成するには、複数のコンピュータで複数の手順を完了する必要があります。

SAN クライアントおよびファイバートランスポートに使用するすべての NetBackup ホストを、ホスト ID ベースのセキュリティ証明書を使用してプロビジョニングする必要があります。ホストは互いに通信できる必要があります。

表 5-1 は、構成手順とその実行順序を示します。

表 5-1 SAN クライアントおよびファイバートランスポートの構成処理

手順	作業	項
手順 1	FT メディアサーバーの構成	p.32 の「 ファイバートランスポートメディアサーバーの設定 」を参照してください。
手順 2	SAN クライアントの構成	p.52 の「 SAN クライアントの構成 」を参照してください。 p.55 の「 クラスタ内の SAN クライアントの構成 」を参照してください。
手順 3	FT プロパティの構成	p.58 の「 ファイバートランスポートのプロパティの構成について 」を参照してください。
手順 4	SAN クライアントの使用設定の構成	p.64 の「 SAN クライアントの使用設定 」を参照してください。

ファイバートランスポートメディアサーバーの設定

表 5-2 に FT メディアサーバーを構成するための処理を説明します。

表 5-2 FT メディアサーバーを構成するための処理

手順	作業	項
手順 1	FTメディアサーバーの構成についての概要を読みます。	<p>深刻な問題の回避に役立つ情報が得られる場合があります。</p> <p>p.63 の「Linux 並列 FT 接続について」を参照してください。</p> <p>p.25 の「SAN クライアントおよびファイバートランスポートメディアサーバー用 HBA について」を参照してください。</p> <p>p.33 の「ターゲットモードドライバについて」を参照してください。</p> <p>p.34 の「nbhba モードと ql2300_stub ドライバについて」を参照してください。</p> <p>p.34 の「FC に接続されるデバイスについて」を参照してください。</p> <p>p.35 の「HBA ポートを識別する方法」を参照してください。</p> <p>p.36 の「Solaris での HBA ポートの検出について」を参照してください。</p> <p>p.36 の「ファイバーのトランスポートのメディアサーバーおよび VLAN について」を参照してください。</p>
手順 2	メディアサーバーで nbhba モードを開始します。	p.37 の「 nbhba モードの開始 」を参照してください。

手順	作業	項
手順 3	HBA ポートにマーク付けします。	p.39 の「ファイバートランスポートメディアサーバー HBA ポートのマーク付け」を参照してください。
手順 4	FT サービスを構成します。	p.41 の「メディアサーバーのファイバートランスポートサービスの設定」を参照してください。

16 gb ターゲットモード HBA をサポートするファイバートランスポートメディアサーバーの構成

表 5-3 16 gb ターゲットモード HBA をサポートする FT メディアサーバーを構成するための処理

手順	作業	項
手順 1	FT メディアサーバーの構成についての概要を読みます。	深刻な問題の回避に役立つ情報が得られる場合があります。 p.63 の「Linux 並列 FT 接続について」を参照してください。 p.33 の「ターゲットモードドライバについて」を参照してください。 p.36 の「ファイバーのトランスポートのメディアサーバーおよび VLAN について」を参照してください。
手順 2	FT サービスを構成します。	p.45 の「16 gb ターゲットモード HBA サポート向けのメディアサーバーファイバートランスポートサービスの構成」を参照してください。
手順 3	16 gb ターゲットモード HBA をサポートする FTMS の状態を表示します (省略可能)。	p.51 の「16 gb ターゲットモード HBA をサポートする FTMS の状態の表示」を参照してください。
手順 4	16 gb ターゲットモード HBA をサポートする HBA ポートを識別します (省略可能)。	p.51 の「16 gb ターゲットモード HBA をサポートする HBA ポートの識別」を参照してください。

ターゲットモードドライバについて

NetBackup FT メディアサーバーでは、QLogic または Emulex Fibre Channel の Host Bus Adapter (HBA) ポートが NetBackup SAN クライアントに接続されます。Cohesity はそれらの HBA 上のポート用の特別なターゲットモードドライバを提供します。それらのポートはターゲットモードで動作する必要があります。ターゲットモードドライバがデフォルトのイニシエータモードドライバに代わって使用されます。ターゲットモードは、QLogic HBA または Emulex HBA にのみ適用されます。ターゲットモードの構成処理は QLogic HBA ポートまたは Emulex HBA ポートにのみ影響します。

HBA ポートへのターゲットモードドライバのバインド後、それらのポートは SCSI 照会で 2 つの ARCHIVE Python テープデバイスとして表示されます。ただし、それらはテープデバイスではないため、NetBackup のデバイス検出ではテープデバイスとして表示されません。各ポートが 2 つのテープデバイスとして表示されるのは、オペレーティングシステムがポートごとに 1 つのデータストリームのみを許可するためです。各ポートの 2 つの擬似テープデバイスはスループットを高めます。

p.63 の「Linux 並列 FT 接続について」を参照してください。

nbhba モードと ql2300_stub ドライバについて

メディアサーバーの HBA ドライバを構成する処理の最初の手順は、nbhba モードを開始することです。nbhba モードでは、ホストのすべての QLogic ISP2312 と ISP24xx HBA ポートに Cohesity 提供の ql2300_stub ドライバをバインドします。

ql2300_stub ドライバは、標準イニシエータモードのドライバがポートにバインドされるのを防ぎます。QLogic ドライバが HBA ポートにバインドされると、NetBackup nbhba コマンドはターゲットモードで動作させるポートにマーク付けすることができません。ターゲットモードのドライバも HBA ポートにバインドできません。

ql2300_stub ドライバを使うと NetBackup で QLogic ポートの NVRAM のデバイス ID を読み込み、変更することもできます。nbhba モードを開始し、SAN クライアントに接続する QLogic HBA のポートにマーク付けした後、ポートはターゲットモードで動作します。

FT サーバーが起動すると、コンピュータは nbhba モードを終了します。

メモ: Linux オペレーティングシステムでは、ql2300_stub ドライバをカーネルにロードするときに警告メッセージがコンソールまたはシステムログに表示される場合があります。

p.84 の「Cohesity モジュールのロード時のカーネルの警告メッセージ」を参照してください。

FC に接続されるデバイスについて

nbhba モードでは、QLogic ISP2312 と ISP24xx HBA ポートに接続されているすべてのデバイスが利用できません。ディスクまたはテープデバイスを QLogic HBA に接続すると、それらのデバイスは利用不能になります。そのコンピュータで nbhba モードを終了するまでデバイスは利用できません。

警告: HBA は、起動デバイスが QLogic ISP2312 または ISP24xx ポートに接続されているコンピュータ上には構成しないでください。構成すると、コンピュータを起動できなくなる場合があります。QLogic HBA に接続されているデバイスに重要なファイルシステムをマウントした場合も、コンピュータを起動できなくなることがあります。HBA の構成を始める前に、QLogic HBA に接続されているファイルシステムをマウント解除してください。

デバイスが QLogic HBA に接続されているかどうかを判断するには、デバイスとマウント済みファイルシステムを調べてください。

QLogic HBA は、QLogic HBA によって接続されている起動デバイスが含まれていない別の NetBackup メディアサーバーに構成することができます。その後、QLogic HBA を NetBackup FT メディアサーバーにインストールして、FT サービスを構成できます。構成が終了したら、HBA を構成したメディアサーバーから nbhba ドライバを削除してください。

p.72 の「ファイバートランスポートメディアサーバーの無効化」を参照してください。

この処理により、コンピュータ上の nbhba モードも終了します。

HBA ポートを識別する方法

ポートにマーク付けするコンピュータに複数の HBA がある場合は、HBA とワールドワイドネーム (WWN) の関連を判断しにくいことがあります。HBA ポートにマーク付けする NetBackup nbhba コマンドにはポートの WWN が必須です。ポートの WWN はワールドワイドポートネーム (WWPN) とも呼ばれます。

問題を回避するには、他にファイバーチャネル HBA がインストールされていない NetBackup メディアサーバーに、すべての QLogic HBA をインストールします。すべての HBA ポートにマーク付けしてから、HBA を適切な NetBackup メディアサーバーにインストールします。

警告: QLogic HBA は、マザーボード上にチップセットとして存在する場合があります。問題を回避するために、組み込みの QLogic ポートがコンピュータに含まれているかどうかを判断する必要があります。

マーク付けする QLogic HBA だけを含むコンピュータでポートにマーク付けできない場合は、次の情報が役に立つ場合があります。

- HBA のカード上でポートの WWN を確認できる場合があります。HBA の WWN を調べてください。
- ファイバーチャネルスイッチに、接続されて動作している HBA ポートの WWN が表示される場合があります。
- SAN ユーティリティソフトウェアによっては、HBA ポートの WWN を表示する機能が備わっている場合があります。
- Solaris 10 で、`fcinfo hba-port` コマンドの使用によって固有のドライバの WWN を表示できます。
- NetBackup の nbhba コマンドの `-l` オプションを使うとポート WWN のアドレスを簡単に比較できます。(コンピュータは nbhba モードである必要があります。)QLA-234x シリーズでは、同じカード上のポートの WWN は、2 番目と 6 番目のバイトが異なります。

す。次の例は、2 つの 2 ポート HBA を示しています。1 行目と 2 行目が 1 つの HBA を示し、3 行目と 4 行目が別の HBA を示しています。

```
/usr/opensv/netbackup/bin/admincmd/nbhba -l
1 2312 21:00:00:E0:8B:83:9D:A1 "QLA2342 " 0 0 101
2 2312 21:01:00:E0:8B:A3:9D:A1 "QLA2342 " 1 0 101
3 2312 21:00:00:E0:8B:8F:28:7B "QLA2342 " 0 0 101
4 2312 21:01:00:E0:8B:AF:28:7B "QLA2342 " 1 0 101
```

この出力はポートがイニシエータモードであることも示します。右端から 2 番目の列に 0 が表示され、右端の列が 8 で始まっていません。

- HBA の金属の取り付け金具に LED がある場合は、ポートにマーク付けすると LED が緑色に変わります (黄色はイニシエータモード)。(コンピュータは nbhba モードである必要があります。)これにより、正しいカードのポートにマーク付けしたかどうかを確認できます。正しいカードでない場合は、それらのポートをイニシエータモードに戻し、正しいポートにマーク付けするまで、他のポートにマーク付けすることができます。

Solaris での HBA ポートの検出について

Solaris 10 Update 7 より前のシステムでは、NetBackup は PCI バスを検出し、1 つのバスのポートのみをターゲットモードで使用可能にします。

次に示すのは Solaris 10 Update 7 より前のシステム上でのポート検出動作です。

- 最初に選択するのは、最も多くの 2312 ターゲットモードポートが存在するバスです。
- 2312 ターゲットモードポートがない場合は、最も多くの 24xx ターゲットモードポートが存在するバスが使用されます。
- 他のバス上のターゲットモードポートは使用されません。

Solaris 10 Update 7 からは、Solaris 10 で複数のバス上でのターゲットポートがサポートされます。

ファイバーのトランスポートのメディアサーバーおよび VLAN について

VLAN 用の複数のネットワークインターフェースを備えている FT メディアサーバーについては、NetBackup がホスト用の他のネットワークインターフェースの前に、ホストのプライマリネットワークインターフェースを認識する必要があります。各 NetBackup ホストは、[追加のサーバー (Additional Servers)]リスト内の他の NetBackup ホストを認識します。このリストはホストのプロパティの[サーバー (Servers)]ページに表示されます。

FT サーバーのプライマリホスト名は、FT メディアサーバーホストの他のインターフェース名の前に表示されていることを確認してください。次の NetBackup ホストの[追加サーバー (Additional servers)]リストでこの確認を行ってください。

- プライマリサーバー

- FT メディアサーバー
- FT メディアサーバーがバックアップするすべての SAN クライアント

プライマリインターフェースを決定するオペレーティングシステムコマンドを使用できる場合もあります。Unix タイプのオペレーティングシステムにはhostnameコマンドがあり、プライマリインターフェースの短い名前を表示します。また、domainnameコマンドでは、プライマリインターフェースのドメイン名を表示します。Windows で `pconfig -all` コマンドを使用すると、ホストとドメインの情報を表示できます。

p.83 の「バックアップはファイバートランスポートデバイスが使用可能であっても LAN にフェールオーバーする」を参照してください。

nbhba モードの開始

HBA ポートにマーク付けする前に、QLogic HBA ポートに `ql2300_stub` ドライバをバインドする nbhba モードを開始する必要があります。

nbhba モードを開始する方法については、次の項を参照してください。

- 「Linux で nbhba モードを開始する方法」
- 「Solaris で nbhba モードを開始する方法」

root ユーザーである必要があります。

Linux で nbhba モードを開始する方法

- 1 HBA が SAN に接続されていないことを確認します。
- 2 `nbftsrv_config -nbhba` コマンドとオプションを起動します。コンピュータが nbhba モードになります。次に例を示します。ご使用のシステムでの出力は異なる場合があります。

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -nbhba
Installing nbhba driver.
Are you sure you want to unload QLogic driver: qla2300? [y,n]
(y)
```

- 3 y と入力して、QLogic ドライバをアンロードします。処理が次のように続行されます。

```
Removing qla2300
```

メモ: Linux オペレーティングシステムでは、ql2300_stub ドライバをカーネルにロードするときに警告メッセージがコンソールまたはシステムログに表示される場合があります。

p.84 の「Cohesity モジュールのロード時のカーネルの警告メッセージ」を参照してください。

- 4 HBA ポートにマーク付けして続行してください。

p.39 の「ファイバートランスポートメディアサーバー HBA ポートのマーク付け」を参照してください。

Solaris で nbhba モードを開始する方法

- 1 HBA が SAN に接続されていないことを確認します。
- 2 nbftsrv_config -nbhba コマンドとオプションを起動します。コンピュータが nbhba モードになります。次に例を示します。ご使用のシステムでの出力は異なる場合があります。

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -nbhba
Installing nbhba driver.
Waiting for driver references to ql2300_stub to free up (this
may take some time).
The following driver aliases need to be removed:
qlc "pci1077,2312.1077.10a"
Would you like to run update_drv to remove these now? [y,n] (y)
```

