

Veritas NetBackup™ ログリ ファレンスガイド

リリース 8.1.2

Veritas NetBackup™ ログリファレンスガイド

最終更新日: 2018-10-18

マニュアルバージョン: NetBackup 8.1.2

法的通知と登録商標

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

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

この製品には、サードパーティの所有物であることをベリタスが示す必要のあるサードパーティソフトウェア（「サードパーティプログラム」）が含まれている場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このベリタス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から入手できます。

<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。Veritas Technologies LLC からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供されるものであり、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。Veritas Technologies LLC は、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202、「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となります。業務用またはホスト対象サービスとしてベリタスによって提供されている場合でも同様です。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。

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

<http://www.veritas.com>

テクニカルサポート

テクニカルサポートは世界中にサポートセンターを設けています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の **Web** サイトにアクセスしてください。

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

次の URL で Veritas Account の情報を管理できます。

<https://my.veritas.com>

既存のサポート契約に関する質問については、次に示す地域のサポート契約管理チームに電子メールでお問い合わせください。

世界全域 (日本を除く)

CustomerCare@veritas.com

Japan (日本)

CustomerCare_Japan@veritas.com

マニュアル

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 ページに最終更新日付が記載されています。最新のマニュアルは、次のベリタス **Web** サイトで入手できます。

<https://sort.veritas.com/documents>

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

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

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

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

目次

第 1 章

ログの使用	9
ログについて	9
UNIX システムログについて	10
NetBackup でのログの保持について	11
統合ログとレガシーログのサイズの制限について	13
統合ログについて	13
NetBackup の統合ログの収集	15
統合ログメッセージの種類	16
統合ログのファイル名の形式	17
統合ログを使うエンティティのオリジネータ ID	18
統合ログファイルの場所の変更について	24
統合ログファイルのロールオーバーについて	25
統合ログファイルの再利用について	26
vxlogview コマンドを使用した統合ログの表示について	27
vxlogview コマンドで使用される問い合わせ文字列について	28
vxlogview を使用した統合ログの表示の例	31
vxlogmgr を使用した統合ログの管理の例	32
vxlogcfg を使用した統合ログの設定の例	35
レガシーログについて	37
レガシーログを使う UNIX クライアントプロセス	39
レガシーログを使う PC クライアントプロセス	41
レガシーログのファイル名の形式	43
サーバーのレガシーデバッグログのディレクトリ名	44
メディアおよびデバイス管理のレガシーデバッグログのディレクトリ名	46
レガシーログファイルに書き込まれる情報量を制御する方法	47
レガシーログのサイズと保持の制限について	48
レガシーログのローテーションの構成	49
グローバルログレベルについて	50
ログレベルの変更	52
Windows クライアントのログレベルの変更	53
Media Manager のデバッグログを上位レベルに設定する	53
クライアントのログの保持制限の設定	54
Windows のイベントビューアのログオプション	55
NetBackup 管理コンソールのエラーメッセージのトラブルシューティング	58

	ログおよび一時ファイルに必要な追加のディスク容量について	59
	詳細なデバッグログの有効化	60
第 2 章	バックアッププロセスおよびログ記録	62
	バックアップ処理	62
	NetBackup プロセスの説明	64
	バックアップとリストアの起動プロセス	65
	バックアップ処理およびアーカイブ処理	65
	バックアップおよびアーカイブ: UNIX クライアントの場合	66
	多重化されたバックアップ処理	67
	バックアップログについて	67
	ベリタステクニカルサポートへのバックアップログの送信	68
第 3 章	メディア、デバイスプロセスおよびログ記録	71
	メディアおよびデバイスの管理の開始プロセス	71
	メディアおよびデバイスの管理プロセス	73
	Shared Storage Option の管理プロセス	74
	バーコード操作	76
	メディアおよびデバイスの管理コンポーネント	78
第 4 章	リストアプロセスおよびログ記録	87
	リストアプロセス	87
	UNIX クライアントのリストア	91
	Windows クライアントのリストア	93
	リストアログについて	94
	ベリタステクニカルサポートへのリストアログの送信	95
第 5 章	高度なバックアップおよびリストア機能	97
	SAN クライアントファイバートランSPORTのバックアップ	97
	SAN クライアントファイバートランSPORTのリストア	100
	ホットカタログバックアップ	102
	ホットカタログのリストア	104
	合成バックアップ	106
	合成バックアップの問題レポートに必要なレガシーログディレクトリの作 成	109
	合成バックアップの問題レポートに必要なログ	110
第 6 章	ストレージのログ記録	111
	NDMP バックアップのログ記録	111
	NDMP リストアログ記録	114

第 7 章	NetBackup 重複排除ログ	117
	メディアサーバー重複排除プール (MSDP) への重複排除のバックアップ 処理	117
	クライアント重複排除のログ	120
	重複排除の設定ログ	120
	メディアサーバーの重複排除のログ記録と pdplugin ログ記録	122
	ディスク監視のログ記録	123
	ログ記録のキーワード	123
第 8 章	OpenStorage Technology (OST) のログ記録	125
	OpenStorage Technology (OST) バックアップのログ記録	125
	OpenStorage Technology (OST) の構成と管理	127
第 9 章	SLP (Storage Lifecycle Policy) および自動イメージ ジレプリケーション (A.I.R.) のログ記録	131
	ストレージライフサイクルポリシー (SLP) と自動イメージレプリケーション (A.I.R.) について	131
	ストレージライフサイクルポリシー (SLP) 複製プロセスフロー	132
	自動イメージレプリケーション (A.I.R.) のプロセスフローのログ記録	134
	インポートのプロセスフロー	136
	SLP および A.I.R. のログ記録	137
	SLP の構成と管理	138
第 10 章	NetBackup の安全な通信のログ記録	139
	NetBackup の安全な通信のログ記録について	139
	Tomcat のログ記録	140
	NetBackup Web サービスのログ記録	141
	コマンドラインのログ記録	143
	NetBackup cURL のログ記録	143
	Java のログ記録	143
	埋め込み認証クライアント (EAT) のログ記録	144
	認証サービス (AT) のログ記録	144
	vssat のログ記録	144
	NetBackup プロキシヘルパーのログ記録	145
	オリジネータ ID 486	145
	NetBackup プロキシトンネルのログ記録	146
	オリジネータ ID 490	146
	PBX のログ	147
	ベリタステクニカルサポートへの安全な通信のログの送信	148

第 11 章	スナップショット技術	151
	Snapshot Client のバックアップ	151
	VMware バックアップ	153
	スナップショットバックアップおよび Windows Open File Backup	157
第 12 章	ログの場所	161
	acsssi のログ	162
	bpbackup のログ	162
	bpbkar のログ	163
	bpbrm のログ	163
	bpcd のログ	164
	bpcompatd のログ	164
	bpdbm のログ	165
	bpjobd のログ	165
	bprd のログ	166
	bprestore のログ	166
	bptestnetconn ログ	166
	bptm のログ	167
	daemon のログ	167
	ltid のログ	168
	nbemm のログ	168
	nbjm のログ	169
	nbpem のログ	169
	nbproxy のログ	170
	nbrb のログ	170
	NetBackup Web サービスのログ記録	171
	NetBackup Web サーバー証明書のログ記録	171
	PBX のログ	173
	reqlib のログ	173
	robots のログ	174
	tar ログ	174
	txxd および txxcd のログ	175
	vnetd のログ	175
第 13 章	Java ベースの管理コンソールのログ記録	177
	Java ベースの管理コンソールのログ記録について	177
	Java ベースの管理コンソールのログ記録プロセスフロー	178
	Java ベースの管理コンソールと bpjava-* 間におけるセキュアなチャンネル の設定	179
	Java ベースの管理コンソールと nbsl または nbvault 間におけるセキュア なチャンネルの設定	180

NetBackup サーバーとクライアントでの Java ベースの管理コンソールの
ログ記録に関する設定 181

NetBackup がインストールされていない Windows コンピュータでの Java
ベースのリモート管理コンソールのログ記録 182

Java GUI の問題をトラブルシューティングするときのログの設定と収集
..... 182

ログ記録を元に戻す操作 184

索引 186

ログの使用

この章では以下の項目について説明しています。

- ログについて
- UNIX システムログについて
- NetBackup でのログの保持について
- 統合ログとレガシーログのサイズの制限について
- 統合ログについて
- レガシーログについて
- グローバルログレベルについて
- クライアントのログの保持制限の設定
- Windows のイベントビューアのログオプション
- NetBackup 管理コンソールのエラーメッセージのトラブルシューティング

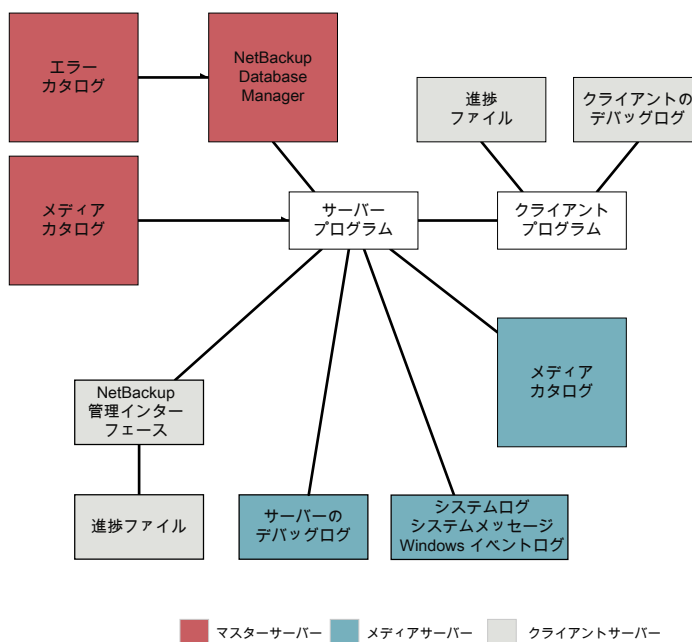
ログについて

NetBackup で使用される様々なログとレポートは、発生した問題のトラブルシューティングに役立ちます。

ユーザーは、ログとレポートの情報がシステム上のどこにあるかを把握しておく必要があります。

図 1-1 に、クライアントおよびサーバー上でのログとレポート情報の場所、およびこれらの情報を利用可能にするプロセスを示します。

図 1-1 NetBackup Enterprise システムのログ



この図に示すプログラムとデーモンについて説明する機能概要を確認することができます。

また、NetBackup レポートを使って問題のトラブルシューティングに役立てることができます。NetBackup レポートは状態とエラーについての情報を提供します。レポートを実行するには、NetBackup 管理コンソールを使用します。

<http://www.veritas.com/docs/DOC5332>のレポートに関する情報を参照してください。

メモ: NetBackup ログのログエントリの形式は、予告なしに変更される場合があります。

UNIX システムログについて

NetBackup サーバーのデーモンおよびプログラムによって、syslogd を介して情報がログに書き込まれる場合があります。その後、syslogd によってメッセージが表示されるか、または情報が適切なシステムログやコンソールログに書き込まれます。

UNIX では、NetBackup で syslogd を使用して、ロボットおよびネットワークのエラーが自動的にシステムログに書き込まれます。Windows では、NetBackup によって、ロボットおよびドライブのエラーがイベントビューアのアプリケーションログに記録されます。ど

らのオペレーティングシステムでも、ロボットによって制御されているドライブの状態 (起動状態および停止状態) が変化すると、ログのエントリも追加されます。

メモ: HP-UX では、sysdiag ツールを使用して、ハードウェアのエラーに関する追加情報を入手できる場合があります。

システムログに NetBackup による追加のログ記録を有効にするには、次のいずれかのコマンド使用してください。

- デバイス管理プロセスを起動する ltid コマンドを使用します。ltid コマンドに -v オプションを指定すると、このコマンドによって起動されるすべてのデーモンで -v オプションが有効になります。
- 特定のデーモンを起動するコマンド (acsd -v など) を使用します。

UNIX では、デーモンの起動に使用するコマンドに詳細オプション (-v) を指定して、システムログに対するデバッグログを有効にします。

ltid またはロボットソフトウェアのトラブルシューティングを行うには、システムのログを有効にしておく必要があります。システムログの設定については、syslogd(8) のマニュアルページを参照してください。エラーは LOG_ERR、警告のログは LOG_WARNING と記録されます。また、デバッグ情報は LOG_NOTICE と記録されます。facility の形式は [daemon] です。

システムログメッセージのシステム上の場所については、syslogd のマニュアルページを参照してください。

NetBackup でのログの保持について

このセクションでは、ログの要件に応じてログを再利用または削除するときに役に立つ NetBackup のさまざまなログの保持オプションについて説明します。

メモ: 次の場所にあるログを使って、NetBackup のログ削除動作を確認できます。

Windows の場合: `install_path\NetBackup\logs\nbutils`

UNIX の場合: `/usr/opensv/logs/nbutils`

表 1-1 NetBackup のログの保持オプション

ログの保持オプション	このオプションは以下の目的で使 用します。	参照リンク
次までログを保持する: GB (Keep logs up to GB)	統合ログとレガシーログのサイズを制限しま す。 NetBackup プロセス全体のログサイズが設 定された値に達すると、古いログが削除され ます。 このオプションは、[NetBackup 管理コンソ ール (Administration Console)]>[NetBackup の管理 (Management)]>[ホストプロパティ (Host Properties)]>[ログ (Logging)]ダイ アログで利用できます。	p.13 の「 統合ログとレガシーログのサイズの制限に ついて 」を参照してください。
NumberOfLogFiles	NetBackup プロセスについて、保持する統 合ログファイルの数を制限します。 ログファイルの数がこの設定値を超えると、 最も古いログファイルがログクリーンアップ時 に削除対象になります。 このオプションは、コマンドラインインター フェースを使って設定できます。	p.26 の「 統合ログファイルの再利用について 」を 参照してください。
MaxLogFileSizeKB とそ の他の vxlogcfg オプ ション	統合ログファイルが大きくなりすぎるのを防 ぎます。 設定したファイルサイズまたは時間に達した 場合、現在のログファイルは閉じられます。 ログプロセスの新しいログメッセージは、新し いログファイルに書き込まれます (ロールオー バーされます)。 これらのオプションは、コマンドラインインター フェースを使って設定できます。	p.25 の「 統合ログファイルのロールオーバーにつ いて 」を参照してください。
[ログを保持する日数 (Keep logs for days)]	NetBackup がレガシーログを保護する日数 を制限します。 この設定値に達すると、ログが削除されます。 [NetBackup 管理コンソール (Administration Console)]>[NetBackup の管理 (Management)]>[ホストプロパティ (Host Properties)]>[ログ (Logging)]ダイ アログボックス。	p.48 の「 レガシーログのサイズと保持の制限につ いて 」を参照してください。

ログの保持オプション	このオプションは以下の目的で使用します。	参照リンク
MAX_LOGFILE_SIZE と MAX_NUM_LOGFILES	保持するレガシーログのサイズとレガシーログファイルの数を制限します。 これらのオプションは、コマンドラインインターフェースを使って設定できます。	p.49 の「 レガシーログのローテーションの構成 」を参照してください。

メモ: 重要な NetBackup プロセスのログを有効にする前に、ログの保持オプションを確認し、適切なオプションを選択してください。

統合ログとレガシーログのサイズの制限について

NetBackup のログのサイズを制限するには、NetBackup 管理コンソールの[次までログを保持する: GB (Keep logs up to GB)]オプションでログサイズを指定します。NetBackup ログのサイズがこの設定値まで増加すると、古いログが削除されます。GB でログサイズを設定するには、値を GB でドロップダウンリストから選択できるチェックボックスにチェックマークを付けます。

メモ: NetBackup サーバーの場合、[次までログを保持する: GB (Keep logs up to GB)]オプションの推奨値は 25 GB 以上です。NetBackup クライアントの場合、推奨値は 5 GB 以上です。

p.11 の「[NetBackup でのログの保持について](#)」を参照してください。

[次までログを保持する: GB (Keep logs up to GB)]設定は、NetBackup 管理コンソールの[ログ (Logging)]ダイアログボックスにある[ホストプロパティ (Host Properties)]で指定できます。

メモ: 次のディレクトリを作成して、NetBackup のログ削除動作を確認できます。

Windows の場合: `install_path¥NetBackup¥logs¥nbutils`

UNIX の場合: `/usr/opensv/logs/nbutils`

統合ログについて

統合ログとレガシーログは NetBackup で使われるデバッグログの 2 つの形式です。NetBackup のすべてのプロセスは、これらのログの形式のいずれかを使います。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す。

統合ログ機能は、ログファイル名およびメッセージを共通の形式で作成します。これらのログファイルは、テキストエディタで簡単に表示することができません。統合ログファイルは、バイナリ形式のファイルで、一部の情報が関連するリソースファイルに含まれています。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。

p.18 の「[統合ログを使うエンティティのオリジネータ ID](#)」を参照してください。

レガシーログとは違って、統合ログではログ用のサブディレクトリを作成する必要はありません。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サブ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サブ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`

[NetBackup 管理コンソール (NetBackup Administration Console)]でログを管理できます。左ペインで、[NetBackup の管理 (NetBackup Management)]>[ホストプロパティ (Host Properties)]>[マスターサーバー (Master Servers)]または[メディアサーバー (Media Servers)]を展開します。変更するサーバーをダブルクリックします。ダイアログボックスの左ペインで、[ログ (Logging)]をクリックします。

また、次のコマンドの使用によって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。 p.35 の「vxlogcfg を使用した統合ログの設定の例」 を参照してください。
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。 p.32 の「vxlogmgr を使用した統合ログの管理の例」 を参照してください。
vxlogview	統合ログによって生成されたログを表示します。 p.31 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。

これらのコマンドは次のディレクトリに存在します。

Windows の `install_path¥NetBackup¥bin`
場合

UNIX の場合 `/usr/opensv/netbackup/bin`

これらのコマンドについて詳しくは『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

レガシーログの詳細情報を参照できます。

p.37 の「レガシーログについて」を参照してください。

NetBackup の統合ログの収集

この項では、例を使用して NetBackup の統合ログの収集方法を示します。

NetBackup の統合ログを収集する方法

- 1 次のコマンドを実行して /upload という名前のディレクトリを作成します。

```
# mkdir /upload
```

- 2 次のコマンドを実行して /upload ディレクトリに (NetBackup のみの) 統合ログをコピーします。

```
# vxlogmgr -p NB -c --dir /upload
```

出力例は次のとおりです。

```
Following are the files that were found:
```

```
/usr/opensv/logs/bmrsetup/51216-157-2202872032-050125-0000000.log
```

```
/usr/opensv/logs/nbem/51216-111-2202872032-050125-0000000.log
```

```
/usr/opensv/logs/nbrb/51216-118-2202872032-050125-0000000.log
```

```
/usr/opensv/logs/nbjm/51216-117-2202872032-050125-0000000.log
```

```
/usr/opensv/logs/nbpem/51216-116-2202872032-050125-0000000.log
```

```
/usr/opensv/logs/nbsl/51216-132-2202872032-050125-0000000.log
```

```
Total 6 file(s)
```

```
Copying
```

```
/usr/opensv/logs/bmrsetup/51216-157-2202872032-050125-0000000.log
```

```
...
```

```
Copying
```

```
/usr/opensv/logs/nbem/51216-111-2202872032-050125-0000000.log ...
```

```
Copying
```

```
/usr/opensv/logs/nbrb/51216-118-2202872032-050125-0000000.log ...
```

```
Copying
```

```
/usr/opensv/logs/nbjm/51216-117-2202872032-050125-0000000.log ...
```

```
Copying
```

```
/usr/opensv/logs/nbpem/51216-116-2202872032-050125-0000000.log ...
```

```
Copying
```

```
/usr/opensv/logs/nbsl/51216-132-2202872032-050125-0000000.log ...
```

- 3 /upload ディレクトリに移動して、ディレクトリの内容を一覧表示します。

```
# cd /upload
ls
```

出力例は次のとおりです。

```
51216-111-2202872032-050125-00000000.log
51216-116-2202872032-050125-00000000.log
51216-117-2202872032-050125-00000000.log
51216-118-2202872032-050125-00000000.log
51216-132-2202872032-050125-00000000.log
51216-157-2202872032-050125-00000000.log
```

- 4 ログファイルに `tar` コマンドを実行します。

```
# tar -cvf file_name.logs ./*
```

統合ログメッセージの種類

統合ログファイルには、次の種類のメッセージが表示されます。

アプリケーションログ メッセージ アプリケーションログメッセージには、通知メッセージ、警告メッセージおよびエラーメッセージが含まれます。アプリケーションメッセージは、常に記録されます。無効化することはできません。このメッセージはローカライズされません。

アプリケーションメッセージの例を次に示します。

```
12/04/2015 15:48:54.101 [Application] NB
51216 nbjm 117 PID:5483 TID:14 File
ID:117 [reqid=-1446587750] [Info]
V-117-40 BPBRM pid = 17446
```


診断ログメッセージ 診断ログメッセージは、レガシーデバッグログメッセージと同等の統合ログです。このメッセージは、様々な詳細レベルで記録できます (レガシーログの詳細レベルと同様です)。このメッセージはローカライズされます。

診断メッセージは `vxlogcfg` コマンドを使用して無効にすることができます。

診断メッセージの例を次に示します。

```
12/04/2015 15:48:54.608 [Diagnostic] NB
51216 nbjm 117 PID:5483 TID:14 File
ID:117 [No context] 3 V-117-298
[JobInst_i::requestResourcesWithTimeout]
callback object timeout=600
```

デバッグログメッセージ デバッグログメッセージは、主にベリタス社の技術者が使用します。診断メッセージと同様に、様々な詳細レベルで記録できます。このメッセージはローカライズされません。

デバッグメッセージは `vxlogcfg` コマンドを使用して無効にすることができます。

デバッグメッセージの例を次に示します。

```
12/04/2015 15:48:56.982 [Debug] NB
51216 nbjm 117 PID:5483 TID:14 File
ID:117 [jobid=2 parentid=1] 1
[BackupJob::start()] no pending proxy
requests, start the job
```

統合ログのファイル名の形式

統合ログでは、ログファイルの名前に標準化された形式を使用します。次にログファイル名の例を示します。

```
/usr/opencv/logs/nbpem/51216-116-2201360136-041029-0000000000.log
```

表 1-2 に、ログファイル名の各部分の説明を示します。

表 1-2 統合ログのファイル名の形式の説明

例	説明	詳細
51216	product ID (製品 ID)	製品を識別します。NetBackup プロダクト ID は 51216 です。プロダクト ID はエンティティ ID とも呼ばれています。

例	説明	詳細
116	オリジネータ ID	ログを記録したエンティティ(プロセス、サービス、スクリプト、他のソフトウェアなど)を識別します。番号 116 は、nbpem プロセス (NetBackup Policy Execution Manager) のオリジネータ ID です。
2201360136	ホスト ID	ログファイルを作成したホストを識別します。ログファイルが移動されていないかぎり、この ID はログファイルが存在するホストを表します。
041029	日付	ログが記録された日付を YYMMDD の形式で示します。
0000000000	ローテーション	特定のオリジネータごとのログファイルのインスタンス番号を示します。ロールオーバー番号 (ローテーション) はログファイルのインスタンスを示します。デフォルトでは、ログファイルはファイルサイズに基づいて別のファイルに書き換えられます (ローテーションが行われます)。このオリジネータで、ログファイルが最大サイズに達し、新しいログファイルが作成されると、この新しいファイルには 0000000001 が設定されます。 p.25 の「統合ログファイルのロールオーバーについて」 を参照してください。

ログ構成ファイルはオリジネータ ID のログファイルが書き込まれるディレクトリの名前を指定します。これらのディレクトリとディレクトリが保持するログファイルは、次に記載されているものを除き、次のディレクトリに書き込まれます。

[p.18 の「統合ログを使うエンティティのオリジネータ ID」](#)を参照してください。

Windows の場合 `install_path¥NetBackup¥logs`

UNIX の場合 `/usr/opensv/logs`

統合ログを使うエンティティのオリジネータ ID

多くのサーバープロセス、サービス、およびライブラリでは統合ログを使用します。UNIX クライアントと Windows クライアントも統合ログを使用します。オリジネータ ID (OID) は NetBackup のプロセス、サービス、ライブラリに対応します。

OID はプロセス、サービス、またはライブラリを識別します。プロセスは自身のログファイルにエントリを作成します。プロセスは、同じファイルに同様にエントリを作成する、一意の OID を持つライブラリを呼び出すことができます。このため、ログファイルはさまざまな OID のエントリを含む場合があります。複数のプロセスで同じライブラリを使うことができるため、ライブラリの OID が複数の異なるログファイルに出力されることがあります。

[表 1-3](#) に統合ログを使う NetBackup サーバーと NetBackup クライアントのプロセス、サービス、ライブラリを示します。

表 1-3 統合ログを使うサーバーエンティティのオリジネータ ID

オリジネータ ID	エンティティ	説明
18	nbatd	認証サービス (nbatd) は、ユーザーの ID を検証し、クレデンシャルを発行するサービス (デーモン) です。これらのクレデンシャルは Secure Sockets Layer (SSL) 通信で使われます。 (nbatd) ディレクトリは <code>usr/netbackup/sec/at/bin</code> ディレクトリ (UNIX の場合) または <code>install_path¥NetBackup¥sec¥at¥bin</code> ディレクトリ (Windows の場合) の下に作成されます。
103	pbx_exchange	PBX (Private Branch Exchange) サービスは、Veritas 製品サービスに接続されるファイアウォール外部のクライアントへのシングルポートアクセスを可能にします。サービス名は <code>VRTSpbx</code> です。ログは、 <code>/opt/VRTSpbx/log</code> (UNIX の場合) または <code>install_path¥VxPBX¥log</code> (Windows の場合) に書き込まれます。PBX プロダクト ID は 50936 です。
111	nbemm	Enterprise Media Manager (EMM) は NetBackup のデバイスとメディアの情報を管理する NetBackup サービスです。マスターサーバー上でのみ実行されます。
116	nbpem	nbpem (NetBackup Policy Execution Manager) はポリシーおよびクライアントタスクを作成し、ジョブの実行予定時間を決定します。マスターサーバー上でのみ実行されます。
117	nbjm	nbjm (NetBackup Job Manager) は、 Policy Execution Manager が送信したジョブを受け取り、必要なリソースを取得します。マスターサーバー上でのみ実行されます。
118	nbrb	NetBackup Resource Broker (nbrb) は、利用可能なリソースのキャッシュリストを保持します。このリストを使用して、バックアップまたはテープのリストアに必要な物理リソースと論理リソースを特定します。nbemm への SQL 呼び出しを開始し、データベースを更新し、割り当て情報を nbjm に渡します。マスターサーバー上でのみ実行されます。
119	bmrtd	NetBackup BMR (Bare Metal Restore) マスターサーバーデーモンです。
121	bmrsavecfg	BMR Save Configuration は、 NetBackup サーバーではなくクライアントで実行されるデータ収集ユーティリティです。
122	bmrcl	BMR Client Utility は、 BMR ブートサーバーで起動され、リストアを実行中のクライアントで実行されます。 UNIX クライアントはリストア中にこのユーティリティを使用して BMR マスターサーバーと通信します。
123	bmrsv	BMR Server Utility です。

オリジネータ ID	エンティティ	説明
124	bmrcreatefloppy	フロッピーディスクを作成する BMR コマンドは BMR Create Floppy ユーティリティを使用します。このユーティリティは BMR ブートサーバーで実行され、Windows 専用です。
125	bmrstrt	BMR Create SRT ユーティリティは共有リソースツリーを作成します。BMR ブートサーバーで実行されます。
126	bmrprep	BMR Prepare to Restore ユーティリティは、クライアントのリストアのために BMR サーバーを準備します。
127	bmrsetup	BMR Setup Commands ユーティリティは BMR のインストール、構成、アップグレード処理をセットアップします。
128	bmrcommon	BMR Libraries and Common Code カタログは BMR ライブラリにログメッセージを提供します。
129	bmrconfig	BMR Edit Configuration ユーティリティはクライアント構成を修正します。
130	bmrcreatepkg	BMR Create Package ユーティリティはリストア操作のために BMR マスターサーバーに Windows ドライバ、Service Pack、修正プログラムを追加します。
131	bmrst	BMR Restore ユーティリティは Windows の BMR クライアントをリストアします。Windows システムでのみ、リストアを実行中のクライアントで実行されます。
132	nbsl	NetBackup Service Layer は NetBackup の GUI と NetBackup のロジック間の通信を簡易化します。nbsl は、NetBackup の複数の環境を管理し、監視するアプリケーションである、NetBackup OpsCenter を実行するために必要です。このプロセスは、マスターサーバー上だけで実行されます。
134	ndmpagent	NDMP エージェントデーモンは NDMP のバックアップとリストアを管理します。メディアサーバー上で実行されます。
137	ライブラリ	libraries は NetBackup ライブラリのログレベルを制御します。アプリケーションメッセージおよび診断メッセージはユーザーが、デバッグメッセージは Veritas の技術者が使用します。
140	mmui	メディアサーバーのユーザーインターフェースは EMM (Enterprise Media Manager) のために使われます。
142	bmrepadm	BMR External Procedure はリストア操作の間に使われる BMR 外部プロセスを管理します。
143	mds	EMM Media and Device Selection プロセスは EMM (Enterprise Media Manager) のメディア選択コンポーネントとデバイス選択コンポーネントを管理します。

オリジネータ ID	エンティティ	説明
144	da	EMM Device Allocator は共有ドライブのために使われます。
146	NOMTRS	NetBackup OpsCenter レポートサービスは NetBackup OpsCenter の一部です。
147	NOMClient	NetBackup OpsCenter Client は NetBackup OpsCenter の一部です。
148	NOMServer	NetBackup OpsCenter Server は NetBackup OpsCenter の一部です。
151	ndmp	ndmp (NDMP メッセージログ) は NDMP プロトコルメッセージ、avrd、ロボットプロセスを処理します。
154	bmrovradm	BMR Override Table Admin Utility は Bare Metal Restore のカスタム上書き機能を管理します。
156	ace	NBACE プロセスは、CORBA インターフェースを使用する任意のプロセス用の (ACE/TAO) CORBA コンポーネントのログレベルを制御します。デフォルトのレベルは 0 (重要なメッセージのみをログに記録) です。このログ機能は、ベリタス社の技術者が使用します。 ベリタス社テクニカルサポートからログレベルを上げるように指示された場合、オリジネータ ID 137 のデバッグレベルを 4 以上に上げます。 警告: デバッグのログレベルが 0 より大きい場合、大量のデータが生成されます。
158	ncfrai	NetBackup クライアントのリモートアクセスインターフェース。
159	ncftfi	NetBackup クライアントのトランスポート。
163	nbsvcmon	NetBackup Service Monitor はローカルコンピュータで実行される NetBackup サービスを監視し、異常終了したサービスの再起動を試行します。
166	nbvault	NetBackup Vault Manager は NetBackup Vault を管理します。すべての NetBackup Vault の操作中は nbvault を NetBackup Vault サーバー上で実行している必要があります。
178	dsm	DSM (Disk Service Manager) は、ディスクストレージおよびディスクストレージユニット上の設定操作および取得操作を実行します。
199	nbftsrvr	ファイバートランスポート (FT) サーバープロセスは、NetBackup ファイバートランスポート用に設定したメディアサーバー上で実行されます。FT 接続のサーバー側で、nbftsrvr は、データフローの制御、SCSI コマンドの処理、データバッファの管理、および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を行います。nbftsrvr は SAN クライアントの一部です。

オリジネータ ID	エンティティ	説明
200	nbftclnt	FT (ファイバートランスポート) クライアントプロセスは SAN クライアントの一部で、クライアント上で実行されます。
201	fsm	FSM (FT Service Manager) は EMM (Enterprise Media Manager) のコンポーネントで、SAN クライアントの一部です。
202	stssvc	このストレージサービスはストレージサーバーを管理し、メディアサーバー上で実行されます。
210	ncfive	NetBackup クライアントの Exchange ファイアドリルウィザード。
219	rsrcevtmgr	Resource Event Manager (REM)。nbemm 内部で実行される CORBA でロード可能なサービスです。REM は、Disk Polling Service と連携して、空き領域およびボリュームの状態を監視し、ディスクに空きがない状態を検出します。
220	dps	NetBackup クライアントの Disk Polling Service。
221	mpms	MPMS (Media Performance Monitor Service) は、RMMS 内のすべてのメディアサーバー上で実行され、ホストの CPU 負荷および空きメモリの情報を収集します。
222	nbrmms	RMMS (Remote Monitoring and Management Service) は、EMM でメディアサーバー上のディスクストレージの検出および構成に使用するコンジットです。
226	nbstserv	このストレージサービスは、ライフサイクルイメージの複製操作を制御します。
230	rdsm	RDMS (Remote Disk Service Manager) インターフェースは Remote Manager and Monitor Service で動作します。RDMS はメディアサーバー上で動作します。
231	nbevtmgr	Event Manager Service は、システムの連携のために非同期イベント管理サービスを提供します。
248	bmrlauncher	Windows BMR Fast Restore イメージの BMR Launcher Utility は、BMR 環境を構成します。
254	SPSV2RecoveryAsst	NetBackup クライアントの Recovery Assistant (SharePoint Portal Server 用)。
261	aggs	アーティファクトジェネレーターによって生成されたソース。
263	wingui	Windows 版 NetBackup 管理コンソール。
271	nbecmsg	レガシーエラーコード。

オリジネータ ID	エンティティ	説明
272	expmgr	Expiration Manager はストレージライフサイクル操作の容量管理およびイメージの期限切れを処理します。
286	nbkms	暗号化キーマネージメントサービスは、メディアサーバーの NetBackup Tape Manager プロセスに暗号化キーを提供する、マスターサーバーベースの対称キー管理サービスです。
293	nbaudit	NetBackup Audit Manager。
294	nbauditmsgs	NetBackup 監査メッセージ。
309	ncf	NetBackup Client Framework。
311	ncfnbservercom	NetBackup クライアント/サーバー通信。
317	ncfbedspi	NetBackup クライアント Beds プラグイン。
318	ncfwinpi	NetBackup クライアント Windows プラグイン。
321	dbaccess	NetBackup Relational Database アクセスライブラリ。
348	ncforaclepi	NetBackup クライアント Oracle プラグイン。
351	ncflbc	ライブ参照クライアントです。
352	ncfgre	個別リストアです。
355	ncftarpi	NetBackup TAR プラグイン。
356	ncfvxmspi	NetBackup クライアント VxMS プラグイン。
357	ncfnbrestore	NetBackup リストア。
359	ncfnbbrowse	NetBackup ブラウザ。
360	ncforautil	NetBackup クライアント Oracle ユーティリティ。
361	ncfdb2pi	NetBackup クライアント DB2 プラグイン。
362	nbars	NetBackup Agent Request Service。
363	dars	データベースエージェント要求によるサーバーのプロセスコールです。
366	ncfnbcs	NetBackup Client Service。
369	impmgr	NetBackup インポートマネージャ。
371	nbim	Indexing Manager。

オリジネータ ID	エンティティ	説明
372	nbhsm	保留サービスです。
375	ncfnbusearchserverpi	NetBackup クライアント検索サーバープラグイン。
377	ncfnbdiscover	NetBackup クライアントコンポーネント検出。
380	ncfnbquiescence	NetBackup クライアントコンポーネントの静止または静止解除。
381	ncfnbdboffline	NetBackup クライアントコンポーネントのオフライン化またはオンライン化。
386	ncfvmwarepi	NetBackup NCF VMware プラグイン。
387	nbrntd	NetBackup Remote Network Transport。複数のバックアップストリームが同時に実行された場合、Remote Network Transport Service はログファイルに大量の情報を書き込みます。このような場合、OID 387 のログレベルを 2 以下に設定します。 p.52 の「ログレベルの変更」 を参照してください。
395	stsem	STS Event Manager です。
396	nbutils	NetBackup ユーティリティ。
400	nbdisco	NetBackup Discovery。
401	ncfmssqlpi	NetBackup クライアント MSSQL プラグイン。
402	ncfexchangeapi	NetBackup クライアント Exchange プラグイン。
403	ncfsharepointpi	NetBackup クライアント SharePoint プラグイン。
412	ncffilesyspi	NetBackup クライアントファイルシステムプラグイン。
480	libvcloudsuite	NetBackup vCloudSuite ライブラリ。
486	nbpxyhelper	vnetd プロキシヘルパープロセス。
490	nbpxytnl	vnetd プロキシの HTTP トンネル。
491	ncfcloudpi	NetBackup クラウド検出プラグイン
497	ncfcloudpi	NetBackup クラウド検出プラグイン

統合ログファイルの場所の変更について

統合ログファイルは、大量のディスク領域を使用する可能性があります。必要に応じて、次を入力して異なる場所にそれらを書き込みます。

UNIX の場合

```
/usr/opensv/netbackup/bin/vxlogcfg -a -p NB -o Default -s LogDirectory=new_log_path
```

ここで、new_log_path は、/bigdisk/logs などのフルパスです。

Windows の場合

```
install_path¥NetBackup¥bin¥vxlogcfg -a -p NB -o Default -s LogDirectory=new_log_path
```

ここで、new_log_path は、D:¥logs などのフルパスです。

統合ログファイルのロールオーバーについて

ログファイルが大きくなりすぎないようにするため、またはログファイル作成のタイミングまたは頻度を制御するために、ログのロールオーバーオプションを設定することができます。設定したファイルサイズまたは時間に達した場合、現在のログファイルは閉じられます。ログプロセスの新しいログメッセージは、新しいログファイルに書き込まれます (ロールオーバーされます)。

p.11 の「[NetBackup でのログの保持について](#)」を参照してください。

ファイルサイズ、時刻、または経過時間に基づいて実行されるように、ログファイルのロールオーバーを設定できます。で記述されているオプションを指定して vxlogcfg 表 1-4 コマンドを使用して、条件を設定します。

表 1-4 統合ログファイルのロールオーバーを制御する vxlogcfg オプション

オプション	説明
MaxLogFileSizeKB	RolloverMode に FileSize を設定した場合に、ログファイルが切り替えられる最大サイズを指定します。
RolloverAtLocalTime	RolloverMode に LocalTime を設定した場合に、ログファイルがロールオーバーされる時刻を指定します。
RolloverPeriodInSeconds	RolloverMode に Periodic を設定した場合に、ログファイルがロールオーバーされるまでの時間を秒数で指定します。
MaxLogFileSizeKB または RolloverAtLocalTime	ファイルサイズ制限またはローカル時間制限のいずれかが先に達したときは、いつでもログファイルのロールオーバーが実行されることを指定します。 コマンドの例: vxlogcfg -a -p 51216 -g Default MaxLogFileSizeKB=256 RolloverAtLocalTime=22:00

オプション	説明
MaxLogFileSizeKB または RolloverPeriodInSeconds	ファイルサイズ制限または期間制限のいずれかが先に達したときは、いつでもログファイルのロールオーバーが実行されることを指定します。

vxlogcfg の詳しい説明は、『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

デフォルトでは、ログファイルは、**51200 KB** のファイルサイズ単位でロールオーバーします。ログファイルのサイズが **51200 KB** に達すると、そのファイルは閉じられ、新しいログファイルが開かれます。

次の例では、**NetBackup (prodid 51216)** のロールオーバーモードを **Periodic** に設定しています。

```
# vxlogcfg -a --prodid 51216 --orgid 116 -s RolloverMode=Periodic  
RolloverPeriodInSeconds=86400
```

前の例は **RolloverMode** オプションを指定して **vxlogcfg** コマンドを使います。nbpem (オリジネータ **ID 116**) のロールオーバーモードを **Periodic** に設定します。また、nbpem のログファイルの次のロールオーバーが実施されるまでの間隔を **24 時間 (86400 秒)** に設定しています。

ログファイルのロールオーバーが行われ、ローテーション ID が増加しているファイル名の例を次に示します。

```
/usr/opensv/logs/nbpem/51216-116-2201360136-041029-0000000000.log  
  
/usr/opensv/logs/nbpem/51216-116-2201360136-041029-0000000001.log  
  
/usr/opensv/logs/nbpem/51216-116-2201360136-041029-0000000002.log
```

さらに、ログファイルのローテーションを次で使うことができます。

- 統合ログ機能を使うサーバープロセスのログ
p.18 の「[統合ログを使うエンティティのオリジネータ ID](#)」を参照してください。
- 特定のレガシーログ
- Bare Metal Restore プロセス **bmrsavecfg** が作成する統合ログファイル

統合ログファイルの再利用について

最も古いログファイルの削除は再利用と呼ばれます。統合ログファイルを次のように再利用できます。

p.11 の「[NetBackup でのログの保持について](#)」を参照してください。

ログファイルの数を制限する

NetBackup が保持するログファイルの最大数を指定します。ログファイルの数が最大数を超えると、最も古いログファイルがログクリーンアップ時に削除対象になります。vxlogcfg コマンドの NumberOfLogFiles オプションでその数を定義します。

次の例では、NetBackup (プロダクト ID 51216) の各統合ログオリジネータに許可されるログファイルの最大数を 8000 に設定しています。特定のオリジネータのログファイルの数が 8000 を超えると、最も古いログファイルがログクリーンアップ時に削除対象になります。

```
# vxlogcfg -a -p 51216 -o ALL -s  
NumberOfLogFiles=8000
```

p.35 の「[vxlogcfg を使用した統合ログの設定の例](#)」を参照してください。

ログファイルが保持される日数を指定する

[ログを保持する日数 (Keep logs for days)]プロパティを使って、ログが保持される最大日数を指定します。最大日数に達すると、統合ログとレガシーログは自動的に削除されます。

NetBackup 管理コンソールの左ペインで、[NetBackup の管理 (Management)]>[ホストプロパティ (Host Properties)]>[マスターサーバー (Master Servers)]を展開します。変更するサーバーをダブルクリックします。新しいダイアログボックスが表示されます。左ペインで[ログ (Logging)]、[ログを保持する日数 (Keep logs for days)]をクリックします。