- 3 y と入力して、ドライバエイリアスを削除します。処理が次のように続行されます。

```
/usr/sbin/update_drv -v -d -i "pci1077,2312.1077.10a" qlc
Done copying driver into system directories.
Done adding driver.
MUST REBOOT TO COMPLETE INSTALLATION.
```

- 4 ホストを再起動します。

- 5 HBA ポートにマーク付けして続行してください。

p.39 の「ファイバートランスポートメディアサーバー HBA ポートのマーク付け」を参照してください。

ファイバートランスポートメディアサーバー HBA ポートのマーク付け

ターゲットモードで動作させる QLogic HBA 上のポートにマーク付けする必要があります。この処理では、NVRAM のポートデバイス ID が変更されます。FT サーバーが起動すると、NetBackup のターゲットモードドライバは、マークされている QLogic HBA ポートに自動的にバインドされます。

ポートにマーク付けする前に、nbhba モードを開始する必要があります。

p.37 の「nbhba モードの開始」を参照してください。

次の手順は、HBA ポートにマーク付けする方法、および必要に応じてこの処理を逆順で実行し、イニシエータモードのドライバにポートを戻す方法を説明します。

- 「HBA ポートにマーク付けする方法」
- 「イニシエータモードドライバに戻す方法」

これらの変更を行うには root ユーザーである必要があります。

HBA ポートにマーク付けする方法

- 1 nbhba コマンドと -l オプションを使用してメディアサーバーの QLogic HBA のポートを表示してください。次に例を示します。ご使用のシステムでの出力は異なる場合があります。

```
/usr/opensv/netbackup/bin/admincmd/nbhba -l
1 2312 21:00:00:E0:8B:83:9D:A1 "QLA2342 " 0 0 101
2 2312 21:01:00:E0:8B:A3:9D:A1 "QLA2342 " 1 0 101
3 2312 21:00:00:E0:8B:8F:28:7B "QLA2342 " 0 0 101
4 2312 21:01:00:E0:8B:AF:28:7B "QLA2342 " 1 0 101
```

QLA-234x シリーズでは、同じカード上のポートの WWN は、2 番目と 6 番目のバイトが異なります。この出力は、2 つの 2 ポート HBA を示しています。1 行目と 2 行目が 1 つの HBA を示し、3 行目と 4 行目が別の HBA を示しています。HBA はイニシエータモードです。右端から 2 番目の列に 0 が表示され、右端の列が 8 で始まっていません。

代わりに、nbhba-l オプションを使用して冗長な出力を生成します。これにより、モードをより簡単に識別できます。

- 2 nbhba コマンドを実行してポートにマーク付けします。構文は次のとおりです。

```
/usr/opensv/netbackup/bin/admincmd/nbhba -modify -wwn string
-mode target
```

たとえば、次の 2 つのコマンドを実行すると、手順 1 での出力例にある一方の HBA の 2 つのポートが変更されます。

```
nbhba -modify -wwn 21:00:00:E0:8B:8F:28:7B -mode target
nbhba -modify -wwn 21:01:00:E0:8B:AF:28:7B -mode target
```

- 3 nbhba コマンドと `-L` オプションを使用してサーバー上の HBA カードのポートを表示し、変更を確認します。次に例を示します。ご使用のシステムでの出力は異なる場合があります。

```
/usr/opensv/netbackup/bin/admincmd/nbhba -L
HBA Port #1
  Device ID = 2312
  World Wide Name = 21:00:00:E0:8B:83:9D:A1
  Model Name = "QLA2342 "
  Port = 0
  Mode = initiator (designated for other use) (101)
HBA Port #2
  Device ID = 2312
  World Wide Name = 21:01:00:E0:8B:A3:9D:A1 "QLA2342
  Model Name = "QLA2342 "
  Port = 1
  Mode = initiator (designated for other use) (101)
HBA Port #3
  World Wide Name = 21:00:00:E0:8B:8F:28:7B
  Slot = ""
  Port = 0
  Fibre Not Attached
  Mode = target (designated for FT Server) (8101)
HBA Port #4
  World Wide Name = 21:01:00:E0:8B:AF:28:7B
  Slot = ""
  Port = 1
  Fibre Not Attached
  Mode = target (designated for FT Server) (8101)
```

nbhba `-l` オプションを使用すると、生成される出力でモードを識別することもできます。

```
/usr/opensv/netbackup/bin/admincmd/nbhba -l
1 2312 21:00:00:E0:8B:83:9D:A1 "QLA2342 " 0 0 101
2 2312 21:01:00:E0:8B:A3:9D:A1 "QLA2342 " 1 0 101
3 2312 21:00:00:E0:8B:8F:28:7B "QLA2342 " 0 1 8101
4 2312 21:01:00:E0:8B:AF:28:7B "QLA2342 " 1 1 8101
```

右端の 2 つの列はターゲットモードとしてマーク付けされているポートを示します。右端から 2 番目の列に 1 が表示され、右端の列は 8 で始まっています。右端の列の他の数字は重要ではありません。

- 4 必要に応じて、HBA を適切なメディアサーバーに転送します。

- 5 必要に応じて、HBA を SAN に接続します。
- 6 FT サービスを構成して続行してください。

p.41 の「[メディアサーバーのファイバートランスポートサービスの設定](#)」を参照してください。

イニシエータモードドライバに戻す方法

- ◆ HBA がインストールされている nbhba FT サーバーで NetBackup コマンドを起動します。コマンドの構文は次のとおりです。

```
/usr/opensv/netbackup/bin/admincmd/nbhba -modify -wwn  
world_wide_port_name -mode initiator
```

メディアサーバーのファイバートランスポートサービスの設定

SAN クライアントを構成する前に、メディアサーバー FT サービスを構成する必要があります。FT サーバーは、クライアントのオペレーティングシステムがターゲットモードドライバ (FT デバイス) を検出できるように、メディアサーバー上で実行する必要があります。メディアサーバーで動作する NetBackup FT サーバーは、2 つのサービス (nbftsrvr および nbfdrv64) で構成されます。

nbftsrvr_config スクリプトはファイバートランスポート用にメディアサーバーを構成します。この処理では、スクリプトによって次のことが実行されます。

- 必須ドライバがインストールされる。
- FT サーバー起動スクリプトがインストールされる。
- FT サーバーが起動する。
FT サーバーが起動すると、NetBackup のターゲットモードドライバは、マークされている QLogic HBA ポートに自動的にバインドされます (デフォルトの QLogic ドライバは、マークされていないポートにすでにバインドされています)。HBA ポートは、標準イニシエータモードを再度使用するように構成するまで、ターゲットモードで動作します。
- コンピュータ上の nbhba モードが終了する (nbhba モードである場合)

SAN クライアントに接続しているすべての NetBackup メディアサーバーの FT サービスを構成します。

手順については、次の項を参照してください。

- [「Linux でファイバートランスポートサービスを設定するには」](#)
- [「Solaris でファイバーのトランスポートサービスを設定する方法」](#)

ルートユーザーである必要があります。

メモ: `nbftsrv_config` と `nbftserver` スクリプトを使用してファイバートランスポートメディアサーバーを構成したら、バックアップとリストアに使用された **NetBackup SAN** クライアント上の **HBA** ポートのターゲットドライバを再ロードします。この手順により、クライアントオペレーティングシステムは、ファイバートランスポートメディアサーバーがエクスポートするテープデバイスを確実に検出します。または、クライアントコンピュータを再起動してドライバを再ロードし、デバイスツリーを更新することもできます。

Linux でファイバートランスポートサービスを設定するには

- 1 nbftsrv_config スクリプトを実行します。次に例を示します。ご使用のシステムでの出力は異なる場合があります。

```
/usr/opencv/netbackup/bin/admincmd/nbftsrv_config
Installing the Jungo driver and Fibre Transport Server.
The following automatic startup and shutdown scripts
(respectively) have been installed. They will cause the
NetBackup Fibre Transport Server daemon to be automatically shut
down and restarted each time the system boots.
/etc/rc.d/rc2.d/S21nbftserver
/etc/rc.d/rc3.d/S21nbftserver
/etc/rc.d/rc5.d/S21nbftserver
/etc/rc.d/rc0.d/K03nbftserver
/etc/rc.d/rc1.d/K03nbftserver
/etc/rc.d/rc6.d/K03nbftserver
It may be necessary to temporarily unload your QLogic drivers
to free up the ports for the nbhba drivers.
This is an optional step. If you choose not to do this, you may
not have access to all of the HBA ports until a subsequent
reboot.
Would you like to uninstall and reinstall your native QLogic
drivers now? [y,n] (y) y
```

- 2 このセッション中にスタブドライバ (ql2300_stub) がマークされている HBA ポートにバインドされるように、QLogic ドライバを一時的にアンロードする必要があります。

y と入力した場合は、この構成処理でコンピュータを再起動する必要はありません。ただし、このセッションの間、コンピュータの QLogic HBA に接続されている重要なデバイスを利用できない場合があります。重要なデバイスを引き続き利用できるようにするには、n を入力します。その後、プロンプトが表示されたら、再起動する必要があります。起動処理で、マークされたポートにスタブドライバがバインドされ、デフォルトの QLogic ドライバがマークされていないポートにバインドされます。

n を入力した場合は手順 5 に進みます。

y を入力した場合は、次のように、各 QLogic ドライバをアンロードするためのプロンプトが再度表示されます。

```
Are you sure you want to unload QLogic driver: qla2300? [y,n]
(y) y
```

- 3 QLogic ドライバをアンロードするには、`y` と入力します。処理が次のように続行されます。

```
Removing qla2300
Adding qla2300.
Adding qla2xxx.
Would you like to start the SANsurfer agent (qlremote)? [y,n]
(y) y
```

- 4 QLogic SANsurfer エージェントがロードされると、構成処理によって、エージェントを起動するかどうかを尋ねられます。QLogic SANsurfer エージェントを起動するには、`y` を入力します。処理が次のように続行されます。

```
Starting qlremote agent service
Started SANsurfer agent.
/etc/udev/permissions.d/50-udev.permissions updated with Jungo
WinDriver permissions.
NetBackup Fibre Transport Server started.
Would you like to make these changes persist after a reboot?
[y,n] (y) y
```

- 5 コンピュータの再起動後に FT サーバーが常に起動するようにするには、`y` を入力します。処理が次のように続行されます。

```
Running mkinitrd. Previous initrd image is saved at
/boot/initrd-2.6.9-11.ELsmp.img.05-21-07.11:24:03.
```

手順 2 で `y` を入力した場合は、FT サービスが起動し、ターゲットモードドライバが、マークされた HBA ポートにバインドされます。

- 6 手順 2 で `n` を入力した場合は、プロンプトが表示されたときにコンピュータを再起動します。

FT サービスが起動され、ターゲットモードドライバが、マークされた HBA ポートにバインドされます。

Solaris でファイバーのトランスポートサービスを設定する方法

- 1 nbftsrv_config スクリプトを実行します。次に例を示します。ご使用のシステムでの出力は異なる場合があります。

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config
Installing the Jungo driver and Fibre Transport Server.
Waiting for driver references to ql2300_stub to free up (this
may take some time).
The following automatic startup and shutdown scripts
(respectively) have been installed. They will cause the
NetBackup Fibre Transport Server daemon to be automatically shut
down and restarted each time the system boots.
/etc/rc2.d/S21nbftserver
/etc/rc0.d/K03nbftserver
Adding "pci1077,2312.1077.101" to qlc.
No third party drivers found with conflicting driver aliases.
Done copying driver into system directories.
Done adding driver.MUST REBOOT TO COMPLETE INSTALLATION.
```

- 2 ホストを再起動します。

FT サービスが起動され、ターゲットモードドライバが、マークされた HBA ポートにバインドされます。

16 gb ターゲットモード HBA サポート向けのメディアサーバーファイバートランスポートサービスの構成

SAN クライアントを構成する前に、メディアサーバー FT サービスを構成する必要があります。FT サーバーは、クライアントのオペレーティングシステムがターゲットモードドライバ (FT デバイス) を検出できるように、メディアサーバー上で実行する必要があります。メディアサーバーで動作する NetBackup FT サーバーは、1 つのサービス (nbftsrvr) で構成されます。

nbftsrv_config スクリプトはファイバートランスポート用にメディアサーバーを構成します。この処理では、スクリプトによって次のことが実行されます。

- 必須ドライバがインストールされる。
- FT サーバー起動スクリプトがインストールされる。
- FT サーバーが起動する。
FT サーバーが起動すると、NetBackup のターゲットモードドライバのバインドが、QLogic または Emulex HBA ポートに自動的に実行されます。FTMS を無効にするまで、HBA ポートはターゲットモードで動作します。

SAN クライアントに接続しているすべての NetBackup メディアサーバーの FT サービスを構成します。

手順については、次の項を参照してください。

- 「Linux でファイバートランスポートサービスを設定するには」

ルートユーザーである必要があります。

メモ: nbftsrv_config と nbftserver スクリプトを使用してファイバートランスポートメディアサーバーを構成したら、追加手順として、バックアップとリストアに使用された NetBackup SAN クライアント上の HBA ポートのターゲットドライバを再ロードする必要があります。この手順により、クライアントオペレーティングシステムは、ファイバートランスポートメディアサーバーがエクスポートするテープデバイスを確実に検出します。または、クライアントコンピュータを再起動してドライバを再ロードし、デバイスツリーを更新することもできます。

Emulex LPe31000/LPe35000 シリーズをターゲットモード HBA として使用する場合は、ファームウェアのバージョンがサポートされていることを確認します。ファームウェアがサポートされていない場合は、SAN クライアントとファイバートランスポートを構成する前に、ファームウェアを特定のバージョンにアップグレードします。サポートされているファームウェアバージョンについては、次の場所のハードウェア互換性リストを参照してください。

<http://www.netbackup.com/compatibility>

Linux でファイバートランスポートサービスを設定するには

- 1 nbftsrv_config スクリプトを実行します。次に例を示します。ご使用のシステムでの出力は異なる場合があります。

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -install
Checking for SCST drivers and firmwares in the package. [yes]
Checking if the server is not NetBackup Appliance. [yes]
Checking for kernel version 4.18.0-372.9.1. [yes]
Checking for QLogic QLE2562 8Gb or QLE2692 16Gb or QLE2770
QLE2772 32Gb, or other supported QLogic 16/32Gb HBA cards on
the server. [yes]
Checking for Emulex LPe31002 16Gb, LPe31004 16Gb, and other
supported Emulex 32Gb HBA cards on the server. [yes]
```

DISCLAIMER:

NOTE:

1. When you install the SAN client with 16Gb/32Gb HBA, the script stops the original qla2xxx and lpfc driver and updates the firmware ql2500_fw.bin. QLogic QLE2562 8Gb and QLE2692 16Gb and QLE2770 QLE2772 32Gb HBA models, Emulex LPe31002 16Gb, LPe31004 16Gb, and other qualified QLogic/Emulex 32Gb HBA models are supported by this NetBackup version.
2. Ensure that there is no other process that uses the HBAs. If there is an active process that uses qla2xxx or lpfc, manually restart the process after the installation completes.
3. If you use the SANSurfer agent during the deployment of the environment, the script stops and restarts the SANSurfer agent daemon (qlremote).
4. Stop all the backup jobs that use the FT user interface.