ログファイルを明示的に削除する

リサイクルを開始し、ログファイルを削除するには、次のコマンドを実行します。

```
# vxlogmgr -a -d
```

vxlogmgr によってファイルを手動で削除または移動できない場合は、[ログを保持する (Keep logs)]プロパティに従って、古い統合ログおよびレガシーログが削除されます。

p.32 の「[vxlogmgr を使用した統合ログの管理の例](#)」を参照してください。

vxlogcfg LogRecycle オプションがオン (true) の場合、統合ログの[ログを保持する日数 (Keep logs for days)]設定は無効になります。この場合、統合ログファイルは、特定のオリジネータのログファイルの数が vxlogcfg コマンドの NumberOfLogFiles オプションに指定した数を超えると、削除されます。

vxlogview コマンドを使用した統合ログの表示について

vxlogview コマンドを使用すると、統合ログ機能で作成されたログを表示できます。これらのログは次のディレクトリに保存されます。

UNIX の場合 `/usr/opensv/logs`

Windows の場合 `install_path¥NetBackup¥logs`

統合ログファイルは、レガシーログで書き込まれたファイルとは異なり、簡単にテキストエディタで表示することはできません。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。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。

NetBackup ログファイルと PBX ログファイルを表示するために vxlogview を使えます。

vxlogview コマンドを使って PBX のログを表示するには次のことを行います。

- 権限があるユーザーであることを確認します。UNIX と Linux の場合は、root 権限を持たなければなりません。Windows の場合は、管理者権限を持たなければなりません。
- PBX プロダクト ID を指定するには、vxlogview コマンドラインでパラメータとして -p 50936 を入力します。

vxlogview はすべてのファイルを検索するため、低速の処理になる場合があります。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結果をより速く表示する方法の例については、次のトピックを参照してください。

vxlogview コマンドで使用される問い合わせ文字列について

vxlogview コマンドを使用すると、統合ログ機能で生成されたログを表示できます。

vxlogview コマンドは次のオプションを含んでいます。 -w (- -where) *QueryString*

QueryString は、データベースの WHERE 句と同様のテキスト表現です。問い合わせ文字列式を使用して、統合ログ機能システムからログエントリを検索します。式は、関係演算子、整数型定数、文字列型定数と、単一の値に評価される複数のログフィールド名の組み合わせです。式は、AND や OR などの論理演算子を使用して、グループ化することもできます。

サポートされている比較演算子は、次のとおりです。

< より小さい

> より大きい

<= 以下

>= 以上

= 等しい

!= 等しくない

サポートされている論理演算子は、次のとおりです。

&& 論理 AND

|| 論理 OR

表 1-5 に、特定のフィールドのデータデータ型、およびその説明と例を示します。複数の例がリストにあるとき、例は両方とも同じ結果になります。

表 1-5 フィールドのデータ型

フィールド名	型	説明	例
PRODID	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。	PRODID = 51216 PRODID = '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
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 = '11/27/04 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'

フィールド名	型	説明	例
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うち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'

問い合わせ文字列を書く場合、次を考慮します。

大文字と小文字の区別 フィールド名、重大度の種類およびメッセージの種類は大文字と小文字が区別されません。たとえば、次のエントリは有効です。

- sev = info
- msgtype = diag

文字列の定数 文字列の定数は、一重引用符で囲んで指定する必要があります。たとえば、PRODID = 'NBU' と指定します。

日付 開始日と終了日は次の形式で指定できます。

- 地域ごとの短い日付表示形式に対応する文字列の定数
- 1970 年 1 月 1 日午前 0 時から経過した秒数の UNIX long 型の整数。

表 1-6 に、問い合わせ文字列の例を示します。

表 1-6 問い合わせ文字列の例

例	説明
<pre>(PRODID == 51216) && ((PID == 178964) ((STDATE == '2/5/15 09:00:00 AM') && (ENDATE == '2/5/15 12:00:00 PM')))</pre>	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。
<pre>((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')))</pre>	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。
<pre>(STDATE <= '04/05/15 0:0:0 AM')</pre>	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 Veritas 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。

表 1-7 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	<pre>vxlogview -p 51216 -d all</pre>
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。 <pre>vxlogview --prodid 51216 --display D,T,m,x</pre>
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。 <pre># vxlogview -o 116 -t 00:20:00</pre>
特定の期間からのログメッセージの表示	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。 <pre># vxlogview -o nbpem -b "05/03/15 06:51:48 AM" -e "05/03/15 06:52:48 AM"</pre>

項目	例
より速い結果の表示	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。 <pre># vxlogview -i nbpem</pre> <code>vxlogview -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、<code>vxlogview</code> の結果が速く戻されます。一方、<code>vxlogview -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。 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、<code>vxlogview</code> 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。 <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。
ジョブ ID の検索	特定のジョブ ID のログを検索できます。 <pre># vxlogview -i nbpem grep "jobid=job_ID"</pre> <code>jobid=</code>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。 ジョブ ID の検索には、任意の <code>vxlogview</code> 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。<code>jobid=job_ID</code> 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。

`vxlogview` コマンドの詳細については、『NetBackup コマンドリファレンスガイド』を参照してください。ガイドは次の URL から入手できます。

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

vxlogmgr を使用した統合ログの管理の例

次の例は、`vxlogmgr` コマンドを使って統合ログファイルを管理する方法を示します。ログファイルの管理は、ログファイルの削除や移動などの操作を含んでいます。

表 1-8 vxlogmgr コマンドの使用例

項目	例
ログファイルの表示	nbrb サービスのすべての統合ログファイルを表示します。 <pre># vxlogmgr -s -o nbrb /usr/opensv/logs/nbrb/51216-118-1342895976-050503-00.log /usr/opensv/logs/nbrb/51216-118-1342895976-050504-00.log /usr/opensv/logs/nbrb/51216-118-1342895976-050505-00.log Total 3 file(s)</pre>
最も古いログファイルの削除	<Check Alignment of PHs> vxlogcfg の NumberOfLogFiles オプションに 1 が設定されている場合、次の例を実行すると、nbrb サービスのログファイルのうち、最も古い 2 つのログファイルが削除されます。 <pre># vxlogcfg -a -p 51216 -o nbrb -s NumberOfLogFiles=1 # vxlogmgr -d -o nbrb -a Following are the files that were found: /usr/opensv/logs/nbrb/51216-118-1342895976-050504-00.log /usr/opensv/logs/nbrb/51216-118-1342895976-050503-00.log Total 2 file(s) Are you sure you want to delete the file(s)? (Y/N): Y Deleting /usr/opensv/logs/nbrb/51216-118-1342895976-050504-00.log ... Deleting /usr/opensv/logs/nbrb/51216-118-1342895976-050503-00.log ...</pre>
最も新しいログファイルの削除	NetBackup によって 15 日以内に作成されたすべての統合ログファイルを削除します。 <pre># vxlogmgr -d --prodid 51216 -n 15</pre> ログファイルを削除する前に、それらのログファイルを必ず切り替え (ローテーション) します。
特定のオリジネータのログファイルの削除	オリジネータが nbrb のすべての統合ログファイルを削除します。 <pre># vxlogmgr -d -o nbrb</pre> ログファイルを削除する前に、それらのログファイルを必ず切り替え (ローテーション) します。
すべてのログファイルの削除	NetBackup のすべての統合ログファイルを削除します。 <pre># vxlogmgr -d -p NB</pre> ログファイルを削除する前に、それらのログファイルを必ず切り替え (ローテーション) します。

項目	例
ログファイル数の管理	vxlogmgr コマンドを、vxlogcfg コマンドの NumberOfLogFiles オプションと組み合わせて使用することで、ログファイルを手動で削除できます。 たとえば、NumberOfLogFiles オプションが 2 に設定され、10 の統合ログファイルがあり、クリーンアップが実行されていないとします。次を入力することで、最も新しい 2 つのログファイルを保持し、他のすべてのオリジネータを削除します。 <pre># vxlogmgr -a -d</pre> 次のコマンドでは、すべての PBX オリジネータの 2 つの最新のログファイルが保持されます。 <pre># vxlogmgr -a -d -p ics</pre> 次のコマンドを実行すると、nbrb サービスの古いログファイルだけを削除します。 <pre># vxlogmgr -a -d -o nbrb</pre>
ディスク領域の使用状況の管理	cron ジョブなどで vxlogmgr -a -d コマンドを定期的に行うことで、ログを削除したり、統合ログが使用しているディスク領域を監視できます。 特定のオリジネータが使用するディスク領域は、次のようにして計算できます。 オリジネータの NumberOfFiles * オリジネータの MaxLogFileSizeKB 統合ログ機能を使用する合計ディスク領域は、それぞれのオリジネータが使用するディスク領域の合計です。すべてのオリジネータの NumberOfFiles 設定および MaxLogFileSizeKB 設定が変更されていない場合、統合ログ機能を使用する合計ディスク容量は次のとおりです。 オリジネータの数 * デフォルトの MaxLogFileSizeKB * デフォルトの NumberOfFiles vxlogcfg コマンドを使って、現在の統合ログ設定を表示します。 たとえば、次の条件を想定します。 ■ vxlogmgr -a -d -p NB が、1 時間に 1 回の cron ジョブに構成されている。 ■ すべてのオリジネータの MaxLogFileSizeKB および NumberOfFiles が、デフォルト設定のまま変更されていない。 ■ ホストのアクティブな NetBackup オリジネータの数は 10 です。(BMR も NDMP も実行していない NetBackup マスターサーバーに特有。) ■ MaxLogFileSizeKB のデフォルトが 51200 である。 ■ NumberOfFiles のデフォルトが 3 である。 統合ログ機能を使用する合計ディスク領域を計算するには、上記の式に例からの値を挿入します。結果として、次の処理が行われます。 10 * 51200 * 3 KB = 1,536,000 KB の追加のディスク領域が 1 時間ごとに使用されます。

vxlogmgr の詳しい説明は、『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

vxlogcfg を使用した統合ログの設定の例

vxlogcfg コマンドを使用してログレベルやロールオーバーの設定を変更できます。

vxlogcfg コマンドには次の性質があります。

- vxlogcfg コマンドでのみ、統合ログの診断メッセージおよびデバッグメッセージをオフに設定できます。レガシーログのメッセージの書き込みは、最小レベルには設定できますが、オフに設定することはできません。
- 絶対パスを指定する必要があります。相対パスを使わないでください。

次の例は、vxlogcfg コマンドを使って統合ログ機能の設定を構成する方法を示します。

表 1-9 vxlogcfg コマンドの使用例

項目	例
最大ログファイルサイズの設定	デフォルトでは、統合ログファイルの最大サイズは 51200 KB です。ログファイルのサイズが 51200 KB に達すると、そのファイルは閉じられ、新しいログファイルが開かれます。 MaxLogFileSizeKB オプションを使用して最大ファイルサイズを変更できます。次のコマンドでは、NetBackup 製品のデフォルトの最大ログサイズが 100000 KB に変更されます。 <pre># vxlogcfg -a -p 51216 -o Default -s MaxLogFileSizeKB=100000</pre> MaxLogFileSizeKB を有効にするには、RolloverMode オプションに FileSize を設定する必要があります。 <pre># vxlogcfg -a --prodid 51216 --orgid Default -s RolloverMode=FileSize</pre> MaxLogFileSizeKB は、オリジネータごとに設定できます。構成されていないオリジネータではデフォルト値が使用されます。次の例では、nbrb サービス (オリジネータ ID 118) のデフォルト値を上書きしています。 <pre># vxlogcfg -a -p 51216 -o nbrb -s MaxLogFileSizeKB=1024000</pre>

項目	例
ログの再利用の設定	次の例では、nbemm ログ (オリジネータ ID 111) に対して自動ログファイル削除を設定しています。 <pre># vxlogcfg -a --prodid 51216 --orgid 111 -s RolloverMode=FileSize MaxLogFileSizeKB=512000 NumberOfLogFiles=999 LogRecycle=TRUE</pre> この例では、nbemm ログのロールオーバーモードを FileSize に設定し、ログの再利用をオンに設定しています。ログファイルの数が 999 を超えると、最も古いログファイルが削除されます。例 5 に、ログファイルの数を制御する方法を示します。
デバッグレベルおよび診断レベルの設定	次の例は、プロダクト ID NetBackup (51216) のデフォルトのデバッグレベルおよび診断レベルを設定しています。 <pre># vxlogcfg -a --prodid 51216 --orgid Default -s DebugLevel=1 DiagnosticLevel=6</pre>

項目	例
統合ログ機能の設定の表示	次の vxlogcfg の例では、特定のオリジネータ (nbrb サービス) で有効になっている統合ログ機能の設定を表示する方法を示しています。出力に MaxLogFileSizeKB、NumberOfLogFiles および RolloverMode が含まれていることに注意してください。 <pre># vxlogcfg -l -o nbrb -p NB Configuration settings for originator 118, of product 51,216... LogDirectory = /usr/opensv/logs/nbrb/ DebugLevel = 1 DiagnosticLevel = 6 DynaReloadInSec = 0 LogToStdout = False LogToStderr = False LogToOslog = False RolloverMode = FileSize LocalTime LogRecycle = False MaxLogFileSizeKB = 51200 RolloverPeriodInSeconds = 43200 RolloverAtLocalTime = 0:00 NumberOfLogFiles = 3 OIDNames = nbrb AppMsgLogging = ON L10nLib = /usr/opensv/lib/libvxexticu L10nResource = nbrb L10nResourceDir = /usr/opensv/resources SyslogIdent = VRTS-NB SyslogOpt = 0 SyslogFacility = LOG_LOCAL5 LogFilePermissions = 664</pre>

vxlogcfg の詳しい説明は、『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

レガシーログについて

レガシーログと統合ログは **NetBackup** で使われるデバッグログの 2 つの形式です。**NetBackup** のすべてのプロセスは統合ログまたはレガシーログを使います。

p.13 の「[統合ログについて](#)」を参照してください。

レガシーデバッグログの場合、各プロセスが個別のログディレクトリにデバッグアクティビティのログファイルを作成します。**NetBackup** のレガシーデバッグログのディレクトリは次のディレクトリにあります。

Windows	<code>install_path¥NetBackup¥logs</code> <code>install_path¥Volmgr¥debug</code>
UNIX	<code>/usr/opensv/netbackup/logs</code> <code>/usr/opensv/volmgr/debug</code>

これらの最上位ディレクトリには、レガシーログを使用する **NetBackup** の各プロセスのディレクトリが含まれます。デフォルトでは、**NetBackup** は使用する可能性があるすべてのログディレクトリのサブセットのみを作成します。たとえば、デフォルトでは UNIX サーバーで次のディレクトリが作成されます。

- nbfp
- nbliveup
- nblogadm
- user_ops

レガシーログを使用するすべての **NetBackup** プロセスでログ記録を有効化するには、ログアシスタントを使用していない限り、ログファイルのディレクトリを新たに作成する必要があります。ログアシスタントについて詳しくは、『**NetBackup** 管理者ガイド Vol. 1』を参照してください。このガイドは、次の場所から入手できます。

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

p.44 の「サーバーのレガシーデバッグログのディレクトリ名」を参照してください。

p.46 の「メディアおよびデバイス管理のレガシーデバッグログのディレクトリ名」を参照してください。

次のバッチファイルを使用して、すべてのデバッグログディレクトリを一度に作成することができます。

- Windows の場合: `install_path¥NetBackup¥logs¥mklogdir.bat`
- UNIX の場合: `/usr/opensv/netbackup/logs/mklogdir`

`mklogdir` コマンドについて詳しくは『**NetBackup** コマンドリファレンスガイド』を参照してください。このガイドは、次の場所から入手できます。

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

ディレクトリが作成された後、**NetBackup** は各プロセスに関連付けられるディレクトリにログファイルを作成します。デバッグログファイルは、プロセスの起動時に作成されます。

ログファイルがあるサイズに達すると、NetBackup プロセスはそのファイルを閉じて新しいログファイルを作成します。

p.43 の「[レガシーログのファイル名の形式](#)」を参照してください。

NetBackup 状態収集デーモン (vmscd) でデバッグログを有効にするには、nbemm を起動する前に次のディレクトリを作成します。

Windows の場合 `install_path¥Volmgr¥debug¥vmscd¥`

UNIX の場合 `/usr/opensv/volmgr/debug/vmscd`

または、ディレクトリの作成後に vmscd を再起動します。

レガシーログを使う UNIX クライアントプロセス

多くの UNIX クライアントのプロセスでレガシーログが使用されます。UNIX クライアントでレガシーデバッグログを有効にするには、次のディレクトリに適切なサブディレクトリを作成します。

次のバッチファイルを使用して、すべてのデバッグログディレクトリを一度に作成することができます。

Windows の場合 `Install_path¥NetBackup¥Logs¥mklogdir.bat`

UNIX の場合 `/usr/opensv/netbackup/logs/mklogdir`

表 1-10 UNIX クライアントに適用されるレガシーデバッグログのディレクトリを示します。

表 1-10 レガシーログを使う UNIX クライアントプロセス

ディレクトリ	関連するプロセス
bp	メニュー方式のクライアントユーザーインターフェースプログラム。
bparchive	アーカイブプログラム。bp のデバッグにも使用できます。
bpbackup	バックアッププログラム。bp のデバッグにも使用できます。
bpbkcar	バックアップイメージの生成に使用されるプログラム。
bpcd	NetBackup Client デーモンまたは NetBackup Client Manager。
bpclimagelist	クライアントの NetBackup イメージまたはリムーバブルメディアの状態レポートを生成するコマンドラインユーティリティ。
bpclntcmd	NetBackup システムの機能のテストとファイバートランスポートサービスの有効化を行うコマンドラインユーティリティ。

ディレクトリ	関連するプロセス
bphdb	NetBackup データベースエージェントクライアントで、データベースをバックアップするためのスクリプトを起動するプログラム。 詳しくは、該当する NetBackup データベースエージェントの管理者ガイドを参照してください。
bpjava-msvc	NetBackup-Java アプリケーションのサーバー認証サービス。このサービスは、 NetBackup-Java インターフェースアプリケーションの起動中に、inetd によって起動されます。このプログラムによって、アプリケーションを起動したユーザーが認証されます。
bpjava-usvc	bpjava-msvc によって起動される NetBackup プログラム。 NetBackup-Java バックアップ、アーカイブおよびリストア (BAR) インターフェースを起動すると表示されるログオンダイアログボックスでログオンに成功すると起動されます。このプログラムによって、bpjava-msvc が実行されているホスト上の Java ベースのユーザーインターフェースから送信されるすべての要求が処理されます。
bplist	バックアップおよびアーカイブを実行されたファイルを表示するプログラム。bp をデバッグするのにも役立ちます。 NetBackup 7.6 以前のバージョンでは、bpclntcmd コマンドと bpclimagelist コマンドで bplist ディレクトリにデバッグログメッセージを送信します。 NetBackup 7.6 では、bpclntcmd と bpclimagelist はそれぞれ bpclntcmd と bpclimagelist のディレクトリにデバッグログメッセージを送信します。
bpmount	複数のデータストリームに対するローカルマウントポイントおよびワイルドカード拡張を決定するプログラム。
bporaexp	クライアントのコマンドラインプログラム。 Oracle のデータを XML 形式でエクスポートします。サーバーの bprd と通信します。
bporaexp64	クライアントの 64 ビットコマンドラインプログラム。 Oracle のデータを XML 形式でエクスポートします。サーバーの bprd と通信します。
bporaimp	クライアントのコマンドラインプログラム。 Oracle のデータを XML 形式でインポートします。サーバーの bprd と通信します。
bporaimp64	クライアントの 64 ビットコマンドラインプログラム。 Oracle のデータを XML 形式でインポートします。サーバーの bprd と通信します。
bprestore	リストアプログラム。bp のデバッグにも使用できます。
bptestnetconn	ホストの任意の指定のリスト (NetBackup 構成のサーバーリストを含む) での DNS と接続の問題をテストおよび分析します。
db_log	これらのログについて詳しくは、 NetBackup Database Extension 製品に付属する NetBackup のマニュアルを参照してください。

ディレクトリ	関連するプロセス
mtfrd	これらのログには、mtfrd プロセスの情報が含まれ、Backup Exec メディアのインポートおよびリストアの各フェーズ 2 に使用されます。
tar	リストア時の nbtar プロセス。
user_ops	user_ops ディレクトリは、NetBackup のインストール時に、すべてのサーバーおよびクライアント上に作成されます。NetBackup Java インターフェースプログラムは、このディレクトリを使って、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)] プログラム (jbpSA) が生成する一時ファイル、ジョブファイルおよび進捗ログファイルを格納します。すべての Java ベースのプログラムで操作を正常に実行するには、このディレクトリが存在し、だれでも読み込み、書き込みおよび実行できるように許可モードを設定している必要があります。このディレクトリには、Java ベースのプログラムを使用するすべてのユーザー用のディレクトリが含まれます。 また、NetBackup Java を実行可能なプラットフォーム上では、NetBackup Java インターフェースのログファイルが、nbjlogs サブディレクトリに書き込まれます。user_ops ディレクトリ階層にあるすべてのファイルは、KEEP_LOGS_DAYS 構成オプションの設定に従って削除されます。

レガシーログを使う PC クライアントプロセス

ほとんどの PC クライアントプロセスでレガシーログが使用されます。Windows クライアントで詳細なレガシーデバッグログを有効にするには、次の場所にディレクトリを作成します。作成するディレクトリ名はログを作成するプロセスに対応します。

C:\Program Files\VERITAS\NetBackup\Logs\

メモ: 次の場所は、ディレクトリが配置されるデフォルトの場所です。クライアントのインストールでは、別の場所を指定することができます。

表 1-11 に、これらのクライアントで使用可能なレガシーデバッグログディレクトリを示します。

表 1-11 レガシーログを使う PC クライアントプロセス

ディレクトリ	NetBackup クライアント	説明
bpineta	すべての Windows クライアント	クライアントのサービスログ。これらのログには、bpineta32 プロセスの情報が含まれます。

ディレクトリ	NetBackup クライアント	説明
bparchive	すべての Windows クライアント	コマンドラインから実行されるアーカイブプログラム。
bpbackup	すべての Windows クライアント	コマンドラインから実行されるバックアッププログラム。
bpbkar	すべての Windows クライアント	Backup Archive Manager 。これらのログには、bpbkar32 プロセスの情報が含まれます。
bpcd	すべての Windows クライアント	NetBackup Client デーモンまたは NetBackup Client Manager 。これらのログには、サーバーとクライアント間の通信の情報が含まれます。
bpjava-msvc		NetBackup-Java アプリケーションのサーバー認証サービス。このサービスは、 NetBackup Java インターフェースアプリケーションの起動中に、Client Service によって起動されます。このプログラムによって、アプリケーションを起動したユーザーが認証されます。(すべての Windows プラットフォーム)
bpjava-usvc		bpjava-msvc によって起動される NetBackup プログラム。 NetBackup-Java バックアップ、アーカイブおよびリストア (BAR) インターフェースを起動すると表示されるログオンダイアログボックスでログオンに成功すると起動されます。このプログラムによって、bpjava-msvc が実行されている NetBackup ホスト上の Java ベースのユーザーインターフェースから送信されるすべての要求が処理されます。(すべての Windows プラットフォーム)
bplist	すべての Windows クライアント	コマンドラインから実行される表示プログラム。
bpmount	すべての Windows クライアント	クライアント上で複数ストリームクライアントのドライブ名を収集するために使用されるプログラム。
bprestore	すべての Windows クライアント	コマンドラインから実行されるリストアプログラム。

ディレクトリ	NetBackup クライアント	説明
bptestnetconn	すべての Windows クライアント	ホストの任意の指定のリスト (NetBackup 構成のサーバーリストを含む) での DNS と接続の問題のテストおよび分析に役立つ複数のタスクを実行するプログラム。
tar	すべての Windows クライアント	tar 処理。これらのログには、tar32 プロセスの情報が含まれます。
user_ops	すべての Windows クライアント	user_ops ディレクトリは、NetBackup のインストール時に、すべてのサーバーおよびクライアント上に作成されます。 NetBackup Java インターフェースプログラムでは、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)] プログラム (jbpsA) によって生成された一時ファイル、ジョブファイルおよび進捗ログファイルが、このディレクトリに格納されます。すべての Java ベースのプログラムで操作を正常に実行するには、このディレクトリが存在し、だれでも読み込み、書き込みおよび実行できるように許可モードを設定している必要があります。user_ops ディレクトリには、Java ベースのプログラムを使用するすべてのユーザー用のディレクトリが含まれます。 また、NetBackup Java を実行可能なプラットフォーム上では、NetBackup Java インターフェースのログファイルが、nbjlogs サブディレクトリに書き込まれます。user_ops ディレクトリ階層のすべてのファイルは、KEEP_LOGS_DAYS 構成オプションの設定に従って削除されます。

レガシーログのファイル名の形式

NetBackup レガシーログは次の形式の名前を持つデバッグログファイルを作成します。

```
user_name.mmddyy_nnnnn.log
```

次の項目はログファイル名の要素を示します。

<i>user_name</i>	これはプロセスを実行するユーザーの名前で、次のようになります。 ■ UNIX の root ユーザーの場合、<i>user_name</i> は root です。 ■ UNIX の root ユーザー以外のユーザーの場合、<i>user_name</i> はユーザーのログイン ID です。 ■ Windows の管理者グループに属するすべてのユーザーの場合、<i>user_name</i> は ALL_ADMINS です。 ■ Windows のユーザーの場合、<i>user_name</i> は username@domain_name または username@machine_name です。
<i>mmddyy</i>	これは NetBackup がログファイルを作成した月、日、年です。
<i>nnnnn</i>	これはログファイルのカウンタ (ローテーション番号) です。カウンタがログファイル数の設定値を超えると、最も古いログファイルが削除されます。 MAX_NUM_LOGFILES 構成パラメータでプロセスごとのレガシーログファイルの最大数を設定します。

レガシーデバッグログディレクトリのすべてのログファイルの保持期間は次のオプションを使用して管理されます。

- NetBackup の [ホストプロパティログ (Host Properties Logging)] ダイアログボックスの [ログを保持する日数 (Keep logs for days)] 設定。デフォルトは 28 日です。
- NetBackup の [ホストプロパティログ (Host Properties Logging)] ダイアログボックスの [ログを保持する最大サイズ (Keep logs up to size)] 設定。
- レガシーログの設定。
p.48 の「[レガシーログのサイズと保持の制限について](#)」を参照してください。

レガシーデバッグログディレクトリに新しいログファイル名と古いログファイル名が混在する場合、ファイルは、[ログを保持する (Keep logs)] 設定およびデバッグログ制限機能の設定に従って管理されます。

サーバーのレガシーデバッグログのディレクトリ名

表 1-12 に、サーバーのレガシーデバッグログをサポートするために作成する必要があるディレクトリを示します。各ディレクトリはプロセスに対応します。指定されない場合、各ディレクトリは次のディレクトリの下に作成する必要があります。

Windows の場合	<code>install_path\NetBackup\logs</code>
UNIX の場合	<code>/usr/opensv/netbackup/logs</code>

表 1-12 レガシーデバッグログのディレクトリ名

ディレクトリ	関連するプロセス
admin	管理コマンド
bpbrm	NetBackup Backup Restore Manager
bpcd	NetBackup Client デーモンまたは NetBackup Client Manager。このプロセスは NetBackup Client Service によって起動されます。
bpjobd	NetBackup Jobs Database Manager プログラム
bpdm	NetBackup disk manager
bpdbm	NetBackup Database Manager。このプロセスは、マスターサーバー 上だけで実行されます。Windows システムでは、これは NetBackup Database Manager サービスです。
bpjava-msvc	NetBackup Java アプリケーションのサーバー認証サービス。このサービスは、NetBackup インターフェースアプリケーションの起動時に開始されます。UNIX サーバーの場合は、inetd によって起動されます。Windows サーバーの場合は、NetBackup Client Service によって起動されます。 このプログラムによって、アプリケーションを起動したユーザーが認証されます。
bpjava-susvc	bpjava-msvc によって起動される NetBackup プログラム。NetBackup- インターフェースを起動すると表示されるログオンダイアログボックスでログオンに成功すると起動されます。このプログラムによって、bpjava-msvc プログラムが実行されている NetBackup マスターサーバーまたはメディアサーバーホスト上の Java ベースのユーザーインターフェースから送信されるすべての要求が処理されます (すべての Windows プラットフォーム)。
bprd	NetBackup Request デーモンまたは NetBackup Request Manager。Windows システムでは、このプロセスは NetBackup Request Manager サービスと呼ばれます。
bpsynth	合成バックアップのための NetBackup プロセス。nbjm は bpsynth を開始します。bpsynth はマスターサーバー 上で実行されます。
bptm	NetBackup テープ管理プロセス
nbatd	認証デーモン (UNIX と Linux) またはサービス (Windows)。nbatd は NetBackup サービスまたはデーモンのインターフェースへのアクセスを認証します。
nbazd	認可デーモン (UNIX と Linux) またはサービス (Windows)。nbatd は NetBackup サービスまたはデーモンのインターフェースへのアクセスを認可します。
syslogs	システムログ ltid またはロボットソフトウェアのトラブルシューティングを行うには、システムのログを有効にしておく必要があります。syslogd のマニュアルページを参照してください。

ディレクトリ	関連するプロセス
user_ops	user_ops ディレクトリは、NetBackup のインストール時に、すべてのサーバーおよびクライアント上に作成されます。NetBackup- インターフェースプログラムでは、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)] プログラム (jbpSA) によって生成された一時ファイル、ジョブファイルおよび進捗ログファイルが、このディレクトリに格納されます。すべての Java ベースのプログラムで操作を正常に実行するには、このディレクトリが存在し、だれでも読み込み、書き込みおよび実行できるように許可モードを設定している必要があります。user_ops ディレクトリには、Java ベースのプログラムを使用するすべてのユーザー用のディレクトリが含まれます。 また、Java を実行可能なプラットフォーム上では、NetBackup Java インターフェースのログファイルが、nbjlogs サブディレクトリに書き込まれます。user_ops ディレクトリ階層のすべてのファイルは、KEEP_LOGS_DAYS 構成オプションの設定に従って削除されます。
vnetd	ベリタス社ネットワークデーモン。ファイアウォールフレンドリなソケットの接続を作成するために使用されます。inetd(1M) プロセスによって起動されます。 メモ: /usr/opensv/logs ディレクトリまたは /usr/opensv/netbackup/logs に vnetd ディレクトリが存在する場合、ログはそのいずれかに記録されます。両方の場所に vnetd ディレクトリが存在している場合、/usr/opensv/netbackup/logs/vnetd だけにログが記録されます。

ログを書き込むプログラムおよびデーモンについての詳細情報を参照できます。

p.67 の「[多重化されたバックアップ処理](#)」を参照してください。

UNIX システムでは、/usr/opensv/netbackup/logs ディレクトリの README ファイルも参照してください。

メディアおよびデバイス管理のレガシーデバッグログのディレクトリ名

デバッグログディレクトリはメディア管理プロセスとデバイス管理プロセスのログを有効にします。表 1-13 に、メディア管理およびデバイス管理のレガシーデバッグログをサポートするために作成する必要があるディレクトリを示します。各ディレクトリはプロセスに対応します。

表 1-13 メディアおよびデバイスの管理のレガシーデバッグログ

ディレクトリ	関連するプロセス
acsssi	UNIX の場合、 NetBackup と StorageTek ACSLS サーバー間のトランザクションのデバッグ情報。
デーモン	vmd (Windows の場合、 NetBackup Volume Manager サービス) のデバッグ情報、および関連するプロセス (oprdr および rdevmi)。ディレクトリの作成後に vmd を停止して再起動します。

ディレクトリ	関連するプロセス
ltid	Media Manager device デーモン ltid (UNIX の場合) または NetBackup Device Manager サービス (Windows の場合)、および avrd のデバッグ情報。ディレクトリの作成後に ltid を停止して再起動します。
reqlib	vmd または EMM にメディア管理サービスを要求するプロセスのデバッグ情報。ディレクトリの作成後に vmd を停止して再起動します。
robots	tlldcd、tl8cd、tl4d デーモンを含む、すべてのロボットデーモンのデバッグ情報。ロボットデーモンを停止して、再起動します。
tpcommand	tpconfig、tpautoconf などのデバイス構成コマンド、および NetBackup 管理コンソールのデバッグ情報。
vmacd	NetBackup 状態収集デーモンのデバッグ情報。ディレクトリの作成後に vmacd を停止して再起動します。

指定されない場合、各ディレクトリは次のディレクトリの下に作成する必要があります。

Windows の場合 `install_path\Volmgr\debug`

UNIX の場合 `/usr/opensv/volmgr/debug`

NetBackup では、デバッグ用の各ディレクトリに、ログファイルが毎日 1 つずつ作成されます。

次のディレクトリを削除するか、または名前を変更することによってデバッグログを無効にできます。

Windows の場合: NetBackup `install_path\Volmgr\debug\daemon`
Volume Manager サービス

UNIX の場合: vmd コマンド `/usr/opensv/volmgr/debug/daemon`

p.43 の「[レガシーログのファイル名の形式](#)」を参照してください。

p.48 の「[レガシーログのサイズと保持の制限について](#)」を参照してください。

p.46 の「[メディアおよびデバイス管理のレガシーデバッグログのディレクトリ名](#)」を参照してください。

レガシーログファイルに書き込まれる情報量を制御する方法

レガシーログレベルを設定して、NetBackup プロセスがログに書き込む情報量を増やすことができます。

メディアおよびデバイスの管理以外のレガシーログに影響する設定を次に示します。

- [グローバルログレベル (Global logging level)]を上げます。
p.52 の「[ログレベルの変更](#)」を参照してください。

メモ: この設定は統合ログにも影響します。

- UNIX の場合、`/usr/opensv/netbackup/bp.conf` ファイルに `VERBOSE` エントリを追加します。
値を指定しないで `VERBOSE` を入力すると、詳細度の値はデフォルトで **1** に設定されます。より詳細なログを作成するには、`VERBOSE = 2` (または **3** 以上の値) と入力します。この設定は、レガシーログだけに影響します。

警告: 詳細度の値を高く設定すると、デバッグログのサイズは非常に大きくなる可能性があります。

- 個々のプロセスのログレベルを設定します。
[ホストプロパティ (Host Properties)] で、[ログ (Logging)] ダイアログボックスの個々のプロセスのログレベルを変更します。または、プログラムまたはデーモンの起動時に詳細フラグを指定します (可能な場合)。
また、次のとおり、個々のプロセスのログレベルを `bp.conf` ファイルの負の値に設定することもできます。
`<processname>_VERBOSE = -2` 対応するプロセスのログを完全に無効にします。
ログのプロパティについて詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

メディアおよびデバイスの管理のレガシーログのログレベルは、非詳細 (デフォルト) と詳細の **2** つです。レベルを詳細 (高) に設定するには、`vm.conf` ファイルに `VERBOSE` というエントリを追加します。必要に応じて、ファイルを作成します。`VERBOSE` エントリを追加した後で、`ltid` と `vmd` を再起動します。このエントリは、イベントビューアのアプリケーションログおよびシステムログに影響します。`vm.conf` ファイルは、次のディレクトリに存在します。

Windows の場合 `install_path\Volmgr\`

UNIX の場合 `/usr/opensv/volmgr/`

レガシーログのサイズと保持の制限について

特定の NetBackup プロセスはレガシーデバッグログを書き込みます。レガシーデバッグログは非常に大きくなる可能性があるため、解決できない問題が存在するときのみ有効にします。ログが不要になったら、ログおよび関連するディレクトリを削除します。

p.11 の「[NetBackup でのログの保持について](#)」を参照してください。

NetBackup でログを保持する期間を制限するには、[ログの保持(日) (Keep logs for days)]フィールドで日数を指定します。デフォルトは 28 日です。[ログ (Logging)]ダイアログボックスの[ホストプロパティ (Host Properties)]で日数を指定できます。

メモ: プロパティ [ログの保持 (Keep logs)]および[Vault ログの保持 (Keep vault logs)]は、[クリーンアップ (Clean-up)]ホストプロパティから[ログ (Logging)]ホストプロパティに移動されました。[ログ (Logging)]のプロパティ画面で、これらのプロパティはそれぞれ [ログの保持(日) (Keep logs for days)]および[Vault ログの保持 (Keep Vault logs for)]と表示されます。

ログのプロパティについて詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

ログファイルを管理するその他の方法については、『[レガシーログのローテーションの構成](#)』を参照してください。

他の NetBackup プロセスによって作成されるログには(メディアおよびデバイス管理ログを除いて)、[ログの保持(日) (Keep logs for days)]プロパティを使用します。[ログの保持(日) (Keep logs for days)]プロパティはデバッグログ制限機能の設定を上書きする場合があります。[ログの保持(日) (Keep logs for days)]が 10 日に設定され、デバッグログ制限機能の設定で 10 日以上が許可されている場合、ログは 11 日目に削除されます。

メディアおよびデバイスの管理のレガシーログで、ログファイルのローテーションを管理するには、vm.conf ファイルの DAYS_TO_KEEP_LOGS 設定を使用します。デフォルトは 30 日です。vm.conf ファイルは、次のディレクトリに存在します。

Windows の場合 `install_path\Volmgr\`

UNIX の場合 `/usr/opensv/volmgr/`

ログを 3 日間保有するには、vm.conf ファイルに次を入力します。

```
DAYS_TO_KEEP_LOGS = 3
```

このエントリを使う方法について詳しくは、『[NetBackup 管理者ガイド Vol. 2](#)』を参照してください。

レガシーログのローテーションの構成

レガシーログの最大ファイルサイズおよび保持するログファイルの最大数を指定できます。

p.11 の「[NetBackup でのログの保持について](#)」を参照してください。

レガシーログの場合、**NetBackup** は `bp.conf` 設定ファイルを使用してログファイルの最大サイズを設定します。bpsetconfig コマンドを使用して、**bp.conf** パラメータ、`MAX_LOGFILE_SIZE` および `MAX_NUM_LOGFILES` を構成し、ログ設定を行います。

`MAX_LOGFILE_SIZE` のデフォルト値は **500 MB** で、`MAX_NUM_LOGFILES` のデフォルト値は **0 (無限)** です。

レガシーログのローテーションを構成する方法

- ◆ ディレクトリごとのログファイルの最大ファイルサイズまたは最大数を変更するには、`MAX_LOGFILE_SIZE` オプションと `MAX_NUM_LOGFILES` オプションを使用します。これらのオプションは、次のディレクトリに存在する bpsetconfig コマンドの一部です。

Windows の場合 `Install_path¥NetBackup¥bin¥admincmd¥`

UNIX の場合 `/usr/opensv/netbackup/bin/admincmd/`

次の UNIX の例を使用して、ファイルの最大サイズに **512 MB** を設定し、1 つのログディレクトリあたりの最大ログファイル数に **4** を設定しています。

```
#bpsetconfig

bpsetconfig> MAX_LOGFILE_SIZE = 512

bpsetconfig> MAX_NUM_LOGFILES = 4

bpsetconfig>

CTRL-D
```

bpsetconfig の詳しい説明は、『**NetBackup コマンドリファレンスガイド**』を参照してください。

グローバルログレベルについて

[グローバルログレベル (Global logging level)]は、統合ログとレガシーログの両方を参照します。ログレベルはどの位の情報がログメッセージに含まれるかを決定します。レベル数が高いほど、より大量の詳細がログメッセージに含まれます。

表 1-14 は、すべてのログレベルおよび各レベルで含められる詳細について説明します。

表 1-14 グローバルログレベル

ログレベル	説明
最小のログ	非常に重要な少量の診断メッセージおよびデバッグメッセージが含まれます。 [ホストプロパティログ (Host Properties Logging)] ページまたはログアシスタントは最小のログを設定できます。 レガシーログは、最小のログを表すのに次の値を使います： ■ Windows の場合：レジストリは次の16進値を表示します：0xffffffff ■ UNIX の場合：bp.conf ファイルはVERBOSE=0 表示します (グローバル)。processname_VERBOSE = 0 は、個々の処理のグローバルなデフォルトを使用して示します。 グローバルな VERBOSE の値が 0 以外の値に設定されている場合、個々の処理は値 -1 を使って減らすことができます。たとえば、processname_VERBOSE = -1 のようにします。 統合ログでは、最小のログを表すのに値 1 を使います。
ログを無効にする	[ホストプロパティログ (Host Properties Logging)] ページまたはログアシスタントは、ログを無効にできます。 レガシーログは、無効なログを表すのに次の値を使います： ■ UNIX の場合：bp.conf ファイルは、個々のプロセスに対して VERBOSE=-2 (グローバル) または processname_VERBOSE = -2 を表示します。 ■ Windows の場合：レジストリは次の16進値を表示します：0xffffffff 統合ログでは、無効なログを示すのに値 0 を使います。
1	最小のログと関連付けられる少量の診断メッセージに詳細な診断メッセージおよびデバッグメッセージを追加します。
2	進捗メッセージが追加されます。
3	情報ダンプが追加されます。
4	ファンクションのエントリおよび終了が追加されます。
5	すべてが含まれています。最も詳細なレベルのメッセージ。

デフォルトでは、統合ログは、レベル 0 のデバッグメッセージおよびレベル 5 のアプリケーションメッセージが記録されるように設定されています。

次の操作はログレベルに影響します。

- [グローバルログレベル (Global logging level)] リストで 0 (ゼロ) を指定した場合、レガシーログと統合ログの両方で最小レベルが設定されます。ただし、統合ログの診断メッセージおよびデバッグメッセージの場合、ログレベルはオフにできます。診断メッ

セージおよびデバッグメッセージはログに記録されません。このレベルは、NetBackup 管理コンソールの[グローバルログレベル (Global logging level)]リストでは設定できません。vxlogcfg コマンドまたはログアシスタントで、それを設定できます。

p.52 の「[ログレベルの変更](#)」を参照してください。

p.35 の「[vxlogcfg を使用した統合ログの設定の例](#)」を参照してください。

- [グローバルログレベル (Global logging level)]リストを変更すると、サーバーまたはクライアントの NetBackup および Enterprise Media Manager (EMM) のすべてのプロセスのログレベルに影響します。(ただし、PBX のログとメディアおよびデバイスの管理のログには影響しません。)この設定は、構成済みの設定よりも優先されます。
- bp.conf ファイルの VERBOSE エントリまたは vm.conf ファイルのエントリを変更した場合は、レガシーログだけに影響します。
p.47 の「[レガシーログファイルに書き込まれる情報量を制御する方法](#)」を参照してください。