Do you acknowledge this disclaimer? [y,n] (n) y

- 2 このセッションで HBA ポートが検出されるように、QLogic ドライバが再ロードされま
す。

```
Proceeding to deploy SCST environment [ok]
```

```
Stopping the NetBackup Fibre Transport Server.
```

```
Waiting for nbftsrvr to shut down (this may take some time).
```

HBA-Type Speed	Port WWN	Status	Supported Speeds	Current
LPe31000-M6-D	10:00:00:10:9b:df:92:0e	Online	4 Gbit, 8 Gbit, 16 Gbit	16 Gbit
QLE2772	21:00:f4:c7:aa:0c:2a:87	Online	8 Gbit, 16 Gbit, 32 Gbit	32 Gbit
QLE2692	21:00:f4:c7:aa:0b:d6:88	Online	4 Gbit, 8 Gbit, 16 Gbit	16 Gbit
QLE2692	21:00:f4:c7:aa:0b:d6:89	Online	4 Gbit, 8 Gbit, 16 Gbit	16 Gbit
QLE2772	21:00:f4:c7:aa:0c:2a:86	Online	8 Gbit, 16 Gbit, 32 Gbit	32 Gbit
LPe35000-M2-D	10:00:00:10:9b:f1:63:a8	Linkdown	8 Gbit, 16 Gbit, 32 Gbit	unknown

NOTE:

The types of HBA cards listed below are filtered by the chip model. All of these HBA cards are not verified. Choose supported HBA card according to NetBackup hardware compatibility list. Some of the WWNs may be used to connect to an external storage and other external devices.

```
Do you want to continue? [y,n] (n)
```

3 ポート番号を入力し、このセッション中の操作の警告を確認します。

```
Please input the Port WWNs you want to use as the targets (separated by commas like:
wwn1,wwn2...):10:00:00:10:9b:1d:4c:6a,10:00:00:10:9b:1d:4c:6b
The input is: 10:00:00:10:9b:1d:4c:6a,10:00:00:10:9b:1d:4c:6b
The targets you defined are Emulex HBAs
The targets you defined: 10:00:00:10:9b:1d:4c:6a 10:00:00:10:9b:1d:4c:6b
Do you want to redefine the targets? [y,n] (n) n
Do you want to add additional targets? [y,n] (n) n
The targets you defined: 10:00:00:10:9b:1d:4c:6a 10:00:00:10:9b:1d:4c:6b
The targets you have defined contain 16Gb HBA cards.
```

NOTE:

1. Make sure that you do not use a WWN that is used to connect to external storage.
 2. Make sure to define the input WWNs as targets.
 3. Make sure the WWNs can be zoned with WWNs of clients.
- Do you want to continue to setup the WWNs as targets? [y,n] (n) y

4 FTMS 環境が配備されます。

```
-----  
FTMS environment installation started.  
-----
```

```
Successfully created the dependent path: /var/lib/scst/pr.  
Successfully created the dependent path: /var/lib/scst/vdev_mode_pages.  
Successfully copied /usr/opensv/netbackup/bin/driver/lancerg6_A12.8.340.8.grp to  
/lib/firmware/LPE31004.grp.  
Successfully copied  
/usr/opensv/netbackup/bin/driver/scst/ocs_fc_scst.ko.3.10.0-1160.el7.x86_64 to  
/lib/modules/3.10.0-1160.15.2.el7.x86_64/extra/ocs_fc_scst.ko.  
Successfully copied /usr/opensv/netbackup/bin/driver/scst/scst.ko.3.10.0-1160.el7.x86_64  
to /lib/modules/3.10.0-1160.15.2.el7.x86_64/extra/scst.ko.  
Successfully copied  
/usr/opensv/netbackup/bin/driver/scst/scst_user.ko.3.10.0-1160.el7.x86_64 to  
/lib/modules/3.10.0-1160.15.2.el7.x86_64/extra/scst_user.ko.  
Successfully created /etc/modprobe.d/ocs_fc_scst.conf.  
Successfully copied /usr/opensv/netbackup/bin/nbftsrvr to  
/usr/opensv/netbackup/bin/nbftsrvr_old.  
Successfully copied /usr/opensv/netbackup/bin/goodies/nbftserver_scst to  
/etc/rc.d/init.d/nbftserver.  
Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc2.d/S21nbftserver.  
Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc3.d/S21nbftserver.  
Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc5.d/S21nbftserver.  
Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc0.d/K03nbftserver.  
Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc1.d/K03nbftserver.  
Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc6.d/K03nbftserver.  
Successfully enabled nbftserver.  
Successfully created /etc/modules-load.d/scst.conf.  
Successfully find PCIID:0000:07:00.0 for target:10:00:00:10:9b:1d:4c:6a  
Successfully find PCIID:0000:07:00.1 for target:10:00:00:10:9b:1d:4c:6b  
Successfully bind target mode for pciid: 0000:07:00.0.  
Successfully bind target mode for pciid: 0000:07:00.1.  
Successfully rebind emulex target ports.  
Successfully modify the attribute of  
/sys/kernel/scst_tgt/targets/ocs_xe201/10:00:00:10:9b:1d:4c:6a/enabled with value 1.  
Successfully write /sys/class/fc_host/host13/issue_lip with value 1  
Enable target: 10:00:00:10:9b:1d:4c:6a  
Successfully modify the attribute of  
/sys/kernel/scst_tgt/targets/ocs_xe201/10:00:00:10:9b:1d:4c:6b/enabled with value 1.  
Successfully write /sys/class/fc_host/host14/issue_lip with value 1  
Enable target: 10:00:00:10:9b:1d:4c:6b
```

```
Previous initramfs image is saved at
/boot/initramfs-3.10.0-1160.15.2.el7.x86_64.img.03-19-21.19:31:51.
Running dracut, it may take several minutes to complete...
/sbin/dracut succeeded
Successfully moved /boot/initramfs-3.10.0-1160.15.2.el7.x86_64.img.tmp to
/boot/initramfs-3.10.0-1160.15.2.el7.x86_64.img
NetBackup Fibre Transport Server started.
-----
Driver ocs_fc_scst is loaded
-----
Driver scst is loaded
-----
Driver scst_user is loaded

-----
FTMS environment installation completed.
-----
```

16 gb ターゲットモード HBA をサポートする FTMS の状態の表示

NetBackup の `nbftsrv_config` コマンドの `-scst -state` オプションで、FTMS の状態について確認できます。コンピュータで FTMS の 16/32 Gb ターゲットモード HBA サポートを有効にしておく必要があります。

例:

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -list_port
```

```
FTMS Target Ports List:
21:00:f4:e9:d4:53:bb:c4
```

```
FTMS daemon(nbftsrvr) state:
FTMS daemon (nbftsrvr) is running.
```

このコマンドは、定義済みの FTMS ターゲットポートと FTMS デーモンの状態を表示します。

16 gb ターゲットモード HBA をサポートする HBA ポートの識別

NetBackup `nbftsrv_config` コマンドの `-scst -list_port` オプションで、ターゲットとして定義されているポートの世界ワイド名 (WWN) または世界ワイドポート名 (WWPN) を識別できます。コンピュータで FTMS の 16/32 GB ターゲットモード HBA サポートを有効にしておく必要があります。

例:

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -list_port
```

HBA タイプ (HBA-Type)	ポートの WWN (Port WWN)	状態 (Status)	現在のモード (Current Mode)	モードの設定 (Set Mode)	サポートされる 速度 (Supported Speeds)	現在の速度 (Current Speed)
QLE2692	21:00: f4:e9:d4: 53:bb:c4	Online	Target	Target	8 Gbit, 16 Gbit	16 Gbit

メモ: 一覧表示される HBA カードの種類は QLogic HBA の QLE2772、QLE2770、QLE2692、QLE2562、および Emulex LPe31000/35000 シリーズ HBA です。QLogic HBA をターゲットとして使用し、イニシエータ HBA が必要な場合は、Emulex HBA を使用してイニシエータとして機能させることができます。

SAN クライアントの構成

表 5-4 は、SAN クライアントの構成手順を示します。

表 5-4 SAN クライアントおよびファイバートランスポートの構成処理

手順	作業	項
手順 1	SAN クライアントでのファイアウォールの構成	p.52 の「 SAN クライアントのファイアウォールの構成について 」を参照してください。
手順 2	SAN クライアントドライバの構成	p.53 の「 SAN クライアントのドライバの要件 」を参照してください。
手順 3	SAN クライアントの FT サービスの構成	p.54 の「 SAN クライアントのファイバートランスポートサービスの構成 」を参照してください。

SAN クライアントのファイアウォールの構成について

NetBackup SAN クライアントには、NetBackup プライマリサーバーへの接続が必要です。

したがって、ファイアウォール (ソフトウェアまたはハードウェア) では、クライアントが NetBackup プライマリサーバーと通信できる必要があります。

SAN クライアントのドライバの要件

NetBackup の SAN クライアントのオペレーティングシステムには、ファイバートランスポート通信のために SCSI パススルー方式を可能にするデバイスドライバが必要となる場合があります。

SAN クライアントのオペレーティングシステムが正しく構成されれば、ターゲットモードの各メディアサーバー HBA ポートは 2 つの ARCHIVE Python デバイスとして認識されます。

表 5-5 に、サポートされる SAN クライアントの各オペレーティングシステムのドライバ要件を示します。

表 5-5 SAN クライアントのオペレーティングシステムのドライバ要件

オペレーティングシステム	ドライバ要件
AIX	クライアントシステムは標準のテープドライバを必要とします。ドライバは、変更せずに使用できます。 ドライバを構成する方法については、次の URL で利用可能な『NetBackup デバイス構成ガイド』を参照してください。 http://www.veritas.com/docs/DOC5332
Linux	クライアントシステムには、SCSI 汎用 (sg) ドライバとパススルーデバイスファイルが必須です。 ドライバを構成する方法については、次の URL で利用可能な『NetBackup デバイス構成ガイド』を参照してください。 http://www.veritas.com/docs/DOC5332
Solaris	Solaris が NetBackup メディアサーバー上の FT デバイスを認識するように <code>/kernel/drv/st.conf</code> ファイルを変更する必要があります。 ファイルを変更する方法については、次の URL で利用可能な『NetBackup デバイス構成ガイド』を参照してください。 http://www.veritas.com/docs/DOC5332
Windows の場合	デバイスドライバは必要ありません。メディアサーバーの FT デバイスは、Windows デバイスマネージャの[その他のデバイス]セクションに ARCHIVE Python SCSI Sequential Devices と表示されます。

一部のオペレーティングシステムでは、特定のパッチおよびドライバの更新が必要です。詳しくは、『NetBackup リリースノート』を参照してください。

<http://www.veritas.com/docs/DOC5332>

SAN クライアントのファイバートランスポートサービスの構成

SAN クライアントとして機能させる NetBackup クライアントで、SAN クライアントのファイバートランスポートサービスを有効にする必要があります。この処理で、SAN クライアントのオペレーティングシステムは FT メディアサーバー上の FT デバイスを検出します。

警告: NetBackup SAN クライアントを、NetBackup サーバーとして使用することはできません。したがって、システムでは、NetBackup クライアントソフトウェアのみがインストールされるように、SAN クライアントにするクライアントを構成します。

p.55 の「[クラスタ内の SAN クライアントの構成](#)」を参照してください。

p.56 の「[SAN クライアントのクラスタの仮想名の登録](#)」を参照してください。

NetBackup クライアントを SAN クライアントとして構成する方法

- 1 PBX サービスがクライアントで有効になっていることを次のように確認します。
 - UNIX と Linux システムで、NetBackup の `bpps -x` コマンドを実行し、`pbx_exchange` プロセスが有効になっていることを確認します。
 - Windows システムで、コンピュータ管理コンソールを使用して、Private Branch Exchange サービスが有効になっていることを確認します。
- 2 クライアントで次のコマンドを実行して、SAN クライアントのファイバートランスポートサービス (`nbftclnt`) を有効にします。

UNIX および Linux の場合:

```
/usr/opensv/netbackup/bin/bpclntcmd -sanclient 1
```

Windows の場合:

```
install_path¥NetBackup¥bin¥bpclntcmd.exe -sanclient 1
```

- 3 次の手順を実行して、SAN クライアントの FT サービスを起動します。
 - Linux の場合: システムを起動します。これによって、オペレーティングシステムのデバイス検出も開始されます (代わりに、NetBackup の `bp.start_all` コマンドを実行して、クライアント FT サービスを起動することもできます)。
 - AIX と Solaris の場合: NetBackup の `bp.start_all` コマンドを実行します。このコマンドは、次のディレクトリに存在します。
`/usr/opensv/netbackup/bin`
 - Windows の場合: システムを起動します。これによって、オペレーティングシステムのデバイス検出も開始されます。