- vxlogcfg コマンドで変更を行った場合は、統合ログレベルだけに影響します。

[グローバルログレベル (Global logging level)]リストへの変更は、次のログプロセスのレベルに影響しません。

- PBX のログ
PBX ログにアクセスする方法について詳しくは、『[NetBackup トラブルシューティング ガイド](#)』を参照してください。
- メディアおよびデバイスの管理のログ (vmd, ltid, avrd、ロボットデーモン、Media Manager コマンド)
p.46 の「[メディアおよびデバイス管理のレガシーデバッグログのディレクトリ名](#)」を参照してください。
- デバッグレベルがデフォルト設定から変更されている、統合ログの任意のプロセス

ログレベルの変更

ログレベルはどの位の情報がログメッセージに含まれるかを決定します。ログの範囲は 0 から 5 です。レベル数が高いほど、より大量の詳細がログメッセージに含められます。

ログレベルを変更する方法

- 1 NetBackup 管理コンソールの左ペインで、[NetBackup の管理 (NetBackup Management)]>[ホストプロパティ (Host Properties)]を展開します。
- 2 [マスターサーバー (Master Servers)]、[メディアサーバー (Media Servers)]または[クライアント (Clients)]を選択します。
- 3 右ペインで、バージョンおよびプラットフォームを表示するサーバーまたはクライアントをクリックします。次にダブルクリックすると、プロパティが表示されます。
- 4 プロパティダイアログボックスの左ペインで、[ログ (Logging)]をクリックします。

- 5 [グローバルログレベル (Global logging level)]リストでは、0 から 5 の値を選択します。
変更は、統合ログとレガシーログの両方のログレベルに影響します。
p.50 の「[グローバルログレベルについて](#)」を参照してください。
- 6 [OK]をクリックします。

Windows クライアントのログレベルの変更

クライアントプロセスによってログに書き込まれる情報量を増やすことができます。

Windows クライアントのログレベルを変更する方法

- 1 クライアントで、バックアップ、アーカイブおよびリストアインターフェースを開きます。
- 2 [ファイル (File)]メニューをクリックして[NetBackup クライアントのプロパティ (NetBackup Client Properties)]を選択します。
- 3 [NetBackup クライアントのプロパティ (NetBackup Client Properties)]ダイアログボックスで、[トラブルシューティング (Troubleshooting)]タブを選択します。
- 4 [詳細 (Verbose)]プロパティフィールドで、0 から 5 のデバッグレベルを入力します。
テクニカルサポートが特に指定しないかぎり、デフォルトのレベルの 0 (ゼロ) を使用します。これより高いレベルでは、ログに大量の情報が蓄積される可能性があります。
- 5 [OK]をクリックします。

Bare Metal Restore の bmrsavecfg プロセスによって作成される統合ログファイルでは、vxlogcfg コマンドを使用してログレベルを制御することもできます。

p.35 の「[vxlogcfg を使用した統合ログの設定の例](#)」を参照してください。

ログレベルを高くすると、ログのサイズが非常に大きくなるため、解決できない問題が発生した場合だけ、この操作を実行してください。

Media Manager のデバッグログを上位レベルに設定する

数多くのエラー状態を解決するには、デバッグログを上位レベルに設定します。その後、操作を再試行して、デバッグログを調べます。

デバッグログレベルを上げる方法

- 1 必要なディレクトリおよびフォルダを作成して、レガシーデバッグログを有効にします。
- 2 `vm.conf` ファイルに[VERBOSE (詳細)]オプションを追加して、メディアおよびデバイスの管理プロセスの詳細レベルを上げます。このファイルは、`/usr/openv/volmgr/` (UNIX および Linux の場合) および `install_path\Volmgr\` (Windows の場合) に存在します。
- 3 デーモンおよびサービスを再起動するか、可能な場合、詳細オプションを指定してコマンドを実行します。

クライアントのログの保持制限の設定

UNIX、および Windows で、NetBackup がクライアントのログを保持する日数を指定できます。

UNIX クライアントでログの保持制限を設定する方法

- 1 NetBackup 管理コンソールの左ペインで、[ホストプロパティ (Host Properties)] > [クライアント (Clients)]を展開します。
- 2 右ペインで、変更するクライアントをダブルクリックします。
- 3 プロパティダイアログボックスで[UNIX クライアント (UNIX Client)]をクリックします。
- 4 [クライアントの設定 (Client Settings)]ダイアログボックスで、[ユーザー主導バックアップ、アーカイブおよびリストアの状態を保持する期間 (Keep status of user-directed backups, archives, and restores for)]フィールドを見つけます。
- 5 ログファイルを保持する日数を入力し、[OK]をクリックします。

Windows クライアントでログの保持制限を設定する方法

- 1 NetBackup 管理コンソールの[ファイル (File)]メニューで、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]をクリックします。
- 2 [バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]インターフェースの[ファイル (File)]メニューで、[NetBackup クライアントのプロパティ (NetBackup Client Properties)]をクリックします。
- 3 [NetBackup クライアントのプロパティ (NetBackup Client Properties)]ダイアログボックスで、[全般 (General)]タブを選択します。
- 4 [ユーザー主導バックアップ、アーカイブおよびリストアの状態を保持する期間 (Keep status of user-directed backups, archives, and restores for)]フィールドで、ログファイルを保持する日数を入力します。
- 5 [OK]をクリックします。

Windows のイベントビューアのログオプション

NetBackup Windows マスターサーバーは、NetBackup プロセスからのメッセージをアプリケーションイベントログおよび通常の場合に書き込むように設定できます。これらのメッセージは、Windows イベントビューアで確認することができ、サードパーティのツールを使って、アプリケーションイベントログでこれらのメッセージを監視することもできます。

アプリケーションイベントログへのメッセージの書き込みに使用できる 2 つのログオプションがあります。これらのオプションは別々に使うことも、組み合わせて使うこともでき、次のようにログに書き込むプロセスのタイプに固有です。

- 統合されたプロセス (nbrb のようにプロセス名が **nb** で始まるプロセス) を監視するには、vxlogview コマンドを使用します。
- レガシープロセス (bpdbm のようにプロセス名が **bp** で始まるプロセス) を監視するには、eventlog ファイルを設定します。

メモ: vxlogcfg コマンドまたは eventlog ファイルでこの設定を有効にするには、NetBackup サービスを再起動する必要があります。

オリジネータの統合されたログアプリケーションと診断メッセージを Windows イベントビューアアプリケーションログに配信するには、vxlogcfg コマンドを使用して、そのオリジネータの LogToOslog 値を **true** に設定します。

次の例では、Windows イベントビューアのアプリケーションログに nbrb のアプリケーションメッセージと診断メッセージを送ります。

```
# vxlogcfg -a -o nbrb -p NB -s "LogToOslog=true"
```

また、オペレーティングシステムのログ記録が nbrb で有効化されると、次の例のメッセージが Windows イベントビューア アプリケーションログに書き込まれます。

```
from nbrb - request ID {1C7FF863-4BCB-46EA-8B35-629A43A4FF1F} failed with status 0  
(Not Enough Valid Resources); releasing 2 allocated resources
```

メモ: この設定を有効にするには、NetBackup サービスを再起動する必要があります。

このオプションを変更すると、無視できるエラーメッセージも Windows イベントビューア アプリケーションログに書き込まれます。たとえば、次のコマンドを指定する場合、

```
# vxlogcfg -a -o nbpem -p NB -s "LogToOslog=true"
```

次のような無視できるメッセージの例が、ストレージライフサイクルポリシーが存在しない場合に、Windows イベントビューアアプリケーションログに書き込まれます。

```
call NBProxy::getClientList failed to nbproxy with status 227
```

vxlogcfg の詳しい説明は、『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

eventlog ファイルを使うには、次の操作を実行します。

- **NetBackup** マスターサーバー上に次のファイルを作成します。

```
install_path¥NetBackup¥db¥config¥eventlog
```

- 必要に応じて、eventlog ファイルにエントリを追加します。次に例を示します。

```
56 255
```

メモ: この設定を有効にするには、**NetBackup** サービスを再起動する必要があります。

eventlog のパラメータは重大度と種類を表します。パラメータには次の性質があります。

- | | |
|----------------|---|
| 重大度 (Severity) | <ul style="list-style-type: none"> ■ 1 番目のパラメータとして表示されます。 ■ NetBackup がアプリケーションログに書き込むメッセージを制御します。 ■ ファイルが空の場合、デフォルトの重大度はエラー (16) です。 ■ ファイルにパラメータが 1 つしか含まれない場合、そのパラメータは重大度のレベルとして使用されます。 |
| 種類 (Type) | <ul style="list-style-type: none"> ■ 2 番目のパラメータとして表示されます。 ■ NetBackup がアプリケーションログに書き込むメッセージの種類を制御します。 ■ ファイルが空の場合、デフォルトの種類はバックアップ状態 (64) です。 |

どちらのパラメータも 10 進数で指定され、次の値を表すビットマップと等価です。

- | | |
|----------------|---|
| 重大度 (Severity) | 1 = 不明
2 = デバッグ
4 = 情報
8 = 警告
16 = エラー
32 = 重要 |
|----------------|---|

種類 (Type)	1 = 不明
	2 = 一般
	4 = バックアップ
	8 = アーカイブ
	16 = 検索
	32 = セキュリティ
	64 = バックアップ状態
	128 = メディアデバイス

eventlog ファイルを構成して、複数の異なる重大度と種類を含んでいるメッセージをログに記録できます。eventlog ファイルで **56 255** のエントリを指定すると、結果は次のようになります。

エントリ 56 重大度が警告、エラーおよび重要のメッセージを含むログを生成します。(56 = 8 + 16 + 32)

エントリ 255 すべての種類のメッセージを含むログを生成します。(255 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128)

次のメッセージの例は、**Windows** イベントビューアのアプリケーションログに書き込まれます。

```
16 4 10797 1 cacao bush nbpem backup of client bush exited with status
71
```

各値の定義は次のとおりです (左から順)。

- 重大度: 16 (エラー)
- 種類: 4 (バックアップ)
- ジョブ ID = 10797
- ジョブグループ ID: 1
- サーバー: cacao
- クライアント: bush
- プロセス: nbpem
- 文字列: クライアント bush のバックアップが状態 71 で終了しました (backup of client bush exited with status 71)

NetBackup 管理コンソールのエラーメッセージのトラブルシューティング

NetBackup 管理コンソールのほとんどのエラーメッセージは次の場所に表示されます。

- 注意を促すダイアログボックス
- コンソール右下のエラーメッセージペイン

エラーが他の場所に表示された場合は、Java の例外エラーです。これらのエラーは、[NetBackup 管理コンソール (NetBackup Administration Console)] ウィンドウのステータスバー (下部) に表示されます。Java API または NetBackup 管理コンソールによって書き込まれた stdout または stderr メッセージが含まれるログファイルにエラーが表示される場合もあります。Veritas では、Java の例外のエラーを文書に記録しません。

4 種類のエラーメッセージが NetBackup 管理コンソールに表示されます。

表 1-15 エラーメッセージの種類

エラーの種類	説明 (Description)
NetBackup の状態コードおよびメッセージ	NetBackup 管理コンソールで実行される操作によって、NetBackup の他の部分でエラーが検出される場合があります。これらのエラーは、通常、NetBackup の状態コードおよびメッセージの章に記載されているとおりに表示されます。 メモ: エラーメッセージには、状態コードが付かない場合もあります。 状態コードを見つけるには、アルファベット順の NetBackup メッセージを調べ、リンクをクリックして詳細な説明を参照します。 『状態コードリファレンスガイド』を参照してください。
NetBackup 管理コンソール: アプリケーションサーバーの状態コードおよびメッセージ	これらのメッセージには、500 番台の状態コードが付きます。状態コード 500、501、502、503 および 504 が付いたメッセージは、"ログインできません。状態: (Unable to login, status:)" で始まります。状態コード 511 および 512 が付いたメッセージは、"ログインできません。状態: (Unable to login, status:)" で始まる場合とそうでない場合があります。 メモ: エラーメッセージには、状態コードが付かない場合もあります。 『状態コードリファレンスガイド』を参照してください。

エラーの種類	説明 (Description)
Java の例外	これらの例外は、Java API または NetBackup 管理 API によって生成されます。これらのメッセージの先頭は、例外の名前です。次に例を示します。 <pre>java.lang.ClassCastException</pre> または <pre>vrts.nbu.NBUCommandExecutionException</pre> Java の例外は、通常、次のいずれかの位置に表示されます。 ■ NetBackup 管理ウィンドウのステータスバー (下部) ■ jnbSA または jbpSA が生成するログファイル ■ Windows ディスプレイコンソールの .bat ファイルの出力ファイル (設定されている場合) p.58 の「NetBackup 管理コンソールのエラーメッセージのトラブルシューティング」を参照してください。
オペレーティングシステムのエラー	NetBackup のマニュアルのメッセージと一致しないメッセージは、ほとんどの場合、オペレーティングシステムのメッセージです。

ログおよび一時ファイルに必要な追加のディスク容量について

正常な操作のために、NetBackup 管理コンソールはログと一時ファイルを保存する追加のディスク容量を必要とします。ディスク容量は次の場所で利用可能である必要があります。

- ログインダイアログボックスで指定したホスト
- /usr/opensv/netbackup/logs/user_ops
- 管理コンソールが起動されたホスト
- /usr/opensv/netbackup/logs/user_ops/nbjlogs

それぞれのファイルシステムで利用可能な領域がない場合、次の問題が発生することがあります。

- アプリケーションの応答に時間がかかる
- データが不完全になる
- ログイン中に応答がない
- NetBackup インターフェースの機能が低下する (ツリーにはバックアップ、アーカイブ、リストアノードおよびファイルシステムの分析ノードしか表示されないなど)
- 予想外のエラーメッセージ:

- NetBackup-Java アプリケーションサーバーへのログオン中に、"ソケットに接続できない"というエラーが発生する
- [ログインできません。状態: 35 要求されたディレクトリを作成できません (Unable to login, status: 35 cannot make required directory)]
- [/bin/sh: null: not found (1)]
- [An exception occurred: vrts.nbu.admin.bpmgmt.CommandOutputException: Invalid or unexpected class configuration data: *<the rest of the message will vary>*]
- 空白の警告ダイアログボックスが表示される

詳細なデバッグログの有効化

NetBackup 管理コンソールは、NetBackup サーバーのリモート管理を可能にする分散アプリケーションです。すべての管理は、NetBackup 管理コンソールのアプリケーションサーバーを介して行われます。このアプリケーションサーバーは、認証サービスおよびユーザーサービスで構成されます。

ログオンダイアログボックスからのログオン要求は、認証サービスへ送信され、妥当性が確認されます。Windows または UNIX の認証ファイルや認証プロセスで、ユーザー名およびパスワードが有効である必要があります。

妥当性の確認が完了すると、認証サービスによって、そのユーザーアカウントでユーザーサービスが起動されます。その後、すべての NetBackup 管理タスクは、そのユーザーサービスのインスタンスを介して実行されます。追加のユーザーサービスプロセスが開始されて、コンソールからの要求が処理されます。

UNIX と Windows の両方で、認証サービスは bpjava-msvc アプリケーションです。ユーザーサービスは bpjava-susvc または bpjava-usvc アプリケーションです。詳細なデバッグログを有効にするには、最初にこれらのアプリケーションのログのディレクトリを作成する必要があります。

表 1-16 詳細なデバッグログの有効化

手順	処理	説明
手順 1	ログのディレクトリを作成します	ログオンダイアログボックスで指定した NetBackup クライアントまたはサーバーで、次のディレクトリを作成します。 - bpjava-msvc - bpjava-susvc (NetBackup サーバーの場合) - bpjava-usvc (NetBackup クライアントの場合) 次の場所にディレクトリを作成します。 - install_path¥NetBackup¥logs (Windows の場合) /usr/opensv/netbackup/logs (UNIX の場合) p.13 の「統合ログについて」を参照してください。 p.37 の「レガシーログについて」を参照してください。
手順 2	Debug.properties ファイルを編集します	Debug.properties ファイルに次の行を追加します。 <pre>debugMask=0x00040000</pre> Debug.properties ファイルは、次の場所で確認できます。 /usr/opensv/java jnbSA または jbpSA コマンドを実行する UNIX マシン上でファイルを変更します。ログファイル名は、jnbSA コマンドまたは jbpSA コマンドを実行した xterm ウィンドウに表示されます。 - install_path¥VERITAS¥java NetBackup Windows ディスプレイコンソールを使う場合、この場所でファイルを変更します。
手順 3	nbjava.bat ファイルを編集します	NetBackup がインストールされていないホストの Windows ディスプレイコンソールを使う場合は、この手順を実行します。 nbjava.bat ファイルを編集し、ファイルへの出力を指定します。 nbjava.bat ファイルは install_path¥VERITAS¥java にあります。詳細については、nbjava.bat ファイルを参照してください。

この詳細なデバッグログによって、管理コンソールで構成できる **NetBackup** 管理コンソールログよりも多くの情報を取得できます。次の URL にある『**NetBackup** 管理者ガイド Vol. 1』を参照してください。

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

NetBackup の **Windows** コンピュータから **Java** ベースの **NetBackup** 管理コンソールを起動するときにログを作成する方法について詳しくは、次を参照してください。

p.177 の「[Java ベースの管理コンソールのログ記録について](#)」を参照してください。

バックアッププロセスおよび ログ記録

この章では以下の項目について説明しています。

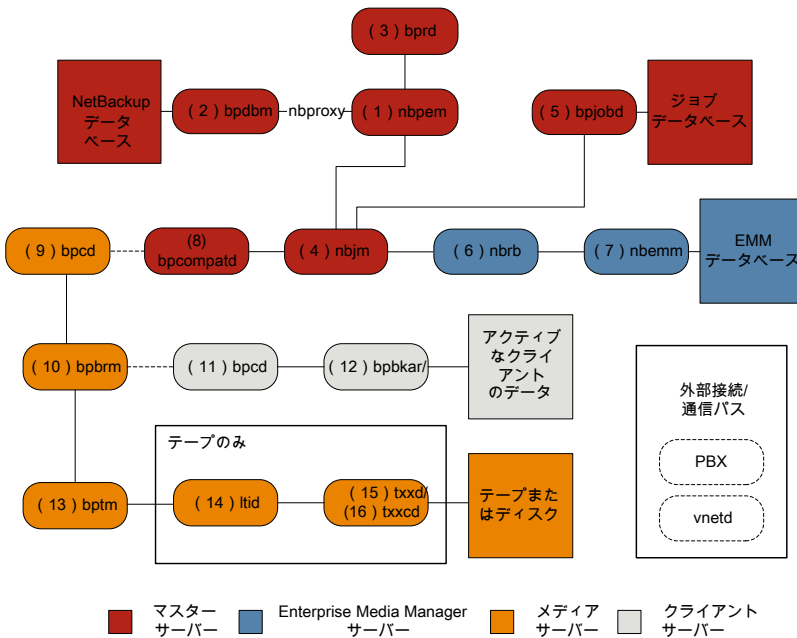
- [バックアップ処理](#)
- [NetBackup プロセスの説明](#)
- [バックアップログについて](#)
- [ベリタステクニカルサポートへのバックアップログの送信](#)

バックアップ処理

バックアッププロセスの動作の仕組みを理解することは、トラブルシューティングでどのプロセスを確認すべきかを判断するのに役立つ最初のステップです。

[図 2-1](#) は、スケジュールバックアップ時のバックアップ手順とプロセスフローを示しています。

図 2-1 バックアッププロセスの基本フロー



バックアップの基本手順

- (1) NetBackup Policy Execution Manager (nbpem) は、ジョブの期限になるとバックアップを開始します。ジョブの期限を判断するため、nbpem はプロキシサービス nbproxy を使用して (2) NetBackup Database Manager (bpdbm) からバックアップポリシー情報を取得します。
ユーザーが開始するバックアップの場合、nbpem が (3) NetBackup Request デモモン (bprd) から要求を受信したときにバックアップが開始されます。
- ジョブが期限になると、nbpem は (4) NetBackup Job Manager (nbjm) にバックアップの送信と jobid の取得を要求します。
- nbjm サービスは (5) bpjobd と通信し、ジョブデータベースのジョブリストにジョブが追加されます。ジョブはキューへ投入済みとなり、アクティビティモニターに表示されます。
- ジョブがジョブデータベースに追加されると、nbjm は (6) NetBackup Resource Broker (nbrb) を通してリソースをチェックします。
- nbrb プロセスは (7) Enterprise Media Manager (nbemm) から必須リソースを確保し、リソースが割り当て済みであることを nbjm に伝えます。

- 6 リソースが割り当てられると、nbjm はイメージデータベースを呼び出して一時的な場所にイメージファイルを作成します。バックアップヘッダーテーブルの必須エントリも同時に作成されます。ジョブはアクティビティモニターで[アクティブ (Active)]として表示されます。
- 7 ジョブを実行すると、nbjm は (8) bpcompatd を使用して (9) メディアサーバーのクライアントサービス (bpcd) への接続を開きます。bpcompatd サービスは構内交換機 (PBX) および NetBackup レガシーネットワークサービス (vnetd) を通して接続を作成します。
- 8 bpcd サービスは (10) NetBackup バックアップおよびリストアマネージャ (bpbrm) を開始します。
- 9 bpbrm サービスは (11) クライアントサーバーの bpcd (PBX および vnetd 経由) と通信し、(12) Backup Archive Manager (bpbkar) を開始します。bpbrm は (13) テープ管理プロセス (bptm) も開始します。
- 10 テープバックアップの場合、bptm はドライブを予約し、(14) 論理テープインターフェースデーモン (ltid) にマウント要求を発行します。ltid サービスは (15) ロボットドライブデーモン (txxd、xx は使用するロボットの種類によって異なります) を呼び出します。txxd デーモンは (16) メディアをマウントするロボット制御デーモン (txxcd) へのマウント要求と通信します。
ディスクバックアップの場合、bptm はディスクと直接通信します。
- 11 bpbkar は、メディアストレージまたはディスクストレージに書き込まれる bptm を通してバックアップデータを送信します。
- 12 バックアップが完了すると nbjm に伝達され、bpjobd にメッセージが送信されます。ジョブはアクティビティモニターで[完了 (Done)]として表示されます。nbjm サービスは次の予定時刻を再計算する nbpem にジョブの終了状態をレポートします。

バックアップに関するプロセスごとにログファイルがあります。これらのログはバックアップで発生した問題の診断に使用できます。

バックアッププロセスフローには含まれませんが、バックアップの問題の解決に有用な追加のログには、bpbackup、reqlib、daemon、robots、acsssi などがあります。

NetBackup プロセスの説明

次のトピックでは、UNIX 版および Windows 版の NetBackup のバックアップ処理およびリストア処理の機能概要について説明します。具体的には、重要なサービスまたはデーモンとプログラム、およびそれらがバックアップおよびリストア操作中に実行される順序について説明します。また、インストールされるソフトウェアのデータベースおよびディレクトリ構造についても説明します。

p.65 の「バックアップとリストアの起動プロセス」を参照してください。

p.65 の「バックアップ処理およびアーカイブ処理」を参照してください。

p.66 の「バックアップおよびアーカイブ: UNIX クライアントの場合」を参照してください。

p.67 の「多重化されたバックアップ処理」を参照してください。

バックアップとリストアの起動プロセス

NetBackup マスターサーバーの起動時に、NetBackup に必要なすべてのサービス、デーモン、プログラムがスクリプトによって自動的に開始されます (スクリプトが使用する起動コマンドは、プラットフォームに応じて異なります)。

メディアサーバーの場合も同様です。NetBackup によって、ロボットデーモンも含めた追加プログラムが必要に応じて自動的に起動されます。

SAN のクライアントおよびファイバートランSPORTのスタートアップ処理について詳しくは、『NetBackup SAN クライアントおよびファイバートランSPORTガイド』を参照してください。

メモ: デーモンやプログラムは明示的に起動する必要はありません。必要なプログラムは、バックアップまたはリストアの操作中に自動的に起動されます。

すべてのサーバーおよびクライアントで実行されるデーモンは、NetBackup Client デーモン `bpcd` です。UNIX クライアントでは、`inetd` によって `bpcd` が自動的に起動されるため、特別な操作は必要ありません。Windows クライアントでは、`bpnetd` が `inetd` と同様に動作します。

メモ: UNIX のすべての NetBackup プロセス

は、`/usr/openv/netbackup/bin/bp.start_all` のコマンドを手動で実行することで開始できます。

バックアップ処理およびアーカイブ処理

バックアップ処理およびアーカイブ処理は、クライアントの種類によって異なります。次ではスナップショット、SAN クライアント、合成バックアップおよび NetBackup カタログバックアップを含むバックアップおよびリストアに関連する NetBackup のさまざまな処理について説明します。

ジョブのスケジューラの処理は次の要素から構成されています。

- `nbpem` サービス (Policy Execution Manager) はポリシークライアントタスクを作成してジョブの実行予定時間を決定します。ジョブを開始し、ジョブの完了時に、ポリシーとクライアントの組み合わせに対して次のジョブを実行するタイミングを決定します。
- `nbjm` サービス (Job Manager) は次の処理を実行します。

- `bplabel` や `tpreq` のようなコマンドからのバックアップジョブまたはメディアジョブを実行する `nbpem` からの要求を受け入れます
- ストレージユニット、ドライブ、メディア、クライアントとポリシーのリソースのような各ジョブのリソースを要求します。
- ジョブを実行してメディアサーバーの処理を開始します。
- メディアサーバーの `bpbrm` からのフィールド更新は更新を処理してジョブデータベースおよびイメージデータベースにルーティングします。
- 事前処理の要求を `nbpem` から受信してクライアント上で `bpmount` を開始します。
- `nbrb` サービス (Resource Broker) は次の処理を実行します。
 - `nbjm` からの要求に応じてリソースを割り当てます。
 - Enterprise Media Manager サービスからの物理リソースを取得します (`nbemm`)。
 - クライアント 1 人あたりの多重化グループ、1 クライアントあたりの最大ジョブ数、1 ポリシーあたりの最大ジョブ数のような論理リソースを管理します。
 - ドライブのアンロードを開始して保留中の要求キューを管理します。
 - 現在のドライブの状態について定期的にメディアサーバーに問い合わせを行います。

NetBackup マスターサーバーと Enterprise Media Manager (EMM) サーバーは同じ物理ホスト上にある必要があります。

マスターサーバーは `nbpem` と `nbjm` のサービスを使用することによって、NetBackup ポリシーでの構成に従ってジョブを実行するように機能します。

EMM サービスは、マスターサーバーのためのリソースを割り当てます。EMM サービスは、すべてのデバイス構成情報のリポジトリです。EMM サービスには、`nbemm` とそのサブコンポーネントのほかに、デバイスとリソースの割り当てのための `nbrb` サービスが含まれます。

バックアップおよびアーカイブ: UNIX クライアントの場合

UNIX クライアントの場合、NetBackup では、ファイルと `raw` パーティションの両方に対して、スケジュールバックアップ、即時手動バックアップおよびユーザー主導バックアップがサポートされています。また、ファイルのユーザー主導アーカイブもサポートされています。`raw` パーティションのアーカイブはサポートされていません。すべての操作は、開始されると、サーバーで同じデーモンおよびプログラムが実行されるという点で類似しています。

バックアップ操作の開始方法は、次のようにそれぞれ異なります。

- スケジュールバックアップは nbpem サービスがジョブの指定時刻到達を検出すると開始します。nbpem は、スケジュールされた実行予定のクライアントバックアップのポリシー構成を確認します。
- 即時手動バックアップは、管理者が **NetBackup** 管理コンソールでこのオプションを選択した場合、または bpbakcup-i コマンドを実行した場合に開始されます。この場合、bprd によって nbpem が起動され、管理者が選択したポリシー、クライアントおよびスケジュールが処理されます。
- ユーザー主導のバックアップまたはアーカイブは、クライアント側のユーザーがそのクライアント側のユーザーインターフェースを介してバックアップまたはアーカイブを開始したときに開始されます。ユーザーは、コマンドラインに bpbakcup コマンドまたは bparchive コマンドを入力することもできます。この処理によって、クライアントの bpbakcup プログラムまたは bparchive プログラムが起動され、要求がマスターサーバーの **NetBackup Request** デーモン bprd に送信されます。bprd によってユーザー要求が受信されると、nbpem と通信し、ポリシー構成に含まれているスケジュールが確認されます。デフォルトでは、nbpem によって、要求元のクライアントが含まれているポリシーで最初に検出されたユーザー主導スケジュールが選択されます。ユーザー主導のバックアップまたはアーカイブでは、ポリシーおよびスケジュールを指定することもできます。**UNIX** の **bp.conf** 内の **BPBACKUP_POLICY** オプションおよび **BPBACKUP_SCHED** オプションおよび **Windows** の同等のオプションの説明を参照できます。
詳しくは、『**NetBackup 管理者ガイド Vol. 1**』を参照してください。

多重化されたバックアップ処理

多重化されたバックアップの処理は多重化されていないバックアップと本質的に同じです。メディア上で多重化されているバックアップイメージごとに個別の bpbarm プロセスおよび bptm プロセスが作成される点が異なります。また、**NetBackup** によって、各イメージには個別の共有メモリーブロックセットも割り当てられます。多重化されたバックアップの他のクライアントとサーバーの処理は同じです。

バックアップログについて

バックアップで発生した問題を診断するためのさまざまなログがあります。

次のコマンドログファイルは、メディアおよびマスターサーバーのエラーのレビューで使われます。

p.169 の「**nbpem のログ**」を参照してください。

p.170 の「**nbproxy のログ**」を参照してください。

p.165 の「**bpdbm のログ**」を参照してください。

p.166 の「**bprd のログ**」を参照してください。

- p.169 の「[nbjm のログ](#)」を参照してください。
- p.165 の「[bpjobd のログ](#)」を参照してください。
- p.170 の「[nbrb のログ](#)」を参照してください。
- p.168 の「[nbemm のログ](#)」を参照してください。
- p.164 の「[bpcompatd のログ](#)」を参照してください。
- p.173 の「[PBX のログ](#)」を参照してください。
- p.175 の「[vnetd のログ](#)」を参照してください。
- p.164 の「[bpcd のログ](#)」を参照してください。
- p.163 の「[bpbrm のログ](#)」を参照してください。
- p.163 の「[bpbkar のログ](#)」を参照してください。
- p.167 の「[bptm のログ](#)」を参照してください。
- p.168 の「[ltid のログ](#)」を参照してください。
- p.175 の「[txxd および txxcd のログ](#)」を参照してください。

次のログファイルは、バックアップ処理のフローに含まれませんが、バックアップの問題を解決するのに役立ちます。

- `acsssi`
- `bpbackup`
- `daemon`
- `reqlib`
- `robots`

- p.162 の「[acsssi のログ](#)」を参照してください。
- p.162 の「[bpbackup のログ](#)」を参照してください。
- p.167 の「[daemon のログ](#)」を参照してください。
- p.173 の「[reqlib のログ](#)」を参照してください。
- p.174 の「[robots のログ](#)」を参照してください。

サポートが必要な場合は、ベリタステクニカルサポートにログを送信してください。

- p.68 の「[ベリタステクニカルサポートへのバックアップログの送信](#)」を参照してください。

ベリタステクニカルサポートへのバックアップログの送信

バックアップで問題が発生した場合は、問題のレポートおよび関連するログをベリタステクニカルサポートに送信して支援を依頼できます。

p.110 の「[合成バックアップの問題レポートに必要なログ](#)」を参照してください。

表 2-1 は、ベリタステクニカルサポートがバックアップの問題を診断するのに必要になるログのリストおよび推奨ログレベルを示します。

メモ: ベリタスは統合ログの診断レベルをデフォルトレベルの 6 に設定することをお勧めします。

p.50 の「[グローバルログレベルについて](#)」を参照してください。

表 2-1 特定のバックアップ問題で収集するログ

問題の種類	収集するログ
バックアップスケジュールの問題	■ デバッグレベル 5 の nbpem ログ ■ デバッグレベル 5 の nbjm ログ ■ 詳細 4 の nbproxy ログ ■ 詳細 2 の bpdbm ログ ■ 詳細 5 の bprd ログ メモ: bprd ログは手動バックアップまたはユーザーが開始するバックアップの問題にのみ必要です。
アクティブにならない、キューに登録されたバックアップジョブの問題	■ デバッグレベル 3 の nbpem ログ ■ デバッグレベル 5 の nbjm ログ ■ デバッグレベル 4 の nbrb ログ ■ 詳細 4 の nbproxy ログ ■ 詳細 2 の bpdbm ログ ■ デフォルトレベルの nbemm ログ ■ デバッグレベル 2 の mds ログ メモ: mds ログは nbemm ログに書き込みます。

問題の種類	収集するログ
書き込みを行わない、アクティブなバックアップジョブの問題	■ デバッグレベル 5 の nbjm ログ ■ デバッグレベル 4 の nbrb ログ ■ 詳細 2 の bpdbrm ログ ■ 詳細 5 の bpbbrm ログ ■ 詳細 5 の bptm ログ ■ 詳細 5 の bpcd ログ 問題がテープのロードまたはロード解除の場合は、サポートは以下のログも必要とします ■ ltid ログ ■ reqlib ログ ■ daemon ログ ■ robots ログ ■ acsssi ログ (UNIX のみ)

p.53 の「Media Manager のデバッグログを上位レベルに設定する」を参照してください。

p.67 の「バックアップログについて」を参照してください。

メディア、デバイスプロセス およびログ記録

この章では以下の項目について説明しています。

- [メディアおよびデバイスの管理の開始プロセス](#)
- [メディアおよびデバイスの管理プロセス](#)
- [Shared Storage Option](#) の管理プロセス
- [バーコード操作](#)
- [メディアおよびデバイスの管理コンポーネント](#)

メディアおよびデバイスの管理の開始プロセス

メディアおよびデバイスの管理プロセスは、NetBackup の起動時に自動的に開始されます。これらの処理を手動で開始するには、`bp.start_all` (UNIX) または `bpup` (Windows) を実行します。`ltid` コマンドは必要に応じて自動的にその他のデーモンとプログラムを開始します。デーモンは初期スタートアップ後に稼働している必要があります。

p.72 の [図 3-1](#) を参照してください。

`tl8d` や `tlhd` のようなロボットデーモンの場合には関連付けられたロボットもデーモンを実行するように設定する必要があります。デーモンを開始や停止する追加の方法が利用可能です。

p.79 の [表 3-1](#) を参照してください。

TL8、TLH、および TLD は、次のような形式のデーモンを必要とします。

ロボット

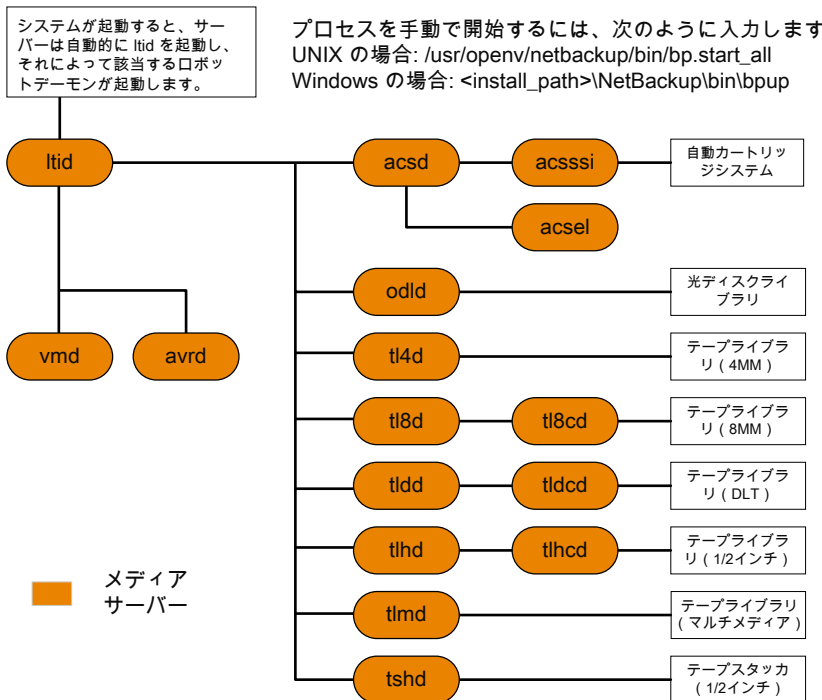
ロボットドライブが接続されている各ホストには、ロボットデーモンが存在する必要があります。これらのデーモンは `ltid` とロボット間のインターフェースを提供します。ロボット内部の異なるドライブが異なるホストに接続できる場合にはロボットデーモンはロボット制御デーモンと通信します (図 3-1 を参照)。

ロボット制御

ロボット内のドライブが異なるホストに接続可能な場合、ロボット制御デーモンによってロボットが集中制御されます。ロボット制御デーモンはドライブが接続されているホストのロボットデーモンからマウント要求やマウント解除要求を受信します。そしてロボットに受信した要求を伝えます。

ロボットのすべてのデーモン開始に関係するホストを知る必要があります。

図 3-1 メディアおよびデバイスの管理の開始



メディアおよびデバイスの管理プロセス

メディア管理やデバイス管理のデーモンの実行中には、**NetBackup** またはユーザーがデータの格納や取り出しを要求できます。スケジュールサービスは最初にこの要求を処理します。

p.65 の「[バックアップ処理およびアーカイブ処理](#)」を参照してください。

デバイスをマウントする結果要求が `nbjm` から `nbrb` に渡され、`nbemm` (**Enterprise Media Manager** サービス) から物理リソースを取得します。

バックアップにロボットのメディアが必要な場合には `ltid` がマウント要求をローカルホストに構成済みのロボットのドライブを管理するロボットデーモンに送信します。その後でロボットデーモンはメディアをマウントし、ロボットデーモンと `ltid` で共有しているメモリでドライブをビジー状態に設定します。デバイスモニターにもドライブのビジー状態が表示されます。

p.74 の [図 3-2](#) を参照してください。

メディアが物理的にロボット内に存在する場合、メディアがマウントされ、操作が続行されます。ロボットにメディアがない場合には `nbrb` が保留中の要求を作成し、デバイスモニターに保留中の要求として表示します。オペレータはメディアをロボットに挿入して適切なデバイスモニターコマンドを使ってマウント要求を実行する要求を再送信する必要があります。

メディアが非ロボット (スタンドアロン) ドライブ用であり要求の条件を満たすメディアを含まない場合にはマウント要求が発行されます。要求が **NetBackup** から発行され、ドライブに適切なメディアが含まれている場合、そのメディアが自動的に割り当てられ、操作が続行されます。

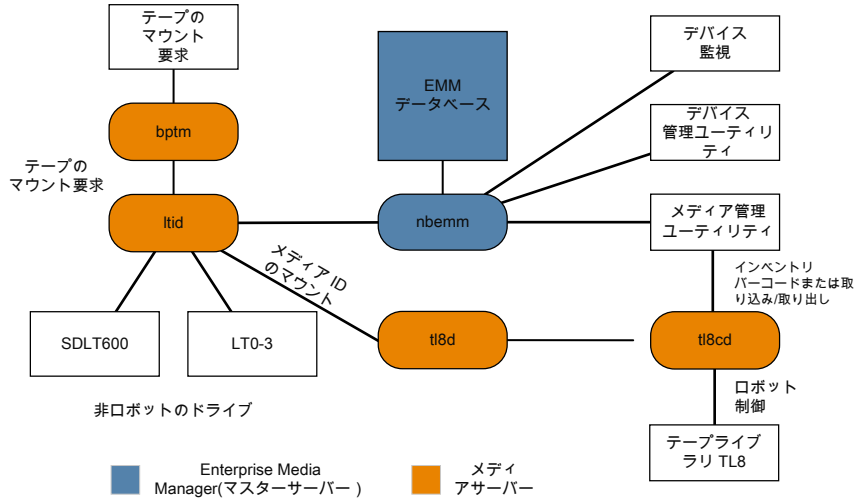
非ロボットドライブ用 **NetBackup** のメディアの選択について詳しくは、『**NetBackup 管理者ガイド Vol. 2**』を参照してください。

メモ: UNIX のテープをマウントするときには、`drive_mount_notify` スクリプトが呼び出されます。このスクリプトは、`/usr/opensv/volmgr/bin` ディレクトリに存在します。このスクリプトについての情報は、そのスクリプト自身に含まれています。マウントが解除される場合、類似したスクリプト (同じディレクトリ内の `drive_unmount_notify`) が呼び出されます。

メディアアクセスポートを通してロボットボリュームが追加または削除された場合には、メディア管理ユーティリティが適切なロボットデーモンと通信してボリュームの場所またはバーコードを検証します。また、メディア管理ユーティリティによって、ロボットインベントリ操作のロボットデーモンも (ライブラリまたはコマンドラインインターフェースを介して) 呼び出されます。

[図 3-2](#) に、メディアおよびデバイスの管理プロセスの例を示します。

図 3-2 メディアおよびデバイスの管理プロセスの例



Shared Storage Option の管理プロセス

Shared Storage Option (SSO) は、テープドライブの割り当ておよび構成に関する、メディアおよびデバイスの管理の拡張機能です。SSOを使うと、複数のNetBackupメディアサーバーまたはSANメディアサーバー間で(スタンドアロンまたはロボットライブラリの)個々のテープドライブを動的に共有できます。

Shared Storage Option について詳しくは、『[NetBackup 管理者ガイド Vol. 2](#)』を参照してください。

次で Shared Storage Option の管理プロセスを提示される順に示します。

- NetBackup またはユーザーはバックアップを開始できます。nbjm プロセスはバックアップのマウント要求を作ります。
- nbrb から EMM サーバーに対して、バックアップのためのドライブの取得が要求されます。
- nbrb から EMM サーバーのデバイスアロケータ (DA) に対して、選択されたドライブのスキャンの停止が要求されます。
- nbemm から適切なメディアサーバー (選択されたドライブのスキャンホスト) に対して、ドライブのスキャンの停止が要求されます。メディアサーバーの共有メモリで oprd、ltid、avrd がスキャン停止要求を実行します。
- 選択されたドライブでのスキャンが停止されると、nbemm から nbrb に通知されます。

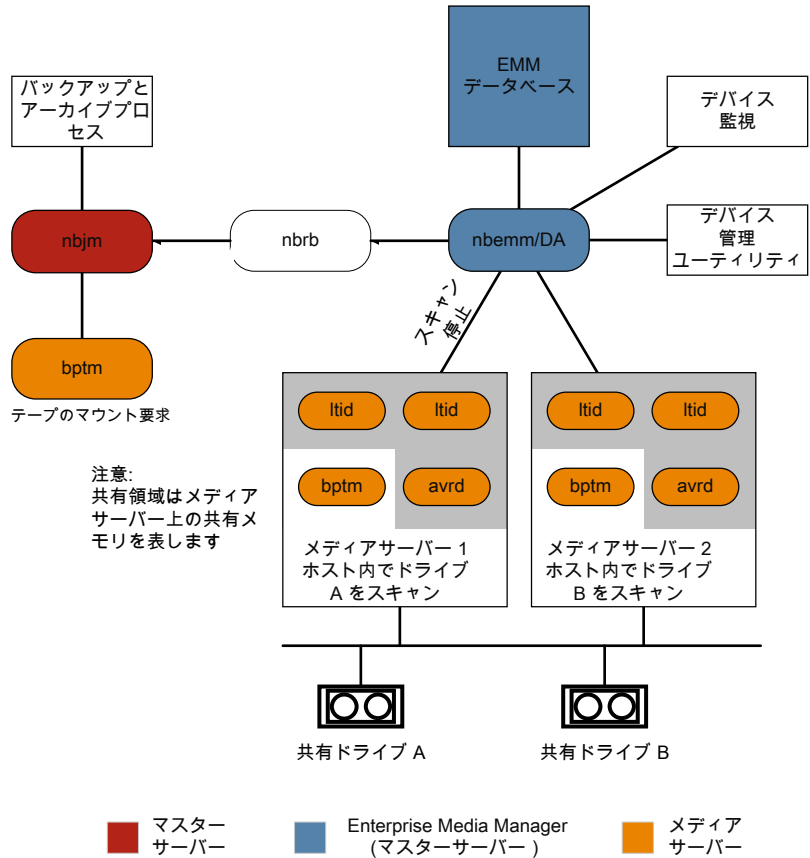
- nbrb から nbjm に対して、選択されたドライブ (A) がバックアップに利用可能であることが通知されます。
- nbjm がマウント要求とドライブの選択を bptm に転送し、bptm がバックアップを続行します。書き込み操作の整合性を保護するため、bptm では、SCSI RESERVE 状態が使用されます。

NetBackup のドライブ予約について詳しくは、『NetBackup 管理者ガイド Vol. 2』を参照してください。

- メディアのマウント操作が開始されます。
- bptm によってドライブの位置確認が実行され、他のアプリケーションによってドライブ上のテープが巻き戻されていないことが確認されます。bptm はテープへの実際の書き込みも行います。
- バックアップが完了したときに nbjm は nbrb にリソースの解放を指示します。
- nbrb によって、EMM でのドライブの割り当てが解除されます。
- EMM からスキャンホストに対して、ドライブのスキャンの再開が指示されます。メディアサーバーの共有メモリで oprd、ltid、avrd がスキャン要求を実行します。

図 3-3 に、Shared Storage Option の管理プロセスを示します。

図 3-3 SSO コンポーネントでのメディアおよびデバイスの管理プロセスの流れ



バーコード操作

バーコードの読み込みは、メディアおよびデバイスの管理ではなく、主にロボットハードウェアの機能です。ロボットにバーコードリーダーが備えられている場合、テープのバーコードがスキャンされ、ロボットの内部メモリに格納されます。これによって、スロット番号と、そのスロット内のテープのバーコードが関連付けられます。関連付けは、ロボットに対して問い合わせを行うことで、**NetBackup** によって行われます。

ロボットがバーコードをサポートしている場合には、**NetBackup** はテープをマウントする前に確認の追加測定として自動的にテープのバーコードを EMM データベースの内容

と比較します。バーコードを読み込めるロボットのメディアに対する要求はその他の要求と同じように始まります。

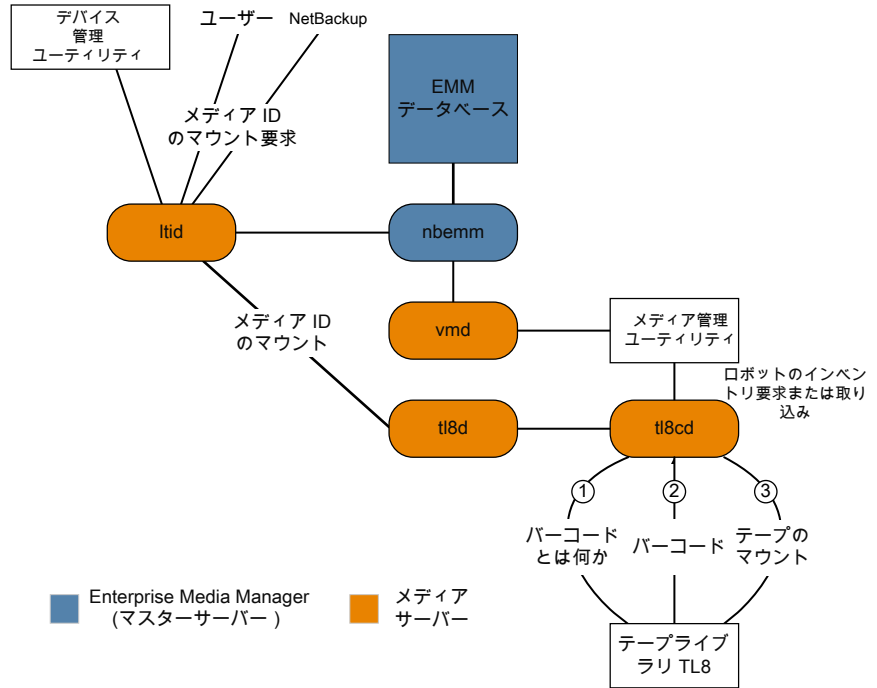
p.78 の [図 3-4](#) を参照してください。

ltid コマンドのメディア ID があるロボットのロボットデーモンに対するマウント要求はメディア ID と場所情報を含みます。この要求によりロボットデーモンはロボット制御デーモンまたは指定スロットにあるテープのバーコードのロボットを問い合わせます。(これは、正しいメディアがそのスロット内に存在するかどうかを確認するための事前確認です)。そのメモリに含まれるバーコードの値が、ロボットによって戻されます。

ロボットデーモンはこのバーコードと ltid から受信した値を比較して次のいずれかの処理を実行します。

- バーコードが一致せず、マウント要求が **NetBackup** のバックアップジョブ用でない場合には、ロボットデーモンが ltid に通知して保留中の操作要求 ([テープは不適切な場所に配置されています (**Misplaced Tape**)]) をデバイスモニターに表示します。この場合、オペレータは、スロットに適切なテープを挿入する必要があります。
- バーコードが一致せずマウント要求が **NetBackup** のバックアップジョブ用である場合にはロボットデーモンが ltid に通知してマウント要求を取り消します。その後、**NetBackup (bptm)** から nbjm および EMM に対して、新しいボリュームが要求されます。
- バーコードが一致する場合、ロボットデーモンがロボットに対して、そのテープをドライブに移動するように要求します。その後、ロボットによってテープがマウントされます。操作の開始時に、アプリケーション (**NetBackup** など) によってメディア ID が確認され、そのメディア ID がそのスロット内のメディア ID とも一致する場合、操作が続行されます。**NetBackup** では、メディア ID が不適切な場合、[Media Manager がドライブ内で誤ったテープを見つけました (**media manager found wrong tape in drive**)] エラー (**NetBackup** 状態コード 93) が表示されます。

図 3-4 バーコード要求



メディアおよびデバイスの管理コンポーネント

このトピックでは、メディア管理とデバイス管理に関連するファイルとディレクトリの構造、プログラムとデーモンについて示します。

図 3-5 に UNIX サーバーのメディア管理とデバイス管理のファイル構造とディレクトリ構造を示します。Windows 版 NetBackup サーバーにも同等のファイルおよびディレクトリが存在し、それらは NetBackup がインストールされているディレクトリ (デフォルトでは C:\Program Files\VERITAS ディレクトリ) に配置されます。

図 3-5 メディアおよびデバイスの管理のディレクトリおよびファイル

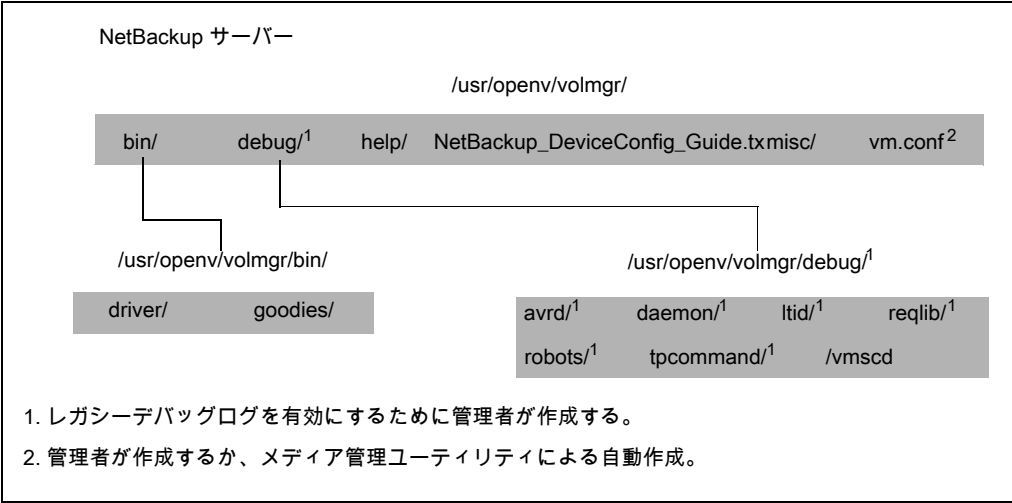


表 3-1 に、特に重要なファイルおよびディレクトリを示します。

表 3-1 メディアおよびデバイスの管理のディレクトリおよびファイル

ファイルまたはディレクトリ	内容
bin	メディアおよびデバイスの管理に必要なコマンド、スクリプト、プログラム、デーモン、ファイルが含まれているディレクトリ。bin の下にある次のサブディレクトリが利用可能です。 driver: ロボットを制御するために各種のプラットフォームで使う SCSI ドライバが含まれています。 goodies: vmconf スクリプトとスキャンユーティリティを含みます。
debug	Volume Manager デーモンとvmd のレガシーデバッグログ、vmd と ltid のすべての要求元のレガシーデバッグログ、デバイス構成のレガシーデバッグログです。デバッグログを実行するには、管理者はこれらのディレクトリを作成する必要があります。
help	メディアおよびデバイスの管理のプログラムが使用するヘルプファイルです。これらのファイルは ASCII 形式です。
misc	メディアおよびデバイスの管理の各種コンポーネントに必要なロックファイルと一時ファイルです。

ファイルまたはディレクトリ	内容
vm.conf	メディアおよびデバイスの管理の構成オプション。

表 3-2 にメディア管理とデバイス管理のプログラムとデーモンを示します。この表では、プログラムまたはデーモンの起動方法と停止方法、およびその動作が記録されるログ (存在する場合) について説明します。UNIX では、`/usr/opensv/volmgr/bin` の下にこの表のすべてのコンポーネントがあります。Windows では、これらは `install_path\volmgr\bin` にあります。

メモ: 次の表には、システムログに関する説明が含まれています。UNIX では、`syslog` がこのログを管理します (この機能はデーモンです)。Windows の場合、システムログはイベントビューアによって管理されます (ログの形式はアプリケーションです)。

表 3-2 メディアおよびデバイスの管理のデーモンおよびプログラム

プログラムまたはデーモン	説明
acsd	自動カートリッジシステムデーモンは、自動カートリッジシステムとともに動作し、<code>acsssi</code> プロセス (UNIX の場合) または <code>STK Libattach</code> サービス (Windows の場合) を通して ACS ロボットを制御するサーバーと通信します。 UNIX の場合、<code>acsssi</code> プログラムおよび <code>acsse</code> プログラムの説明を参照してください。 起動方法: <code>ltid</code> を起動します (UNIX の場合は、<code>ltid</code> を起動しなくても、<code>/usr/opensv/volmgr/bin/acsd</code> コマンドを実行して起動することもできます)。 停止方法: <code>ltid</code> を停止します (UNIX の場合は、<code>ltid</code> を停止しなくても、PID (プロセス ID) を検索し、<code>kill</code> コマンドを実行して停止することもできます)。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。<code>vm.conf</code> ファイルに <code>VERBOSE</code> を追加すると、デバッグ情報が記録されます。UNIX では、<code>-v</code> オプションを指定してデーモンを起動しても、デバッグ情報が記録されます。このオプションは、<code>ltid</code> を介して、または <code>vm.conf</code> ファイルに <code>VERBOSE</code> を追加することによって使用できます。
acsse	UNIX だけで使用できます。 『NetBackup デバイス構成ガイド』を参照してください。

プログラムまたはデーモン	説明
acsssi	UNIX だけで使用できます。 『NetBackup デバイス構成ガイド』を参照してください。
avrd	自動ボリューム認識デーモンは、自動ボリューム割り当ておよびラベルスキャンを制御します。このデーモンによって、NetBackup では、ラベル付けされたテープボリュームを読み込んだり、関連付けられたリムーバブルメディアを要求プロセスに自動的に割り当てることができます。 起動方法: ltid を開始します (UNIX の場合は、ltid を開始しなくても、/usr/openv/volmgr/bin/avrd コマンドを実行して起動することもできます)。 停止方法: ltid を停止します (UNIX の場合は、ltid を停止しなくても、PID (プロセス ID) を検索し、kill コマンドを実行して停止することもできます)。 デバッグログ: すべてのエラーは、システムログに書き込まれます。vm.conf ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。UNIX では、avrd を中止し、-v オプションを指定してデーモンを起動しても、デバッグ情報が記録されます。
ltid	device デーモン (UNIX の場合) または NetBackup Device Manager サービス (Windows の場合) は、テープの予約および割り当てを制御します。 起動方法: UNIX では、/usr/openv/volmgr/bin/ltid コマンドを実行します。Windows では、[メディアおよびデバイスの管理 (Media and Device Management)] ウィンドウの [Device Manager サービスの停止/再起動 (Stop/Restart Device Manager Service)] コマンドを実行します。 停止方法: UNIX では、/usr/openv/volmgr/bin/stoptlid コマンドを実行します。Windows では、[メディアおよびデバイスの管理 (Media and Device Management)] ウィンドウの [Device Manager サービスの停止/再起動 (Stop/Restart Device Manager Service)] コマンドを実行します。 デバッグログ: エラーは、システムログと ltid のデバッグログに書き込まれます。-v オプション (UNIX だけで利用可能) を指定してデーモンを起動するか、または vm.conf ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。

プログラムまたはデーモン	説明
tl4d	4MM テープライブラリデーモンは、ltid と 4MM テープライブラリの間のインターフェースで、SCSI インターフェースを通してロボットと通信します。 起動方法: ltidを開始します (UNIX の場合は、ltidを開始しなくても、usr/opensv/volmgr/bin/tl4d コマンドを実行して起動することもできます)。 停止方法: ltidを停止します (UNIX の場合は、ltidを停止しなくても、PID(プロセス ID)を検索し、kill コマンドを実行して停止することもできます)。 デバッグログ: すべてのエラーは、システムログに書き込まれます。 vm.conf ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。UNIX では、-v オプションを指定してデーモンを (単独または ltid を通して) 開始してもデバッグ情報が記録されます。
tl8d	8MM テープライブラリデーモンは、TL8 ロボットのロボット制御を提供します (8MM テープライブラリまたは 8MM テープスタック)。同じ TL8 ロボット内の 8MM テープライブラリデーモンドライブが、ロボットが制御されているホストと異なるホストに接続されている場合があります。tl8d は、ローカル ltid とロボット制御間のインターフェースです。TL8 ロボットのドライブに対するデバイスパスがホストにある場合、そのドライブに対するマウント要求またはマウント解除要求は、最初にローカル ltid に送られ、続いてローカル tl8d に送られます (すべて同じホスト内)。その後 tl8d は、ロボットを制御するホスト上 (または別のホスト上) の tl8cd に要求を転送します。 起動方法: ltidを開始します (UNIX の場合は、ltidを開始しなくても、usr/opensv/volmgr/bin/tl8d コマンドを実行して起動することもできます)。 停止方法: ltidを停止します (UNIX の場合は、ltidを停止しなくても、PID(プロセス ID)を検索し、kill コマンドを実行して停止することもできます)。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。vm.conf ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。UNIX では、-v オプションを指定してデーモンを (単独または ltid を通して) 開始してもデバッグ情報が記録されます。

プログラムまたはデーモン	説明
tl8cd	8MM テープライブラリ制御デーモンは、TL8 ロボットのロボット制御を提供し、SCSI インターフェースを通してロボットと通信します。tl8cd は、ドライブが接続されているホストの tl8d からのマウント要求およびマウント解除要求を受信して、これらの要求をロボットに送信します。 起動方法: ltid を起動します (UNIX の場合は、ltid を起動しなくても、/usr/openv/volmgr/bin/tl8cd コマンドを実行して起動することもできます)。 停止方法: ltid を停止するか、または tl8cd -t コマンドを実行して停止します。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。vm.conf ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。UNIX では、-v オプションを指定してデーモンを (単独または ltid を通して) 開始してもデバッグ情報が記録されます。
tlidd	DLT テープライブラリデーモンは、tlidd と連携して TLD ロボットへの要求を処理します (DLT テープライブラリと DLT テープスタッカ)。tlidd は、前述の tl8d の場合と同じ方法でローカル ltid とロボット制御 (tlidd) 間のインターフェースを提供します。 起動方法: ltid を開始します (UNIX の場合は、ltid を開始しなくても、/usr/openv/volmgr/bin/tlidd コマンドを実行して起動することもできます)。 停止方法: ltid を停止します (UNIX の場合は、ltid を停止しなくても、PID (プロセス ID) を検索し、kill コマンドを実行して停止することもできます)。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。vm.conf ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。UNIX では、-v オプションを指定してデーモンを (単独または ltid を通して) 開始してもデバッグ情報が記録されます。

プログラムまたはデーモン	説明
tl8cd	DLT テープライブラリ制御デーモンは、前述の tl8cd の場合と同じ方法で TLD ロボットのロボット制御を提供します。 起動方法: ltid を開始します (UNIX の場合は、ltid を開始しなくても、<code>/usr/openv/volmgr/bin/tl8cd</code> コマンドを実行して起動することもできます)。 停止方法: ltid を停止するか、または <code>tl8cd -t</code> コマンドを実行して停止します。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。<code>vm.conf</code> ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。UNIX では、<code>-v</code> オプションを指定してデーモンを (単独または ltid を通して) 開始してもデバッグ情報が記録されます。
tlhd	1/2 インチテープライブラリデーモンは、tlhcd と動作して、IBM 自動テープライブラリ (ATL) 内に存在する TLH ロボットへの要求を処理します。tlhd は、前述の tl8d の場合と同じ方法でローカル ltid とロボット制御 (tlhcd) 間のインターフェースを提供します。 起動方法: ltid を開始します (UNIX の場合は、ltid を開始しなくても、<code>/usr/openv/volmgr/bin/tlhd</code> コマンドを実行して起動することもできます)。 停止方法: ltid を停止します (UNIX の場合は、ltid を停止しなくても、PID (プロセス ID) を検索し、<code>kill</code> コマンドを実行して停止することもできます)。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。<code>vm.conf</code> ファイルに VERBOSE を追加すると、デバッグ情報が記録されます。UNIX では、<code>-v</code> オプションを指定してデーモンを (単独または ltid を通して) 開始してもデバッグ情報が記録されます。

プログラムまたはデーモン	説明
tlhcd	1/2 インチテープライブラリ制御デーモンは、前述の tl8cd の場合と同じ方法で IBM 自動テープライブラリ (ATL) 内に存在する TLH ロボットのロボット制御を提供します。 起動方法: ltid を開始します (UNIX の場合は、ltid を開始しなくても、/usr/openv/volmgr/bin/tlhcd コマンドを実行して起動することもできます)。 停止方法: ltid を停止するか、または tlhcd -t コマンドを実行して停止します。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。-v オプションを指定してデーモンを (単独または ltid を通して) 開始すると、デバッグ情報が記録されます。-v オプションは、UNIX だけで使用できます。また、vm.conf ファイルに VERBOSE オプションを追加しても、デバッグ情報が記録されます。
tlmd	マルチメディアテープライブラリデーモンは、ltid と、ADIC Distributed AML Server (DAS) 内に存在する TLM ロボットの間のインターフェースです。ネットワーク API インターフェースを介して TLM ロボットと通信します。 起動方法: ltid を起動します (ltid を起動しなくても、/usr/openv/volmgr/bin/tlmd コマンドを実行して起動することもできます)。 停止方法: ltid を停止します。ltid を停止しなくても、PID (プロセス ID) を検索し、kill コマンドを実行して停止することもできます。 デバッグログ: エラーは、システムログとロボットのデバッグログに書き込まれます。-v オプションを指定してデーモンを (単独または ltid を通して) 開始すると、デバッグ情報が記録されます。-v オプションは、UNIX だけで使用できます。また、vm.conf ファイルに VERBOSE オプションを追加しても、デバッグ情報が記録されます。

プログラムまたはデーモン	説明
tshd	1/2 インチテープスタッカデーモンは、ltid と 1/2 インチカートリッジスタッカ間のインターフェースで、SCSI インターフェースを通してロボットと通信します。このロボットは、Windows ではサポートされていません。 起動方法: ltid を開始します (UNIX の場合は、ltid を開始しなくても、usr/openv/volmgr/bin/tshd コマンドを実行して起動することもできます)。 起動方法: tpconfig コマンド。 停止方法: UNIX では、ユーティリティで [Quit] オプションを使います。Windows では、tpconfig は、完了するまで実行される単なるコマンドラインインターフェースです ([終了 (Quit)] オプションはありません)。 デバッグログ: tpcommand のデバッグログ。
vmd	Volume Manager デーモン (Windows の場合は NetBackup Volume Manager サービス) は、メディアおよびデバイスの管理のリモート管理とリモート制御を可能にします。 起動方法: ltid を起動します。 停止方法: Terminating Media Manager Volume デーモンオプションを使います。 デバッグログ: システムログと (daemon または reqlib デバッグディレクトリが存在する場合) デバッグログ。
vmgcd	Media Manager Status Collector デーモンは、EMM サーバーのデータベースを、5.x のサーバーに接続されているドライブの実際の状態を反映した最新の状態に保持します。 起動方法: EMM サーバー 停止方法: EMM サーバー デバッグログ: /usr/openv/volmgr/debug/vmgcd (UNIX の場合) または install_path\Volmgr\debug\vmgcd (Windows の場合)

リストアッププロセスおよびログ記録

この章では以下の項目について説明しています。

- [リストアッププロセス](#)
- [UNIX クライアントのリストアップ](#)
- [Windows クライアントのリストアップ](#)
- [リストアップログについて](#)
- [ベリタステクニカルサポートへのリストアップログの送信](#)

リストアッププロセス

リストアッププロセスの動作の仕組みを理解することは、特定の問題に対処するためにどのログを確認すべきかを判断するのに役立つ最初のステップです。イメージをテープからリストアップするかディスクからリストアップするかによってプロセスが異なります。

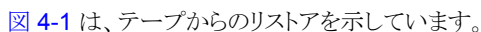
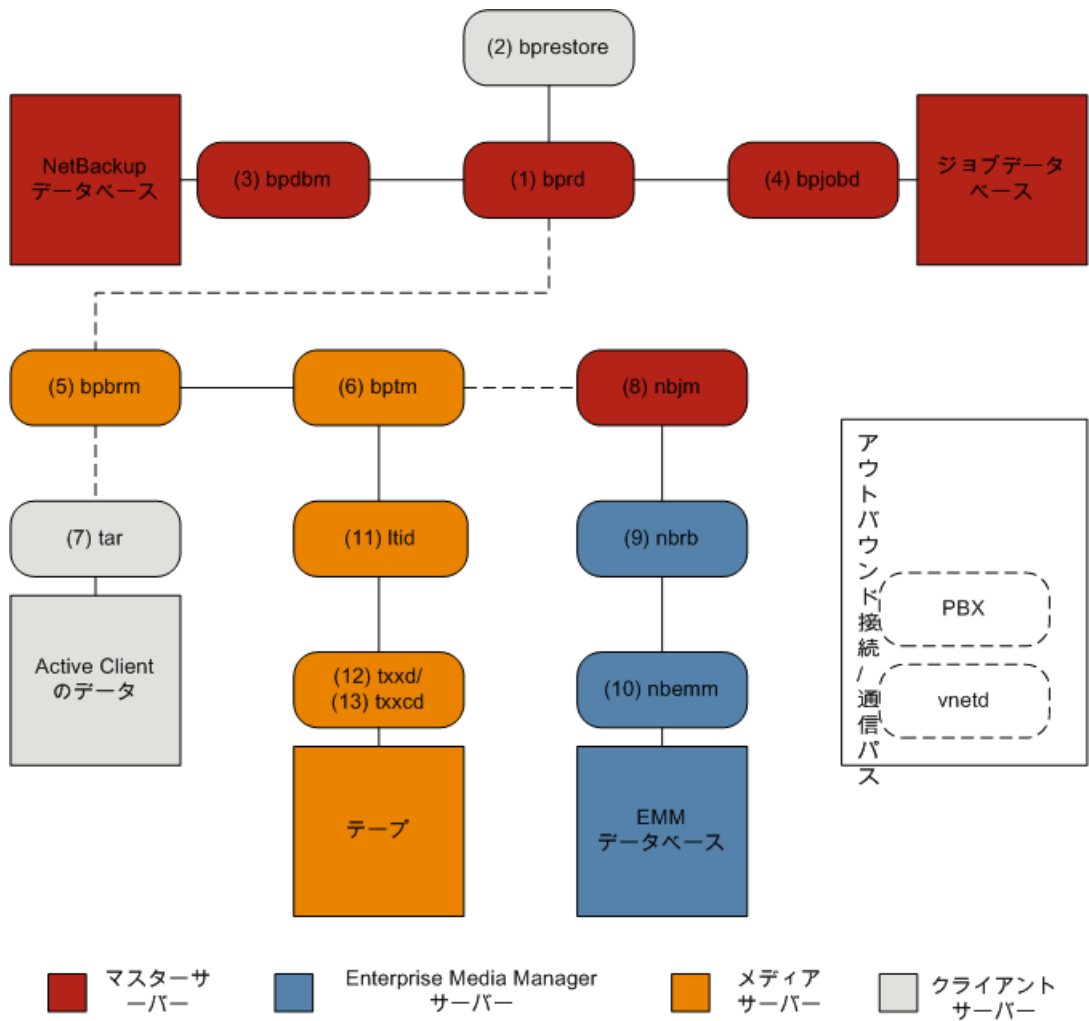
 **図 4-1** は、テープからのリストアップを示しています。

図 4-1 テーププロセスフローからのリストア



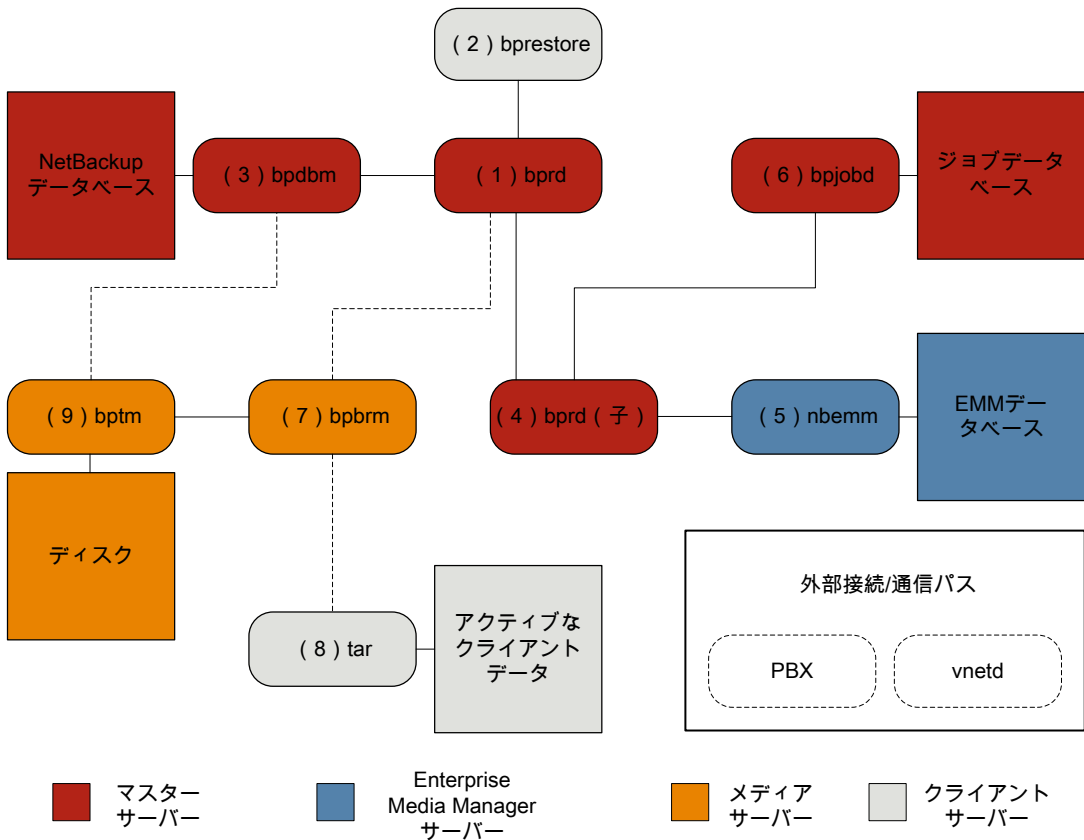
テープからのリストア手順

- 1 (1) NetBackup Request デーモン (bprd) はリストア要求を受信します。この要求はバックアップ、アーカイブおよびリストアのユーザーインターフェースまたは (2) コマンドライン (bprestore) から開始できます。
- 2 bprd は 2 つの子プロセス MAIN bprd と MPX-MAIN-bprd を起動します。MAIN bprd プロセスはイメージおよびメディアの特定に使用され、MPX-MAIN-bprd プロセスはリストア工程の管理に使用されます。分かりやすくするため、これらの 3 つのプロセスすべてをここでは bprd と呼びます。
- 3 bprd サービスは (3) NetBackup Database Manager プログラム (bpdbm) と通信し、要求されたファイルのリストアに必須の情報を取得します。
- 4 情報を取得すると、bprd は (4) bpjobd と通信し、ジョブデータベースのジョブリストにジョブが追加されます。ジョブはアクティビティモニターで表示可能になります。リソースが取得される前でも[アクティブ (Active)]として表示されます。
- 5 bprd サービスは構内交換機 (PBX) および NetBackup Regacy Network (vnetd) を介して実行され、(5) NetBackup Backup Restore Manager (bpbarm) を開始します。
- 6 bpbarm サービスは (6) テープ管理プロセス (bptm) を開始し、リストアに必要なメディアインフォメーションを提供します。また、(7) クライアントのテープアーカイブプログラム (tar) (PBX および vnetd 経由) を開始し、tar と bptm 間の接続を作成します。
- 7 bptm プロセスは、リソース要求を (8) NetBackup Job Manager (nbjm) に PBX および vnetd を介して送信します。
- 8 nbjm プロセスは、(10) Enterprise Media Manager (nbemm) に問い合わせを行う (8) NetBackup Resource Broker (nbrb) にリソース要求を送信します。リソースが割り当てられると、nbrb は、nbjm に伝達し、nbjm は bptm に通知します。
- 9 bptm プロセスは、(11) 論理テープインターフェースデーモン (ltid) にマウント要求を行います。ltid サービスは (12) ロボットドライブデーモン (txxd、xx は使用するロボットの種類によって異なります) を呼び出します。txxd デーモンは (13) メディアをマウントするロボット制御デーモン (txxcd) へのマウント要求と通信します。
- 10 bptm プロセスは、メディアからリストアするデータを読み込み、tar に配信します。
- 11 tar プロセスはクライアントディスクにデータを書き込みます。
- 12 リストアが完了すると、bptm はメディアのマウントを解除し、nbjm に通知します。ジョブはアクティビティモニターで[完了 (Done)]として表示されます。

リストアプロセスフローには含まれませんが、リストアの問題解決に有用な追加のログには、reqlib、daemon、robots、acsssi などがあります。

図 4-2 は、ディスクからのリストアを示しています。

図 4-2 ディスクのプロセスフローからのリストア



ディスクからのリストア手順

- 1 (1) NetBackup Request デーモン (bprd) はリストア要求を受信します。この要求はバックアップ、アーカイブおよびリストアのユーザーインターフェースまたは (2) コマンドライン (bprestore) から開始できます。
- 2 bprd プロセスは (3) NetBackup Database Manager プログラム (bpdbm) に接続して、リストアするファイル、クライアント、およびメディア情報を識別します。
- 3 The bprd プロセスは (4) bprd 子プロセスを開始します。bprd 子プロセスは (5) Enterprise Media Manager (nbemm) を呼び出し、ディスクストレージユニットが利用可能であるかを検証します。
- 4 bprd 子プロセスは (6) bpjobd と通信して jobid を割り当てます。リストアジョブはアクティビティモニターで表示可能になります。

- 5 bprd プロセスは、構内交換機 (PBX) および NetBackup Legacy Network Service (vnetd) を介して (7) メディアサーバーの NetBackup Backup Restore Manager (bpbrm) を開始します。
- 6 bpbrm サービスは、PBX および vnetd を使用して (8) クライアントシステムのテープアーカイブプログラム (tar) との通信を確立します。また、(9) テープ管理プロセス (bptm) も開始します。
- 7 bptm プロセスは bpdgm 呼び出し (PBX および vnetd 経由)、フラグメント情報を取得してディスクをマウントします。
- 8 bptm プロセスはディスクからバックアップイメージを読み込み、要求データを tar にストリーミングします。
- 9 tar プロセスはデータをストレージの宛先にコミットします。

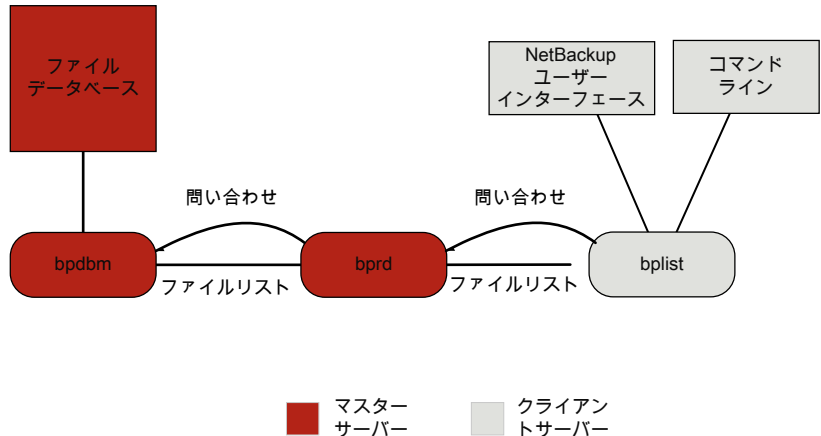
リストアに関するプロセスごとにログファイルがあります。これらのログはリストアで発生した問題の診断に使用できます。

UNIX クライアントのリストア

リストアを開始する前に、クライアントの bplist プログラムを使ってバックアップイメージで利用可能なファイルをリストするファイルカタログを参照し、目的のファイルを選択します。bplist をコマンドラインから直接開始することができます。これにより、NetBackup のユーザーインターフェースプログラムが bplist を使うことができます。

ファイルリストを取り込むために、bplist は問い合わせをマスターサーバーの Request デーモン (bprd) に送信します (図 4-3を参照)。Request デーモンはその後で bpdgm に情報を問い合わせるクライアントの bplist に伝送します。

図 4-3 リストの処理 - UNIX クライアント



リストアの処理手順は、(示される順序で) 次のように実行されます。

- リストアを開始すると、NetBackup によってクライアントの bprestore プログラムが起動され、そのプログラムによって要求が NetBackup Request デーモン bprpd に送信されます。この要求によって、ファイルおよびクライアントが識別されます。その後、NetBackup Request デーモンによって、bpcd (NetBackup Client デーモン) を使用して Backup Restore Manager (bpbrm) が起動されます。

メモ: Backup Exec イメージをリストアする場合は、クライアントで bpbrm が nbtar でではなく mtfrd を起動します。サーバープロセスは、NetBackup のリストアの場合と同じです。

- 対象のデータが存在するディスクデバイスまたはテープデバイスがマスターサーバーに接続されている場合、マスターサーバーで、bprpd によって Backup Restore Manager が起動されます。そのディスクユニットまたはテープユニットがメディアサーバーに接続されている場合、そのメディアサーバーで、bprpd によって Backup Restore Manager が起動されます。
- この Backup Restore Manager が bptm を起動し、クライアントデーモン (bpcd) を使ってクライアントの NetBackup nbtar とサーバーの bptm 間の接続を確立します。
- テープの場合: bptm 処理は、イメージカタログに基づいて、どのメディアがリストアに必要であるかを識別します。bptm はその後で nbrb から nbjm を通じて必要なメディアの割り当てを要求します。nbjm はその後で mds (nbemmの一部) にリソースを確認

します。nbemm はメディアを割り当て、(テープメディア用の) 適切なドライブを選択して割り当てます。

bptm から ltid に対して、ドライブへのテープのマウントが要求されます。

ディスクの場合: ディスクは本質的に並列アクセスをサポートするので、bptm が nbrb の割り当てを要求する必要はありません。System Disk Manager への読み込み要求では、bptm によってファイルパスが使用されます。

- bptm 2つの方法の1つのクライアントにイメージを指示します。サーバーがサーバー自体をリストアする (サーバーおよびクライアントが同じホストに存在する) 場合は、nbtar によって共有メモリから直接データを読み込みます。サーバーが別のホストに存在するクライアントをリストアする場合は、bptm の子プロセスが作成され、このプロセスによってクライアントの nbtar にデータが送信されます。

メモ: バックアップイメージ全体ではなく、リストア要求を満たすために必要なイメージの一部だけがクライアントに送信される場合もあります。

- NetBackup nbtar プログラムによって、クライアントディスクにデータを書き込みます。

メモ: NetBackup が動作するには、PBX が実行されている必要があります (PBX は次の図には示されていません)。PBX 問題を解決する方法について詳しくは、『NetBackup トラブルシューティングガイド』を参照してください。

Windows クライアントのリストア

NetBackup では、UNIX クライアントの場合と同様の操作が Windows クライアントでもサポートされています。

次に、リストア処理に関連する Windows プロセスを示します。

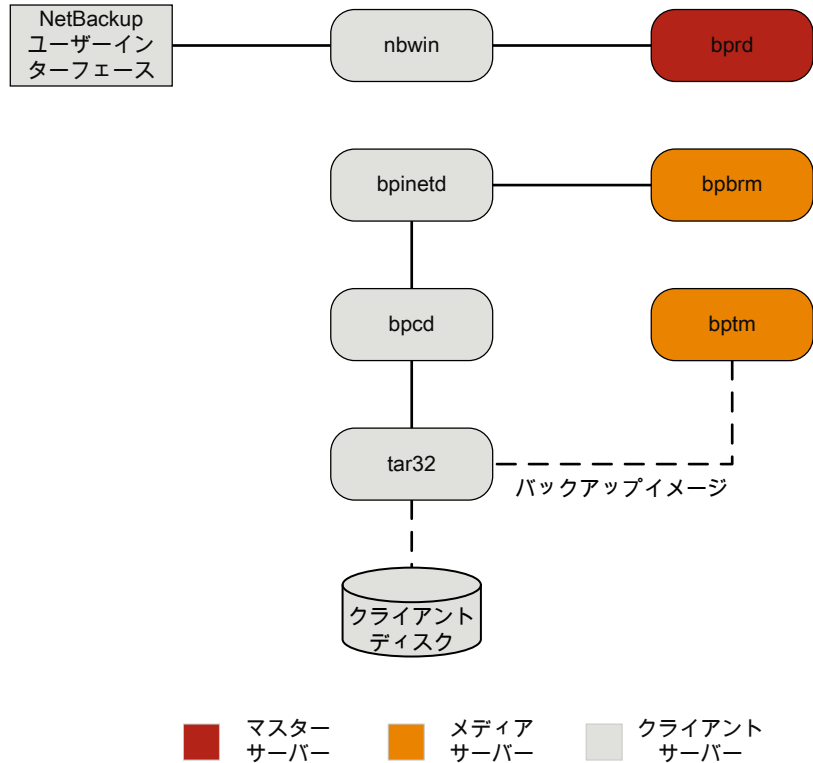
- NBWIN は、クライアントのユーザーインターフェースプログラムです。bpbackup 機能および bparchive 機能が NBWIN に統合されています。
- BPINETD の役割は、UNIX クライアントの inetd と同じです。
- NetBackup Client デーモンは BPCD と呼ばれます。
- TAR32 は、Windows 版 NetBackup の一部で、その役割は UNIX の ntar と同じです。

メモ: Backup Exec イメージのリストアを行う場合は、クライアント上では、bpbrm によって tar32.exe ではなく mtfprd.exe が起動されます。サーバープロセスは、NetBackup のリストアの場合と同じです。

サーバープロセスは、UNIX の場合と同じです。

図 4-4 に、これらの操作に関連するクライアントプロセスを示します。

図 4-4 リストア: Windows クライアントの場合



リストアログについて

リストアで発生した問題を診断するためのさまざまなログがあります。リストアプロセスの動作の仕組みを理解することは、特定の問題に対処するためにどのログを確認すべきかを判断するのに役立つ最初のステップです。

サポートが必要な場合は、ベリタステクニカルサポートにログを送信してください。

p.95 の「[ベリタステクニカルサポートへのリストアログの送信](#)」を参照してください。

リストアエラーのレビューで使われる共通のログファイルは次のとおりです。

- p.166 の「[bprd のログ](#)」を参照してください。
- p.166 の「[bprestore のログ](#)」を参照してください。
- p.173 の「[PBX のログ](#)」を参照してください。
- p.175 の「[vnetd のログ](#)」を参照してください。
- p.165 の「[bpdbm のログ](#)」を参照してください。
- p.165 の「[bpjobd のログ](#)」を参照してください。
- p.163 の「[bpbrm のログ](#)」を参照してください。
- p.167 の「[bptm のログ](#)」を参照してください。
- p.174 の「[tar ログ](#)」を参照してください。
- p.169 の「[nbjm のログ](#)」を参照してください。
- p.170 の「[nbrb のログ](#)」を参照してください。
- p.168 の「[nbemm のログ](#)」を参照してください。
- p.168 の「[ltid のログ](#)」を参照してください。
- p.173 の「[reqlib のログ](#)」を参照してください。
- p.174 の「[robots のログ](#)」を参照してください。
- p.162 の「[acsssi のログ](#)」を参照してください。