- 4 手順 3 で起動されなかったシステムでは、SAN クライアントのオペレーティングシステムにデバイスの検出を強制させるための操作を実行します。

オペレーティングシステムで、ターゲットモードになっているメディアサーバーの各 HBA ポートにつき、FT デバイスは 2 つ検出される必要があります。

SAN クライアントのファイバートランスポートサービス (nbftc1nt) によって、デバイスの検出時にドライバスタック機能が検証されます。検証が失敗した場合、ファイバートランスポートはクライアントで有効になりません。

p.84 の「[SAN クライアントファイバートランスポートサービスの検証](#)」を参照してください。

クライアントの OS が FT デバイスを検出すると、SAN クライアントが NetBackup に登録されます。

- 5 クライアントシステムで FT デバイスが検出されない場合は、次の項目を確認します。
- ファイバーチャネルのドライバが SAN クライアントにインストールされている。
 - ファイバーチャネルスイッチで SAN クライアントの HBA ポートが有効になっている。
 - ファイバーチャネルスイッチでメディアサーバーの HBA ポートが有効になっている。
 - SAN クライアントがファイバーチャネルスイッチのネームサーバーにログインしている。
 - FT メディアサーバーがファイバーチャネルスイッチのネームサーバーにログインしている。
 - SAN クライアントポートで FT メディアサーバーポートがゾーン化されている。
 - ゾーンが有効な構成に含まれている。

また、クライアントシステムの FT デバイスに対してスキャン操作を試行することもできます。

p.67 の「[SAN クライアントからファイバートランスポートデバイスの再スキャン](#)」を参照してください。

クラスタ内の SAN クライアントの構成

SAN クライアントの FT サービスは、クラスタアプリケーションではありません。クラスタ内にある SAN クライアントを保護するには、クラスタ内のすべての SAN クライアントを正しく設定する必要があります。

p.57 の「[コマンドラインの使用による NetBackup 構成オプションの設定](#)」を参照してください。

p.52 の「[SAN クライアントの構成](#)」を参照してください。

表 5-6 クラスタの SAN クライアントを構成する処理

手順	処理	説明
手順 1	各フェールオーバーノードに NetBackup クライアントソフトウェアをインストールします。	『NetBackup インストールガイド』を参照してください。
手順 2	各フェールオーバーノードで SAN クライアントを構成します。	FT サービスがすべてのフェールオーバーノードで実行されていることを確認します。 p.52 の「SAN クライアントのファイアウォールの構成について」を参照してください。 p.53 の「SAN クライアントのドライバの要件」を参照してください。 p.54 の「SAN クライアントのファイバートランスポートサービスの構成」を参照してください。
手順 3	サーバーに仮想ノード名を登録します。	p.56 の「SAN クライアントのクラスタの仮想名の登録」を参照してください。
手順 4	NetBackup ローカルキャッシュを構成します。	クラスタ内の各 SAN クライアントで NetBackup LOCAL_CACHE オプションを NO に設定します。 p.16 の「クラスタリングのための NetBackup SAN クライアントサポート」を参照してください。 p.57 の「コマンドラインの使用による NetBackup 構成オプションの設定」を参照してください。 警告: FT メディアサーバーまたはプライマリサーバーの LOCAL_CACHE 値は変更しないでください。

SAN クライアントのクラスタの仮想名の登録

クライアントを保護するためにクラスタを使う場合は、NetBackup にクラスタの仮想名を登録する必要があります。

p.55 の「クラスタ内の SAN クライアントの構成」を参照してください。

クラスタの仮想名を登録する方法

- 1 データベースに仮想名を追加します。コマンドの構文は次のとおりです。

```
nbemmcmd -addhost -machinename virtual_name -machinetype
app_cluster
```

nbemmcmd コマンドへのパスは次のとおりです。

- UNIX の場合: /usr/opensv/netbackup/bin/admincmd

- Windows の場合: `install_path¥NetBackup¥bin¥admincmd`
- 2 ノード内のすべてのクライアントに対して、仮想名がクライアントのホスト名にリンクされるようにホストを更新します。コマンドの構文は次のとおりです。

```
nbemmcmd -updatehost -add_server_to_app_cluster -machinename  
client_name -clustername virtual_name
```

コマンドラインの使用による NetBackup 構成オプションの設定

Cohesityでは、NetBackup Web UI を選択してホストのプロパティを構成することをお勧めします。

ただし、NetBackup Web UI からは設定できないプロパティもあります。次の NetBackup コマンドを使って、それらのプロパティを設定できます。

NetBackup サーバーの場合: `bpsetconfig`

NetBackup クライアントの場合: `nbsetconfig`

次の例に示すように、構成オプションはキーと値のペアです。

- `CLIENT_READ_TIMEOUT = 300`
- `LOCAL_CACHE = NO`
- `RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE`
- `SERVER = server1.example.com`

SERVER オプションのようなオプションを複数回指定できます。

コマンドラインを使って構成オプションを設定するには

- 1 プロパティを設定するホストのコマンドウィンドウまたはシェルウィンドウで、適切なコマンドを呼び出します。コマンドは、次のように、オペレーティングシステムと NetBackup ホストの種類 (クライアントまたはサーバー) によって異なります。

UNIX の場 NetBackup クライアントの場合:

合 `/usr/opensv/netbackup/bin/nbsetconfig`

NetBackup サーバーの場合:

`/usr/opensv/netbackup/bin/admincmd/bpsetconfig`

Windows NetBackup クライアントの場合:

の場合 `install_path¥NetBackup¥bin¥nbsetconfig.exe`

NetBackup サーバーの場合:

`install_path¥NetBackup¥bin¥admincmd¥bpsetconfig.exe`

- 2 コマンドプロンプトで、設定する構成オプションのキーと値のペアを 1 行に 1 組ずつ入力します。

既存のキーと値のペアを変更できます。

キーと値のペアを追加できます。

追加する任意の新しいオプションの許可される値と形式を理解していることを確認してください。

- 3 構成の変更を保存するには、オペレーティングシステムに応じて、次のコマンドを入力します。

Windows の場合: `Ctrl + Z Enter`

UNIX の場合: `Ctrl + D Enter`

ファイバートランスポートのプロパティの構成について

NetBackup の [ファイバートランスポート (Fibre Transport)] プロパティでは、SAN クライアントがバックアップでファイバートランスポートサービスを使う方法を制御します。

NetBackup はプロパティの階層を使用して、クライアントによる NetBackup ファイバートランスポートの使用により細かい制御を提供します。次の表では、[ホストプロパティ (Host properties)] のプロパティ構成レベルを説明します。

表 5-7 [ファイバートランスポート (Fibre Transport)] プロパティ

詳細度	説明
すべての SAN クライアントのグローバルファイバートランスポートプロパティ	<p>グローバルファイバートランスポートプロパティは、すべての SAN クライアントに適用されます。グローバルファイバートランスポートプロパティは、プライマリサーバーで構成します。</p> <p>プライマリサーバーの[ファイバートランスポート (Fibre transport)] ホストプロパティで、これらのプロパティを構成します。</p>
メディアサーバー (1 つまたは複数) のファイバートランスポートプロパティ	<p>メディアサーバー (1 つまたは複数) のファイバートランスポートプロパティは、メディアサーバー (1 つまたは複数) がバックアップする SAN クライアントに適用されます。これらのプロパティは、プライマリサーバーで構成されるグローバルファイバートランスポートプロパティを上書きします。</p> <p>メディアサーバーの[ファイバートランスポート (Fibre transport)] ホストプロパティで、これらのプロパティを構成します。</p>
SAN クライアント (1 つまたは複数) のファイバートランスポートプロパティ	<p>クライアント (1 つまたは複数) のファイバートランスポートプロパティは特定の SAN クライアント (1 つまたは複数) に適用されます。SAN クライアントのファイバートランスポートプロパティは、メディアサーバーの FT プロパティを上書きします。</p> <p>クライアントの[ファイバートランスポート (Fibre transport)] ホストプロパティで、これらのプロパティを構成します。</p>

p.59 の「[ファイバートランスポートのプロパティの構成](#)」を参照してください。

NetBackup では、ファイバートランスポートに、より詳細な詳細度が 1 つ用意されています。SAN クライアント使用設定は、[ホストプロパティ (Host properties)] で設定するファイバートランスポートプロパティよりも優先されます。

p.64 の「[SAN クライアントの使用設定](#)」を参照してください。

p.31 の「[SAN クライアントおよびファイバートランスポートの構成](#)」を参照してください。

ファイバートランスポートのプロパティの構成

NetBackup の[ファイバートランスポート (Fibre Transport)] プロパティでは、SAN クライアントがバックアップでファイバートランスポートサービスを使う方法を制御します。

NetBackup はプロパティの階層を使用して、クライアントによる NetBackup Fibre Transport (ファイバートランスポート) の使用により細かい制御を提供します。

p.58 の「[ファイバートランスポートのプロパティの構成について](#)」を参照してください。

NetBackup ファイバートランスポートのプロパティを構成するには

- 1 左側で、[ホスト (Host)]、[ホストプロパティ (Host properties)]の順に選択します。
- 2 プロパティのどのレベルを構成するかに応じて、次のいずれかを実行します:

グローバルファイバートランスポートのプロパティを構成するには

プライマリサーバーを選択します。必要に応じて、[接続 (Connect)]を選択してから、[プライマリサーバーの編集 (Edit primary server)]を選択します。

メディアサーバー (1 つまたは複数) のファイバートランスポートのプロパティを構成するには

メディアサーバーを選択します。必要に応じて、[接続 (Connect)]を選択してから、[メディアサーバーの編集 (Edit media server)]を選択します。ファイバートランスポートのホストプロパティをメディアサーバーで利用できるのは、ファイバートランスポートサービスがそのメディアサーバーで有効になっている場合のみです。

クライアント (1 つまたは複数) のファイバートランスポートのプロパティを構成するには

クライアントを選択します。必要に応じて、[接続 (Connect)]を選択してから、[クライアントの編集 (Edit client)]を選択します。

- 3 [ファイバートランスポート (Fibre Transport)]を選択します。
- 4 プロパティを構成します。

p.60 の「[ファイバートランスポート (Fibre Transport)] プロパティ」を参照してください。

[ファイバートランスポート (Fibre Transport)] プロパティ

この設定にアクセスするには、Web UI で[ホスト (Host)]、[ホストプロパティ (Host properties)]の順に選択します。ホストを選択します。必要に応じて、[接続 (Connect)]をクリックします。次に、[プライマリサーバーの編集 (Edit primary server)]、[メディアサーバーの編集 (Edit media server)]、または[クライアントの編集 (Edit client)]をクリックします。[ファイバートランスポート (Fibre Transport)]をクリックします。

[ストレージ (Storage)]、[SAN クライアント (SAN Clients)]で個々の SAN クライアントに対して構成した使用設定により、[ホストプロパティ (Host properties)]で構成する[ファイバートランスポート (Fibre Transport)]プロパティが上書きされることに注意してください。

p.64 の「SAN クライアントの使用設定の構成」を参照してください。

NetBackup の[ファイバートランスポート (Fibre Transport)]プロパティでは、ファイバートランスポートメディアサーバーと SAN クライアントがバックアップとリストアでファイバート

ランスポートサービスを使用する方法を制御します。[ファイバートランスポート (Fibre Transport)] プロパティは選択するホスト形式に次のように適用されます。

表 5-8 ファイバートランスポートプロパティのホスト形式

ホストの種類 (Host type)	説明
プライマリサーバー	すべての SAN クライアントに適用されるグローバルの [ファイバートランスポート (Fibre Transport)] プロパティ。
メディアサーバー	[ファイバートランスポート (Fibre Transport)] の [最大並列ファイバートランスポート接続 (Maximum concurrent Fibre Transport connections)] プロパティは、選択したファイバートランスポートメディアサーバーに適用されます。
クライアント	[ファイバートランスポート (Fibre Transport)] プロパティは、選択した SAN クライアントに適用されます。クライアントのデフォルト値はプライマリサーバーのグローバルプロパティの設定です。クライアントプロパティは [ファイバートランスポート (Fibre Transport)] のグローバルプロパティを強制変更します。

[ファイバートランスポート (Fibre Transport)] プロパティには、次の設定が含まれます。すべてのプロパティがすべてのホストで利用できるわけではありません。この表では、ファイバートランスポートデバイスはファイバートランスポートメディアサーバーの HBA ポートです。ポートはバックアップとリストアのトラフィックを搬送します。1 つのメディアサーバーに複数のファイバートランスポートデバイスが存在する場合があります。