ベリタステクニカルサポートへのリストアログの送信

リストアで問題が発生した場合は、問題のレポートおよび関連するログをベリタステクニカルサポートに送信して支援を依頼できます。

- p.110 の「[合成バックアップの問題レポートに必要なログ](#)」を参照してください。

[表 4-1](#)は、ベリタステクニカルサポートがリストアの問題を診断するのに必要になるログのリストおよび推奨ログレベルを示します。

メモ: ベリタスは統合ログの診断レベルをデフォルトレベルの **6** に設定することをお勧めします。

- p.50 の「[グローバルログレベルについて](#)」を参照してください。
-

表 4-1 特定のリストア問題で収集するログ

問題の種類	収集するログ
テープのリストアジョブの問題	■ デバッグレベル 5 の nbjm ログ ■ デバッグレベル 1 の nbemm ログ ■ デバッグレベル 4 の nbrb ログ ■ 詳細 1 の bpdbm ログ ■ 詳細 5 の bprd ログ ■ 詳細 5 の bpbrm ログ ■ 詳細 5 の tar ログ ■ 詳細 5 の bpcd ログ 問題がメディアまたはドライブの場合は、サポートは以下のログも必要とします ■ reqlib ログ ■ daemon ログ ■ robots ログ ■ acsssi ログ (UNIX のみ)
ディスクのリストアジョブの問題	■ 詳細 1 の bpdbm ログ ■ 詳細 5 の bprd ログ ■ 詳細 5 の bpbrm ログ ■ 詳細 5 の bptm ログ ■ 詳細 5 の bpdm ログ ■ 詳細 5 の tar ログ ■ 詳細 5 の bpcd ログ

p.53 の「Media Manager のデバッグログを上位レベルに設定する」を参照してください。

p.94 の「リストアログについて」を参照してください。

高度なバックアップおよびリストア機能

この章では以下の項目について説明しています。

- [SAN クライアントファイバートランスポートのバックアップ](#)
- [SAN クライアントファイバートランスポートのリストア](#)
- [ホットカタログバックアップ](#)
- [ホットカタログのリストア](#)
- [合成バックアップ](#)

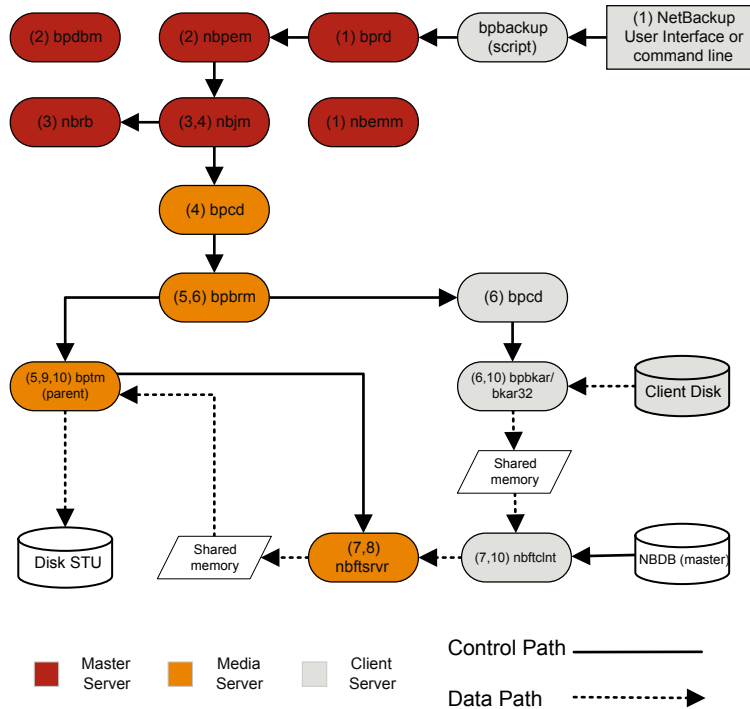
SAN クライアントファイバートランスポートのバックアップ

次に、SAN クライアントのバックアッププロセスを示します。

SAN クライアントの機能によって、ディスクへのバックアップ時に、NetBackup メディアサーバーと SAN 接続された NetBackup クライアントとの間でデータを高速に移動できます。バックアップデータは、SAN 接続されたクライアントからメディアサーバーへ、ファイバーチャネル接続を使用して送信されます。

FT Service Manager (FSM) は、SAN クライアントの一部としてマスターサーバー内に存在するドメインレイヤーサービスです。FSM は、SAN クライアントリソースの検出、構成、イベントの監視を行います。FSM はクライアントとメディアサーバーからファイバーチャネル情報を収集し、NetBackup リレーショナルデータベース (NBDB) に情報をポピュレートします。FSM は NBDB のサブプロセスとして動作して NBDB のログにログメッセージを書き込みます。FSM は、NetBackup クライアント上の nbftclnt プロセスやメディアサーバー上の nbftsrvr プロセスと相互作用します。

図 5-1 SAN クライアントのバックアッププロセスのフロー



SAN クライアントのバックアッププロセスの処理手順は次のとおりです。

SAN クライアントのバックアップ手順

- 1 NetBackup マスターサーバーまたはプライマリクライアントがバックアップを開始します。NetBackup Request デーモン (bprd) から Policy Execution Manager (nbpem) にバックアップ要求が送信されます。nbpem によってポリシーの構成内容が処理されます。

nbpem、nbjm、nrb、nbemm など、その他のすべてのデーモンおよびプログラムは、必要に応じて起動されます。

- 2 Policy Execution Manager サービス (nbpem) によって、次の操作が実行されます。

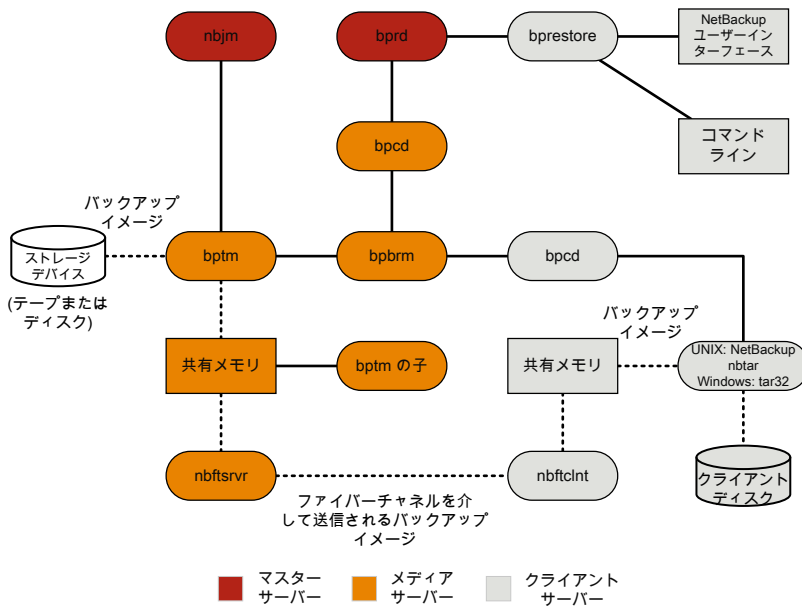
- bpdbm からポリシーリストが取得されます。
- スケジュールが設定されたすべてのジョブの作業リストが作成されます。
- 各ジョブの実行時間が計算されます。

- 実行時間の順に作業リストがソートされます。
 - その時点における実行予定のすべてのジョブが nbjm に送信されます。
 - 次の実行ジョブに対して呼び起こしタイマーが設定されます。
 - ジョブが終了すると、次のジョブの実行予定時刻が再計算され、その時点における実行予定のすべてのジョブが nbjm に送信されます。
- 3** Job Manager サービス (nbjm) は Resource Broker (nbrb) からバックアップリソースを要求します。これにより、nbrb から SAN クライアント用の共有メモリの使用に関する情報が返されます。
- 4** nbjm サービスはクライアントデーモン bpcd を使って Backup Restore Manager bpbrm を開始し、バックアップを開始します。
- 5** bpbrm サービスは bptm を開始します。これにより次が実行されます。
- nbjm からの SAN クライアント情報を要求します。
 - バックアップ要求を FT サーバープロセス (nbftsrvr) に送信します。
 - バックアップ要求をクライアント (nbftclnt) 上の FT クライアントプロセスに送信します。これにより、メディアサーバー上で nbftsrvr に対するファイバーチャネル接続が開始され、共有メモリが割り当てられ、共有メモリ情報がバックアップ ID ファイルに書き込まれます。
- 6** bpbrm サービスは bpcd を使って bpbkar を開始します。これにより、次のことが実行されます。
- BID ファイルから共有メモリ情報が読み込まれます (ファイルが利用可能になるまで待機します)。
 - bpbrm にイメージ内のファイル情報を送信します。
 - bpbkar にファイルデータを書き込み、必要に応じて圧縮して共有バッファにデータを書き込みます。
 - バッファがいっぱいのときやジョブが完了したときは、バッファにフラグを設定します。
- 7** FT クライアントプロセス (nbftclnt) は、共有メモリバッファのフラグが設定されるのを待ちます。その後、イメージデータを FT サーバー (nbftsrvr) の共有メモリバッファに転送し、バッファフラグを消去します。
- 8** nbftsrvr サービスは nbftclnt からのデータを待ち、共有メモリバッファに書き込まれたデータを書き込みます。転送が完了すると、nbftsrvr によってバッファにフラグが設定されます。

- 9 bptm は、共有メモリバッファのフラグが設定されるまで待機します。フラグが設定されると、bptm によってバッファのデータがストレージデバイスに書き込まれ、バッファのフラグがクリアされます。
- 10 ジョブの最後に、次の処理が実行されます。
 - bpbkar から bpbrm および bptm に対して、ジョブが完了したことが通知されます。
 - bptm から bpbrm へ、データ書き込みの最終状態が送信されます。
 - bptm から nbftclnt に対して、ファイバーチャネル接続のクローズが要求されます。
 - nbftclntによってファイバーチャネル接続がクローズされ、BID ファイルが削除されます。

SAN クライアントファイバートランスポートのリストア

図 5-2 ファイバートランスポートを介した SAN クライアントのリストア



SAN クライアントのリストアのプロセスの流れは次のとおりです (示される順序)。

- リストアを開始すると、**NetBackup** によってクライアントの **bprestore** プログラムが起動され、そのプログラムによって要求が **NetBackup Request** デーモン **bprd** に送信されます。この要求によって、ファイルおよびクライアントが識別されます。その後、**NetBackup Request** デーモンによって、**bpcd** (**NetBackup Client** デーモン) を使用して **Backup Restore Manager** (**bpbrm**) が起動されます。

メモ: **Backup Exec** イメージのリストアを行う場合は、クライアント上では、**bpbrm** によって **tar32.exe** ではなく **mtfrd.exe** が起動されます。サーバープロセスは、**NetBackup** のリストアの場合と同じです。

- 対象のデータが存在するディスクまたはテープがマスターサーバーに接続されている場合、マスターサーバーで、**bprd** によって **Backup Restore Manager** が起動されます。そのディスクユニットまたはテープユニットがメディアサーバーに接続されている場合、そのメディアサーバーで、**bprd** によって **Backup Restore Manager** が起動されます。
- **bpbrm** によって **bptm** が起動され、バックアップ ID と **shmfat** (共有メモリ) フラグが **bptm** に渡されます。
- **bptm** によって、次の処理が実行されます。
 - ジョブマネージャサービスから **SAN** クライアントの情報を要求します (**nbjrm**)。
 - **FT** サーバープロセスにリストア要求を送信します (**nbftsrvr**)。
 - クライアントの **FT** クライアントプロセスにリストア要求を送信します (**nbftclnt**)。
nbftclnt はメディアサーバーの **nbftsrvr** へのファイバーチャネル接続を開き、共有メモリを割り当て、共有メモリ情報をバックアップ ID ファイルに書き込みます。
- **bpbrm** によって、**bpcd** を介して **tar** が起動され、バックアップ ID、ソケット情報、**shmfat** (共有メモリ) フラグが **tar** に渡されます。
- **bptm** によって、次の処理が実行されます。
 - ストレージデバイスからイメージが読み込まれます。
 - **bptm** の子プロセスが作成されます。この処理では、バックアップイメージがフィルタリングされて、リストア用に選択されたファイルだけがクライアントに送信されます。
 - サーバー上の共有バッファにイメージデータが書き込まれます。
 - バッファに空きがない場合、またはジョブが完了した場合、バッファにフラグが設定されます (一部のバッファがクライアントに送信される場合もあります)。
- **tar** によって、次の処理が実行されます。
 - 状態情報と制御情報が **bpbrm** に送信されます。

- ローカルのバックアップ ID ファイルから共有メモリ情報が読み込まれます (ファイルが利用可能になるまで待機します)。
- データの読み込み準備が完了したことを示すバッファフラグを待機します。
- バッファからデータが読み込まれ、ファイルが抽出されてリストアされます。shmfat (共有メモリ) フラグが設定されている場合、tar はデータのフィルタリングが完了していると判断します。
- FT サーバープロセス nbftsrvr は、共有メモリバッファのフラグが設定されるまで待機します。フラグが設定されると、nbftsrvr はイメージデータを FT クライアント (nbftclnt) の共有メモリバッファに転送し、バッファのフラグをクリアします。
- FT クライアント (nbftclnt) が nbftsrvr からデータを受け取るまで待機し、データをクライアントの共有メモリバッファに書き込みます。その後に nbftclnt はバッファのフラグを設定します。
- ジョブの最後に、次の処理が実行されます。
 - bptm から tar および bpbrm に対して、ジョブが完了したことが通知されます。
 - bptm から nbftclnt に対して、ファイバーチャネル接続のクローズが要求されます。
 - nbftclntによってファイバーチャネル接続がクローズされ、BID ファイルが削除されます。

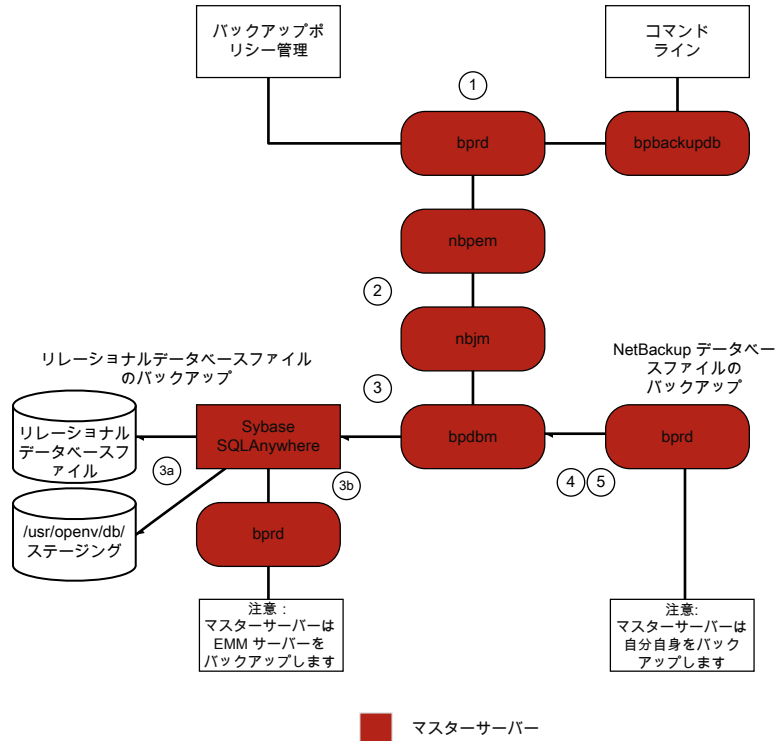
ホットカタログバックアップ

ホットカタログバックアップはポリシー形式のバックアップであり、通常のバックアップポリシーと同様に柔軟にスケジュールできます。このバックアップ形式は、他のバックアップ処理が継続的に行われている非常に使用頻度の高い **NetBackup** 環境で使用することを目的としています。

NetBackup 管理コンソールのオプションを使用して **NetBackup** カタログの手動バックアップを開始することができます。または、カタログが自動的にバックアップされるように **NetBackup** ポリシーを構成することができます。

図 5-3 はホットカタログバックアップ処理を示します。

図 5-3 ホットカタログバックアップ処理



NetBackup は次のホットカタログバックアップジョブを開始します。

- 管理者によって手動で開始されるか、またはカタログバックアップポリシーのスケジュールによって開始される親ジョブ。
- マスターサーバーの ID のリカバリ時に使用する .drpkg ファイルを作成する子ジョブ。 .drpkg ファイルを正常に作成した後、ステージングの前に、同じ子ジョブは、次の場所にあるステージングディレクトリに、SQL Anywhere データベースファイルのオンラインバックアップを実行します。
UNIX の場合: /usr/opensv/db/staging
Windows の場合: install_path¥Veritas¥NetBackupDB¥staging
- NBDB データベースファイルのバックアップを行う子ジョブ。

ファイルが準備領域に格納されると、通常のバックアップと同様の方法で、SQL Anywhere データベースエージェントによってこれらのファイルのバックアップが行われます。

- **NetBackup** データベースファイル (/usr/opensv/netbackup/db 内のすべてのファイル) のバックアップを行う子ジョブ。

NetBackup によってディザスタリカバリファイルが作成されます。ポリシーで電子メールオプションが選択されている場合は、このファイルが管理者に電子メールで送信されます。

ホットカタログバックアップに関するメッセージについては、次のログを参照してください。

- bpdbrm, bpbkar, bpbbrm, bpcd, bpbackup, bprd

リレーショナルデータベースファイルにのみ関するメッセージについては、**EMM** の **server.log** ファイルと次のディレクトリにある bpdbrm ログファイルを参照してください。

- **UNIX** の場合: /usr/opensv/netbackup/logs/bpdbrm
/usr/opensv/db/log/server.log
- **Windows** の場合: `install_path¥NetBackup¥logs¥bpdbrm`
`install_path¥NetBackupDB¥log¥server.log`

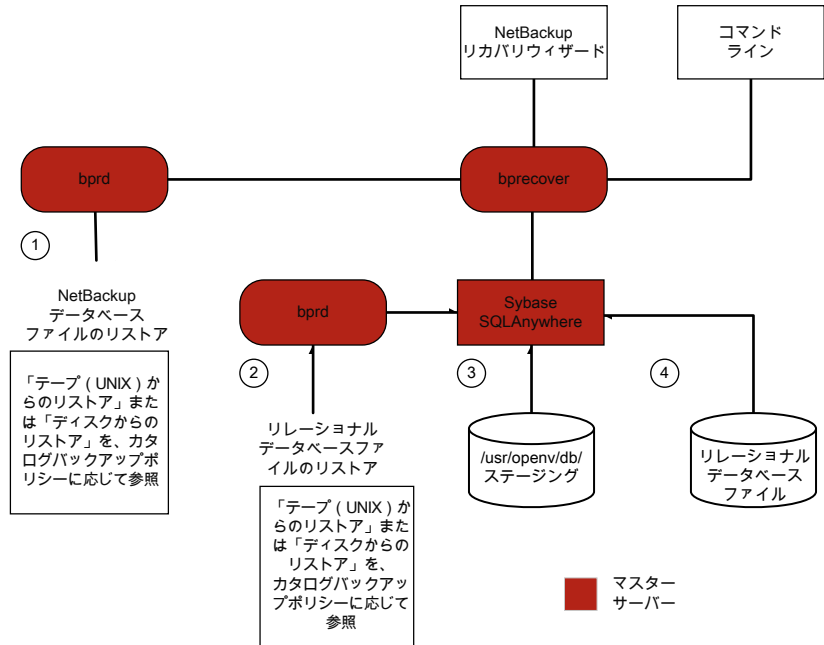
ホットカタログのリストア

NetBackup 管理コンソールの **NetBackup** カタログリカバリウィザード、または `bprecover` コマンドを使用して、カタログのリストアを開始できます。詳しくは、『**NetBackup** **トラブルシューティングガイド**』の「ディザスタリカバリ」の章を参照してください。

メモ: ディザスタリカバリのような状況でホットカタログのリストアを実行する前に、マスターサーバーの ID が、ディザスタリカバリのインストールまたは `nbhostidentity -import -infile drpkg.path` コマンドによってリカバリされている必要があります。ID がリカバリされると、ホットカタログのリカバリは通常どおりに完了できます。

図 5-4 にカタログのリストアおよびリカバリのプロセスを説明します。

図 5-4 カタログのリストアおよびリカバリ



ホットカタログバックアップからの NetBackup データベースとリレーショナルデータベース (NBDB) ファイルのリストアは、次のステップで構成されます (示される順序)。

- NetBackup カタログのイメージと設定ファイルがリストアされます。
- NBDB ファイルがリストアされます。データベースファイルは、`/usr/openv/db/staging` (UNIX の場合)、または `install_path¥NetBackupDB¥staging` (Windows の場合) にリストアされます。
- このステージングディレクトリへのファイルのリストアが行われた後、NBDB がリカバリされます。
- NBDB ファイルは、ステージングディレクトリから `bp.conf` ファイルの `VXDBMS_NB_DATA` 設定 (UNIX の場合)、または対応するレジストリキー (Windows の場合) で指定された場所に移動されます。デフォルトの場所は、`/usr/openv/db/data` (UNIX の場合)、`install_path¥NetBackupDB¥data` (Windows の場合) です。
リレーショナルデータベースファイルが再配置される場合、これらのファイルは、ステージングディレクトリから `/usr/openv/db/data/vxdbms.conf` ファイル (UNIX の場合) または `install_path¥NetBackupDB¥data¥vxdbms.conf` ファイル (Windows

の場合) に移動されます。NetBackup リレーショナルデータベースのファイルを再配置する方法について詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

合成バックアップ

NetBackup の典型的なバックアップ処理では、クライアントにアクセスしてバックアップを作成します。合成バックアップとは、クライアントを使用せずに作成されたバックアップイメージのことです。合成バックアップ処理では、クライアントを使用する代わりに、コンポーネントイメージと呼ばれる、以前に作成したバックアップイメージを使用して完全イメージまたは累積増分イメージが作成されます。

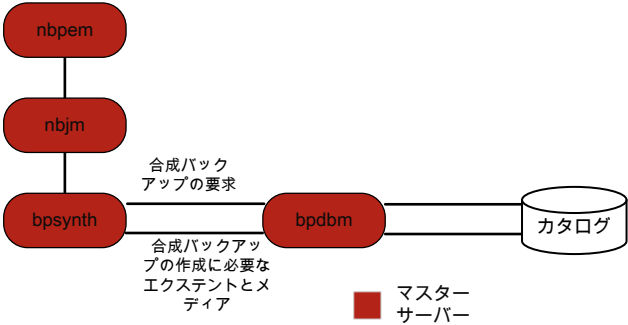
メモ: 合成アーカイブは存在しません。

たとえば、既存の完全イメージとその後の差分増分イメージを合成して、新しい完全イメージを作成できます。以前の完全イメージと増分イメージが、コンポーネントイメージです。新しく作成された合成完全イメージは、従来の処理で作成されたバックアップと同様に動作します。またこの合成完全イメージは、最新の増分と同時期のクライアントのバックアップになります。合成イメージは、ファイルを含む最新のコンポーネントイメージから各ファイルの最新バージョンをコピーすることによって作成されます。合成バックアップは[True Image Restore]と[移動検出 (Move Detection)]オプションを選択したポリシーを使って作成する必要があります。このオプションによって、クライアントのファイルシステムから削除されたファイルが、合成バックアップに表示されないようにすることができます。

従来のバックアップのように、nbpem は合成バックアップを開始します。nbpem は nbjrm に要求を送信して合成バックアップを開始し、その後で nbjrm がマスターサーバー上で動作する bpsynth を開始します。合成バックアップイメージの作成が制御され、コンポーネントイメージからの必要なファイルの読み込みが制御されます。デバッグログディレクトリに bpsynth というディレクトリが存在する場合、追加のデバッグログメッセージは、このディレクトリ内のログファイルに書き込まれます。

bpsynth では、複数のフェーズで合成イメージを作成します。

表 5-1

フェーズ	説明
1 - カタログ情報とエクステントの準備	フェーズ 1 では、bpsynth はデータベースマネージャ bpdbm の合成バックアップ要求を作ります。bpsynth はコンポーネントイメージカタログのエントリと TIR 情報を使って新しい合成イメージのカタログを構築します。また、コンポーネントイメージから合成イメージにコピーされるエクステントも作成されます。bpdbm サービスは bpsynth にエクステントのリストを返します。(エクステントとは、特定のコンポーネントイメージ内の開始ブロック番号と連続したブロックの数のことです。)通常はエクステントのセットを各コンポーネントイメージから新しい合成イメージにコピーする必要があります。 次の図に、フェーズ 1 の動作を示します。 
2 - リソースの取得	フェーズ 2 では、bpsynth が新しいイメージの書き込みリソース (ストレージユニット、ドライブ、メディア) が取得されます。また、コンポーネントイメージが含まれるすべての読み込みメディアが予約され、最初に読み込むメディア用のドライブが取得されます。 コンポーネントイメージが BasicDisk に存在する場合、リソースの予約は行われません。

フェーズ	説明
3 - データのコピー	フェーズ 3 では、bpsynth がメディアサーバー上で (テープとディスクの) ライター bptm を開始して新しい合成イメージを書き込みます。また、リーダー bptm (テープ用) または bpdm (ディスク用) 処理も開始します。リーダープロセスによって、コンポーネントイメージのすべてのエクステントが読み込まれます。 次の図に、フェーズ 3 の動作を示します。 <pre> graph TD bpsynth([bpsynth]) --- parent_bptm1([親 bptm]) parent_bptm1 --- child_bptm([子 bptm]) child_bptm -- "データフロー" --> parent_bptm2([親 bptm または bpdm]) parent_bptm2 --- component_image[コンポーネントイメージ] parent_bptm1 --- new_image[新しいイメージ] </pre> ■ マスターサーバー ■ メディアサーバー bpsynth によってメディアサーバー上で起動されるのは、bptm (ライター) および bpdm (リーダー) の親プロセスだけです。その後、親プロセスによって子プロセスが起動されます。親と子のプロセス間の通信は、共有メモリのバッファを介して行われます。 bpsynth プロセスによって、各コンポーネントイメージのエクステント (開始ブロックおよび数) が、対応する bptm または bpdm リーダーの子プロセスに送信されます。 bptm または bpdm リーダーの親プロセスによって、適切なメディアから共有バッファにデータが読み込まれます。bptm または bpdm リーダーの子プロセスによって、共有バッファにあるデータが、ソケットを介して bptm ライターの子プロセスに送信されます。bptm ライターの子プロセスによって、データが共有バッファに書き込まれます。bptm ライターの親プロセスによって、共有バッファからメディアにデータがコピーされ、bpsynth に、合成イメージの作成が完了したことが通知されます。

フェーズ	説明
4-イメージの検証	フェーズ 4 では、bpsynth プロセスによってイメージの妥当性がチェックされます。これで、新しいイメージが NetBackup で認識されるようになり、他の完全バックアップまたは累積増分バックアップと同様に使用できます。 合成バックアップには、移動検出機能を使った True Image Restore (TIR) が各コンポーネントイメージで選択されることと、コンポーネントイメージが合成イメージである必要があります。

合成バックアップの問題レポートに必要なレガシーログディレクトリの作成

レガシーログディレクトリが作成されていない場合、そのディレクトリを作成する必要があります。このディレクトリが存在しない場合、ログをディスクに書き込むことができません。

表 5-2 レガシーログディレクトリの作成

手順	処理	説明
手順 1	マスターサーバー上にディレクトリを作成します。	次のディレクトリを作成します。 <code>install_path/netbackup/logs/bpsynth</code> <code>install_path/netbackup/logs/bpdm</code> <code>install_path/netbackup/logs/vnetd</code>
手順 2	メディアサーバー上にディレクトリを作成します。	次のディレクトリを作成します。 <code>install_path/netbackup/logs/bpcd</code> <code>install_path/netbackup/logs/bptm</code>
手順 3	[グローバルログレベル (Global logging level)]を変更します。	[ホストプロパティ (Host Properties)]で、マスターサーバーを選択し、[グローバルログレベル (Global logging level)]を 5 に設定します。 [ホストプロパティ (Host Properties)]ウィンドウで構成を表示する方法について詳しくは、『NetBackup トラブルシューティングガイド』を参照してください。 p.52 の「ログレベルの変更」を参照してください。 p.50 の「グローバルログレベルについて」を参照してください。
手順 4	ジョブを再実行します。	ジョブを再度実行して、作成したディレクトリからログを収集します。 bptm ログは、イメージの読み込みおよび書き込みがテープデバイスまたはディスクに対して行われる場合にだけ必要です。bpdm ログは、イメージの読み込みがディスクに対して行われる場合にだけ必要です。 イメージが複数のメディアサーバーから読み込まれる場合、bptm または bpdm のデバッグログは、各メディアサーバーから収集される必要があります。

p.110 の「[合成バックアップの問題レポートに必要なログ](#)」を参照してください。

合成バックアップの問題レポートに必要なログ

合成バックアップの問題をデバッグするには、問題レポートおよび追加項目にすべてのログを含める必要があります。ベリタス社テクニカルサポートにすべての情報を送ってください。

次のログの形式を含めます。

- 統合ログ機能によって作成されるログファイル
p.15 の「[NetBackup の統合ログの収集](#)」を参照してください。
- レガシーログ機能によって作成されるログファイル
p.109 の「[合成バックアップの問題レポートに必要なレガシーログディレクトリの作成](#)」を参照してください。

次の追加項目を含めます。

試行ファイル 試行ファイルは、次のディレクトリに存在します。

```
install_path/netbackup/db/jobs/trylogs/jobid.t
```

合成バックアップジョブのジョブ ID が 110 の場合、試行ファイルは 110.t という名前になります。

ポリシー属性 次のコマンドを使ってポリシーの属性を取得します。

```
install_path/netbackup/bin/admincmd/bppllist  
policy_name -L
```

ここで、*policy_name* は、合成バックアップジョブを実行したポリシーの名前です。

ストレージユニットのリスト 次のコマンドからストレージユニットのリストを取得します。

```
install_path/netbackup/bin/admincmd/bpstulist -L
```

p.109 の「[合成バックアップの問題レポートに必要なレガシーログディレクトリの作成](#)」を参照してください。

ストレージのログ記録

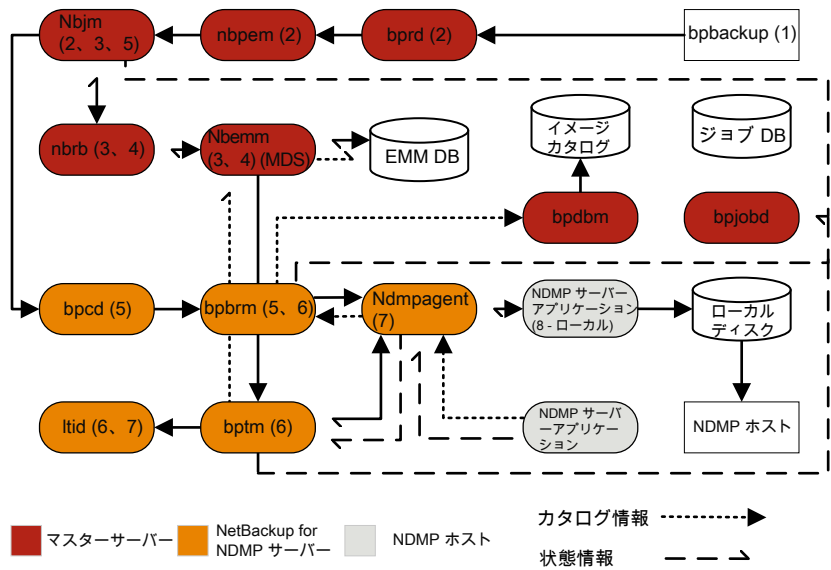
この章では以下の項目について説明しています。

- [NDMP バックアップのログ記録](#)
- [NDMP リストアログ記録](#)

NDMP バックアップのログ記録

次に、NDMP バックアップ処理を示します。

図 6-1 NDMP バックアッププロセス



NDMP バックアップ操作の基本的な処理手順は次のとおりです。

NDMP バックアップ手順

- 1 NetBackup 管理者は `bpbbackup` コマンドを実行してバックアップジョブを開始します。または、NetBackup 管理コンソールで作成したスケジュール設定済みポリシーでジョブを開始できます。
- 2 `bpbbackup` 処理はマスターサーバーに接続してバックアップ要求を作成します。NetBackup Request Manager (`bprd`) はバックアップ要求を Policy Execution Manager (`nbpem`) に送信し、Policy Execution Manager はジョブを Job Manager (`nbjm`) にサブミットします。
- 3 `nbjm` はジョブを実行する必要がある Resource Broker (`nbrb`) のリソースを要求します。`nbrb` は Enterprise Media Management (`nbemm`) のメディアとデバイスの選択 (MDS) にアクセスしてリソース要求を評価します。MDS はこのジョブに使うリソースを識別するために EMM データベースを問い合わせます。
- 4 MDS は `nbrb` にジョブのリソースリストを提供し、`nbrb` は `nbjm` にこのリストを渡します。
- 5 `nbjm` はこのバックアップジョブに関連付けられたメディアサーバーと通信を開始します。クライアントサービス (`bpcd`) を経由してメディアサーバーの Backup Restore Manager (`bpbbrm`) を開始します。
- 6 `bpbbrm` はメディアサーバーの Tape Manager (`bptm`) を開始します。最終的に、親 `bptm` プロセスはバックアップジョブに使うテープをマウントするように `ltid` に要求します。
- 7 NetBackup for NDMP サーバーで、次のいずれかを実行します。要求したテープをストレージデバイスにマウントするのに必要な NDMP SCSI ロボットコマンドを送信します。
 - NDMP エージェントサービス (`ndmpagent`) は直接接続するテープをマウントするために NDMP コマンドを発行するファイラに接続します。
 - メディアサーバーの `ltid` は要求したテープをストレージデバイスにマウントするのに必要な NDMP SCSI ロボットコマンドを発行します。
- 8 NDMP バックアップの種類に応じて次のいずれかを実行します。
 - ローカルバックアップ。NetBackup は NDMP サーバーアプリケーションがテープにバックアップを作成するように NDMP コマンドを送信します。LAN を経由せずに NDMP ホストのローカルディスクとテープドライブ間でデータを移動します。
 - 3-Way バックアップ (プロセスの流れ図には表示されない)。NetBackup はバックアップを実行する NDMP サーバーアプリケーションに NDMP コマンドを送信します。メディアサーバーは両方の NDMP サーバーと NDMP 通信を確立します。バックアップを作成したデータを収める NDMP サーバーから、テープスト

レージにバックアップを書き込む NDMP サーバーにネットワークを経由してデータを移動します。

- リモートバックアップ (プロセスの流れ図には表示されない)。バックアップの書き込みに使うデバイスは **NetBackup** ストレージユニットに関連付けられます。

NetBackup メディアサーバーの `bptm` はテープドライブにテープをマウントします。**NetBackup** は NDMP サーバーに NDMP コマンドを送信して NDMP 以外のメディアマネージャストレージユニットのバックアップを開始します。NDMP ホストから **NetBackup** メディアサーバーにネットワークを経由してデータを移動すると、メディアサーバーは選択したストレージユニットにデータを書き込みます。

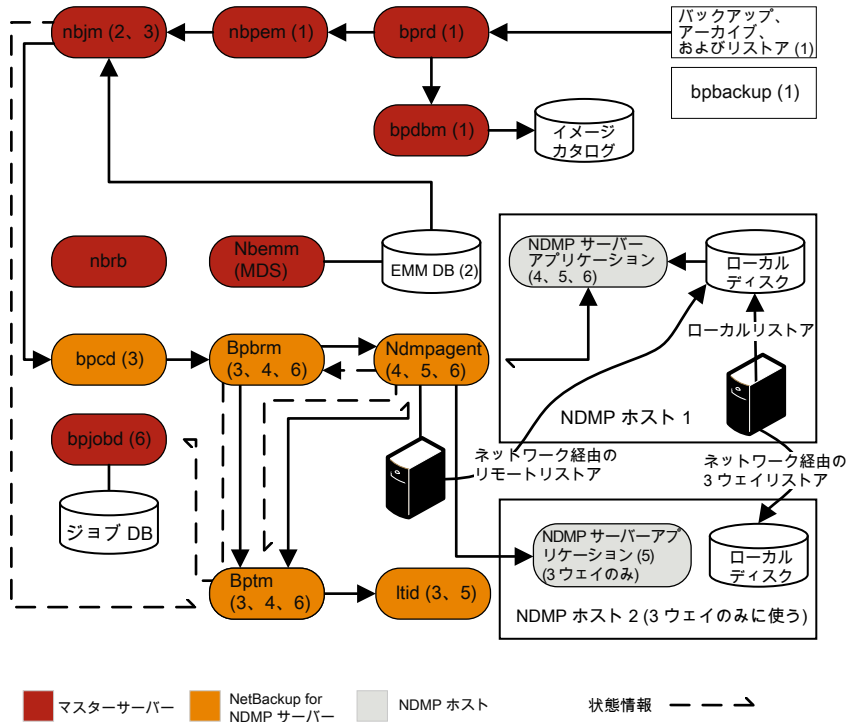
- 9 バックアップ操作中とその完了時に、NDMP サーバーはバックアップ操作に関する状態を **NetBackup for NDMP** サーバーに送信します。**NetBackup** の複数のプロセスはジョブに関する情報を `bpjobjd` に送信し、`bpjobjd` はこの情報を使って **NetBackup** アクティビティモニターに表示されるジョブ状態を更新します。

状態、カタログ、およびその他のジョブ情報の移動がプロセスの流れ図に破線で示されます。

NDMP リストアログ記録

次に NDMP リストアプロセスを示します。

図 6-2 NDMP リストア処理



NDMP リストア操作の基本処理手順は次のとおりです。

NDMP リストア手順

- 1 **NetBackup** のマスターサーバーまたはメディアサーバーの **NetBackup** 管理コンソール管理者は、イメージカタログを参照したり、NDMP イメージからリストアするファイルを選択したりしてリストアジョブを開始します。この処理は標準バックアップイメージからリストアするファイルの選択に似ています。**NetBackup** マスターサーバーはリストアの実行に必要な特定のメディアを識別します。この図では、メディアはテープボリュームです。
- 2 マスターサーバーは、リストアするデータおよび必要なメディアを特定した後にリストアジョブを送信します。ジョブマネージャ (`nbjm`) は、必要なリソースを要求します。このリソースの要求により、リストアするデータを含むメディアが割り当てられます。この例では、テープドライブはリストア操作時に使います。

- 3 マスターサーバーはリストアジョブに使うメディアサーバーに接続し、**Restore Manager** (bpbrm) プロセスを開始してリストアジョブを管理します。bpbrm は、nbjm にテープボリュームを問い合わせる **Tape Manager** プロセス (bptm) を開始します。bptm は論理テープインターフェースデーモン (ltid) にテープのマウントを要求します。
- 4 **NetBackup for NDMP** サーバーで、**NDMP** エージェント (ndmpagent) はファイラに接続し、**NDMP** コマンドを発行して直接接続されているテープをマウントします。ltid は **NDMP** コマンドを送信してストレージデバイスで要求されたテープをマウントします。または、メディアサーバー自体が通常の **Media Manager** ストレージユニットのようにテープのマウント要求を発行します。
- 5 **NDMP** リストア操作の種類に応じて次のいずれかが実行されます。
 - ローカルリストア。テープドライブからローカルディスクにリストア操作を開始するために、**NetBackup** は **NDMP** サーバーに **NDMP** コマンドを送信します。リストアデータはテープドライブから **NDMP** ホストのローカルディスクに LAN を経由せずに移動します。
 - 3-Way リストア。**NetBackup** メディアサーバーはリストアに使う **NDMP** サーバー両方の **NDMP** 通信を確立します。**NDMP** サーバーのテープから他の **NDMP** サーバーのディスクストレージにデータのリストアを開始するには、メディアサーバーから両方の **NDMP** サーバーに **NDMP** コマンドを送信します。リストアデータは **NDMP** ホスト間でネットワーク経由で移動します。
 - リモートリストア。**NetBackup** は **NDMP** サーバーがリストアを実行できるようにするために **NDMP** サーバーに **NDMP** コマンドを送信します。メディアサーバーの bptm はリストアデータをテープから読み込み、ディスクストレージにデータを書き込む **NDMP** ホストにネットワークを経由して送信します。
- 6 **NDMP** サーバーはリストア操作に関する状態情報を **NetBackup for NDMP** サーバーに送信します。**NetBackup** の各種の処理 (nbjm、bpbrm、bptm など) はマスターサーバーにジョブの状態情報を送信します。マスターサーバーの **Jobs Database Manager** (bpjobjd) プロセスはジョブデータベースのリストアジョブの状態を更新します。この状態はアクティビティモニターに表示されます。

NetBackup 重複排除ログ

この章では以下の項目について説明しています。

- [メディアサーバー重複排除プール \(MSDP\) への重複排除のバックアップ処理](#)
- [クライアント重複排除のログ](#)
- [重複排除の設定ログ](#)
- [メディアサーバーの重複排除のログ記録と pdplugin ログ記録](#)
- [ディスク監視のログ記録](#)
- [ログ記録のキーワード](#)