表 5-9 [ファイバートランスポート (Fibre Transport)] プロパティ

プロパティ	説明
<p>最大並列ファイバートランスポート接続 (Maximum concurrent Fibre Transport connections)</p>	<p>このプロパティは、ファイバートランスポートメディアサーバーを選択した場合にのみ表示されます。</p> <p>このプロパティは選択したメディアサーバー (複数可) に許可するファイバートランスポート接続の数を指定します。1 つの接続は 1 つのジョブに相当します。</p> <p>値が設定されない場合には、NetBackup は次のデフォルトを使います。</p> <ul style="list-style-type: none"> ■ NetBackup Appliance モデル 5330 とそれ以降の場合: 32 ■ NetBackup Appliance モデル 5230 とそれ以降の場合: 32 ■ NetBackup ファイバートランスポートメディアサーバーの場合: メディアサーバー上の速い HBA ポート数の 8 倍に加えて遅い HBA ポートの数の 4 倍が使われます。速いポートは 8 GB 以上、遅いポートは 8 GB 未満です。 <p>サーバーまたはメディアサーバーを使うには次の最大接続数まで入力できます:</p> <ul style="list-style-type: none"> ■ Linux ファイバートランスポートメディアサーバーホストの場合: 40 Linux 上で同時に使う接続は 32 以下に設定することを推奨します。 Linux ホストの場合には、NetBackup touch ファイル (NUMBER_DATA_BUFFERS_FT) の設定によってその最大値を大きくできます。 p.63 の「Linux 並列 FT 接続について」を参照してください。 ■ NetBackup Appliance モデル 5330 とそれ以降の場合: 40 ■ NetBackup Appliance モデル 5230 とそれ以降の場合: 40 ■ Solaris ファイバートランスポートメディアサーバーホストの場合: 64 <p>NetBackup では、ファイバートランスポート用に 1 台のメディアサーバーに対して 644 バッファがサポートされます。各接続で使われるバッファ番号を決定するには、入力した値で 644 を割ります。接続ごとのバッファがある場合、各接続のパフォーマンスが改善します。</p>
<p>プライマリサーバー構成のデフォルトを使用 (Use defaults from the primary server configuration)</p>	<p>このプロパティは、クライアントを選択した場合にのみ表示されます。</p> <p>このプロパティは、プライマリサーバーで構成されているプロパティにクライアントが従うように指定します。</p>
<p>優先 (Preferred)</p>	<p>分単位で構成された待機期間内に FT デバイスが利用可能である場合、FT デバイスを使用するように指定します。待機期間の経過後に FT デバイスが利用できない場合、NetBackup は LAN 接続を使用して操作を行います。</p> <p>プライマリサーバーで指定したグローバルプロパティの場合、デフォルトは[優先 (Preferred)]です。</p>

プロパティ	説明
常時 (Always)	<p>SAN クライアントのバックアップおよびリストアに対して NetBackup では常に FT デバイスが使用されるように指定します。NetBackup は、操作を開始する前に FT デバイスが利用可能になるまで待機します。</p> <p>ただし、FT デバイスは動作している必要があります。そうでない場合、NetBackup は LAN を使います。すべての FT デバイスが実行されていない、設定されていない、または SAN クライアントのライセンスが期限切れであるなどの理由で、FT デバイスが存在しない場合があります。</p>
失敗 (Fail)	<p>FT デバイスが動作していない場合に NetBackup がジョブを失敗するように指定します。FT デバイスが動作していてもビジーの場合には、NetBackup はデバイスが利用可能になるまで待機してから、デバイスに次のジョブを割り当てます。すべての FT デバイスが動作していない、設定されていない、または SAN クライアントのライセンスが期限切れであるなどの理由で、FT デバイスが存在しない場合があります。</p>
使用しない (Never)	<p>SAN クライアントのバックアップおよびリストアに対して NetBackup ではファイバートランスポートパイプを使用しないように指定します。NetBackup では、バックアップとリストアに LAN 接続が使用されます。</p> <p>プライマリサーバーに[使用しない (Never)]を指定した場合、ファイバートランスポートは NetBackup 環境で無効になります。[使用しない (Never)]を選択すれば、クライアントごとにファイバートランスポートの使用方法を構成できます。</p> <p>SAN クライアントに[使用しない (Never)]を指定すれば、ファイバートランスポートはクライアントで無効になります。</p>

Linux 並列 FT 接続について

NetBackup では、[ファイバートランスポート (Fibre transport)]ホストプロパティの[最大並列 FT 接続 (Maximum concurrent FT connections)]設定を使用して、ホストごとに許可される、ファイバートランスポートメディアサーバーへの同時接続数の合計を設定します。

p.60 の「[\[ファイバートランスポート \(Fibre Transport\)\]プロパティ](#)」を参照してください。

Linux での同時接続の合計数が目的よりも少ない場合、同時接続の合計数を増やすことができます。その結果、各クライアントのバックアップまたはリストアジョブが使用するバッファが減ります。この場合、バッファが少ないために各ジョブが遅くなります。同時接続数を増やすには、接続ごとのバッファ数を減らしてください。そのためには、次のファイルを作成し、[表 5-10](#) のサポートされている値の 1 つをファイルに含めます。

```
/usr/opensv/netbackup/db/config/NUMBER_DATA_BUFFERS_FT
```

[表 5-10](#) に **NetBackup** で NUMBER_DATA_BUFFERS_FT ファイルに対してサポートされる値を示します。**NetBackup** では、ファイバートランスポート用に 1 台のメディアサーバーに対して 644 バッファがサポートされます。

表 5-10 1 つの FT 接続のバッファに対してサポートされる値

NUMBER_DATA_BUFFERS_FT	同時接続の総数: NetBackup 5230 と 5330 以降のアプライアンス	同時接続の総数: Linux FT メディアサーバー
16	40	40
12	53	53
10	64	64

必要に応じて、[ファイバートランスポート (Fibre transport)] ホストプロパティの [最大並列 FT 接続 (Maximum concurrent FT connections)] 設定を使用して、メディアサーバーの接続数を制限できます。

SAN クライアントの使用設定の構成

SAN クライアント使用設定には、特定のクライアントがバックアップ用 NetBackup Fibre Transport を使う方法を設定できます。これらの設定は、ホストプロパティのファイバートランスポート設定を強制変更します。

p.60 の「[\[ファイバートランスポート \(Fibre Transport\)\] プロパティ](#)」を参照してください。

p.58 の「[ファイバートランスポートのプロパティの構成について](#)」を参照してください。

SAN クライアントの使用設定を構成する方法

- 1 NetBackup Web UI を開き、プライマリサーバーにサインインします。
- 2 左側で [ストレージ (Storage)]、[SAN クライアント (SAN clients)] の順に選択します。
- 3 SAN クライアントを見つけます。
- 4 [処理 (Actions)]、[使用設定 (Usage preferences)] の順に選択します。
- 5 プロパティを構成します。
p.64 の「[SAN クライアントの使用設定](#)」を参照してください。
- 6 [保存 (Save)] を選択します。

SAN クライアントの使用設定

次の表は SAN クライアントのファイバートランスポート使用設定を説明したものです。

表 5-11 **SAN クライアントのファイバートランスポート使用設定**

プロパティ	説明
プライマリサーバー構成のデフォルトを使用 (Use defaults from the primary server configuration)	このプロパティは、プライマリサーバーで構成されているプロパティにクライアントが従うように指定します。
優先 (Preferred)	<p>分単位で構成された待機期間内に FT デバイスが利用可能である場合、FT デバイスを使用するように指定します。待機期間の経過後に FT デバイスが利用できない場合、NetBackup は LAN 接続を使用して操作を行います。</p> <p>プライマリサーバーで指定したグローバルプロパティの場合、デフォルトは[優先 (Preferred)]です。</p>
常時 (Always)	<p>SAN クライアントのバックアップおよびリストアに対して NetBackup では常に FT デバイスが使用されるように指定します。NetBackup は、操作を開始する前に FT デバイスが利用可能になるまで待機します。</p> <p>ただし、FT デバイスは動作している必要があります。そうでない場合、NetBackup は LAN を使います。すべての FT デバイスが実行されていない、設定されていない、または SAN クライアントのライセンスが期限切れであるなどの理由で、FT デバイスが存在しない場合があります。</p>
失敗 (Fail)	FT デバイスが動作していない場合に NetBackup がジョブを失敗するように指定します。FT デバイスが動作していてもビジーの場合には、NetBackup はデバイスが利用可能になるまで待機してから、デバイスに次のジョブを割り当てます。すべての FT デバイスが実行されていない、設定されていない、または SAN クライアントのライセンスが期限切れであるなどの理由で、FT デバイスが存在しない場合があります。
使用しない (Never)	<p>SAN クライアントのバックアップおよびリストアに対して NetBackup では FT パイプを使用しないように指定します。NetBackup では、バックアップとリストアに LAN 接続が使用されます。</p> <p>SAN クライアントに[使用しない (Never)]を指定すれば、ファイバートランスポートはクライアントで無効になります。</p>

SAN クライアントおよびファイバートランスポートの管理

この章では以下の項目について説明しています。

- [ファイバートランスポートサービスの有効化または無効化](#)
- [16 gb ターゲットモード HBA サポート向けのファイバートランスポートサービスの有効化および無効化](#)
- [SAN クライアントからファイバートランスポートデバイスの再スキャン](#)
- [SAN クライアントのファイバートランスポートジョブの詳細の表示](#)
- [ファイバートランスポートトラフィックの表示](#)
- [SAN クライアントの削除](#)

ファイバートランスポートサービスの有効化または無効化

NetBackup の FT メディアサーバーの FT サービスを有効または無効にできます。

FT サーバーを構成するサービスを次に示します。

- nbftsrvr サービスは、FT パイプのサーバー側を管理します。
- nbfdrv64 サービスは、メディアサーバーのターゲットモードドライバを制御します。

nbfdrv64 サービスは、nbftsrvr サービスによって起動されます。1 つのサービスを停止すると、もう一方のサービスが停止します。1 つのサービスが異常終了すると、もう一方のサービスが停止します。

これらのサービスは、アクティビティモニターに表示されるのではなく、オペレーティングシステムのプロセス表示に表示されます。

警告: UNIX の `kill -9` コマンドおよびオプションを `nbfdrv64` プロセスを終了するために使用しないでください。 `nbfdrv64` プロセスが停止すると、SAN クライアントは FT デバイスを検出できません。この場合、FT デバイスが再び検出されるようにするには、`nbfdrv64` の再起動後に、クライアントシステムの再起動が必要になる場合があります。

FT サービスを有効または無効にする方法

- 1 NetBackup Web UI を開き、プライマリサーバーにサインインします。
- 2 左側で [ストレージ (Storage)]、[メディアサーバー (Media servers)] の順に選択します。
- 3 [メディアサーバー (Media servers)] タブを選択します。
- 4 FT メディアサーバーを選択します。
- 5 [FT サービスの有効化 (Enable FT services)] または [FT サービスの無効化 (Disable FT services)] を選択します。

16 gb ターゲットモード HBA サポート向けのファイバートランスポートサービスの有効化および無効化

NetBackup の FT メディアサーバーの FT サービスを有効または無効にできます。

FT サーバーを構成するサービスを次に示します。

- `nbftsrvr` サービスは、FT パイプのサーバー側を管理します。

このサービスは、アクティビティモニターに表示されるのではなく、オペレーティングシステムのプロセス表示に表示されます。

FT サービスを有効または無効にする方法

- 1 NetBackup Web UI を開き、プライマリサーバーにサインインします。
- 2 左側で [ストレージ (Storage)]、[メディアサーバー (Media servers)] の順に選択します。
- 3 FT メディアサーバーを選択します。
- 4 [FT サービスの有効化 (Enable FT Services)] または [FT サービスの無効化 (Disable FT Services)] のいずれかを選択します。

SAN クライアントからファイバートランスポートデバイスの再スキャン

再スキャン操作を行うと、クライアントの新しい FT デバイスが検索されます。スキャンで新しい FT デバイスが検出されると、NetBackup はデータベースにそれらを追加します。再

スキャン操作は、時間のかかる計算操作です。再スキャンを実行しても、特にクライアントシステムによって再起動を要求されたときに再起動を実行しない場合、新しいデバイスが検出されないことがあります。

オペレーティングシステムの性能および HBA ドライバとその設定によって、スキャンで新しいファイバーチャネルデバイスが検索されることがあります。

SAN クライアントを再スキャンする方法

- 1 NetBackup Web UI を開き、プライマリサーバーにサインインします。
- 2 左側で[ストレージ (Storage)]>[SAN クライアント (SAN clients)]を選択します。
- 3 クライアントを選択します。
- 4 [処理 (Actions)]、[FT デバイスの再スキャン (Rescan FT devices)]の順に選択します。
- 5 次の操作の状態を監視します。
 - 開始済み (Initiated)
 - クライアントシステムの再起動が必要
 - 失敗
- 6 必要に応じて、クライアントシステムを再起動します。

SAN クライアントのファイバートランスポートジョブの詳細の表示

アクティビティ 모니터の[ジョブ (Jobs)]タブに、進行中または完了したジョブがすべて表示されます。

[トランスポート形式 (Transport type)]列に、SAN クライアントと NetBackup メディアサーバー間のトランスポート形式が表示されます。[ファイバートランスポート (Fibre Transport)]はファイバートランスポートを、空白は非アクティブな状態を、[LAN]は LAN を示します。

ジョブの[詳細 (Details)]タブに、次の情報を含むジョブの詳細な情報が表示されます。

- ヘッダー領域の[トランスポート形式 (Transport type)]フィールドに、[ジョブ (Jobs)]タブと同じ情報が表示されます。
- ジョブの詳細内のメッセージに、FT トランスポートを使用するジョブの状態が次のように表示されます。

p.69 の「[ファイバートランスポートトラフィックの表示](#)」を参照してください。

ジョブの詳細を表示する方法

- 1 アクティビティモニターに移動します。
- 2 [ジョブ (Jobs)] タブで、ジョブを選択します。

ジョブの詳細には、[概要 (Overview)] タブと[詳細 (Details)] タブの情報が含まれています。

ファイバートランスポートトラフィックの表示

FT メディアサーバーと SAN クライアント間の現在のアクティビティを表示できます。次の 2 つの表示が利用可能です。

FT メディアサーバー ビュー メディアサーバーの表示では、選択した FT メディアサーバーの受信方向のバックアップ (および送信方向のリストア) の通信がすべて表示されます。

この表示を使用して、選択したメディアサーバーに対してデータを送受信できる SAN クライアントを判断できます。

p.69 の「[メディアサーバーの観点から FT のアクティビティを表示する方法](#)」を参照してください。

SAN クライアント ビュー SAN クライアントの表示では、選択したクライアントの送信方向のバックアップ (および受信方向のリストア) の通信がすべて表示されます。

この表示を使用して、選択したクライアントに対してデータを送受信できる FT メディアサーバーを判断できます。

p.70 の「[クライアントの観点から FT のアクティビティを表示する方法](#)」を参照してください。

p.68 の「[SAN クライアントのファイバートランスポートジョブの詳細の表示](#)」を参照してください。

メディアサーバーの観点から FT のアクティビティを表示する方法

- 1 NetBackup Web UI を開き、プライマリサーバーにサインインします。
- 2 左側で [ストレージ (Storage)]、[メディアサーバー (Media servers)] の順に選択します。
- 3 [メディアサーバー (Media servers)] タブを選択します。
- 4 FT メディアサーバーを見つけます。
- 5 [処理 (Action)]、[FT 接続の表示 (View FT connections)] の順にクリックします。NetBackup に、メディアサーバーの接続アクティビティが表示されます。

クライアントの観点から FT のアクティビティを表示する方法

- 1 NetBackup Web UI を開き、プライマリサーバーにサインインします。
- 2 左側で[ストレージ (Storage)]、[SAN クライアント (SAN clients)]の順に選択します。
- 3 クライアントを見つけます。
- 4 [処理 (Action)]、[FT 接続の表示 (View FT connections)]の順にクリックします。
NetBackup に、クライアントの接続アクティビティが表示されます。

SAN クライアントの削除

NetBackup 構成から SAN クライアントを削除するには、次の手順を実行します。SAN クライアントは NetBackup クライアントのままですが、SAN クライアントとしては機能しなくなります。

SAN クライアントを削除する方法

- 1 クライアントのサービスを停止します。
- 2 NetBackup Web UI を開き、プライマリサーバーにサインインします。
- 3 左側で[ストレージ (Storage)]、[SAN クライアント (SAN clients)]の順に選択します。
- 4 クライアントを見つけます。
- 5 [処理 (Actions)]、[削除 (Delete)]の順に選択します。

SAN クライアントとファイバートランスポートの無効化

この章では以下の項目について説明しています。

- [SAN クライアントの無効化](#)
- [ファイバートランスポートメディアサーバーの無効化](#)
- [16 gb ターゲットモード HBA サポートのファイバートランスポートメディアサーバーの無効化](#)

SAN クライアントの無効化

SAN クライアントとファイバートランスポートコンポーネントはアンインストールできません。ただし、SAN クライアントを無効にできます。無効にすると、クライアントは SAN で FT メディアサーバーにバックアップできません。

SAN クライアントを無効にすると、NetBackup 環境から削除できます。

p.70 の「[SAN クライアントの削除](#)」を参照してください。

UNIX 上の NetBackup SAN クライアントサービスを無効にする方法

- 1 サービスを停止するには、クライアントで次のコマンドを実行します。

```
/usr/opensv/netbackup/bin/nbftclnt -terminate
```

- 2 コンピュータの再起動後にホストが SAN クライアントサービスを開始しないようにホストを構成するには、次のコマンドを実行します。

```
/usr/opensv/netbackup/bin/bpplntcmd -sanclient 0
```

Windows 上の NetBackup SAN クライアントサービスを無効にする方法

- 1 Windows の [コンピュータの管理] を使用して NetBackup SAN クライアントサービスを停止します。
- 2 再起動後にホストが SAN クライアントサービスを起動しないようにホストを構成するには、次のコマンドを実行します。

```
install_path¥NetBackup¥bin¥bpclntcmd.exe -sanclient 0
```

ファイバートランスポートメディアサーバーの無効化

ファイバートランスポートコンポーネントはアンインストールできません。ただし、FT メディアサーバーを無効にすると、メディアサーバーからオペレーティングシステム FT 起動スクリプトを削除できます。この処理は nbhba ドライバも削除して nbhba モードを終了します。これにより、メディアサーバーで NetBackup ファイバートランスポートがサポートされなくなります。

警告: Solaris システムでは、FT サービスと /etc/driver_aliases ドライバを削除した後に nbhba ファイルエントリが残ることがあります。エントリの形式は、qla2300 "pci1077,xxx" または qla2300 "pciex1077,xxx" です。エントリが残っていても問題はありませんが、エントリの削除を試行した場合に、システムが起動しない可能性があります。Sun Microsystems 社では、/etc/driver_aliases ファイルは編集しないことを推奨しています。

FT メディアサーバーを無効にしてドライバを削除する方法

- 1 FT メディアサーバーで、次のスクリプトを実行します。

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -d
```

- 2 次の起動スクリプトが削除されたことを確認します。

Linux システムでは、スクリプトは次のとおりです:

```
/etc/rc.d/rc2.d/S21nbftserver
/etc/rc.d/rc3.d/S21nbftserver
/etc/rc.d/rc5.d/S21nbftserver
/etc/rc.d/rc0.d/K03nbftserver
/etc/rc.d/rc6.d/K03nbftserver
/lib/modules/ 2.6.*smp/kernel/drivers/misc/ql2300_stub.ko
/lib/modules/ 2.6.*smp/kernel/drivers/misc/windrvr6.ko
```

Solaris システムでは、スクリプトは次のとおりです:

```
/etc/rc2.d/S21nbftserver
/etc/rc0.d/K03nbftserver
/usr/kernel/drv/windrvr6.conf
/usr/kernel/drv/sparcv9/windrvr6
/usr/kernel/drv/sparcv9/ql2300_stub
```

- 3 起動スクリプトが削除されていない場合には、手動で削除します。
- 4 次のスクリプトを実行します。

```
/usr/opensv/netbackup/bin/admincmd/nbftconfig -ds
ft_server_host_name
```

16 gb ターゲットモード HBA サポートのファイバートランスポートメディアサーバーの無効化

ファイバートランスポートコンポーネントはアンインストールできません。ただし、FT メディアサーバーを無効にすると、メディアサーバーからオペレーティングシステム FT 起動スクリプトを削除できます。この処理によって、SCSTドライバ、QLogicドライバまたはEmulexドライバも削除されます。これにより、メディアサーバーで NetBackup ファイバートランスポートがサポートされなくなります。

FT メディアサーバーを無効にしてドライバを削除する方法

- 1 FT メディアサーバーで、次のスクリプトを実行します。

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -uninstall
```

- 2 次の起動スクリプトが削除されたことを確認します。

```
scripts: (/etc/rc.d/)
    /etc/rc.d/init.d/nbftserver
    /etc/rc.d/rc2.d/S21nbftserver
    /etc/rc.d/rc3.d/S21nbftserver
    /etc/rc.d/rc5.d/S21nbftserver
    /etc/rc.d/rc0.d/K03nbftserver
    /etc/rc.d/rc1.d/K03nbftserver
    /etc/rc.d/rc6.d/K03nbftserver
drivers: (lib/modules/xxx/extra)
    q1a2x00tgt.ko
    q1a2xxx.ko
    scst.ko
    scst_user.ko
firmwares: (/lib/firmware)
    q12700-firmware-8.07.10.bin and q12700_fw.bin
    q12500-firmware-8.04.00.bin and q2500_fw.bin
folders:
    /var/lib/scst/vdev_mode_pages
    /var/lib/scst/pr
    /usr/share/doc/q12500-firmware-8.04.00
/etc/modules-load.d/scst.conf
```

- 3 起動スクリプトが削除されていない場合には、手動で削除します。ファイルを削除した後、ファイル名を `q12500_fw_original.bin` から `q12500_fw.bin` に変更します。
- 4 次のスクリプトを実行します。

```
/usr/opensv/netbackup/bin/admincmd/nbftconfig -ds
ft_server_host_name
```

メモ: /boot パーティションに十分なディスク容量がない場合は、`initramfs-3.10.0-514.26.2.el7.x86_64.img.10-23-17.17:22:37` のようなイメージを手動で削除して、ディスク容量を増やします。

SAN クライアントとファイバートランスポートのトラブルシューティング

この章では以下の項目について説明しています。

- [SAN クライアントとファイバートランスポートのトラブルシューティングについて](#)
- [SAN クライアントのトラブルシューティングの TechNote](#)
- [ファイバートランスポートログの表示](#)
- [統合ログについて](#)
- [ファイバートランスポートサービスの起動および停止](#)
- [16 gb ターゲットモード HBA サポート向けのファイバートランスポートサービスの起動および停止](#)
- [バックアップはファイバートランスポートデバイスが使用可能であっても LAN にフェールオーバーする](#)
- [Cohesity モジュールのロード時のカーネルの警告メッセージ](#)
- [SAN クライアントのサービスが起動しない](#)
- [SAN クライアントファイバートランスポートサービスの検証](#)
- [SAN クライアントがファイバートランスポートを選択しない](#)
- [メディアサーバーのファイバートランスポートデバイスが非アクティブ](#)
- [ファイバートランスポートデバイスの検出なし](#)

SAN クライアントとファイバートランスポートのトラブルシューティングについて

SAN クライアントとファイバートランスポートのトラブルシューティングに関する情報が利用可能です。

- p.76 の「[SAN クライアントのトラブルシューティングの TechNote](#)」を参照してください。
- p.76 の「[ファイバートランスポートログの表示](#)」を参照してください。
- p.81 の「[ファイバートランスポートサービスの起動および停止](#)」を参照してください。
- p.83 の「[バックアップはファイバートランスポートデバイスが使用可能であっても LAN にフェールオーバーする](#)」を参照してください。
- p.84 の「[SAN クライアントのサービスが起動しない](#)」を参照してください。
- p.84 の「[SAN クライアントファイバートランスポートサービスの検証](#)」を参照してください。
- p.85 の「[SAN クライアントがファイバートランスポートを選択しない](#)」を参照してください。
- p.86 の「[メディアサーバーのファイバートランスポートデバイスが非アクティブ](#)」を参照してください。
- p.87 の「[ファイバートランスポートデバイスの検出なし](#)」を参照してください。

SAN クライアントのトラブルシューティングの TechNote

SAN クライアントとファイバートランスポートのトラブルシューティングについて詳しくは、Cohesity Technical Support の Web サイトで、次の TechNote を参照してください。

https://www.veritas.com/content/support/ja_JP/article.100029180

TechNote の内容は、新しい情報に合わせて更新されます。TechNote には、このマニュアルよりも新しい情報が記載されている場合があります。

ファイバートランスポートログの表示

FT プロセスで生成されるログメッセージを表示することによって、ファイバートランスポートの動作および状態を監視できます。VxUL (Unified Logging) では、ログファイルに標準化された名前とファイル形式が使用されます。オリジネータ ID によって、ログメッセージを書き込むプロセスが識別されます。

表 8-1 に、FT の動作に関する情報を記録するプロセスに対応付けられた VxUL オリジネータ ID を示します。

表 8-1 ファイバートランスポートのオリジネータ ID

オリジネータ ID	ID を使用する FT プロセス
199	nbftsrvr と nbfdrv64。メディアサーバーのファイバートランスポートサービス。 16 gb ターゲットモード HBA サポートの場合、nbftsrvr のみサポートされます。メディアサーバーのファイバートランスポートサービス。 メモ: 2 つの方法のうち 1 つのみを使用できます。
200	nbftclnt。クライアントのファイバートランスポートサービス。
201	FT Service Manager。Enterprise Media Manager サービスで動作します。

VxUL のログファイルを表示および管理するには、NetBackup のログコマンドを使用する必要があります。

p.77 の「[統合ログについて](#)」を参照してください。

NetBackup プライマリサーバーの [ログ (Logging)] プロパティと [クリーンアップ (Clean-up)] プロパティで収集する情報量と保持期間を設定します。これらのプロパティについて詳しくは、『[NetBackup Web UI 管理者ガイド](#)』を参照してください。

p.76 の「[SAN クライアントとファイバートランスポートのトラブルシューティングについて](#)」を参照してください。

統合ログについて

統合ログ機能では、すべての Cohesity 製品に共通の形式で、ログファイル名およびメッセージが作成されます。vxlogview コマンドを使用した場合だけ、ログの情報を正しく収集して表示することができます。サーバープロセスとクライアントプロセスは統合ログを使用しません。

オリジネータ ID のログファイルはログの構成ファイルで指定した名前の子ディレクトリに書き込まれます。すべての統合ログは次のディレクトリの子ディレクトリに書き込まれます。

Windows の `install_path\NetBackup\logs`
場合

UNIX の場合 `/usr/opensv/logs`

メモ: ログにアクセスできるのは、Linux システムの場合は **root** ユーザーと **service** ユーザー、Windows システムの場合は **administrators** グループに属するユーザーのみです。

ログコントロールには、[ログ (Logging)]ホストプロパティでアクセスできます。また、次のコマンドで統合ログを管理できます。

- `vxlogcfg` 統合ログ機能の構成設定を変更します。
- `vxlogmgr` 統合ログをサポートする製品が生成するログファイルを管理します。
- `vxlogview` 統合ログによって生成されたログを表示します。

p.80 の「[vxlogview を使用した統合ログの表示の例](#)」を参照してください。

vxlogview コマンドを使用した統合ログの表示について

`vxlogview` コマンドを使用した場合だけ、統合ログの情報を正しく収集して表示することができます。統合ログファイルは、バイナリ形式のファイルで、一部の情報は関連するリソースファイルに含まれています。これらのログは次のディレクトリに保存されます。特定プロセスのファイルに検索を制限することによって `vxlogview` の結果をより速く表示することができます。

- UNIX の場合 `/usr/opensv/logs`
- Windows の場合 `install_path¥NetBackup¥logs`

表 8-2 `vxlogview` 問い合わせ文字列のフィールド

フィールド名	形式	説明	例
PRODIG	整数または文字列	プロダクト ID または製品の略称を指定します。	PRODIG = 51216 PRODIG = 'NBU'
ORGID	整数または文字列	オリジネータ ID またはコンポーネントの略称を指定します。	ORGID = 116 ORGID = 'nbpem'
PID	long 型の整数	プロセス ID を指定します。	PID = 1234567
TID	long 型の整数	スレッド ID を指定します。	TID = 2874950