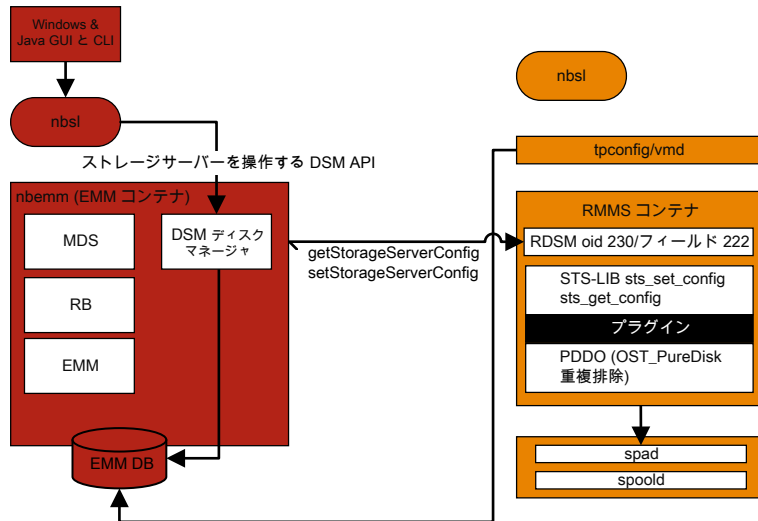
メディアサーバー重複排除プール (MSDP) への重複排除のバックアップ処理

メディアサーバー重複排除プール (MSDP) への重複排除のバックアップ処理は、次のように行われます。

- クライアントの `bpbkar` が、NetBackup バックアップテープマネージャ (`bptm` 処理) にデータを送信します。
- `pdvfs` (プロキシとして `bptm` を使用) が NetBackup Deduplication Manager (`spad`) に接続してメタデータ (イメージレコード) を `spadb` ミニカタログに記録し、NetBackup Deduplication Engine (`spoold`) に接続して、データディレクトリ (`dedup_path¥data`) の `.bhd/.bin` ファイルにイメージデータを格納します。
- `spoold` は、キュー (`dedupe_path¥queue`) ディレクトリの `.tlog` ファイルと、処理されたディレクトリに、`tlogs` を書き込みます。キューディレクトリの `tlog` データは、次のコンテンツルーターのキュー処理ジョブが実行されるときに、`crdb` に後から処理されます。NetBackup 7.6 以降、`.tlog` ファイルにはデータベースへの追加は含まれません。

機能概要は次のとおりです。

図 7-1 MSDP の重複排除の構成



このシナリオでは、クライアントはデータを直接メディアサーバーにバックアップし、メディアサーバーはローカルに格納する前にデータの重複を排除します。これが正しいメディアサーバーで行われていることを確認します。このサーバーは、MSDP ストレージサーバーと必ずしも同じではありません (負荷分散のため)。

重複排除固有のログ記録には、メディアサーバーで次の項目を有効にします。

1. 詳細 5 の bptm のログ:

- `/usr/opensv/netbackup/logs` (Windows の場合:
`install_path¥NetBackup¥logs`) に bptm という名前のログディレクトリを作成します。
- NetBackup 管理コンソールで bptm ログの詳細度を 5 に設定します。そのためには、メディアサーバーの [ホストプロパティ (Host Properties)]、[ログ記録 (Logging)] をクリックします。UNIX/Linux を使っている場合は、`/usr/opensv/netbackup/bp.conf` ファイルに次の行を追加して bptm ログの詳細度を 5 に設定します。

```
BPTM_VERBOSE = 5
```

- 次の場所にある `pd.conf` 構成ファイルを編集します。

Windows の場合:

```
install_path¥NetBackup¥bin¥ost-plugins¥pd.conf
```

UNIX または Linux の場合:

```
/usr/openv/lib/ost-plugins/pd.conf
```

さらに次の行をアンコメントまたは修正します。

```
LOGLEVEL = 10
```

メモ: また、ログを記録するパスを指定するよう、`pd.conf` ファイルで `DEBUGLOG` を修正することもできます。ただし、`DEBUGLOG` のエントリはコメントアウトされたままにすることを推奨します。ログ記録の情報 (PDVFS デバッグログ) は、`bptm` ログと `bpdm` ログに記録されます。

2. 詳細な `spad/spoold` ログ記録 (省略可能) を有効にします。

- `dedup_path¥etc¥puredisk¥spa.cfg` ファイルと `dedup_path¥etc¥puredisk¥contentrouter.cfg` ファイルで、次の行を編集します。
`Logging=long,thread` を `Logging=full,thread` に変更します。
- 適切なメディアサーバーを使っていることを確認し、MSDP ストレージサーバーのサービスを再起動します。

注意: 詳細ログを有効にすると、MSDP のパフォーマンスに影響することがあります。

3. バックアップエラーを再現します。
4. NetBackup 管理コンソールで、[アクティビティモニター (Activity Monitor)]>[ジョブ (Jobs)]をクリックし、ジョブの詳細を開いて[状態の詳細 (Detailed Status)]タブをクリックします。バックアップを実行したメディアサーバーのホスト名および `bptm` のプロセス ID 番号 (PID) が表示されます。
 - `bptm(pid=value)` のような行を探します。これは、`bptm` ログで見つかる `bptm` PID です。
5. メディアサーバーの `bptm` ログで、手順 3 で見つかった `bptm` PID を抽出します。この手順では、単一行のエントリのみが収集されます。複数行のログエントリは未加工のログで確認します。次の例では、**3144** が `bptm` PID です。
 - **Windows** のコマンドライン:

```
findstr "%[3144." 092611.log > bptmpid3144.txt
```

- UNIX/Linux のコマンドライン:

```
grep "%[3144%]" log.092611 > bptmpid3144.txt
```

6. バックアップが開始された日付と失敗した日付が含まれる spoold セッションログを、次のログから収集します。

Windows の場合:

```
dedup_path%log%spoold%mediasvr_IP_or_hostname%bptm%Receive%MMDDYY.log  
dedup_path%log%spoold%mediasvr_IP_or_hostname%bptm%Store%MMDDYY.log
```

UNIX または Linux の場合:

```
dedup_path/log/spoold/mediasvr_IP_or_hostname/bptm/Receive/MMDDYY.log  
dedup_path/log/spoold/mediasvr_IP_or_hostname/bptm/Store/MMDDYY.log
```

クライアント重複排除のログ

クライアント重複排除のログでは、次の場所が使われます。次の重複排除場所オプションのいずれかを選択します。変更を反映させるには、適用可能な MSDP ストレージプールで、`install_path%etc%puredisk%spa.cfg` と `install_path%etc%puredisk%contentrouter.cfg` を編集し、`Logging=full,thread` を指定して、`spad` と `spoold` サービスを再起動します。

- クライアント側のログ (NetBackup Proxy Service のログ) を次に示します。

Windows の場合:

```
install_path%NetBackup%logs%nbostpxy
```

UNIX または Linux の場合:

```
/usr/opensv/netbackup/logs/nbostpxy
```

PBX (nbostpxy (OID450):

```
vxlogcfg -a -p 51216 -o 450 -s DebugLevel=6 -s DiagnosticLevel=6
```

- メディアサーバーのログは次のとおりです。

```
bptm と storage_path%log%spoold%IP_address%nbostpxy.exe%*
```

重複排除の設定ログ

次に重複排除の設定ログを示します。

Windows 向け NetBackup 管理コンソールウィザードのログ記録:

1. wingui (OID: 263):

```
# vxlogcfg -a -p 51216 -o 263 -s DebugLevel=6 -s DiagnosticLevel=6
```

2. 該当する MSDP ストレージプールで、`install_path¥etc¥puredisk¥spa.cfg` と `install_path¥etc¥puredisk¥contentrouter.cfg` を編集します。
Logging=full,thread を指定し、次に、変更を有効にするために、**spad** サービスと **spoold** サービスを再起動します。

■ nbsl (OID: 132):

```
vxlogcfg -a -p 51216 -o 132 -s DebugLevel=6 -s DiagnosticLevel=6
```

■ dsm (OID: 178):

```
vxlogcfg -a -p 51216 -o 178 -s DebugLevel=6 -s DiagnosticLevel=6
```

3. ストレージサービス (`msdp/pdplugin` の応答を NetBackup に記録するために STS のログ記録をオンにする):

```
# vxlogcfg -a -p 51216 -o 202 -s DebugLevel=6 -s DiagnosticLevel=6
```

4. RMMS (Remote Monitoring and Management Service):

```
# vxlogcfg -a -p 51216 -o 222 -s DebugLevel=6 -s DiagnosticLevel=6
```

5. `tpcommand (...¥volmgr¥debug¥tpcommand)`

6. `storage_directory¥log¥msdp-config.log`

コマンドライン設定のログ記録:

■ `nbdevquery` の管理ログ (`storage_server` を追加する)

■ `tpconfig` の `tpcommand` ログ (資格情報を追加する)(`...¥volmgr¥debug¥tpcommand`)

■ `storage_directory¥log¥pdde-config.log`

■ ストレージサービス (`msdp/pdplugin` の応答を NetBackup に記録するために STS のログ記録をオンにする):

```
# vxlogcfg -a -p 51216 -o 202 -s DebugLevel=6 -s DiagnosticLevel=6
```

■ RMMS (Remote Monitoring and Management Service):

```
# vxlogcfg -a -p 51216 -o 222 -s DebugLevel=6 -s DiagnosticLevel=6
```

■ `storage_directory¥log¥pdde-config.log`

NetBackup 管理コンソールのログ記録:

C:¥Program Files¥VERITAS¥Java (Windows の場合) または /usr/opensv/java (UNIX/Linux の場合) にある Debug.Properties ファイルを開きます。次に、ファイルを編集して、次の行のコメントを解除します (または、これらの行が存在しない場合は追加します)。動作している GUI がある場合は、必ず再起動してください。

```
printcmds=true
printCmdLines=true
debugMask=0x0C000000
debugOn=true
```

ログは、C:¥Program Files¥VERITAS¥NetBackup¥logs¥user_ops¥nbjlogs (Windows) または /opt/opensv/netbackup/logs/user_ops/nbjlogs (UNIX/Linux) にあります。最新のログを参照していることを確認します。

- ストレージサービス (msdp/pdplugin の応答を NetBackup に記録するために STS のログ記録をオンにする):
vxlogcfg -a -p 51216 -o 202 -s DebugLevel=6 -s DiagnosticLevel=6
- RMMS (Remote Monitoring and Management Service):
vxlogcfg -a -p 51216 -o 222 -s DebugLevel=6 -s DiagnosticLevel=6
- tpccommand (...¥volmgr¥debug¥tpcommand)
- storage_directory¥log¥msdp-config.log

メディアサーバーの重複排除のログ記録と pdplugin ログ記録

この項では、メディアサーバーの重複排除のログ記録と pdplugin のログ記録について説明します。

- Client Direct およびそのメディアサーバーとの間で Private Branch Exchange (PBX) 通信をトラブルシューティングする場合を除いて、次のコマンドを使って、重複排除のログ記録のための不要な CORBA/TAO をゼロ (0) に減らします。
vxlogcfg -a -p NB -o 156 -s DebugLevel=0 -s DiagnosticLevel=0

バックアップ:

- バックアップの読み書きをするために、メディアサーバーで詳細 5 の bptm を有効にします。
- メディアサーバーの pd.conf ファイルで LOGLEVEL = 10 をコメント解除します。

複製またはレプリケーション:

- 複製の読み書きをするために、メディアサーバーで詳細 5 の bpdm を有効にします。

- メディアサーバーの `pd.conf` ファイルで `LOGLEVEL = 10` をコメント解除します。

注意: 詳細度を有効にすると、パフォーマンスに影響することがあります。

- トレースレベルの `spad` ログ記録と `spoold` ログ記録を有効にすることで、複製またはレプリケーションジョブの失敗が、`bpdm/pdvfs > ソース spad/spoold セッションログ > ソース replication.log > ターゲット spad/spoold` にわたってトレースできます。

ディスク監視のログ記録

STS のログ記録は、MSDP ストレージプールに通信するための資格情報を持つ、任意のメディアサーバーに設定する必要があります。`nbrmms (OID: 222)` を、マスターサーバーと該当する任意のメディアサーバーに設定する必要があります。次の場所のログを使って、ディスクを監視できます。

- ストレージサービス (MSDP プラグインの実行中に **NetBackup** が受け取るレスポンスを表示するために **STS** ログ記録をオンにする):

```
# vxlogcfg -a -p 51216 -o 202 -s DebugLevel=6 -s DiagnosticLevel=6
```
- **RMMS (Remote Monitoring and Management Service)**: # `vxlogcfg -a -p 51216 -o 222 -s DebugLevel=6 -s DiagnosticLevel=6`

ログ記録のキーワード

サポートがログを確認するときは、次のキーワードを使います。

キーワード	説明
最大フラグメントサイズ	51200 KB 以下であることが必要
<code>get_plugin_version</code>	<code>libstspipd.dll</code> (<code>pdplugin</code> バージョン)
<code>get_agent_cfg_file_path_for_mount</code>	PureDisk エージェントの構成ファイルを使う (<code>.cfg</code> のファイル名に注目)、省略名または FQDN を判断。
<code>emmlib_NdmpUserIdQuery</code>	バックアップ、資格情報の検査に使用
解決済み	リモート CR の名前解決
<code>tag_nbu_dsid</code> の読み取り	NBU_PD_SERVER オブジェクトを正しく読み取っているかどうかの確認

キーワード	説明
推奨ルーティングテーブル	フィンガープリントを CR がルーティングするための CR ルーティングテーブル。PDDO が PureDisk を対象にする時より有用。
プライマバックアップ用	プライマリバックアップの dsid
opt-dup コピー用	opt-dup dsid
これは opt-dup です	opt-dup dsid
https	完了したかどうかを確認するための SPA または CR のいずれかへの Web サービスの呼び出し

OpenStorage Technology (OST) のログ記録

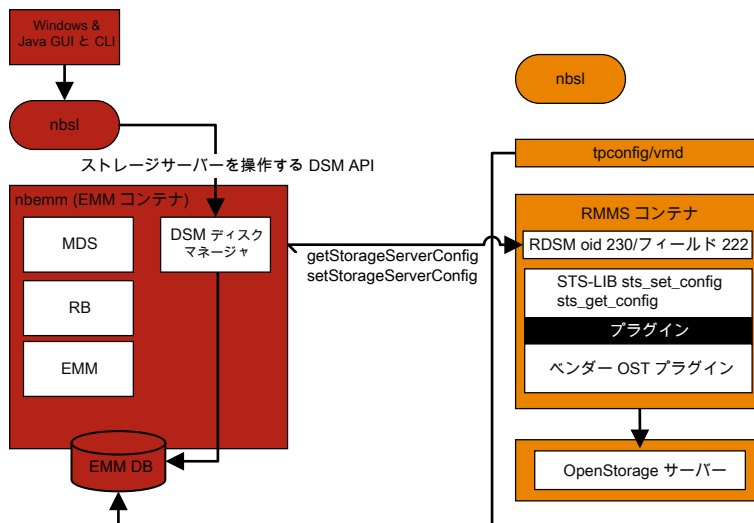
この章では以下の項目について説明しています。

- [OpenStorage Technology \(OST\) バックアップのログ記録](#)
- [OpenStorage Technology \(OST\) の構成と管理](#)

OpenStorage Technology (OST) バックアップのログ記録

次に、OpenStorage Technology (OST) の構成を示します。

図 8-1 OST の構成



このシナリオでは、クライアントはメディアサーバーに直接データをバックアップし、メディアサーバーはベンダープラグインにアクセスしてストレージサーバーにデータを転送します。

OST 固有のログを記録するには、メディアサーバーまたはプラグインホストで次のことを実行してください。

1. レジストリまたは bp.conf ファイルで VERBOSE = 5 を設定します。
2. /usr/openv/netbackup/logs に次のディレクトリがあることを確認します (Windows の場合は、install_path¥NetBackup¥logs)。
 - bptm
 - bpbrm
 - bpstsinfo
3. volmgr/debug/tpcommand ディレクトリを作成します。
4. vm.conf ファイルに VERBOSE を記述します。p.47 の「[レガシーログファイルに書き込まれる情報を制御する方法](#)」を参照してください。
5. 次のプロセスに対して DebugLevel=6 と DiagnosticLevel=6 を設定します。
 - OID 178 (ディスクマネージャサービス、dsm)

- OID 202 (ストレージサービス、stssvc)
- OID 220 (ディスクポーリングサービス、dps)
- OID 221 (メディアパフォーマンスモニターサービス)
- OID 222 (Remote Monitoring and Management Service)
- OID 230 (Remote Disk Manager Service、rdsm)
- OID 395 (STS Event Manager、stsem)

これらの OID は、すべてメディアサーバーの `nbrmms` 統合ログファイルにログ記録されます。

6. ベンダープラグインのログ記録を増やします。ほとんどのベンダーには、**NetBackup** ログに登録される内容に加えてそれぞれのプラグインのログ機能があります。
7. バックアップエラーを再現します。
8. **NetBackup** 管理コンソールで、[アクティビティモニター (Activity Monitor)]>[ジョブ (Jobs)]をクリックし、ジョブの詳細を開いて[状態の詳細 (Detailed Status)]タブをクリックします。バックアップを実行したメディアサーバーのホスト名および `bptm` のプロセス ID 番号 (PID) が表示されます。
 - `bptm(pid=value)` のような行を探します。これは、`bptm` ログで見つかる `bptm` PID です。
9. メディアサーバーの `bptm` ログで、手順 8 で見つかった `bptm` PID を抽出します。この手順では、単一行のエントリのみが収集されます。複数行のログエントリは未加工のログで確認します。次の例では、**3144** が `bptm` PID です。
 - **Windows** のコマンドライン:

```
findstr "%[3144.]" 092611.log > bptmpid3144.txt
```
 - **UNIX/Linux** のコマンドライン:

```
grep "%[3144%]" log.092611 > bptmpid3144.txt
```
10. バックアップの開始日および失敗した日付をカバーするベンダー固有のプラグインログを収集します。

OpenStorage Technology (OST) の構成と管理

OpenStorage Technology (OST) 技術は、ソフトウェアドライバのようなプラグインアーキテクチャを使います。これにより、サードパーティのベンダーは **NetBackup** データストリームとメタデータを各自のデバイスに誘導できます。プラグインは OST パートナーに

よって開発および作成され、**NetBackup** で使うためにメディアサーバーにあります。**NetBackup** は、ストレージサーバーへのパスのために **OST** プラグインに依存します。

ストレージサーバーへの通信はネットワーク経由で行われます。メディアサーバーとストレージサーバーにおける名前解決を正しく構成する必要があります。サポートされているすべてのベンダープラグインは **TCP/IP** ネットワーク経由で通信でき、一部は **SAN** ネットワークのディスクストレージに通信できます。

ディスクアプライアンスの機能を確認するために、**NetBackup** はプラグインを使ってストレージアプライアンスを問い合わせます。機能には、重複排除ストレージ、最適化されたオフホストの複製、および合成バックアップが含まれます。

各 **OST** ベンダーは、異なるログメッセージを報告することがあります。バックアップジョブまたはリストアジョブの **bptm** ログやプラグインログを確認することは、プラグインを介したストレージサーバーへの個々の呼び出しを理解するための最良の方法です。

基本的な手順は次のとおりです。

- リソースを要求する
- **sts open_server**
- イメージを作成する
- 書き込む
- 閉じる
- **sts close_server**

次に、ベンダープラグインログにおける呼び出しの例を示します。

```
2016-03-14 09:50:57 5484: --> stspi_claim
2016-03-14 09:50:57 5484: --> stspi_open_server
2016-03-14 09:50:57 5484: <-- stspi_write_image SUCCESS
2016-03-14 09:50:57 5484: --> stspi_close_image
2016-03-14 09:50:59 5484: <-- stspi_close_server SUCCESS
```

プラグインのバージョンを表示するには、次のコマンドを使います。

- **UNIX/Linux:** `/usr/opensv/netbackup/bin/admincmd/bpstsinfo -pi`
- **Windows:** `install dir¥netbackup¥bin¥admincmd¥bpstsinfo -pi`

ストレージサーバーへの基本的な通信をテストするには、次のコマンドを使います。

- **UNIX/Linux:** `/usr/opensv/netbackup/bin/admincmd/bpstsinfo -li -storage_server storage server name -stype OST_TYPE`
- **Windows:** `install dir¥netbackup¥bin¥admincmd¥bpstsinfo -li -storage_server storage server name -stype OST_TYPE`

構成されているストレージサーバーを表示するには、次のコマンドを使います。

- **UNIX/Linux:** `/usr/opensv/netbackup/bin/admincmd/nbdevquery -liststs -stype OST_TYPE -U`
- **Windows:** `install dir¥netbackup¥bin¥admincmd¥nbdevquery -liststs -stype OST_TYPE -U`

構成されているディスクプールを表示するには、次のコマンドを使います。

- **UNIX/Linux:** `/usr/opensv/netbackup/bin/admincmd/nbdevquery -listdp -stype OST_TYPE -U`
- **Windows:** `install dir¥netbackup¥bin¥admincmd¥nbdevquery -listdp -stype OST_TYPE -U`

構成されているディスクボリュームを表示するには、次のコマンドを使います。

- **UNIX/Linux:** `/usr/opensv/netbackup/bin/admincmd/nbdevquery -listdv -stype OST_TYPE -U`
- **Windows:** `install dir¥netbackup¥bin¥admincmd¥nbdevquery -listdv -stype OST_TYPE -U`

diskpool 情報のフラグを確認します。次に例を示します。

- CopyExtents - 最適化複製をサポート
- OptimizedImage - 最適化された合成とアクセラレータをサポート
- ReplicationSource - **AIR (複製)** をサポート
- ReplicationTarget - **AIR (インポート)** をサポート

ディスクプールの初期構成の後に、次のように `nbdevconfig -updatedp` コマンドを実行して、ベンダーが追加した新しいフラグを認識する必要があります。

- **UNIX/Linux:** `/usr/opensv/netbackup/bin/admincmd/nbdevconfig -updatedp -stype OST_TYPE -dp diskpool -M master`
- **Windows:** `install dir¥netbackup¥bin¥admincmd¥nbdevconfig -updatedp -stype OST_TYPE -dp diskpool -M master`

サポートされているフラグを手動で追加するには、次のコマンドを使うことができます。

- `nbdevconfig -changests -storage_server storage server name -stype OST_TYPE -setattribute OptimizedImage`
- `nbdevconfig -changedp -stype OST_TYPE -dp diskpool name -setattribute OptimizedImage`

ストレージサーバーの次のフラグも確認する必要があります。

- OptimizedImage - アクセラレータをサポート

すべてのメディアサーバーの OpenStorage 資格情報を一覧表示するには、次のコマンドを使います。

- UNIX/Linux: `/usr/opensv/volmgr/bin/tpconfig -dsh -all_hosts`
- Windows: `install dir¥volmgr¥bin¥tpconfig -dsh -all_hosts`

SLP (Storage Lifecycle Policy) および自動イメージレプリケーション (A.I.R.) のログ記録

この章では以下の項目について説明しています。

- [ストレージライフサイクルポリシー \(SLP\) と自動イメージレプリケーション \(A.I.R.\) について](#)
- [ストレージライフサイクルポリシー \(SLP\) 複製プロセスフロー](#)
- [自動イメージレプリケーション \(A.I.R.\) のプロセスフローのログ記録](#)
- [インポートのプロセスフロー](#)
- [SLP および A.I.R. のログ記録](#)
- [SLP の構成と管理](#)

ストレージライフサイクルポリシー (SLP) と自動イメージレプリケーション (A.I.R.) について

ストレージライフサイクルポリシー (SLP) には、データに適用される手順がストレージ操作の形で含まれています。

自動イメージレプリケーション (A.I.R.) を使うと、NetBackup ドメイン間でバックアップをレプリケートできます。A.I.R. では、バックアップをレプリケートするときに、レプリケート先ドメインにカタログエントリが自動的に作成されます。ペリタスは、ディザスタリカバリサイトで

NetBackup カタログを入力するために、ライブカタログレプリケーションではなく A.I.R. を使うことを推奨します。

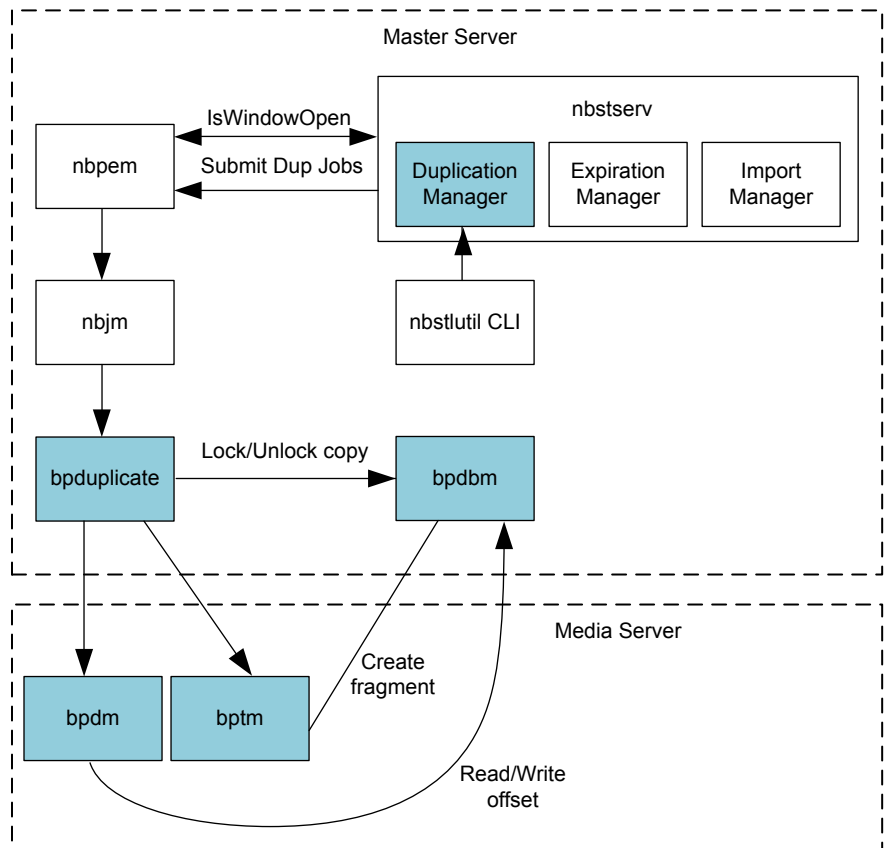
ストレージライフサイクルポリシー (SLP) の操作 (バックアップ、複製、レプリケーション、インポート、スナップショットなど) について理解することは、問題のトラブルシューティングに役立つログを判断するために役立ちます。このトピックでは、主に自動イメージレプリケーション (A.I.R.) と複製のプロセスフローに焦点を当てます。バックアップやスナップショットなどの他の操作のプロセスフローについては、このガイドの他のトピックで説明しています。

SLP と A.I.R. について詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

ストレージライフサイクルポリシー (SLP) 複製プロセスフロー

次の図では、SLP の複製プロセスフローについて説明します。

図 9-1 SLP の複製のプロセスフロー



SLP の複製のプロセスフローは次のとおりです。

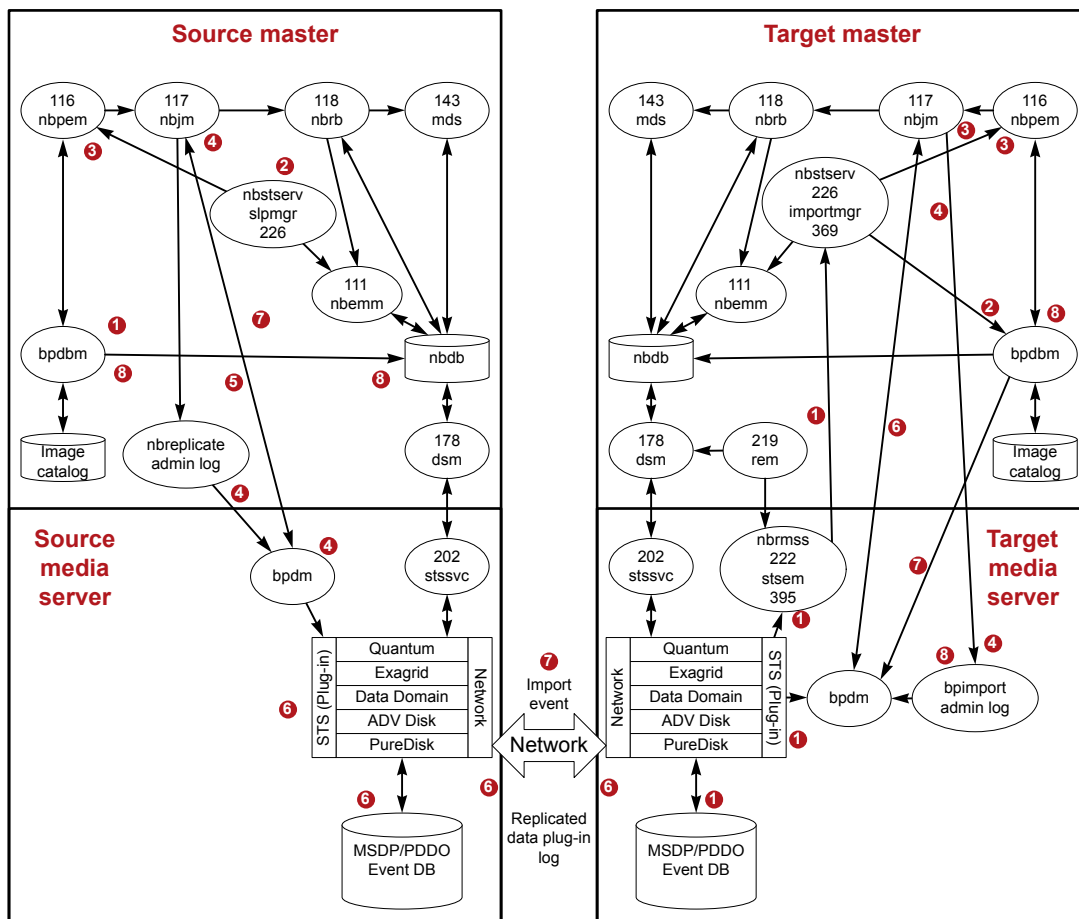
1. SLP マネージャ (nbtserv) が、複製ジョブを送信するために複製ウィンドウが開いているかどうかを確認します。複製ジョブを送信するために開いている SLP ウィンドウが見つかったら、SLP ポリシーによって管理されている関連イメージの処理とバッチ処理が行われ、さらに処理するために nbpem に送信されます。
2. nbpem も、複製操作のために SLP ウィンドウがまだ開いているかどうかを確認します。ウィンドウが開いている場合、nbpem は複製ジョブ構造を作成して nbjm に送信します。
3. nbjm がバックアップ用のリソースを要求して (図には示されていません)、bpduplicate を呼び出します。

4. `bpduplicate` が必要な `bpdm` および `bptm` プロセスを開始し、メディアのロード操作が行われ(図には示されていません)、ローカルソースストレージからイメージが読み込まれて、ローカルの宛先ストレージに書き込まれます。
5. メディアサーバーの `bpdm/bptm` プロセスが終了すると、`bpduplicate` も終了します。

自動イメージレプリケーション (A.I.R.) のプロセスフローのログ記録

次の図は、自動イメージレプリケーション (A.I.R.) のプロセスフローを示しています。

図 9-2 自動イメージレプリケーション (A.I.R.) のプロセスフロー



メモ: A.I.R. レプリケーションでは、MSDP または OST ディスクベースのストレージユニットのみが使用されます。テープストレージユニットと Advanced Disk ストレージユニットは A.I.R. で使用できません。ベーシックディスクストレージユニットは SLP でサポートされていません。

自動イメージレプリケーション (A.I.R.) のプロセスフローは次のとおりです。

1. SLP 制御のバックアップが完了します。バックアップイメージには、レプリケーションや複製などのセカンダリ操作に使用する SLP ポリシーに関する情報が含まれています。
2. nbstserv は一定の間隔 (SLP パラメータ: イメージ処理の間隔) で機能し、レプリケーション用のイメージをバッチ処理します。SLP マネージャ (nbstserv) が、レプリケーションジョブを送信するために SLP ウィンドウが開いているかどうかを確認します。
3. 次に、nbstserv がこのバッチを nbpem に送信します。nbpem がこのジョブを nbjm に渡し、nbrb および nbemm のリソースが確認されます。SLP ウィンドウが開いている場合、nbpem は nbjm にジョブを渡します。
4. nbjm が nbreplicate を開始し (nbreplicate が admin ログに表示されます)、nbreplicate を bpdm に渡します。
5. bpdm が nbjm に物理リソースを要求します。
6. レプリケーションの確認が実行され、レプリケーションが開始されます。bpdm により、ソースストレージサーバーがレプリケーションを開始するタイミングが分かります。その後、ソースストレージサーバーとターゲットストレージサーバーが、実際のデータのレプリケーションを実行するために通信します。

メモ: レプリケーションでは、1 つの bpdm プロセスが操作を制御します。

7. レプリケーションイベントがリモートまたはターゲットのストレージサーバーに送信されます。
8. レプリケーションが完了し、イメージコピーレコードが更新されます。

インポートのプロセスフロー

インポートのプロセスフローは次のとおりです。

1. ディスクストレージの監視を行うメディアサーバーが、A.I.R. インポートイベントのストレージをポーリングします。ポーリングは nbrmms プロセスが行います。インポートイベントに関連付けられたイメージが、マスターサーバー上の (nbstserv 内で実行されている) インポートマネージャに送信されます。

2. インポートマネージャ (OID 369) が、イメージレコードを NBDB データベースに挿入します。
3. nbstserv はインポートする必要があるイメージを一定間隔で検索します。インポートするイメージをバッチ処理し、要求を nbpem に送信します。nbpem がこのジョブを nbjm に渡し、nbrb および nbemm からのリソースが確認されます。
4. nbjm が bpimport を開始します。レプリケートされたイメージについては、インポートイベントが受け取られたときに **NetBackup** がイメージに必要なとするほとんどの情報が取り込まれているため、高速インポートが実行されます。
5. bpimport (admin ログ) がメディアサーバーで bpdm を開始します。
6. bpdm が nbjm から必要な物理リソースを取得します。
7. bpdm がイメージ情報を読み取り、その情報をマスターサーバーの bpdgm に送信します。
8. イメージのインポートが完了し、bpdgm により検証されます。

SLP および A.I.R. のログ記録

nbstserv (マスターサーバー):

```
vxlogcfg -a -p NB -o 226 -s DebugLevel=6 -s DiagnosticLevel=6
```

importmgr (マスターサーバー、インポートマネージャが **226** nbstserv ログ内にログ記録):

```
vxlogcfg -a -p NB -o 369 -s DebugLevel=6 -s DiagnosticLevel=6
```

nbrmms (ディスクストレージの監視を行うメディアサーバーでログ記録):

```
vxlogcfg -a -p NB -o 222 -s DebugLevel=6 -s DiagnosticLevel=6
```

stsem (ストレージサーバーのイベントマネージャ、stsem が **222** nbrmms ログ内にログ記録):

```
vxlogcfg -a -p NB -o 395 -s DebugLevel=6 -s DiagnosticLevel=6
```

複製を実行するメディアサーバーで、適切な bpdm および bptm のレガシーログを表示します。**A.I.R.** レプリケーション操作を開始するメディアサーバーおよび後続のインポートを実行するメディアサーバーで、bpdm のレガシーログを表示して詳細を確認できます。

```
bpdm (verbose 5)
```

```
bptm (verbose 5)
```

プラグインのログ記録を増やして、複製、レプリケーション、およびインポートの操作に関する、bptm/bpdm 内の詳細やサードパーティベンダーの OST プラグインログファイルを取得することができます。

マスターサーバーでは、次のレガシーログも確認のために役立ちます。

- admin: (admin ログはジョブの bpduplicate または nbreplicate コマンドをログ記録する)
- bpdbm: (ファイル、メディア、クライアント情報などのバックアップポリシー情報を含む、NetBackup Database Manager プログラム)

SLP の構成と管理

CLI を使用して構成された SLP ポリシーを表示するには、次のコマンドを実行します。

```
nbstl -L -all_versions
```

SLP の制御下にある (つまり、セカンダリ操作の完了を待機している) イメージを一覧表示するには、次のコマンドを使用します。

```
nbstlutil list -image_incomplete
```

SLP バックログを表示するには、次のコマンドを使用します。

```
nbstlutil report
```

CLI を使用して SLP パラメータを表示するには、bpgetconfig コマンドをマスターサーバー上で実行します。

- UNIX の場合: bpgetconfig | grep SLP
- Windows の場合: bpgetconfig | findstr SLP

(ソースマスターサーバー上で実行された) A.I.R. を使用してレプリケーションされたイメージを一覧表示するには、次のコマンドを使用します。

```
nbstlutil replist
```

(ターゲットマスターサーバー上で実行された) ターゲット環境への A.I.R. のインポートが保留されているイメージを一覧表示するには、次のコマンドを使用します。

```
nbstlutil pendimplist
```

NetBackup の安全な通信 のログ記録

この章では以下の項目について説明しています。

- [NetBackup の安全な通信のログ記録について](#)
- [Tomcat のログ記録](#)
- [NetBackup Web サービスのログ記録](#)
- [コマンドラインのログ記録](#)
- [NetBackup cURL のログ記録](#)
- [Java のログ記録](#)
- [埋め込み認証クライアント \(EAT\) のログ記録](#)
- [認証サービス \(AT\) のログ記録](#)
- [vssat のログ記録](#)
- [NetBackup プロキシヘルパーのログ記録](#)
- [NetBackup プロキシトンネルのログ記録](#)
- [PBX のログ](#)
- [ベリタステクニカルサポートへの安全な通信のログの送信](#)

NetBackup の安全な通信のログ記録について

ここでは、NetBackup ホストとの安全な通信のログ記録に使用されるログについての情報を示します。NetBackup 8.1 以降のホストは、制御型のすべての機能で、安全な通信

を相互に行います。制御型の機能には、コマンドの実行や、バックアップまたはリストアを開始するために必要なさまざまなプロセスの起動が含まれます。現在、ここに bpbkar または tar データ転送は含まれません。NetBackup 8.1 以降のホストが通信を正常に行うには、認証局 (CA) 証明書とホスト ID ベースの証明書が必要です。NetBackup では、ホスト通信にトランスポート層セキュリティ (TLS) プロトコルを使用します。このプロトコルでは、各ホストがそのセキュリティ証明書を提示するとともに、認証局 (CA) の証明書に対してピアホストの証明書を検証する必要があります。

NetBackup 8.0 以降のバージョンでは、マスターサーバーは CA として機能します。マスターサーバーは、適切なインストールと、pbx、nbatd、nbwmc などの証明書を配備するためのサービスの構成に依存します。

NetBackup 8.1 では、すべてのメディアサーバーとクライアントサーバーがアップグレードされると、証明書が配備されます。証明書の配備が失敗した場合、メディアサーバーまたはクライアントサーバーはバックアップまたはリストアを実行できません。NetBackup バージョン 8.1 以降のインストールまたはアップグレード中に、ホストがマスターサーバーから CA 証明書とホスト ID に基づく証明書の両方を正常に取得しなかった場合、バックアップとリストアは機能しません。マスターサーバーの pbx、nbatd、または nbwmc プロセスが実行中でないと、証明書の配備は機能しません。NetBackup 8.1 以降では、バックアップまたはリストアも機能しません。

安全な通信や証明書の生成および配備に関する問題を診断するとき、通常、マスターサーバー上で実行されるサービスやプロセスが関与しています。サービスが実行されており、NetBackup バージョンが期待するものであったことを確認した後は、このセクションで説明するログファイルが問題を特定するために重要になります。

NetBackup の安全な通信について詳しくは、次の URL で安全な通信についてのドキュメントを参照してください。

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

メモ: 環境に NetBackup 8.0 以前のホストが存在する場合、NetBackup 管理コンソールから[セキュリティ管理 (Security Management)]、[グローバルセキュリティ (Global Security)]、[安全な通信 (Secure Communication)]タブの順に移動して、安全でない通信を有効にできます。このタブで、[NetBackup 8.0 以前のホストとの安全でない通信を有効にする (Enable insecure communication with NetBackup 8.0 and earlier hosts)]オプションにチェックマークを付けます。

Tomcat のログ記録

Tomcat ログファイルは、次の場所にあります (マスターサーバー上のみ)。

UNIX の場合: `usr/opensv/wmc/webserver/logs`

Windows の場合: `install_path¥NetBackup¥wmc¥webserver¥logs`

Tomcat ログファイルの詳細度は調整できません。

Tomcat ディレクトリには、`catalina.log`、`nbwmc.log` などのログファイルと、Tomcat の問題のトラブルシューティングに不可欠なその他のログが含まれます。さらに、このディレクトリには、`.hprof` で終わる Tomcat Java ヒープダンプや、`hs_err` で始まるファイル名を持つ Java ダンプが含まれる場合があります。Tomcat や nbwmc の起動の問題やクラッシュの発生に伴ってこれらのファイルが作成される場合は、影響を受ける時間枠のファイルも収集する必要があります。

NetBackup Web サービスのログ記録

NetBackup Web サービスのログは、次の場所にあります (マスターサーバー上のみ)。

UNIX の場合: `usr/openv/logs/nbwebsevice`

Windows の場合: `install path¥netbackup¥logs¥nbwebsevice`

このログディレクトリには、Web サービスのオリジネータのログファイルが含まれています。次のログファイルが含まれますが、これらに制限されるものではありません。

表 10-1 Web サービスの OID とログファイル

オリジネータ ID	ログファイル	説明
439	<code>nbwebsevice¥nbwebsevice</code>	NetBackup Web サービス
466	<code>nbwebsevice¥security</code>	NetBackup セキュリティサービス (セキュリティ Web アプリ)
482	<code>nbwebsevice¥hosts</code>	NetBackup ホスト Web サービス (ホスト Web アプリ)
483	<code>nbwebsevice¥nbconfigmgmt</code>	NetBackup 構成管理サービス (Web アプリ)
484	<code>nbwebsevice¥nbgateway</code>	NetBackup ゲートウェイサービス (Web アプリ)
485	<code>nbwebsevice¥nbwss</code>	NetBackup WebSocket サービス (NBWSS) (Web アプリ)
487	<code>nbwebsevice¥nbcatalogws</code>	NetBackup カタログ Web サービス (Web アプリ)
488	<code>nbwebsevice¥nrbac</code>	NetBackup の役割に基づくアクセス制御 (RBAC) Web サービス (Web アプリ)

オリジネータ ID	ログファイル	説明
489	nbweb service¥nbadminws	NetBackup 管理 Web サービス (Web アプリ)

オリジネータ ID (OID) を使ったプロセスのログ記録は、NetBackup¥bin に配置されている vxlogcfg コマンドを使用して増やしたり減らしたりできます。このコマンドは、以前のプロセスそれぞれについて、ログ記録を追加または削除するために使用できます。次に示す、OID 439 を使用する例を参照してください。

ログ記録を追加するには、-a (追加) オプションを指定して次のコマンドを使用します。

```
vxlogcfg -a -p NB -o 439 -s DebugLevel=6
```

ログ記録を削除するには、-r (削除) オプションを指定して次のコマンドを使用します。

```
vxlogcfg -r -p NB -o 439 -s DebugLevel=6
```

問題がすぐに再び発生する場合は、デフォルトのログファイル設定を 6 に構成し、その後、状況に合わせて設定を 1 に減らすほうが簡単があります。次に例を示します。

ログ記録を増やすには、次のコマンドを使用します。

```
vxlogcfg -a -p NB -o Default -s DebugLevel=6
```

ログ記録を減らすには、次のコマンドを使用します。

```
vxlogcfg -a -p NB -o Default -s DebugLevel=1
```

メモ: 前述の例で、-a オプションを両方のコマンドに追加したのは、デフォルトのログ記録を削除せずに、デバッグレベルのみをデフォルトレベルの 1 に変更するためです。

注意: 変更が実装されるまで 1 分かかる場合があるため、ログファイルのログレベルを変更した後は、必ず最低 1 分は待つようにします。

ファイルシステムがログでいっぱいになる可能性があるため、高いレベルのログ記録を長期間設定したままにしないでください。

OID がデフォルトで 0 に設定されている場合、デフォルトのログレベルが変更されても影響を受けません。これらの OID は、次のとおりです。

- 156: NetBackup ACE/TAO。これによって、ACE/TAO 呼び出しを使用する必要があるすべてのプロセスに対してログ記録されます。

- **486: NetBackup プロキシヘルパー**。これによって、統合された nbpxyhelper ログファイルにログ記録されます。p.145 の「[NetBackup プロキシヘルパーのログ記録](#)」を参照してください。

コマンドラインのログ記録

コマンドラインのログは、次の場所にあります (任意のマスター、メディア、またはクライアントサーバー)。

UNIX の場合: /usr/opensv/netbackup/logs/nbcert

Windows の場合: `install path¥netbackup¥logs¥nbcert`

nbcert ログファイルには、証明書の自動更新中などの、アプリケーションから手動または自動で実行されるすべての nbcertcmd コマンドが記録されます。nbcertcmd を使用して再現される可能性のある問題が発生した場合は、問題をトラブルシューティングするために、bp.conf ファイルまたはレジストリ VERBOSE の設定を **5** に増やす必要があります。ログレベルを増やすには、次のコマンドを使用します。

```
echo VERBOSE = 5 | nbsetconfig
```

NetBackup cURL のログ記録

cURL を呼び出すすべてのプロセスまたはデーモンは、すべてのマスター、メディア、またはクライアントサーバー上で cURL メッセージを記録します。cURL 呼び出しを使用するデーモンやプロセスの cURL メッセージを表示する必要がある場合は、NetBackup cURL のログ記録を増やす必要があります。

cURL のログ記録はデフォルトでは無効になっていますが、次のコマンドを使用して有効にできます。

```
echo ENABLE_NBCURL_VERBOSE=1 | nbsetconfig
```

メモ: NetBackup cURL のログ記録はオンまたはオフにでき、安全な通信に関連する問題が発生したすべての NetBackup クライアントとサーバーで有効にできます。

Java のログ記録

Java のログ記録は、Java が実行されている任意のマスター、メディア、またはクライアントサーバーで発生する可能性があります。Java コンソールにログインできない場合に、nbwmc と安全な通信に関する多くの問題が明らかになります。この場合は、PC やマスターサーバー上など、コンソールを起動している場所に対するログファイルを収集するこ

とをお勧めします。p.182 の「[Java GUI の問題をトラブルシューティングするときのログの設定と収集](#)」を参照してください。

埋め込み認証クライアント (EAT) のログ記録

埋め込み認証クライアント (EAT) のログ記録は、マスターサーバー上でのみ発生します。認証サービス (AT) の呼び出しを実行するすべてのプロセスまたはデーモンで、これらのメッセージが記録されます。NetBackup 8.1 では、AT ログが有効な場合に、認証 (nbatd) ログの内容を、nbatd と連携するすべての NetBackup プロセスに追加できます。AT ログを有効にするには、次のコマンドを使用します。

```
echo EAT_VERBOSE=5 | nbsetconfig
```

有効なログのレベルは、0 から 5 です。

EAT のログ記録を無効にするには、次のコマンドを使用します。

```
echo EAT_VERBOSE=0 | nbsetconfig
```

認証サービス (AT) のログ記録

認証サービス (AT) のログファイルは、次の場所にあります (マスターサーバー上のみ)。

UNIX の場合: /usr/opensv/logs/nbatd

Windows の場合: `install path¥netbackup¥logs¥nbatd OID 18`

ログ記録を増やすには、次のコマンドを使用します。

```
vxlogcfg -a -p NB -o 18 -s DebugLevel=6
```

ログを削除するには、次のコマンドを使用します。

```
vxlogcfg -r -p NB -o 18 -s DebugLevel=6
```

vssat のログ記録

vssat ログファイルは、指定された任意の場所に保存されます。vssat のログ記録を UNIX 上で有効にするには、次のコマンドを使用します。

```
/usr/opensv/netbackup/sec/at/bin/vssat setloglevel -l 4 -f /usr/opensv/logs/nbatd/vssat.log
```

vssat のログ記録を Windows 上で有効にするには、次のコマンドを使用します。


```
install_path¥Veritas¥NetBackup¥sec¥at¥bin¥vssat setloglevel -l 4  
-f C:¥Program Files¥Veritas¥NetBackup¥logs¥nbatd¥vssat.log
```

vssat のログ記録を UNIX 上で無効にするには、次のコマンドを使用します。

```
/usr/opensv/netbackup/sec/at/bin/vssat setloglevel -l 0
```

vssat のログ記録を Windows 上で無効にするには、次のコマンドを使用します。

```
install_path¥Veritas¥NetBackup¥sec¥at¥bin¥vssat setloglevel -l 0
```

NetBackup プロキシヘルパーのログ記録

NetBackup プロキシヘルパーのログファイルは、マスター、メディア、またはクライアントサーバーの次の場所にあります。

UNIX の場合: /usr/opensv/logs/nbpxyhelper

UNIX の起動とシャットダウンの問題の場合: /usr/opensv/netbackup/logs/vnetd

Windows の場合: `install path¥netbackup¥logs¥nbpxyhelper`

Windows の起動とシャットダウンの問題の場合: `install path¥netbackup¥logs¥vnetd`

オリジネータ ID 486

NetBackup プロキシヘルパーのログファイルは、SSL/TLS エラーやその他の安全な通信の問題が原因で通信に問題がある場合に役立ちます。vnetd -standalone コマンドを使用して、プロセスを開始できます。起動とシャットダウンに問題がある場合は、vnetd のログファイルを確認します。

vnetd プロセスの期待される最小数の例を次に示します。

```
/usr/opensv/netbackup/bin/vnetd -proxy inbound_proxy -number 0
```

```
/usr/opensv/netbackup/bin/vnetd -proxy outbound_proxy -number 0
```

```
/usr/opensv/netbackup/bin/vnetd -standalone
```

インバウンドおよびアウトバウンドのプロキシプロセスは、nbpxyhelper ログファイルにログを送信します。それらの間の通信をジョブの詳細を通じて確認できます。:INBOUND または :OUTBOUND の接続 ID を特定し、nbpxyhelper ログファイルでそれらを検索します。:INBOUND と :OUTBOUND の接続は、エラーがある場合にのみ表示されます。次の例を参照してください。

```
Aug 5, 2018 5:13:14 PM - Info nbjm (pid=3442) starting backup job (jobid=268) for
```

```
client nbclient1, policy ANY_nbclient1, schedule Full-EXPIRE_IMMEDIATELY
Aug 5, 2018 5:13:14 PM - Info nbjm (pid=3442) requesting STANDARD_RESOURCE resources from RB
for backup job (jobid=268, request id:{5DD92BD0-98F4-11E8-AEE4-55B66A58DDB2})
Aug 5, 2018 5:13:14 PM - requesting resource __ANY__
Aug 5, 2018 5:13:14 PM - requesting resource nbmaster2.NBU_CLIENT.MAXJOBS.nbclient1
Aug 5, 2018 5:13:14 PM - requesting resource nbmaster2.NBU_POLICY.MAXJOBS.ANY_nbclient1
Aug 5, 2018 5:13:15 PM - Error bpbrm (pid=21177) [PROXY] Connecting host: nbmaster2
Aug 5, 2018 5:13:15 PM - Error bpbrm (pid=21177) [PROXY] ConnectionId:
{5E0FBBD2-98F4-11E8-804A-EC7198374CC6}:OUTBOUND
```

多くのログファイルが作成される可能性があるため、OID 486 はデフォルトで DebugLevel=0 に設定されています。ログ記録を DebugLevel=6 で長期間有効にしたままにしないでください。

ログレベルは、vxlogcfg コマンドを使用して変更できます。次に例を示します。

ログ記録を追加するには、次のコマンドを使用します。

```
vxlogcfg -a -p NB -o 486 -s DebugLevel=6
```

ログを削除するには、次のコマンドを使用します。

```
vxlogcfg -a -p NB -o 486 -s DebugLevel=0
```

メモ: この場合、トラブルシューティングの完了後、ログレベルは明示的に 0 に設定されています。

NetBackup プロキシトンネルのログ記録

NetBackup プロキシトンネルのログは、次の場所にあります (任意のメディアサーバー上)。

UNIX の場合: /usr/openv/logs/nbpxytnl

Windows の場合:install path¥netbackup¥logs¥nbpxytnl

オリジネータ ID 490

NetBackup 8.1 では、マスターサーバーと直接接続できないクライアント用に、メディアサーバーをプロキシトンネルとして使用できます。

プロキシとして機能するメディアサーバーとクライアント間に問題がある場合は、nbpxytnl のログ記録を増やす必要があります。ログレベルは、vxlogcfg コマンドを使用して変更できます。次に例を示します。

ログ記録を追加するには、次のコマンドを使用します。

```
vxlogcfg -a -p NB -o 490 -s DebugLevel=6
```

ログを削除するには、次のコマンドを使用します。

```
vxlogcfg -r -p NB -o 490 -s DebugLevel=6
```

PBX のログ

PBX (Private Branch Exchange) のログは、すべてのマスター、メディア、またはクライアントサーバーの次の場所にあります。

UNIX の場合: /opt/VRTSpx/log

Windows の場合: C:\Program Files (x86)\VERITAS\VxPBX\log

PBX のログファイルは、安全な通信の問題のトラブルシューティングを行うときに重要な役割を果たすことがあります。このようなときに、ログファイルのサイズと数を、ログファイル 5 つとそれぞれ 1 MB というデフォルト設定よりも増やすことが必要になる場合があります。ログファイルのサイズを 50,000 KB にし、ログファイル数を 20 に増やすには、vxlogcfg コマンドを次のように使用します。

Windows の場合

(HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VERITAS\VxICS\logcfg\103 内):

```
C:\Program Files (x86)\VERITAS\VxPBX\bin\vxlogcfg -a -p 50936 -s "MaxLogFileSizeKB=50000"
-o 103
C:\Program Files (x86)\VERITAS\VxPBX\bin\vxlogcfg -a -p 50936 -s "NumberOfLogFiles=20"
-o 103
```

これにより、それぞれ 50 MB のログファイルを 20 個までキャプチャできます。

UNIX の場合:

1. 次のように vxlogcfg コマンドを使用して、ログファイルのサイズを 51,200 KB にし、ログファイルの数を 10 個に増やします。

UNIX の場合 (/etc/vx/VxICS/icsul.conf 内):

```
/opt/VRTSpx/bin/vxlogcfg -a -p 50936 -s "MaxLogFileSizeKB=51200" -o 103
/opt/VRTSpx/bin/vxlogcfg -a -p 50936 -s "NumberOfLogFiles=10" -o 103
```

2. Cd/opt/VRTSpx/log コマンドを使用してディレクトリを変更します。ログファイルのサイズが 1 MB より大きくなっていることを確認します (1 分以内にこの変化を確認できるはずです)。
3. PBX のログ設定を確認するには、構成ファイルを次のように表示できます。
 - /etc/vx/VxICS にディレクトリを変更します。

- `cat icsul.conf` コマンドを使用して、変更が加えられたことを確認します。

次の例を参照してください。

```
cat icsul.conf
#####
# Caution! Do not update/modify file by hand.
# Use vxlogcfg tool to update/modify this file
#####
103.DebugLevel=6
103.AppMsgLogging=ON
103.LogToOslog=false
103.LogDirectory=/var/log/VRTSpxb/
103.L10nResourceDir=/opt/VRTSpxb/resources
103.L10nLib=/optVRTSpxb/lib/libvxexticu.so.3
103.L10nResource=VxPBX
103.MaxLogFileSizeKB=51200
103.RolloverMode=FileSize
103.NumberOfLogFiles=10
103.LogRecycle=true
```

ベリタステクニカルサポートへの安全な通信のログの送信

証明書の配備または安全な通信が原因で問題が発生した場合は、問題のレポートと関連するログをベリタステクニカルサポートに送信して支援を依頼できます。次の表には、ほとんどの問題のトラブルシューティングに必要なログファイルが含まれています。

表 10-2 は、ベリタステクニカルサポートが安全な通信の問題を診断するのに必要になるログのリストおよび推奨ログレベルを示します。

表 10-2 安全な通信の問題のために収集するログ

問題の種類	収集するログ
Java コンソールのログインエラー	マスターサーバーから: ■ 詳細 5 の bpjava-msvc ログ ■ 詳細 5 の bpjava-susvc ログ ■ デバッグレベル 6 の nbsl ログ ■ デバッグレベル 6 で OID 156 (ACE¥TAO) と 137 (NB ライブラリ) を有効にします。それらは、呼び出しプロセスに書き込みます。 ■ 埋め込み認証クライアント (EAT) のログ記録を有効にします。 ■ nbatd ログ (AT ログセクションから) ■ vssat.log (vssat ログを参照) ■ PBX のログファイル ■ NetBackup サポートユーティリティ nbsu コンソールが起動されたエンティティから: ■ nbj または jbp のログファイル
nbwmc のマスターサーバーでの開始または予期しない終了	すべてのログがマスターサーバーに存在します。 ■ nbwebsservice ログ (Web サービスのログを参照) ■ nbwmc ログ、webserver ログ、および問題のデータからのすべてのファイル (hs_err.* または *.hprof ファイルを含む) ■ インストールログファイル ■ nbsu を収集 (インストールログを自動収集するため) ■ nbcert ログ ■ PBX のログファイル
インストール中の証明書の配備	証明書を配備できないサーバーから: ■ nbcert ログ ■ インストールログ ■ nbsu を収集 (インストールログを自動収集するため) ■ デバッグレベル 4 以上の nbpxyhelper ログファイル マスターサーバーから: ■ nbcert ログ ■ デバッグレベル 4 以上の nbpxyhelper ログファイル

問題の種類	収集するログ
安全な接続の確立エラーを原因とするバックアップの失敗	問題のクライアントまたはメディアサーバーから: ■ nbcert ログ ■ デバッグレベル 4 以上の nbpxyhelper ログファイル 接続を拒否しているマスターまたはメディアサーバーから: ■ デバッグレベル 4 以上の nbpxyhelper ログファイル ■ bprd、bptm、および bpbrm など、通信に関係するすべてのプロセスログ。 マスターから: ■ ジョブの詳細 メモ: cURL ログが有効になっていることを確認します。
カタログバックアップ中のディザスタリカバリ (DR) パッケージの作成	マスターサーバーから: ■ 詳細 5 の bpdbrm ログ
Web サーバートンネル (メディア) または Web サーバーのルーター (クライアント)	トンネルとして機能するメディアサーバーから: ■ デバッグレベル 6 の nbpxytnl ログファイル ■ デバッグレベル 4 以上の nbpxyhelper ログファイル クライアント/ルーターから: ■ nbcert ログファイル ■ bpcd ログファイル ■ デバッグレベル 4 以上の nbproxyhelper ログファイル マスターサーバーから: ■ デバッグレベル 4 以上の nbproxyhelper ログファイル メモ: cURL ログが有効になっていることを確認します。

スナップショット技術

この章では以下の項目について説明しています。

- [Snapshot Client のバックアップ](#)
- [VMware バックアップ](#)
- [スナップショットバックアップおよび Windows Open File Backup](#)

Snapshot Client のバックアップ

典型的なスナップショットのバックアップ処理を以下に示します。このシナリオでは、スナップショットはクライアントで作成され、そのクライアントのストレージユニット(ディスクまたはテープ)にバックアップされます。複数のデータストリームを使わない **Windows** オープンファイルバックアップ は例外として、すべてのスナップショットは個別の親ジョブで作成され、その後にスナップショットをバックアップする子ジョブが続きます。非マルチストリームの **Windows** オープンファイルバックアップの場合、bpbrm で bpcd を使って bpfis を呼び出し、個々のデバイスのスナップショットを作成します。システム状態またはシャドーコピーコンポーネントのバックアップでは、bpbkar32 はボリュームシャドーコピーサービス (VSS) を使ってスナップショットを作成します。**Windows** オープンファイルバックアップは、bpfis などの **Snapshot Client** コンポーネントを使用しますが、**Snapshot Client** ライセンスを必要としません。

スナップショット作成およびバックアップのための基本の処理手順は次のとおりです(複数データストリームを用いる Windows オープンファイルバックアップ を含む):

Snapshot Client のバックアップ手順

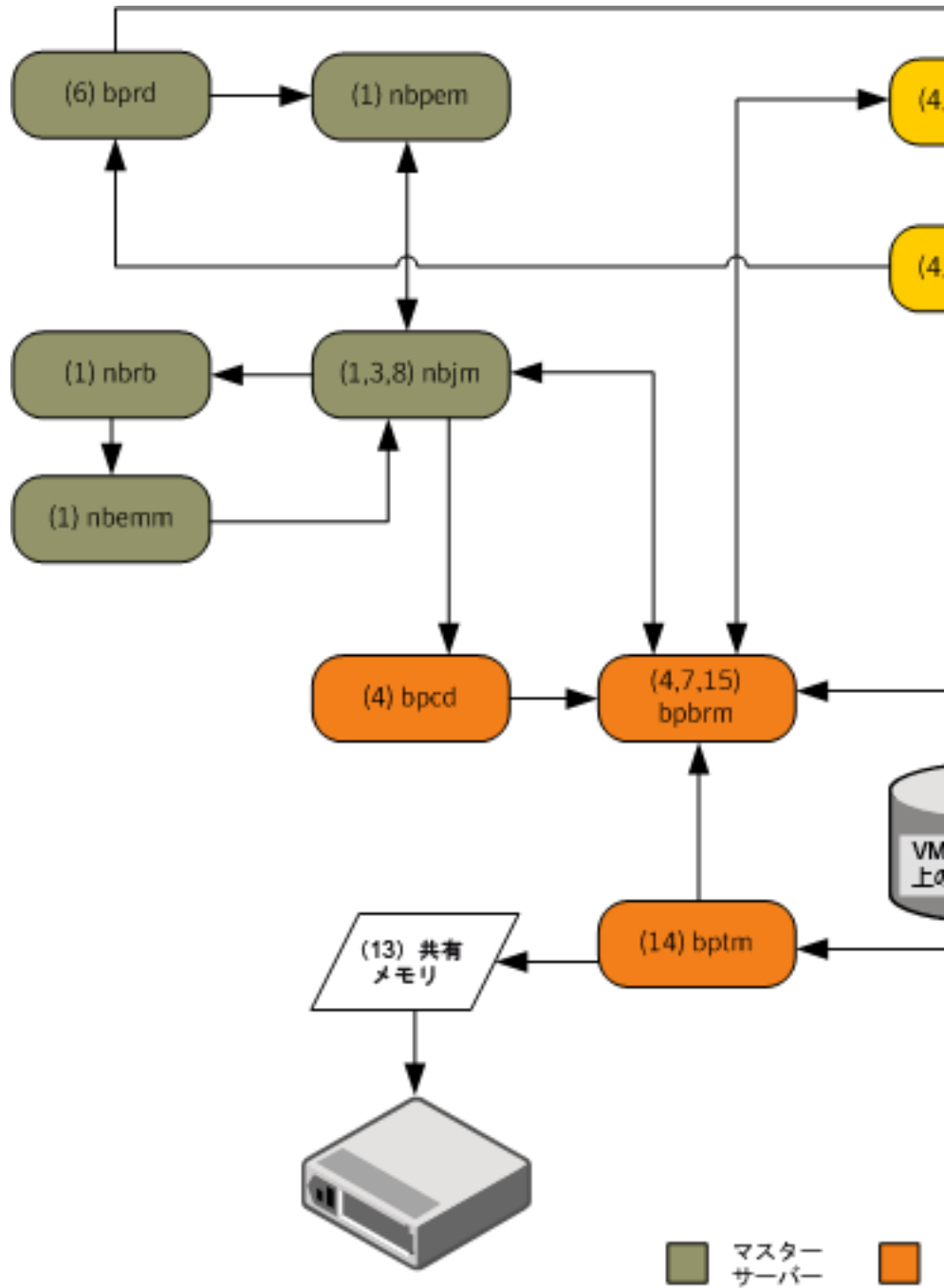
- 1 NetBackup マスターサーバーまたはプライマリクライアントがバックアップを開始し、これにより NetBackup 要求デーモン (bprd) がバックアップ要求を Policy Execution Manager (nbpem) に送信します。nbpem によってポリシーの構成内容が処理されます。
- 2 nbpem は nbjm を使用して、スナップショットを作成する親ジョブを開始します。このジョブは、スナップショットのバックアップを行うジョブとは別のジョブです。
- 3 nbjm によって、メディアサーバー上で bpcd を介して bpbrm のインスタンスが起動され、bpbrm によって、クライアント上で bpcd を介して bpfis が起動されます。
- 4 bpfis によって、スナップショット方式を使用してクライアントのデータのスナップショットが作成されます。
- 5 bpfis は bprd に接続して、bpfis 状態ファイルのクライアントからサーバーへの転送を要求します。この操作はデフォルトで有効になっています。
- 6 bprd はクライアント上の bpcd に bpfis 状態ファイルのリストを送信するように要求します。
- 7 bprd は各状態ファイルをクライアントからマスターにコピーします。
- 8 bpfis はスナップショット情報と完了ステータスを bpbrm に送信して終了します。bpbrm は、順番に、スナップショット情報と状態を nbjm にレポートして終了します。nbjm から nbpem へその情報および状態が送信されます。
- 9 nbpem は nbjm にスナップショット情報から取得したファイルリストを持つバックアップ用の子ジョブを送信します。nbjm は bpbrm を開始してスナップショットをバックアップします。
- 10 bpbrm はクライアント上で bpbkar を開始します。bpbkar によって、ファイルのカタログ情報が bpbrm に送信されます。このカタログ情報が、bpbrm によってマスターサーバー上の NetBackup ファイルデータベース bpdbs に送信されます。
- 11 bpbrm によって、メディアサーバー上でプロセス bptm (親) が起動されます。
- 12 以下のいずれかを実行する: 次の手順は、メディアサーバーがそれ自体をバックアップするか (bptm および bpbkar が同じホスト上に存在する)、または別のホスト上に存在するクライアントをバックアップするかによって異なります。
 - メディアサーバーがそれ自体をバックアップする場合、bpbkar によって、スナップショットに基づいたイメージがメディアサーバー上の共有メモリにブロック単位で格納されます。
 - メディアサーバーが別のホスト上に存在するクライアントをバックアップする場合、サーバー上の bptm プロセスによって、そのプロセスの子プロセスが作成されま

す。子プロセスは、ソケット通信を使用してクライアントからスナップショットに基づいたイメージを受信し、そのイメージをサーバー上の共有メモリにブロック単位で格納します。

- 13 元の `bptm` プロセスによって、バックアップイメージが共有メモリから取り出され、ストレージデバイス (ディスクまたはテープ) に送信されます。
- 14 `bptm` は `bpbrm` にバックアップの完了状態を送信し、それが `nbjm` に渡されます。
- 15 `nbpem` が `nbjm` からバックアップ完了状態を受信すると、`nbpem` は `nbjm` にスナップショットを削除するように指示します。`nbjm` はメディアサーバー上で `bpbrm` の新しいインスタンスを開始し、`bpbrm` はクライアント上で `bpfis` の新しいインスタンスを開始します。スナップショットがインスタントリカバリ形式である場合を除き、`bpfis` によってクライアント上でスナップショットが削除されます。スナップショットがインスタントリカバリ形式の場合はスナップショットは自動的に削除されません。`bpfis` と `bpbrm` は状態をレポートして終了します。

VMware バックアップ

次に、VMware バックアップ処理を示します。



VMware バックアップ操作の基本的な処理手順は次のとおりです。

VMware バックアップ手順

- 1 **Policy Execution Manager (nbpem)** は、ポリシー、スケジュール、仮想マシンが実行予定時間になり、バックアップ処理時間帯が始まるとバックアップジョブをトリガします。バックアップ操作のnbpemプロセス、**Job Manager (nbjm)**、**Resource Broker (nbrb)**、**Enterprise Media Manager (nbemm)**はともにリソース (メディアサーバー、ストレージユニットなど) を識別します。
- 2 **VMware インテリジェントポリシー (VIP)** の場合は、vSphere 環境で使う VMware リソースをスロットルできます。たとえば、vSphere データストアからリソースで実行する並行バックアップジョブを 4 つに制限できます。この制御レベルで、vSphere プラットフォームのユーザーとアプリケーションのエクスペリエンスに与える影響が最小になるようにバックアップ数を調整します。
- 3 nbpem は nbjm を使って、選択したメディアサーバーに接続してこのサーバーで **Backup Restore Manager (bpbrm)** を起動します。アクティビティモニターでスナップショットジョブ (親ジョブとも呼ばれる) がアクティブになります。
- 4 nbjm はメディアサーバーのクライアントサービス (bpcd) を介して bpbrm のインスタンスを起動します。bpbrm は VMware バックアップホストのクライアントサービス (bpcd) を介して **Frozen Image** スナップショット (bpfis) を起動します。bpfis は設定したクレデンシャルサーバーに応じて vCenter または ESX ホストを使って VM データのスナップショットを作成します。

vADPを搭載したbpfisは、クレデンシャルを NetBackup データベースに保存し、VM のスナップショットを開始する vSphere ホスト (vCenter) や ESX/ESXi ホストと接続します。VM が複数の場合は、bpbrm が各 VM の bpfis を開始してスナップショット操作を並行して実行できるようにします。ステップ 2 に示したように、**NetBackup** で VMware リソースの制限を設定して VIP の並行スナップショット数を制御できます。bpfis は、標準 SSL ポート (デフォルトは 443) を使って vSphere ホストに接続します。
- 5 bpfis は **Request Manager (bprd)** に接続して VMware バックアップホストからマスターサーバーに bpfis 状態ファイルの転送を要求します。
- 6 bprd は bpfis 状態ファイルのリストを送信するように VMware バックアップホストの bpcd に要求します。bprd は VMware バックアップホストから各状態ファイルをマスターサーバーにコピーします。
- 7 bpfis はスナップショット情報と完了状態を bpbrm に送信します。bpbrm はスナップショット情報と状態を nbjm に報告します。nbjm からnbpem へその情報および状態が送信されます。
- 8 nbpem によって、スナップショット情報から生成されたファイルリストとともに、バックアップの子ジョブが nbjm に送信されます。nbjm は bpbrm を開始してスナップショットをバックアップします。

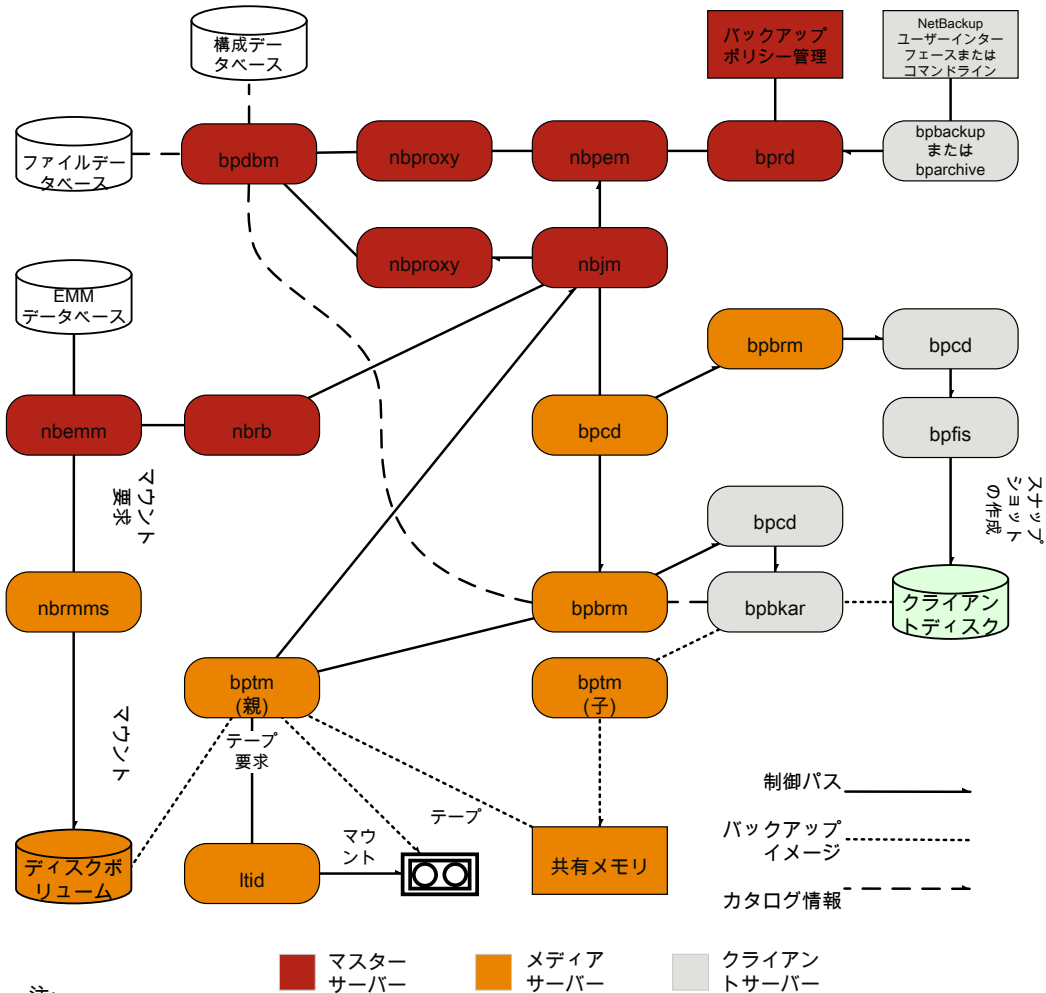
- 9 bpbarm は bpcd を使って VMware バックアップホストの bpbkar を開始します。
- 10 Backup Archive Manager (bpbkar) が、VDDK (VMware Disk Development Kit) の API をロードする VxMS (Veritas Mapping Service) をロードします。vSphere データストアから読み込む場合は API を使います。VxMS は実行時にストリームをマップして vmdk ファイルの内容を識別します。bpbkar が VxMS を使ってファイルカタログ情報を bpbarm に送信し、ここを中継してマスターサーバーのデータベースマネージャ bpbdbm に送ります。
- 11 bpbarm は、メディアサーバーでプロセス bptm (親) の起動も行います。
- 次に、VxMS で実行する Veritas V-Ray 操作を示します。
- VxMS 内で Veritas V-Ray を使うと、Windows と Linux 両方の VM から VMDK 内のファイルすべてのカタログを生成します。この操作はバックアップデータのストリーム配信中に行われます。メディアサーバーの bpbarm はマスターサーバーにこのカタログ情報を送信します。
 - ファイルシステムの i ノードレベルは未使用ブロックと削除済みブロックも識別します。たとえば、VM のアプリケーションが現在 100 GB のみ使用中のファイルに 1 TB の領域を割り当てると、バックアップストリームにはその 100 GB のみが含まれます。同様に、以前完全に割り当てた 1 TB のファイルを削除すると、VxMS はバックアップストリームの削除済みブロックをスキップします (このブロックを新しいファイルに割り当てない場合)。この最適化はバックアップストリームを高速化するだけでなく、重複排除が無効でも必要なストレージを削減します。
 - バックアップ元の重複排除機能が有効になっている場合には、VMware バックアップホストは重複排除します。NetBackup 重複排除プラグインは VxMS が VMDK 内部のファイルシステムで実際のファイルを生成し、参照するマップ情報を使います。この V-Ray ビジョンは VxMS マップ情報を把握する専用のストリームハンドラをロードする NetBackup 重複排除プラグインによって確立されます。
 - これらの操作は VMware バックアップホストで行うので、ESX リソースと VM リソースは使いません。この設定は実働 vSphere に負荷をかけない真のオフホストバックアップです。バックアップ元の重複排除もオフホストシステムで行われます。
- 12 メディアサーバーが VMware バックアップホストの場合には、bpbkar はメディアサーバーで共有メモリのスナップショットベースのイメージをブロックごとに格納します。メディアサーバーがメディアサーバー以外の別の VMware バックアップホストのバックアップを作成する場合は、サーバーの bptm プロセスはそれ自身の子プロセスを作成します。子はソケット通信を使って VMware バックアップホストからスナップショットベースのイメージを受信して共有メモリにイメージをブロック別に格納します。
- 13 元の Tape Manager (bptm) プロセスは、共有メモリからバックアップイメージを取り出してストレージデバイス (ディスクまたはテープ) に送信します。

- 14 bptm は bpbrm にバックアップの完了状態を送信し、bpbrm から nbjm と nbpem に完了状態が渡されます。
- 15 nbpem は nbjm にスナップショットの削除を指示します。nbjm はメディアサーバーの bpbrm の新しいインスタンスを開始し、bpbrm は VMware バックアップホストの bpfis の新しいインスタンスを開始します。bpfis は vSphere 環境のスナップショットを削除します。bpfis と bpbrm は状態をレポートして終了します。

スナップショットバックアップおよび Windows Open File Backup

図 11-1 に、スナップショットバックアップ処理の概要を示します。NetBackup が動作するには、PBX (図で示されていない) が実行されている必要があります。

図 11-1 複数のデータストリームを使用したスナップショットバックアップおよび Windows Open File Backup



注:

*

これらのコンポーネントについて詳しくは、この章の後半の「メディアおよびデバイスの管理機能の説明」を参照してください。

**

メディアサーバーがそれ自体 (同じホスト上のサーバーとクライアント) をバックアップする場合、bptm の子は存在しません。bpbkar は共有メモリにデータを直接送信します。

すべてのスナップショットは個別の親ジョブによって作成され、その後、子ジョブによってスナップショットのバックアップが行われます。

次に、複数のデータストリームを使用する Windows Open File Backup を含むスナップショットの作成とバックアップ処理のシーケンスを示します。

- **NetBackup** マスターサーバーまたはプライマリクライアントがバックアップを開始します。この処理により、**NetBackup Request** デーモン `bprd` から **Policy Execution Manager** `nbpem` にバックアップ要求が送信されます。`nbpem` によってポリシーの構成内容が処理されます。
- `nbpem` によって、(`nbjm` を介して) 親ジョブが開始され、スナップショットが作成されます。このジョブは、スナップショットのバックアップを行うジョブとは別のジョブです。
- `nbjm` によって、メディアサーバー上で `bpcd` を介して `bpbrm` のインスタンスが起動され、`bpbrm` によって、クライアント上で `bpcd` を介して `bpfis` が起動されます。
- `bpfis` によって、スナップショット方式を使用してクライアントのデータのスナップショットが作成されます。
- `bpfis` は完了したときに、スナップショット情報と完了状態を `bpbrm` に送信して終了します。`bpbrm` は、順番に、スナップショット情報と状態を `nbjm` にレポートして終了します。`nbjm` から `nbpem` へその情報および状態が送信されます。
- `nbpem` によって、スナップショット情報から生成されたファイルリストとともに、バックアップの子ジョブが `nbjm` に送信されます。`nbjm` は `bpbrm` を開始してスナップショットをバックアップします。
- `bpbrm` はクライアント上で `bpbkcar` を開始します。`bpbkcar` によって、ファイルのカタログ情報が `bpbrm` に送信されます。このカタログ情報が、`bpbrm` によってマスターサーバー上の **NetBackup** ファイルデータベース `bpbdbm` に送信されます。
- `bpbrm` によって、メディアサーバー上でプロセス `bptm` (親) が起動されます。
- 次の手順は、メディアサーバーが、それ自体をバックアップする (`bptm` と `bpbkcar` が同じホスト上に存在する) か、または別のホスト上に存在するクライアントをバックアップするかによって異なります。メディアサーバーがそれ自体をバックアップする場合、`bpbkcar` によって、スナップショットに基づいたイメージがメディアサーバー上の共有メモリにブロック単位で格納されます。メディアサーバーが別のホスト上に存在するクライアントをバックアップする場合、サーバー上の `bptm` によって、その子プロセスが作成されます。子プロセスは、ソケット通信を使用してクライアントからスナップショットに基づいたイメージを受信し、そのイメージをサーバー上の共有メモリにブロック単位で格納します。
- その後、元の `bptm` プロセスによって、バックアップイメージが共有メモリから取り出され、ストレージデバイス (ディスクまたはテープ) に送信されます。
テープ要求が発行される方法についての情報が利用可能です。

『NetBackupトラブルシューティングガイド UNIX、Windows および Linux』の「メディアおよびデバイスの管理プロセス」を参照してください。

- bptm から bpbrm へバックアップの完了状態が送信されます。bpbrm から nbjm へ完了状態が渡されます。
- nbpem が nbjm からバックアップ完了状態を受信したときに、nbpem はnbjm にそのスナップショットを削除するように指示します。nbjm はメディアサーバー上で bpbrm の新しいインスタンスを開始し、bpbrm はクライアント上で bpfis の新しいインスタンスを開始します。スナップショットがインスタントリカバリ形式である場合を除き、bpfis によってクライアント上でスナップショットが削除されます。スナップショットがインスタントリカバリ形式の場合はスナップショットは自動的に削除されません。bpfis と bpbrm は状態をレポートして終了します。

詳しくは、『NetBackup Snapshot Client 管理者ガイド』を参照してください。

Windows Open File Backup には Snapshot Client は必要ありません。

ログの場所

この章では以下の項目について説明しています。

- [acsssi](#) のログ
- [bpbackup](#) のログ
- [bpbkar](#) のログ
- [bpbrm](#) のログ
- [bpcd](#) のログ
- [bpcompatd](#) のログ
- [bpdbm](#) のログ
- [bpjobd](#) のログ
- [bprd](#) のログ
- [bprestore](#) のログ
- [bptestnetconn](#) ログ
- [bptm](#) のログ
- [daemon](#) のログ
- [ltid](#) のログ
- [nbemm](#) のログ
- [nbjm](#) のログ
- [nbpem](#) のログ
- [nbproxy](#) のログ

- [nbrb](#) のログ
- [NetBackup Web](#) サービスのログ記録
- [NetBackup Web](#) サーバー証明書のログ記録
- [PBX](#) のログ
- [reqlib](#) のログ
- [robots](#) のログ
- [tar](#) ログ
- [txxd](#) および [txxd](#) のログ
- [vnetd](#) のログ

acsssi のログ

UNIX では、NetBackup ACS ストレージサーバーインターフェース (acsssi) が ACS ライブラリソフトウェアホストと通信します。

ログの場所	UNIX の場合: /usr/opensv/volmgr/debug/acsssi
ログが存在するサーバー	メディア
アクセス方法	acsssi プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「 レガシーログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

bpbackup のログ

bpbackup コマンドライン実行可能ファイルはユーザーバックアップの開始に使用されます。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥bpbackup</code> UNIX の場合: /usr/opensv/netbackup/logs/bpbackup
ログが存在するサーバー	クライアント

アクセス方法 bpbbackup プロセスはレガシーのログ方式を使用します。レガシーデバッグログが **NetBackup** サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

bpbkar のログ

バックアップおよびアーカイブマネージャ (bpbkar) はメディアサーバーに送信されてストレージサーバーに書き込まれるクライアントデータを読み込みます。また、バックアップされたファイルのメタデータを収集して files ファイルを作成します。

ログの場所 Windows の場合:
`install_path¥NetBackup¥logs¥bpbkar`
UNIX の場合: `/usr/opensv/netbackup/logs/bpbkar`

ログが存在するサーバー クライアント

アクセス方法 bpbkar プロセスはレガシーのログ方式を使用します。レガシーデバッグログが **NetBackup** サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

bpbrm のログ

NetBackup バックアップおよびリストアマネージャ (bpbrm) は、クライアントおよび bptm プロセスを管理します。また、クライアントおよび bptm のエラー状態を使用して、バックアップおよびリストア操作の最終状態を判断します。

ログの場所 Windows の場合:
`install_path¥NetBackup¥logs¥bpbrm`
UNIX の場合: `/usr/opensv/netbackup/logs/bpbrm`

ログが存在するサーバー メディア

アクセス方法 bpbrrm プロセスはレガシーのログ方式を使用します。レガシーデバッグログが **NetBackup** サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

bpcd のログ

NetBackup クライアントサービス (bpcd) は、リモートホストを認証し、ローカルホストでプロセスを起動します。

ログの場所 **Windows** の場合: `install_path¥NetBackup¥logs¥bpcd`
UNIX の場合: `/usr/opensv/netbackup/logs/bpcd`

ログが存在するサーバー メディアおよびクライアント

アクセス方法 bpcd プロセスはレガシーのログ方式を使用します。レガシーデバッグログが **NetBackup** サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

bpcompatd のログ

NetBackup 互換性サービス (bpcompatd) は、マルチスレッドプロセスと **NetBackup** レガシープロセス間の接続を作成します。

ログの場所 **Windows** の場合:
`install_path¥NetBackup¥logs¥bpcompatd`
UNIX の場合: `/usr/opensv/netbackup/logs/bpcompatd`