フィールド名	形式	説明	例
STDATE	long 型の整数または文字列	秒単位またはロケール固有の短い形式の日時で開始日付を指定します。たとえば、「mm/dd/yy hh:mm:ss AM/PM」の形式を使用しているロケールなどがあります。	STDATE = 98736352 STDATE = '4/26/11 11:01:00 AM'
ENDATE	long 型の整数または文字列	秒単位またはロケール固有の短い形式の日時で終了日付を指定します。たとえば、「mm/dd/yy hh:mm:ss AM/PM」の形式を使用しているロケールなどがあります。	ENDATE = 99736352 ENDATE = '04/27/11 10:01:00 AM'
PREVTIME	文字列	hh:mm:ss の形式で、時間を指定します。このフィールドには、=、<、>、>= および <= の演算子だけを使用できます。	PREVTIME = '2:34:00'
SEV	整数	次の使用可能な重大度の種類のうちのいずれかを指定します。 0 = INFO 1 = WARNING 2 = ERR 3 = CRIT 4 = EMERG	SEV = 0 SEV = INFO
MSGTYPE	整数	次の使用可能なメッセージの種類の中のいずれかを指定します。 0 = DEBUG (デバッグメッセージ) 1 = DIAG (診断メッセージ) 2 = APP (アプリケーションメッセージ) 3 = CTX (コンテキストメッセージ) 4 = AUDIT (監査メッセージ)	MSGTYPE = 1 MSGTYPE = DIAG
CTX	整数または文字列	識別子の文字列としてコンテキストトークンを指定するか、「ALL」を指定してすべてのコンテキストインスタンスを取得して表示します。このフィールドには、= および != の演算子だけを使用できます。	CTX = 78 CTX = 'ALL'

表 8-3 日付を含む問い合わせ文字列の例

例	説明
<code>(PRODID == 51216) && ((PID == 178964) ((STDATE == '2/5/15 09:00:00 AM') && (ENDATE == '2/5/15 12:00:00 PM')))</code>	2015 年 2 月 5 日の午前 9 時から正午までを対象に NetBackup プロダクト ID 51216 のログファイルメッセージを取り込みます。
<code>((prodid = 'NBU') && ((stdate >= '11/18/14 00:00:00 AM') && (enddate <= '12/13/14 12:00:00 PM')) ((prodid = 'BENT') && ((stdate >= '12/12/14 00:00:00 AM') && (enddate <= '12/25/14 12:00:00 PM')))</code>	2014 年 11 月 18 日から 2014 年 12 月 13 日までを対象に NetBackup プロダクト NBU のログメッセージを取り込み、2014 年 12 月 12 日から 2014 年 12 月 25 日までを対象に NetBackup プロダクト BENT のログメッセージを取り込みます。
<code>(STDATE <= '04/05/15 0:0:0 AM')</code>	2015 年 4 月 5 日、またはその前に記録されたすべてのインストール済み Cohesity 製品のログメッセージを取得します。

vxlogview を使用した統合ログの表示の例

次の例は、vxlogview コマンドを使って統合ログを表示する方法を示します。

メモ: ログにアクセスできるのは、Linux システムの場合は root ユーザーと service ユーザー、Windows システムの場合は administrators グループに属するユーザーのみです。

表 8-4 vxlogview コマンドの使用例

項目	例
ログメッセージの全属性の表示	<code>vxlogview -p 51216 -d all</code>
ログメッセージの特定の属性の表示	NetBackup (51216) のログメッセージの日付、時間、メッセージの種類およびメッセージテキストだけを表示します。 <code>vxlogview --prodid 51216 --display D,T,m,x</code>
最新のログメッセージの表示	オリジネータ 116 (nbpem) によって 20 分以内に作成されたログメッセージを表示します。-o 116 の代わりに、-o nbpem を指定することもできます。 <code># vxlogview -o 116 -t 00:20:00</code>

項目	例
特定の期間からのログメッセージの表示	<p>指定した期間内に nbpem で作成されたログメッセージを表示します。</p> <pre># vxlogview -o nbpem -b "05/03/15 06:51:48 AM" -e "05/03/15 06:52:48 AM"</pre>
より速い結果の表示	<p>プロセスのオリジネータを指定するのに <code>-i</code> オプションを使うことができます。</p> <pre># vxlogview -i nbpem</pre> <p>vxlogview <code>-i</code> オプションは、指定したプロセス (nbpem) が作成するログファイルのみを検索します。検索するログファイルを制限することで、vxlogview の結果が速く戻されます。一方、vxlogview <code>-o</code> オプションでは、指定したプロセスによって記録されたメッセージのすべての統合ログファイルが検索されます。</p> <p>メモ: サービスではないプロセスに <code>-i</code> オプションを使用すると、vxlogview によってメッセージ [ログファイルが見つかりません。 (No log files found)] が戻されます。サービスではないプロセスには、ファイル名にオリジネータ ID がありません。この場合、<code>-i</code> オプションの代わりに <code>-o</code> オプションを使用します。</p> <p><code>-i</code> オプションはライブラリ (137、156、309 など) を含むそのプロセスの一部であるすべての OID のエントリを表示します。</p>
ジョブ ID の検索	<p>特定のジョブ ID のログを検索できます。</p> <pre># vxlogview -i nbpem grep "jobid=job_ID"</pre> <p>jobid=という検索キーは、スペースを含めず、すべて小文字で入力します。</p> <p>ジョブ ID の検索には、任意の vxlogview コマンドオプションを指定できます。この例では、<code>-i</code> オプションを使用してプロセスの名前 (nbpem) を指定しています。このコマンドはジョブ ID を含むログエントリのみを返します。jobid=job_ID を明示的に含まないジョブの関連エントリは欠落します。</p>

ファイバートランスポートサービスの起動および停止

ファイバートランスポートサービスは、FT メディアサーバーおよび SAN クライアントの両方で動作します。

メディアサーバーで動作する FT サービスは次のとおりです。

- nbftsrvr サービスは、FT パイプのサーバー側を管理します。
- nbfdrv64 サービスは、メディアサーバーのターゲットモードドライバを制御します。

nbftsrvr サービスは、nbfdrv64 サービスによって起動されます。1 つのサービスを停止すると、もう一方のサービスも停止します。1 つのサービスが異常終了すると、もう一方のサービスが停止します。

nbftc1nt FT サービスは SAN クライアントで動作します。

これらのサービスは、NetBackup アクティビティモニターに表示されるのではなく、オペレーティングシステムのプロセス表示に表示されます。

通常の操作では、サービスを起動したり停止したりする必要はありません。Cohesity のサポート担当者から、トラブルシューティングを行うためにサービスを停止して再起動するように指示される場合があります。

p.66 の「ファイバートランスポートサービスの有効化または無効化」を参照してください。

また、UNIX の `kill` コマンドに `-9` オプションを指定せずに実行して、サービスを停止することもできます。NetBackup の `bp.kill_all` コマンドでも FT サービスは停止しますが、この場合は NetBackup の他のサービスもすべて停止します。

警告: UNIX の `kill -9` コマンドおよびオプションで `nbfdrv64` プロセスを終了しないでください。このコマンドを実行してもプロセスは正常終了しません。また、`nbfdrv64` プロセスが停止すると、SAN クライアントは FT デバイスを検出できません。この場合、FT デバイスが再び検出されるようにするには、`nbfdrv64` の再起動後に、クライアントシステムの再ブートが必要になる場合があります。

NetBackup の `bp.start_all` コマンドは、FT サービスを含むすべての NetBackup サービスを起動します。

16 gb ターゲットモード HBA サポート向けのファイバートランスポートサービスの起動および停止

ファイバートランスポートサービスは、FT メディアサーバーおよび SAN クライアントの両方で動作します。

メディアサーバーで動作する FT サービスは次のとおりです。

- `nbftsrvr` サービスは、FT パイプのサーバー側を管理します。

`nbftc1nt` FT サービスは SAN クライアントで動作します。

これらのサービスは、NetBackup アクティビティモニターに表示されるのではなく、オペレーティングシステムのプロセス表示に表示されます。

通常の操作では、サービスを起動したり停止したりする必要はありません。Cohesity のサポート担当者から、トラブルシューティングを行うためにサービスを停止して再起動するように指示される場合があります。

p.66 の「ファイバートランスポートサービスの有効化または無効化」を参照してください。

また、UNIX の `kill` コマンドに `-9` オプションを指定せずに実行して、サービスを停止することもできます。NetBackup の `bp.kill_all` コマンドでも FT サービスは停止しますが、この場合は NetBackup の他のサービスもすべて停止します。

NetBackup の `bp.start_all` コマンドは、FT サービスを含むすべての NetBackup サービスを起動します。

バックアップはファイバートランスポートデバイスが使用可能であっても LAN にフェールオーバーする

NetBackup FT メディアサーバーに VLAN の複数のネットワークインターフェースが備わっている場合、NetBackup のホスト名の順序が正しく設定されていないと、バックアップは LAN トランスポートにフェールオーバーすることがあります。

p.36 の「ファイバーのトランスポートのメディアサーバーおよび VLAN について」を参照してください。

バックアップに関わるすべてのホストについて、[サーバー (Servers)]ホストプロパティの [追加サーバー (Additional Servers)]リストを確認してください。FT サーバーのプライマリホスト名は、FT メディアサーバーホストの他のインターフェース名の前に表示されていること検証してください。表示されていない場合は、誤ったホスト名の順序を次の表に示すように修正してください。

表 8-5 NetBackup の誤ったホスト名の順序を修正する方法

作業	手順
メディアサーバーの FT サービスを停止します	p.66 の「ファイバートランスポートサービスの有効化または無効化」を参照してください。
NetBackup データベースから FT サーバーを削除します	次の NetBackup コマンドを使用して、FT のメディアサーバーである NetBackup データベースからホストを削除します: <code>nbftconfig -deleteserver -Me hostname</code> ホストは NetBackup メディアサーバーとしてデータベースに残ります。
各ホストの [追加サーバー (Additional Servers)]リストの順序を変更します	必要に応じて、[追加サーバー (Additional Servers)]リストから FT メディアサーバーのネットワークインターフェースの名前をすべて削除します。その後、プライマリホスト名を最初に追加し、残りのホスト名を任意の順序で追加します。[追加サーバー (Additional Servers)]リストはホストのプロパティの [サーバー (Servers)] ページに表示されます。 『NetBackup Web UI 管理者ガイド』を参照してください。
FT サービスをメディアサーバーで起動します	p.66 の「ファイバートランスポートサービスの有効化または無効化」を参照してください。

作業	手順
各 SAN クライアントの FT デバイスをスキャンします	FT メディアサーバーが再スキャン操作の間に検出されると、 NetBackup はデータベースに FT メディアサーバーとして追加します。 p.67 の「 SAN クライアントからファイバートランスポートデバイスの再スキャン 」を参照してください。

Cohesity モジュールのロード時のカーネルの警告メッセージ

Linux オペレーティングシステムでは、**Cohesity** モジュールがカーネルにロードされるときに、以下に類似した警告メッセージがコンソールまたはシステムログで表示される可能性があります。

```
kernel: ql2300_stub: module license 'Proprietary. Send bug reports to support@cohesity.com' taints kernel.
kernel: ql2300_stub: Version: XXn
kernel: ql2300_stub: $Revision: n.nn
```

メッセージは、**Cohesity** モジュールが専用である場合に表示されます。これらのメッセージは無視してください。

SAN クライアントのサービスが起動しない

nbftclnt サービスはクライアントで動作する **SAN** クライアントサービスです。nbftclnt サービスが **UNIX** または **Linux** システムで起動しない場合には、1 つの原因として **NetBackup** 構成ファイルが考えられます。ファイルのパス名は次のとおりです。

```
/usr/opensv/netbackup/bp.conf
```

クライアントのホスト名が **SERVER** と表示されている場合には、nbftclnt サービスは起動しません。クライアントに **SERVER** エントリが存在する場合は、エントリを削除してからクライアントサービスを開始します。

クライアントのホスト名は **CLIENT_NAME** とのみ表示されます。

SAN クライアントファイバートランスポートサービスの検証

SAN クライアントのファイバートランスポートサービス (nbftclnt) では、サービスの起動およびデバイスの検出時に、クライアントシステムのカーネルおよびドライバのスタックが

検証されます。検証によって、カーネルおよびドライバが、サポートされているレベルであることが確認されます。

検証が成功した場合は、SAN クライアントで FT パイプの転送がサポートされています。このため、FT パイプの転送が行われます。検証が失敗すれば、FT パイプの転送は行われません。

検証の失敗を管理するために、次が行われます。

- SAN クライアントのファイバートランスポートサービスによって、サービスのログファイルに `check driver` メッセージが書き込まれます。
- NetBackup は、クライアントの SAN ゾーンにあるすべてのファイバートランスポートターゲットデバイスについて、ファイバートランスポートデバイスの状態を [非アクティブ (`not active`)] に設定します (検証にパスしたゾーン内の他のクライアントのファイバートランスポートデバイスは [アクティブ (`Active`)] のままです)。

クライアントから FT デバイスの状態を表示するには、左側で [ストレージ (`Storage`)] > [SAN クライアント (`SAN clients`)] を選択します。SAN クライアントを見つけ、[操作 (`Actions`)] > [FT デバイスの表示 (`View FT devices`)] を選択します。

ログファイルの `nbftclnt` メッセージは、次のように表示されます。

```
VerifyCheckConditions:failed on <OS Device Name> - check driver
VerifyCheckConditions:failed on <OS Device Name>; <System Error
Message>
```

メッセージの変数は次のとおりです。

- **OS Device Name** は、SAN クライアントが OS のデバイスドライバを開くために使用するデバイス名を示します。
- **System Error Message** は、要求に関連する失敗についての OS 依存のシステムエラーメッセージを示します。

p.76 の「[ファイバートランスポートログの表示](#)」を参照してください。

検証が失敗した場合は、正しいバージョンのオペレーティングシステム、オペレーティングシステムのパッチまたはドライバをインストールします。

サポートされるカーネルおよびドライバのレベルについては、『[NetBackup リリースノート](#)』を参照してください。

SAN クライアントがファイバートランスポートを選択しない

次のいずれかに該当する場合、SAN クライアントはバックアップまたはリストア操作中にファイバートランスポートを選択できないことがあります。

- FTメディアサーバーのホストのオペレーティングシステムで使用する domainname コマンドが完全修飾ドメイン名を戻し、**NetBackup** が短縮名を使用するように構成されている。
- FTメディアサーバーのホストのオペレーティングシステムで使用する domainname コマンドが、**DNS**、**NIS** またはネットワークの問題が原因で失敗し、**NetBackup** が完全修飾ドメイン名を使用するように構成されている。

この場合、バックアップまたはリストアは失敗するか、**SAN** ではなく **LAN** を介して実行されることがあります。

この問題を回避するには、データベースに FT メディアサーバーのエイリアスを追加します。

コマンドの構文は次のとおりです。

- 短縮名のエイリアスを追加する場合

```
nbemmcmd -machinealias -addalias -alias shortservername
-machinename servername.fully.qualified -machinetype media
```

- 完全修飾ドメイン名のエイリアスを追加する場合

```
nbemmcmd -machinealias -addalias -alias
servername.fully.qualified -machinename shortservername
-machinetype media
```

メディアサーバーのファイバートランスポートデバイスが非アクティブ

メディアサーバーの FT デバイスが非アクティブであることが **NetBackup** に表示される場合は、選択した **SAN** クライアントがメディアサーバーのターゲットモードドライバを検出できません。FT デバイスの状態は、[ストレージ (Storage)] > [SAN クライアント (SAN clients)] に表示されます。**SAN** クライアントを選択し、[操作 (Actions)] > [FT デバイスの表示 (View FT devices)] を選択します。FT デバイスは、メディアサーバーの HBA のターゲットモードドライバを表します。

FT デバイスが「非アクティブ」になる理由として、次の状況が考えられます。

- メディアサーバーの nbfdrv64 サービスが停止している。nbfdrv64 サービスはターゲットモードドライバを管理します。このサービスが停止している場合には FT デバイスを利用できません。
- **SAN** クライアントと **SAN** スイッチ間の物理的な接続が失敗するか、または変更された。

- SAN のゾーンの変更によって、メディアサーバーまたは SAN クライアントのいずれかがゾーンから削除された。
- SAN クライアントが FT サービスの検証に失敗した。
p.84 の「[SAN クライアントファイバートランスポートサービスの検証](#)」を参照してください。

あるクライアントに対するすべてのメディアサーバーの FT デバイスが非アクティブになっている場合は、次の順序でトラブルシューティングを実行します。

- SAN クライアントの FT サービスの検証にパスしたことを確認します。
- SAN クライアントから SAN スイッチへの物理的な接続が正しいことを確認します。
- SAN ゾーンが正しいことを確認します。
- nbfdrv64 サービスが各メディアサーバーで有効になっていることを確認します。

nbfdrv64 サービスが停止しているかどうかを判断するには、オペレーティングシステムのプロセス状態コマンドを使ってメディアサーバーのプロセスを調べます。nbftsvr と nbfdrv64 は両方とも有効になっている必要があります。

p.81 の「[ファイバートランスポートサービスの起動および停止](#)」を参照してください。

サービスが起動しない場合は、サービスのログファイルを調べて、サービスが起動しない原因を特定します。

p.76 の「[ファイバートランスポートログの表示](#)」を参照してください。

ファイバートランスポートデバイスの検出なし

FT デバイスが検出されないことを示すメッセージが SAN クライアントの NetBackup ログに表示された場合は、SAN クライアントにパススルードライバが構成されていない可能性があります。

パススルードライバを構成する方法については、次の URL で利用できる『NetBackup デバイス構成ガイド』を参照してください。

<http://www.veritas.com/docs/DOC5332>

AIX に固有の構成の詳細

この付録では以下の項目について説明しています。

- [AIX のリファレンス情報](#)
- [NetBackup の構成を開始する前に \(AIX\)](#)
- [AIX での永続的な名前のサポートについて](#)
- [AIX でのロボット制御デバイスファイルの構成について](#)
- [AIX の SAN クライアントについて](#)
- [AIX での QIC 以外のテープドライブについて](#)
- [AIX の非巻き戻しデバイスファイルについて](#)
- [テープドライブの AIX 非巻き戻しデバイスファイルの作成](#)
- [AIX 動的追跡の無効化](#)

AIX のリファレンス情報

次の情報は AIX に固有です。テープまたはロボットデバイスなどの特定のデバイスには、特定の AIX 構成の必要条件があります。この AIX 参照セクションには、関連する情報が含まれています。

NetBackup の構成を開始する前に (AIX)

オペレーティングシステムを構成する場合、次の事項に従ってください。

- NetBackup で、サーバープラットフォームおよびデバイスがサポートされていることを検証します。NetBackup ハードウェアおよびオペレーティングシステムの互換性リストをダウンロードします。

<http://www.netbackup.com/compatibility>

- **NetBackup** のデバイスを構成する前に、すべての周辺機器を接続し、システムを再起動します。コンピュータが再起動されると、**AIX** は接続された周辺装置用のデバイスファイルを作成します。
- 多くの構成手順は、**smit**(システム管理インターフェースツール)を使用して実行できます。詳しくは、**smit(1)** のマニュアルページを参照してください。
- **smit** および `/usr/sbin/lsdev` コマンドを使用して、デバイスが正しく構成されていることを検証します。
- デバイスおよびロボットソフトウェアデーモンのエラーおよびデバッグ情報を取得するには、**syslogd** デーモンが有効になっている必要があります。詳しくは、**syslogd(1)** のマニュアルページを参照してください。

ハードウェアの構成後、ロボットおよびドライブを **NetBackup** に追加します。

AIX での永続的な名前のサポートについて

NetBackup では、**AIX** デバイスファイルでの永続的な名前のサポートを有効にする必要があります。そうすることによって、システムを再起動した後もターゲットデバイスおよび LUN が変化しなくなります。

永続的な名前のサポートを有効にするためには、**AIX SMIT** ユーティリティまたは **chdev** コマンドを使用してデバイスの論理名を変更します。**AIX** で最初にデバイス構成を行った後に論理名を変更します。詳しくは、**IBM** のマニュアルを参照してください。

AIX でのロボット制御デバイスファイルの構成について

NetBackup はデバイスを設定するときにデバイスファイルを検出します。

ドライブについての情報とデバイスファイルの設定方法について詳しくは、**IBM** 社のマニュアルを参照してください。

IBM 社以外のロボットライブラリの場合には、**Cohesity**はロボット制御ホストに **AIX** ではなくオペレーティングシステムを使うことをお勧めします。

AIX の SAN クライアントについて

NetBackup の SAN クライアントでは、**NetBackup FT** メディアサーバーへのファイバートランスポートの通信に、テープドライブと **SCSI** パススルー方式が使用されます。標準テープドライブを使う **AIX** の SAN クライアントは、**FT** メディアサーバーのファイバートランスポートターゲットを検出できません。メディアサーバー **FT** デバイスは、SAN クライアントの **SCSI** 照会時に **ARCHIVE Python** テープデバイスとして表示されます。ただし、それらはテープデバイスではないため、**NetBackup** のデバイス検出ではテープデバイスとして表示されません。

システムの起動中に、AIX `cfgmgr` コマンドはシステムを使う必要があるすべてのデバイスを設定します。NetBackup SAN クライアントで FT デバイスが検出されない場合は、クライアントのデバイスファイルを手動で設定できます。テープデバイスで使う手順と同じ手順を使います。

AIX での QIC 以外のテープドライブについて

可変長ブロックおよび固定長ブロックとは、オペレーティングシステムがテープから読み込みおよびテープに書き込みを行う方法を意味します。可変モードデバイスでは、すでに書き込まれたテープからの読み込みを、より柔軟に行うことが可能です。多くのテープデバイスには、どちらのモードでもアクセスできます。NetBackup では、1/4 インチカートリッジ (QIC) 以外のドライブは可変長であると見なされます。

詳しくは、`chdev(1)` と `smit(1)` のマニュアルページおよびシステム管理者ガイドを参照してください。smit アプリケーションは、固定長ブロック型デバイスを手動で可変長に変更するための最も有効な方法です。

警告: NetBackup では、QIC 以外のテープドライブを可変長ブロック型デバイスとして構成する必要があります。可変長ブロック型デバイスとして構成しない場合、NetBackup ではデータを書き込むことはできますが、正しく読み込むことができない可能性があります。読み込み中に `tar` 形式でないというエラーが表示される場合があります。

QIC 以外のテープドライブを NetBackup に追加すると、NetBackup によって `chdev` コマンドが発行され、ドライブが可変長ブロック型デバイスとして構成されます。参考までに、NetBackup でドライブを可変モードに構成するために実行するコマンドを次に示します。

```
/usr/sbin/chdev -l Dev -a block_size=0
```

`Dev` は、ドライブの論理識別子 (`rmt0` や `rmt1` など) です。

したがって、可変モード用にドライブを手動で構成する必要がありません。

AIX の非巻き戻しデバイスファイルについて

デフォルトでは、NetBackup は非巻き戻しデバイスファイルを使います。これらの SCSI デバイスファイルは `/dev/` ディレクトリに存在し、形式は次のとおりです。

```
/dev/rmtID.1
```

`ID` は、システムによってデバイスに割り当てられた論理識別子です。`.1` の拡張子は、オープン時非巻き戻しデバイスファイルを指定します。

通常、AIX はブート時にテープドライブのデバイスファイルを自動的に作成します。また、デバイスファイルを作成する必要がある AIX `cfgmgr` コマンドを実行できます。デバイスファイルがなければ、テープドライブ用にそれらを作成する必要があります。

テープドライブの AIX 非巻き戻しデバイスファイルの作成

NetBackup では、テープドライブと NetBackup SAN クライアントに非巻き戻しデバイスファイルを使います。システムの起動中に、AIX `cfgmgr` コマンドはシステムを使う必要があるすべてのデバイスを設定します。必要に応じて、非巻き戻しデバイスファイルを確認して作成するには、次の手順を使うことができます。

非巻き戻しデバイスファイルを確認して作成する方法

- 1 次のコマンドを実行して、システムの I/O コントローラを表示します。

```
/usr/sbin/lsdev -C | grep I/O
```

次の出力例では、SCSI コントローラ 1 (00-01) が論理識別子 `scsi0` に割り当てられています。

```
scsi0 Available 00-01 SCSI I/O Controller
```

- 2 次のコマンドを実行して、システムの SCSI デバイスおよびファイバーチャネルデバイスを表示します。SCSI デバイスの場合は `type` に `scsi` を指定し、ファイバーチャネルプロトコルデバイスの場合は `type` に `fcp` を指定します。

```
/usr/sbin/lsdev -C -s type
```

次の例では、2 台のディスクドライブと 1 台のテープドライブを示します。

```
hdisk0 Available 00-01-00-0,0 400 MB SCSI Disk Drive
hdisk1 Available 00-01-00-1,0 400 MB SCSI Disk Drive
rmt0 Available 00-01-00-3,0 Other SCSI Tape Drive
```

テープドライブ用の既存のデバイスファイルは、出力に `rmt0`、`rmt1` のように表示されます。前述の出力例では、`rmt0` と表示されています。

- 3 目的のテープドライブのデバイスファイルが存在しない場合、次のコマンドを実行してそのファイルを作成します。

```
/usr/sbin/mkdev -c tape -s scsi -t ost -p controller -w id,lun
```

コマンドの引数は次のとおりです。

- `controller` は、ドライブの SCSI アダプタの論理識別子 (`scsi0`、`fscsi0` または `vscsi1` など) です。

- `scsi_id` は、ドライブ接続の SCSI ID です。
 - `lun` は、ドライブ接続の論理ユニット番号です。
- 4 これを検証するために、次の `lsdev` コマンドを実行して、SCSI デバイスファイルを表示します。

```
/usr/sbin/lsdev -C -s scsi
hdisk0 Available 00-01-00-0,0 400 MB SCSI Disk Drive
hdisk1 Available 00-01-00-1,0 400 MB SCSI Disk Drive
rmt0 Available 00-01-00-3,0 Other SCSI Tape Drive
rmt1 Available 00-01-00-5,0 Other SCSI Tape Drive
```

この出力では `rmt1` デバイスファイルが作成されたことを示しています。

- 5 FCP コントローラ上にデバイスファイルが存在しない場合、次のコマンドを実行してそのファイルを作成します。

```
/usr/sbin/cfgmgr -l device
```

`device` は手順 1 で表示されるコントローラ番号です。

- 6 デバイスで可変モードと拡張ファイルマークが使用されるように構成されていることを確認します。 `chdev` コマンドを次のように実行します (`dev` は、ドライブの論理識別子 (`rmt1` など) です)。

```
/usr/sbin/chdev -l dev -a block_size=0
/usr/sbin/chdev -l dev -a extfm=yes
```

- 7 NetBackup でドライブを手動で構成するには、次のデバイスファイルのパス名を入力します。

```
/dev/rmt1.1
```

AIX 動的追跡の無効化

AIX 動的追跡により、NetBackup AIX SAN クライアントのバックアップジョブで問題が発生する場合があります。

ファイバーチャネルデバイスの IBM AIX 動的追跡は、新しい `fscsi` デバイス属性 `dyntrk` によって制御されます。

AIX NetBackup SAN クライアントホストから、動的追跡と `FC_ERROR_RECOV` 用の AIX ファイバーチャネル I/O パラメータを無効にする必要があります。これにより、NetBackup で書き込みバッファのエラーを回避し、NetBackup AIX SAN クライアントのバックアップジョブを問題なく実行できます。

AIX 動的追跡を無効化するには

1 AIX 動的追跡を無効化するには、次のように `dyntrk` と `FC_ERROR_RECOV` 属性を更新します。

- `chdev -l fscsi<fibre channel device ID> -a dyntrk=no`

例: `chdev -l fscsi0 -a dyntrk=no`

- `chdev -l fscsi<fibre channel device ID> -a
fc_err_recov=delayed_fail`

例: `chdev -l fscsi0 -a fc_err_recov=delayed_fail`

2 変更が適用されたことを確認します。

```
lsattr -E -l fscsi<device ID>
```

ファイバーチャネルデバイスの IBM AIX 動的追跡について詳しくは、IBM のマニュアルを参照してください。