ログが存在するサーバー **master**

アクセス方法 bpcompatd プロセスはレガシーのログ方式を使用します。レガシーデバッグログが **NetBackup** サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.67 の「バックアップログについて」を参照してください。

bpdbm のログ

NetBackup Database Manager (bpdbm) は、構成、エラー、およびファイルデータベースを管理します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥bpdbm</code> UNIX の場合: <code>/usr/openv/netbackup/logs/bpdbm</code>
ログが存在するサーバー	master
アクセス方法	bpdbm プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「レガシーログについて」を参照してください。

p.67 の「バックアップログについて」を参照してください。

p.94 の「リストアログについて」を参照してください。

bpjobd のログ

bpjobd サービスはジョブデータベースを管理し、ジョブ状態をアクティビティモニターに中継します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥bpjobd</code> UNIX の場合: <code>/usr/openv/netbackup/logs/bpjobd</code>
ログが存在するサーバー	master
アクセス方法	bpjobd プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「レガシーログについて」を参照してください。

p.67 の「バックアップログについて」を参照してください。

p.94 の「リストアログについて」を参照してください。

bprd のログ

NetBackup Request デーモン (bprd) はバックアップ、リストア、およびアーカイブのクライアント要求および管理要求に応答します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥bprd</code> UNIX の場合: <code>/usr/opensv/netbackup/logs/bprd</code>
ログが存在するサーバー	master
アクセス方法	bprd プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「 レガシーログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

bprestore のログ

bprestore コマンドライン実行可能ファイルはリストアの開始に使用されます。マスターサーバーの bprd と通信します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥bprestore</code> UNIX の場合: <code>/usr/opensv/netbackup/logs/bprestore</code>
ログが存在するサーバー	クライアント
アクセス方法	bprestore プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「 レガシーログについて 」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

bptestnetconn ログ

bptestnetconn コマンドは、ホストの任意の指定のリスト (NetBackup 構成のサーバーリストを含む) での DNS と接続の問題の分析に役立つ複数のタスクを実行します。

指定したサービスへの CORBA 接続に対して `bptestnetconn` を実行すると、その接続について報告が行われ、CORBA 通信を使うサービス間の接続の問題のトラブルシューティングに役立てることができます。コマンドが実行し **NetBackup Web** サービスの応答性をレポートすることもできます。このコマンドは、安全なプロキシプロセスに接続して通信が暗号化されたかどうかや、接続方向を示します。

ログの場所	Windows の場合: <code>install_path¥Veritas¥NetBackup¥logs¥nbutils</code> UNIX の場合: <code>/usr/opensv/logs/nbutils</code>
ログが存在するサーバー	マスター、クライアント、およびメディア
アクセス方法	<code>bptestnetconn</code> プロセスは統合ログ方式を使用します。統合ログファイルを表示および管理するには、 <code>vxlogview</code> および <code>vxlogmgr</code> コマンドを使用します。 p.13 の「 統合ログについて 」を参照してください。

bptm のログ

NetBackup テープ管理プロセス (`bptm`) は、クライアントとストレージデバイス (テープまたはディスク) 間のバックアップイメージの転送を管理します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥bptm</code> UNIX の場合: <code>/usr/opensv/netbackup/logs/bptm</code>
ログが存在するサーバー	メディア
アクセス方法	<code>bptm</code> プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「 レガシーログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

daemon のログ

`daemon` ログには **Volume Manager** サービス (`vmd`) および関連付けられたプロセスのデバッグ情報が含まれます。

ログの場所	Windows の場合: <code>install_path¥Volmgr¥debug¥daemon</code> UNIX の場合: <code>/usr/opensv/volmgr/debug/daemon</code>
ログが存在するサーバー	マスターおよびメディア
アクセス方法	daemon プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「 レガシーログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

ltid のログ

論理テープインターフェースデーモン (ltid) は **NetBackup Device Manager** と呼ばれ、テープの予約と割り当てを制御します。

ログの場所	Windows の場合: <code>install_path¥volmgr¥debug¥ltid</code> UNIX の場合: <code>/usr/opensv/volmgr/debug/ltid</code>
ログが存在するサーバー	メディア
アクセス方法	ltid プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「 レガシーログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

nbemm のログ

マスターサーバーとして定義されたサーバーで、**NetBackup Enterprise Media Manager** (nbemm) はデバイス、メディア、およびストレージユニット構成を管理します。利用可能なリソースのキャッシュのリストを nbrb に提供し、ハートビート情報およびディスクポーリングに基づいてストレージの内部状態 (起動/停止) を管理します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥nbemm</code> UNIX の場合: <code>/usr/opensv/logs/nbemm</code>
ログが存在するサーバー	master
アクセス方法	nbemm プロセスは統合ログ方式を使用します。統合ログファイルを表示および管理するには、 <code>vxlogview</code> および <code>vxlogmgr</code> コマンドを使用します。 p.13 の「 統合ログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

nbjm のログ

NetBackup Job Manager (nbjm) は nbpem およびメディアコマンドからの要求を受け入れ、ジョブに必要なリソースを取得します。それは、アクティビティモニター状態に更新ファイルを提供するために bpjobjd と通信し、必要に応じて bpbmr の Media Manager サービスを開始し、内部ジョブの状態を更新します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥nbjm</code> UNIX の場合: <code>/usr/opensv/logs/nbjm</code>
ログが存在するサーバー	master
アクセス方法	nbjm 処理は統合ログ方式を使用します。統合ログファイルを表示および管理するには、 <code>vxlogview</code> および <code>vxlogmgr</code> コマンドを使用します。 p.13 の「 統合ログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

nbpem のログ

NetBackup Policy Execution Manager (nbpem) はポリシーおよびクライアントタスクを作成し、ジョブをいつ実行するかを判断します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥nbpem</code> UNIX の場合: <code>/usr/opensv/logs/nbpem</code>
ログが存在するサーバー	master
アクセス方法	nbpem プロセスは統合ログ方式を使用します。統合ログファイルを表示および管理するには、 <code>vxlogview</code> および <code>vxlogmgr</code> コマンドを使用します。 p.13 の「 統合ログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

nbproxy のログ

プロキシサービス nbproxy は nbpem および nbjm を有効にしてマスターサーバーカタログに問い合わせを行います。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥nbproxy</code> UNIX の場合: <code>/usr/opensv/netbackup/logs/nbproxy</code>
ログが存在するサーバー	master
アクセス方法	nbproxy プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「 レガシーログについて 」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

nbrb のログ

マスターサーバーで、NetBackup Resource Broker (nbrb) は、ジョブのストレージユニット、メディア、およびクライアントの予約を満たすように、キャッシュしたリソースリストから論理リソースと物理リソースを見つけます。10 分ごとに、ドライブの状態を調べるためにドライブのクエリーを開始します。

ログの場所	Windows の場合: <code>install_path¥NetBackup¥logs¥nbrb</code> UNIX: <code>/usr/opensv/logs/nbrb</code>
ログが存在するサーバー	master

アクセス方法	nbrb プロセスは統合ログ方式を使用します。統合ログファイルを表示および管理するには、vxlogview および vxlogmgr コマンドを使用します。 p.13 の「 統合ログについて 」を参照してください。
p.67 の「 バックアップログについて 」を参照してください。	
p.94 の「 リストアログについて 」を参照してください。	

NetBackup Web サービスのログ記録

本項では、NetBackup Web サービスのログについて説明します。

ログの場所	Web サーバーのログ Windows の場合: <code>install_path¥NetBackup¥wmc¥webserver¥logs</code> UNIX の場合: <code>usr/opencv/wmc/webserver/logs</code> Web アプリケーションのログ Windows の場合: <code>install_path¥NetBackup¥logs¥nbwebsevice</code> UNIX の場合: <code>usr/opencv/logs/nbwebsevice</code>
ログが存在するサーバー	master
アクセス方法	Web サービスは Web アプリケーションの統合ログ方式を使いま す。統合ログファイルを表示および管理するには、vxlogview および vxlogmgr コマンドを使用します。 NetBackup Web サーバーフレームワークは、標準の VxUL 形 式使いません。これらのログの形式について、およびログがど のように作成されるかについて詳しくは、http://tomcat.apache.org にある Apache Tomcat のマニュアルを参照してください。 p.13 の「統合ログについて」を参照してください。

Web サービスログにアクセスする方法について詳しくは、『[NetBackup トラブルシューティングガイド](#)』を参照してください。

NetBackup Web サーバー証明書のログ記録

NetBackup はインストール時に Web サーバー証明書を生成して配備するときに、次の
ログを作成します。

ログの場所

Windows の場合:

```
install_path¥NetBackup¥logs¥nbatd
install_path¥NetBackup¥logs¥nbcert
```

```
C:¥ProgramData¥Veritas¥NetBackup¥InstallLogs¥
WMC_configureCerts_YYYYMMDD_timestamp.txt
```

UNIX の場合:

```
/usr/opensv/logs/nbatd
/usr/opensv/netbackup/logs/nbcert
/usr/opensv/wmc/webserver/logs/configureCerts.log
```

ログが存在するサーバー

master

アクセス方法

nbatd ログは、統合ログを使用します。統合ログファイルを表示および管理するには、vxlogview および vxlogmgr コマンドを使用します。configureCerts.log は VxUL ではなく簡易的なログのスタイルを使います。

nbcert ログは、レガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.13 の「[統合ログについて](#)」を参照してください。

NetBackup は Web サーバー証明書を更新するときに、次のログを作成します。

ログの場所

Windows の場合:

```
install_path¥NetBackup¥logs¥nbatd
install_path¥NetBackup¥logs¥nbwebsevice
```

```
C:¥ProgramData¥Veritas¥NetBackup¥InstallLogs¥
WMC_configureCerts_YYYYMMDD_timestamp.txt
```

UNIX の場合:

```
/usr/opensv/logs/nbatd
/usr/opensv/logs/nbwebsevice
/usr/opensv/wmc/webserver/logs/configureCerts.log
```

ログが存在するサーバー

master

アクセス方法	nbwebservice (OID 466 と 484) と nbatd (OID 18) のログは統合ログを使います。統合ログファイルを表示および管理するには、vxlogview および vxlogmgr コマンドを使用します。configureCerts.log は VxUL ではなく簡易的なログのスタイルを使います。 p.13 の「 統合ログについて 」を参照してください。
--------	--

Web サービスログにアクセスする方法について詳しくは、『[NetBackup トラブルシューティングガイド](#)』を参照してください。

PBX のログ

構内交換機 (PBX) はほとんどの NetBackup プロセスで使用される通信機構です。

ログの場所	Windows の場合: <code>install_path\%VxPBX%\log</code> UNIX の場合: <code>/opt/VRTSpxb/log</code>
ログが存在するサーバー	マスター、メディアおよびクライアント
アクセス方法	PBX プロセスは統合ログ方式を使用します。統合ログファイルを表示および管理するには、vxlogview および vxlogmgr コマンドを使用します。PBX 統合ログファイルにアクセスするためのプロダクト ID は NetBackup プロダクト ID とは異なります。PBX プロダクト ID は 50936 です。 p.13 の「 統合ログについて 」を参照してください。

PBX ログへのアクセス方法について詳しくは、『[NetBackup トラブルシューティングガイド](#)』を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

reqlib のログ

reqlib ログには EMM または Volume Manager サービス (vmd) にメディア管理サービスを要求するプロセスのデバッグ情報が含まれます。

ログの場所	Windows の場合: <code>install_path\%Volmgr%\debug\reqlib</code> UNIX の場合: <code>/usr/openv/volmgr/debug/reqlib</code>
ログが存在するサーバー	マスターおよびメディア

アクセス方法 reqlib プロセスはレガシーのログ方式を使用します。レガシーデバッグログが **NetBackup** サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

robots のログ

robots ログには `txxd` および `txxcd` デーモンなど、すべてのロボットデーモンのデバッグ情報が含まれます。

ログの場所 **Windows** の場合: `install_path¥Volmgr¥debug¥robots`
UNIX の場合: `/usr/opensv/volmgr/debug/robots`

ログが存在するサーバー メディア

アクセス方法 robots プロセスはレガシーのログ方式を使用します。レガシーデバッグログが **NetBackup** サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.175 の「[txxd および txxcd のログ](#)」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

tar ログ

テープアーカイブプログラム (`tar`) はリストアデータをクライアントディスクに書き込みます。**Windows** クライアントでは、バイナリ名は `tar32.exe` で、**UNIX** クライアントでは、バイナリ名は `nbtar` です。

ログの場所 **Windows** の場合: `install_path¥NetBackup¥logs¥tar`
UNIX の場合: `/usr/opensv/netbackup/logs/tar`

ログが存在するサーバー クライアント

アクセス方法

tar プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。

p.37 の「[レガシーログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

txxd および txxcd のログ

ロボットデーモン (txxd、xx は使用するロボットの種類によって異なります) は、ltid とテープライブラリ間のインターフェースを提供します。ロボット制御デーモン (txxcd) は、ロボットを制御し、マウント要求およびマウント解除要求を伝達します。

ログの場所

txxd および txxcd プロセスのログファイルはありません。その代わり、robots デバッグログおよびシステムログがあります。システムログは UNIX では syslog、Windows ではイベントビューアによって管理されます。

p.10 の「[UNIX システムログについて](#)」を参照してください。

p.55 の「[Windows のイベントビューアのログオプション](#)」を参照してください。

アクセス方法

vm.conf ファイルに VERBOSE という語を追加すると、デバッグ情報が記録されます。

p.47 の「[レガシーログファイルに書き込まれる情報量を制御する方法](#)」を参照してください。

UNIX では、-v オプションを指定してデーモンを (単独または ltid を通して) 開始してもデバッグ情報が記録されます。

p.174 の「[robots のログ](#)」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

vnetd のログ

NetBackup レガシーネットワークサービス (vnetd) は、ファイアウォールフレンドリなソケット接続の作成に使用する通信機構です。

ログの場所	Windows の場合: <pre>install_path¥NetBackup¥logs¥vnetd</pre> UNIX の場合: /usr/opensv/logs/vnetd または /usr/opensv/netbackup/logs/vnetd (vnetd ディレクトリがここに存在する場合)。両方の場所に vnetd ディレクトリが存在している場合、/usr/opensv/netbackup/logs/vnetd だけにログが記録されます。
ログが存在するサーバー	マスター、メディアおよびクライアント
アクセス方法	vnetd プロセスはレガシーのログ方式を使用します。レガシーデバッグログが NetBackup サーバーで有効でない場合は、プロセスごとに適切なディレクトリを作成する必要があります。 p.37 の「レガシーログについて」を参照してください。

p.67 の「[バックアップログについて](#)」を参照してください。

p.94 の「[リストアログについて](#)」を参照してください。

Java ベースの管理コンソールのログ記録

この章では以下の項目について説明しています。

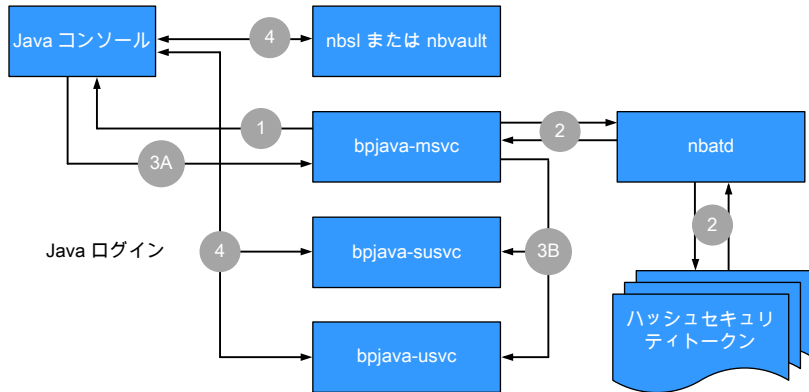
- [Java ベースの管理コンソールのログ記録について](#)
- [Java ベースの管理コンソールのログ記録プロセスフロー](#)
- [Java ベースの管理コンソールと bpjava-* 間におけるセキュアなチャネルの設定](#)
- [Java ベースの管理コンソールと nbsl または nbvault 間におけるセキュアなチャネルの設定](#)
- [NetBackup サーバーとクライアントでの Java ベースの管理コンソールのログ記録に関する設定](#)
- [NetBackup がインストールされていない Windows コンピュータでの Java ベースのリモート管理コンソールのログ記録](#)
- [Java GUI の問題をトラブルシューティングするときのログの設定と収集](#)
- [ログ記録を元に戻す操作](#)

Java ベースの管理コンソールのログ記録について

NetBackup 7.7 以降の NetBackup では、Java ベースの管理コンソールのみが提供されます。管理者はこのコンソールを使って NetBackup を管理できます。このコンソールは、サポートされる Java 対応 UNIX コンピュータまたは NetBackup 管理コンソールがインストールされた Windows コンピュータで直接的に実行できます。

Java ベースの管理コンソールのログ記録プロセスフロー

Java ベースの管理コンソールのログ記録プロセスフローを次に示します。



次の手順では、Java ベースの管理コンソールのログ記録プロセスについて説明します。

1. ユーザーが Java ベースの管理コンソールへのログイン要求を開始します。資格情報は、サーバーセキュリティ証明書を使って SSL (Secure Sockets Layer) を介して bpjava-msvc に送信されます。
2. bpjava-msvc プロセスは nbatd を介してトークンを認証し、サーバー上のハッシュされたセキュリティトークンを読み取ります。
3. 次の手順では、セッションの証明書を使ったプロセスについて説明します。
 - bpjava-msvc プロセスは、セッショントークンとセッションの証明書の指紋を使ってコンソールログインに対する応答を送信します。
 - bpjava-msvc プロセスが適切な bpjava-*usvc プロセスを開始し、セッションの証明書とトークンが次のいずれかのプロセスに渡されます。
 - NetBackup 管理コンソールの bpjava-susvc
 - [バックアップ、アーカイブおよびリストア (BAR) (Backup, Archive, and Restore (BAR))] インターフェースの bpjava-usvc
4. NetBackup の Java ベースの管理コンソールと、nbsl、bpjava-*usvc、nbvault (設定されている場合) の間ではさまざまな呼び出しが行われ、適切な内容がインターフェースに自動入力されます。

Java ベースの管理コンソールと bpjava-* 間におけるセキュアなチャネルの設定

次の手順では、Java ベースの管理コンソールと bpjava-* 間にセキュアなチャネルを設定するためのプロセスフローについて説明します。

メモ: ログインと認証を制御する bpjava-msvc、管理コンソールプロセスである bpjava-susvc、クライアントの[バックアップ、アーカイブおよびリストア (BAR) (Backup, Archive, and Restore (BAR))] インターフェースである bpjava-usvc、のプロセスが使われます。

1. ユーザーはコンソールへのログインを開始します。(サーバーセキュリティ証明書を使って) SSL を介して資格情報が bpjava-msvc に送信されます。
2. bpjava-msvc プロセスは、手順 1 で受信したユーザー資格情報を使っているユーザーを認証します。
3. ユーザーを認証すると、bpjava-msvc プロセスは次を実行します。
 - 自己署名セッション証明書、キー、セッショントークンと呼ばれるエンティティを生成します。
 - デーモン bpjava-*usvc を起動して、NetBackup Java ベースの管理コンソールから追加の要求を収集します。
 - 自己署名セッション証明書とセッショントークンを bpjava-*usvc に渡します。

メモ: bpjava-*usvc プロセスは、セッショントークンを SSL チャネルのサーバーセキュリティ証明書として使います。Java ベースの管理コンソールを認証するためにセッショントークンを使います。このコンソールは、bpjava-*usvc プロセスへの接続時に資格情報を使いません。Java ベースの管理コンソールは認証を行うためにセッショントークンを使います。

- セッショントークンとセッション証明書の指紋を Java ベースの管理コンソールに送信します。
- NetBackup ホストのファイル内にあるセキュアなディレクトリ (`install_path/var`。たとえば `usr/openssl/var`) にセッショントークンとユーザー情報を保持します。このディレクトリは、ルートまたは管理者のみがアクセスできます。ファイル名の形式は次のとおりです。

```
hash(session token)_bpjava-*usvc_pid
```

メモ: `msvc` は、この情報を保存し、`nbsl` または `nbvault` が Java ベースの管理コンソールを認証するときに使うことができるようにします。

- `msvc` プロセスは実行を停止して、終了します。
- 4. `bpjava-*usvc` は、セッション証明書を使って、Java ベースの管理コンソールとのセキュアなチャネルを開始します。このセキュアなチャネルは一方方向の認証済み SSL チャネルです。(サーバー証明書のみが存在します。ピア証明書は存在しません。Java ベースの管理コンソール側からの証明書は存在しません。)
- 5. Java ベースの管理コンソールはセッション証明書を初回の SSL ハンドシェイクの一部として受信します。このコンソールは、セッション証明書の既存の指紋を使ってセッション証明書の真正性を検証します (手順 3 を参照)。Java ベースの管理コンソールは、SSL ハンドシェイクで `bpjava-*usvc` から受信したセッション証明書の指紋を計算します。`msvc` によって送信された指紋と、新しい指紋を比較します。
- 6. 証明書の真正性を確認すると、Java ベースの管理コンソールは手順 3 で受信したセッション証明書を `bpjava-*usvc` に送信します。
- 7. `bpjava-*usvc` は、受信したセッショントークンを既存のトークンを使って検証します (手順 3 を参照)。
- 8. セッショントークンの検証が成功すると、`bpjava-*usvc` と Java ベースの管理コンソール間に信頼が確立されます。
- 9. `bpjava-*usvc` と Java ベースの管理コンソール間でのそれ以降のすべての通信はこの信頼済みのセキュアなチャネル上で発生します。

Java ベースの管理コンソールと nbsl または nbvault 間におけるセキュアなチャネルの設定

次の手順では、Java ベースの管理コンソールと `nbsl` または `nbvault` 間にセキュアなチャネルを設定するためのプロセスフローについて説明します。

1. Java ベースの管理コンソールと `bpjava-*` 間には信頼がすでに確立されています。ユーザー情報とセッショントークンは、次のような名前です定の場所にすでに存在します。

```
hash(session token)_susvc_pid
```

p.179 の「[Java ベースの管理コンソールと `bpjava-\*` 間におけるセキュアなチャネルの設定](#)」を参照してください。

2. Java ベースの管理コンソールは、セキュアな接続の要求を `nbsl/nbvault` に送信します。

3. `nbsl/nbvault` は、その要求を受け入れ、ホスト上のセキュリティ証明書を使ってセキュアなチャネルを開始します。これらのデーモンは、ルートまたは管理者の権限で実行され、セキュリティ証明書にアクセスできます。
4. このセキュアなチャネルは一方の認証済みの **SSL** チャネルです。すなわち、サーバー証明書のみが存在し、ピア証明書は存在しません。**Java** ベースの管理コンソール側からの証明書は存在しません。
5. セキュリティ証明書の信頼オプションは次のとおりです。
 - **Java** ベースの管理コンソールは、セキュリティ証明書に署名した **NetBackup 認証局 (CA)** を信頼する場合、セキュリティ証明書を受け入れます。
 - **Java** ベースの管理コンソールがセキュリティ証明書に署名した **CA** を信頼しない場合、ポップアップダイアログボックスが表示されます。このダイアログボックスでは、ユーザーが証明書に署名した **CA** を信頼するかどうか問われます (これは一度限りのアクティビティです。ユーザーが **CA** を信頼することに同意した後、このダイアログボックスが再び表示されることはありません。)
6. **Java** ベースの管理コンソールはセッショントークンを `nbsl/nbvault` に送信します。p.179 の「[Java ベースの管理コンソールと bpjava-* 間におけるセキュアなチャネルの設定](#)」を参照してください。
7. `nbsl/nbvault` は次の手順を実行してこのセッショントークンを検証します。
 - 受信したセッショントークンのハッシュの生成
 - 所定の場所にあるこのハッシュで始まる名前のファイルの検索
 - ファイルが検出されると、そこから **PID** が抽出されます (手順 1 を参照)。
 - **PID** が有効であるかどうかの確認
8. 検証が成功すると、`nbsl/nbvault` と **Java** ベースの管理コンソールの間に信頼が確立されます。
9. `nbsl/nbvault` と **Java** ベースの管理コンソール間でのそれ以降のすべての通信はこの信頼済みのセキュアなチャネル上で発生します。

NetBackup サーバーとクライアントでの Java ベースの管理コンソールのログ記録に関する設定

NetBackup クライアントまたはサーバーソフトウェアがインストールされているシステムで **Java** のログ記録が自動的に設定されます。**Java** のログは次の既存のログディレクトリに配置されます。

- **UNIX** の場合: `/usr/opensv/netbackup/logs/user_ops/nbjlogs`
- **Windows** の場合: `install directory¥netbackup¥logs¥user_ops¥nbjlogs`

NetBackup がインストールされていない Windows コンピュータでの Java ベースのリモート管理コンソールのログ記録

インストール時に[NetBackup のリモート管理コンソールのインストール (NetBackup Remote Administration Console Installation)] (x64 のみ) オプションを使うと、ホストに NetBackup がインストールされず、デフォルトでは Java アクティビティがログに記録されません。

Veritas テクニカルサポートが正常に Java 操作をログに記録できるようにするために、たとえば %nbjLogFileName% となるように、setconf.bat を変更する必要があります。

ターゲットホストの NB_INSTALL_PATH に対してアクティブなパスが設定されていないため、次の変更を setconf.bat ファイルに対して行う必要があります。手順を次に示します。

1. 次のディレクトリ構造をすべて手動で作成します。

```
C:¥Program Files¥Veritas¥NetBackup¥logs¥user_ops¥nbjlogs
```

2. 次のファイルを編集します。

```
install_path¥Veritas¥Java¥setconf.bat
```

3. 以下の例に示すように、次の行 (ファイルの先頭から 12 行目) を探し、コメント (REM) を削除をしてアクティブ化します。

- 変更前: REM SET NB_INSTALL_PATH=C:¥¥Program Files¥¥Veritas¥¥NetBackup

- 変更後: SET NB_INSTALL_PATH=C:¥¥Program Files¥¥Veritas¥¥NetBackup

4. setconf.bat ファイルに変更を保存します。
5. Java コンソールの次回起動時に、次のディレクトリ内にデフォルトの詳細度 3 のログが生成されます。

```
C:¥Program Files¥Veritas¥NetBackup¥logs¥user_ops¥nbjlogs
```

Java GUI の問題をトラブルシューティングするときのログの設定と収集

インストールすると、ログの詳細なセットを収集するように Java ベースの管理コンソールのログレベルが設定されます。

NetBackup Java GUI は、使用するログ記録レベルを決定するために `Debug.properties` ファイルを使います。

UNIX システムの場合、ファイルは `/usr/opensv/java/Debug.properties` です。

Windows システムの場合、ファイルは

`install_dir\VERITAS\Java\Debug.properties` です。

具体的には、追加のログ記録を有効にするために、次の設定を調整します (これらはデフォルト値です)。

```
printcmds=true
debugMask=0x00040000
```

詳細度を最大値 (トラブルシューティングの推奨値) に上げるには、`debugMask` を `debugMask=0x00160000` に設定します。

1. GUI を開始したシステム上の次の既存のログディレクトリから次の **Java** コンソールログを収集します。

- UNIX の場合: `/usr/opensv/netbackup/logs/user_ops/nbjlogs`
- Windows の場合: `install_directory\netbackup\logs\user\ops\bjlogs`

2. マスターサーバーで **Java** ベースの管理コンソールを介してログインし、`admin`、`bpjava-msvc`、`bpjava-susvc`、`bpjava-usvc` ログディレクトリを作成して、**VERBOSE 5** ログ記録を有効にします。ログ記録レベルの変更を有効にするために **NetBackup** デーモンを再起動する必要はありません。

UNIX システムの場合は、次のディレクトリを作成します。

- `/usr/opensv/netbackup/logs/admin`
- `/usr/opensv/netbackup/logs/bpjava-msvc`
- `/usr/opensv/netbackup/logs/bpjava-susvc`
- `/usr/opensv/netbackup/logs/bpjava-usvc`

3. 次の行を追加して `/usr/opensv/netbackup/bp.conf` ファイルを編集します。

```
ADMIN_VERBOSE = 5
BPJAVA-MSVC_VERBOSE = 5
BPJAVA-SUSVC_VERBOSE = 5
BPJAVA-USVC_VERBOSE = 5
```

4. Windows システムの場合は、次のディレクトリを作成します。

- `install_dir\VERITAS\NetBackup\logs\admin`
- `install_dir\VERITAS\NetBackup\logs\bpjava-msvc`

- `install_dir¥VERITAS¥NetBackup¥logs¥bpjava-susvc`

- `install_dir¥VERITAS¥NetBackup¥logs¥bpjava-usvc`

5. `hkey_local_machine > software > veritas > netbackup > current version > config` にある Windows レジストリを更新して、形式 `DWORD` の次のエントリを追加します。

```
ADMIN_VERBOSE = 5
BPJAVA-MSVC_VERBOSE = 5
BPJAVA-SUSVC_VERBOSE = 5
BPJAVA-USVC_VERBOSE = 5
```

6. 次のコマンドを実行して、詳細な `nbatd` (OID 18) と `nbsl` (OID 132) のログ記録を設定します。OID 137 (NetBackup ライブラリ) と OID 156 (CORBA/ACE) は、ライブラリまたは CORBA/ACE のいずれかへのアクセスを必要とする呼び出し元に書き込みます。

```
vxlogcfg -a -p NB -o 18 -s DebugLevel=6
vxlogcfg -a -p NB -o 132 -s DebugLevel=6
vxlogcfg -a -p NB -o 137 -s DebugLevel=6
vxlogcfg -a -p NB -o 156 -s DebugLevel=6
```

7. 次のディレクトリパスにある `nbatd` と `nbsl` のログを収集します。

UNIX の場合:

- `/usr/opensv/logs/nbsl`
- `/usr/opensv/logs/nbatd`

Windows の場合:

- `install_dir¥VERITAS¥NetBackup¥logs¥nbsl`
- `install_dir¥VERITAS¥NetBackup¥logs¥nbatd`

8. 最後に、次の方法で PBX ログを収集します。

- UNIX の場合: `/opt/VRTSspbx/log` (現在の日時を含むすべてのログを収集)
- Windows の場合: `install_dir¥VERITAS¥pbx¥log`

ログ記録を元に戻す操作

ログ記録の取り消しは、必ず問題のトラブルシューティングに関連するログを収集した後に行います。

ログ構成の設定を削除するには、次のコマンドを使います。


```
vxlogcfg -r -p NB -o 18 -s DebugLevel=6
vxlogcfg -r -p NB -o 132 -s DebugLevel=6
vxlogcfg -r -p NB -o 137 -s DebugLevel=6
vxlogcfg -r -p NB -o 156 -s DebugLevel=6
```

マスターサーバーで、bp.conf ファイル (UNIX) またはレジストリ (Windows) で次の Java VERBOSE エントリをコメントアウトします。

- ADMIN_VERBOSE
- BPJAVA-MSVC_VERBOSE
- BPJAVA-SUSVC_VERBOSE
- BPJAVA-USVC_VERBOSE

記号

- アプリケーションイベントログ 55
- アプリケーションサーバーの状態コード (Java ベースのインターフェース) 58
- イベントビューアのログオプション 55
- エラーメッセージの種類 58
- オペレーティングシステムのエラー 59
- オリジネータ ID
 - リスト 18
- カタログバックアップ 102
- クライアント
 - NetBackup
 - デバッグログ。「UNIX クライアント」を参照。
「Windows クライアントおよび NetWare クライアント」を参照
- クライアント重複排除
 - ログ 120
- グローバルログレベル 50
- グローバルログレベル (Global logging level) 48、52
- コマンドライン
 - ログ記録 143
- サーバー
 - NetBackup のデバッグログ 38
- サーバーセキュリティ証明書 178
- システムログ 10
- ストレージライフサイクルポリシー (SLP) 131
 - ログ記録 137
 - 構成と管理 138
 - 複製のプロセスフロー 132
- スナップショット
 - バックアップ処理の概要 159
- スナップショットバックアップ 157
- セキュアなチャネルの設定
 - Java コンソールと bpjava-* の間 179
 - Java コンソールと nbsl または nbvault の間 180
- セッションの証明書 178
- テープ
 - リストア元 89
- テープからのリストア手順 89
- ディスク
 - リストア元 90

- ログ記録の監視 123
- ディスクからのリストア手順 90
- ディスク容量
 - ログおよび一時ファイル 59
- ディスク領域
 - ログファイル 34
- ディレクトリ構造
 - メディアおよびデバイスの管理 78
- デバッグレベル 53
- デバッグログ 60
 - NetBackup 79
 - vmd 46、79
- デバッグログの有効化 46
- データベースバックアップ (「カタログバックアップ」を参照) 102
- デーモン
 - ロボット 71
 - ロボット制御 71
- ネットワークデーモン (vnetd) 46
- バックアップ
 - NetBackup カタログ 102
 - UNIX クライアント 66
 - スナップショットの概要 157
 - プロセス
 - 重複排除 117
 - リストアの起動プロセス 65
 - ログ記録 62、67
 - 処理 62
 - 多重化 67
 - 合成処理 106
 - 手順、基本 63
- バックアップ、アーカイブおよびリストア (BAR) インターフェース 178
- バックアップの基本手順 63
- バックアップログの送信 68
- バックアップ処理
 - とアーカイブ処理 65
- バーコード操作 76
- ファイバーチャネル 97
- プロセスの説明
 - NetBackup 64

ベリタステクニカルサポート

バックアップログの送信 68

リストアログ 95

ホットカATALOGのリストア 104

ホットカATALOGバックアップ処理 103

メッセージ、エラー 58

メディアおよびデバイスの管理 71

プロセス 73

メディアおよびデバイスの管理コンポーネント 78

メディアサーバー重複排除プール (MSDP) 117

ユーザー主導バックアップ 67

リストアログ 94

ベリタステクニカルサポートへ送信 95

リストア処理 87

Windows クライアント 93

レガシーログ 38

PC クライアント 41

クライアントログ 39

サイズの管理 48

ディレクトリ 39

ローテーションの構成 49

場所 38

レポート

NetBackup 10

ログ

acsssi 162

bpbackup 162

bpbkar 163

bpbrm 163

bpcd 164

bpcompatd 164

bpdbrm 165

bpjobd 165

bprd 166

bprestore 166

bptestnetconn 166

bptm 167

daemon 167

debug

詳細の有効化 60

ltid 168

nbemm 168

nbjm 169

nbpem 169

nbproxy 170

nbrb 170

nbtd 174

PBX 173

PC クライアントのデバッグ

bparchive 42

bpbackup 42

bpbkar 42

bpcd 42

bpnetd 41

bplist 42

bpmount 42

bprestore 42

bptestnetconn 43

tar 43

user_ops 43

PC クライアントのレベルの設定 53

reqlib 173

robots 174

tar 174

UNIX クライアントのデバッグ

backup_tape 40

bp 39

bparchive 39

bpbackup 39

bpbkar 39

bpcd 39

bphdb 40

bpjava-msvc 45

bplist 40

bpmount 40

bprestore 40

nbtd 41

user_ops 41

vnetd 175

Windows のイベントビューアのログオプション 55

クライアント重複排除 120

サーバーのデバッグ

acsssi 46

admin 45

bpbrm 45

bpcd 45

bpdbrm 45

bpdbrm 45

bpdbrm 45

bpjava-susvc 45

bprd 45

bpsynth 45

bptm 45~46

ltid 47

nbtd 19、45

nbazd 45

nbjm 19

- nbpem 19
- reqlib 47
- robots 47
- syslogs 45
- tpcommand 47
- デーモン 46
- システム 10
- バックアップ 67
- ファイルの保持 26
- リストア 94
- レガシー 38
- レベル 50
- レポート
 - NetBackup 10
- ログサイズ保持の設定 13
- 保持期間の設定 48
- 合成バックアップ 110
- 場所の変更 24
- 概要 9
- 構成
 - 重複排除 120
- ログおよび一時ファイルのための追加のディスク容量 59
- ログのレベル 50
- ログの保持オプション 11
- ログの保持制限
 - 設定 54
- ログの保持制限の設定 54
- ログの場所の移動 24
- ログの設定と収集
 - Java GUI の問題をトラブルシューティングするときの 182
- ログレベル
 - UNIX クライアント 52
 - Windows クライアント 53
- ログ記録
 - cURL 143
 - EAT 144
 - Java 144
 - NetBackup プロキシトンネル 146
 - NetBackup プロキシヘルパー 145
 - PBX (Private Branch Exchange) 147
 - Tomcat 140
 - txxd および txxcd 175
 - vssat 144
 - Web サービス 141
 - コマンドライン 143
 - ディスク監視 123
 - 安全な通信 140
 - 認証サービス (AT) 144
- ロボット
 - デーモン 72
 - 制御デーモン 72
- ロボットドライブの選択 73
- ローテーション
 - ログ 25
 - 統合ログ 18
- 保持
 - ログ 26
- 合成バックアップ 106
 - ログ 110
- 問い合わせ文字列 28
- 埋め込み認証クライアント (EAT)
 - ログ記録 144
- 変更
 - ログレベル 52
- 多重化されたバックアップ 67
- 安全な通信
 - ログ記録 140
- 構成
 - MSDP の重複排除 118
 - OpenStorage Technology (OST) 125
- 構成と管理
 - OpenStorage Technology (OST) 128
- 構成ログ
 - 重複排除 120
- 機能概要
 - NetBackup
 - 起動 65
 - メディアおよびデバイスの管理
 - ディレクトリおよびファイル 78
 - メディアとデバイスの管理
 - デバイス管理 73
 - ボリューム管理 73
- 状態収集デーモン 39
- 管理インターフェース
 - エラー 58
 - デバッグログ 60
- 統合ログ 13
 - NetBackup プロダクト ID 17
 - PC クライアントのレベルの設定 53
 - tar ログファイル 16
 - クライアントログ 39
 - サイズの管理 35
 - テクニカルサポートへの送付 15
 - ディスク領域の使用状況の管理 34
 - ファイルのローテーション 25
 - ファイルの形式 28
 - ファイル名の形式 17

- メッセージの種類 16
- レベルの設定 50
- ログの削除 33
- ログファイル数の管理 34
- 使用するプロセス 18
- 保持 26
- 場所 14
- 場所の変更 24
- 設定の構成 35
- 設定の表示 37
- 統合ログとレガシーログのサイズの制限 13
- 統合ログのジョブ ID 検索 32
- 自動イメージレプリケーション (A.I.R.) 131
 - インポートプロセスフロー 136
 - プロセスフローのログ記録 134
 - ログ記録 137
- 試行ファイル 110
- 詳細フラグ 48
- 認証サービス (AT)
 - ログ記録 144
- 起動
 - NetBackup 65
- 重複排除
 - 構成ログ 120
- 開始プロセス 71
 - メディアおよびデバイスの管理 71
- [ログの保持 (Keep logs for)] 設定 26

A

- acsd、説明 80
- acssel、説明 80
- acsssi のログ 162
- acsssi、説明 81
- admin ログ 45
- AT
 - ログ記録 144
- avrd、説明 81

B

- backup_tape ログ 40
- bin
 - メディアおよびデバイスの管理 79
- bjava-usvc プロセス 178
- bp
 - UNIX クライアントログ 39
- bp.conf
 - ファイル 67

- bparchive
 - ログ 39、42
- bpbackup
 - ログ 39、42
- bpbackup のログ 162
- BPBACKUP_POLICY 67
- BPBACKUP_SCHED 67
- bpbkar
 - ログ 39、42、163
- bpbrm 159
 - ログ 45、163
- bpcd
 - UNIX クライアントログ 39、42
 - サーバーログ 45
- bpcd のログ 164
- bpcompatd のログ 164
- bpdbjobs ログ 45
- bpdbm
 - ログ 45、165
- bpdm ログ 45
- bpfis 159
- bphdb
 - log 40
- BPINETD 93
- bpinetd ログ 41
- bpinetd.log 41
- bpjava-*usvc プロセス 178
- bpjava-msvc プロセス 178
- bpjava-msvc ログ 45、61
- bpjava-susvc プロセス 178
- bpjava-usvc ログ 61
- bpjobd のログ 165
- bplist
 - ログ 40、42
- bpmount
 - ログ 40、42
- bporaexp ログ 40
- bporaexp64 ログ 40
- bporaimp ログ 40
- bporaimp64 ログ 40
- bprd のログ 166
- bprd ログ 45
- bprestore
 - ログ 40、42、166
- bpsetconfig 50
- bpsynth 106
- bpctestnetconn
 - ログ 40、43、166
- bptm のログ 167

bptm ログ 45

C

cURL

ログ記録 143

D

daemon のログ 167

Debug.properties ファイル 61

drive_mount_notify スクリプト 73

drive_unmount_notify スクリプト 73

driver ディレクトリ 79

E

EAT

ログ記録 144

EMM サーバー 66

Enterprise Media Manager (EMM) 66

eventlog 56

ファイルのエントリ 56

F

FSM 97

FT Service Manager 97

G

goodies ディレクトリ 79

H

help ファイル

メディアおよびデバイスの管理 79

hostID

統合ログ 18

J

Java

ログ記録 144

Java GUI の問題のトラブルシューティング 182

Java インターフェース

トラブルシューティングの背景 58

Java ベースのリモート管理コンソールのログ記録

NetBackup がインストールされていない Windows
コンピュータでの 182

Java ベースの管理コンソールのログ記録

NetBackup サーバーとクライアントでの設定 181
プロセスフロー 178

Java ベースの管理コンソールの例外エラー 58

Java ベースの管理コンソールのログ記録 177

L

ltid 48

ltid のログ 168

ltid、説明 81

M

MAX_LOGFILE_SIZE 50

MAX_NUM_LOGFILES 50

MaxLogFileSizeKB 34～35、37

misc ファイル 79

mklogdir.bat 38

MSDP

重複排除の構成 118

MSDP の重複排除の構成 118

MSDP への重複排除バックアッププロセス 117

N

nbatd のログ 45

nbazd のログ 45

nbemm 66

nbemm のログ 168

nbftclnt 97、99、101

nbftsrvr 97、99、101

nbjm 19、66、106、159

nbjm のログ 169

nbpem 19、65～67、106、159

nbpem のログ 169

nbproxy のログ 170

nbrb 66

nbrb のログ 170

nbsl 178

nbtar ログ 174

nbvault 178

NBWIN 93

NDMP バックアップ手順 113

NDMP バックアップのログ記録 111

NDMP リストア手順 115

NDMP リストアログ記録 114

NetBackup

プロセスの説明 64

プロダクト ID 17

安全な通信のログ記録 140

NetBackup のプロダクト ID 17

NetBackup プロキシトンネル

ログ記録 146

NetBackup プロキシヘルパー

ログ記録 145

NetBackup 状態収集デーモン。「vmscd」を参照

NetBackup 管理コンソール

エラー 58

デバッグログ 60

NumberOfFiles 34

NumberOfLogFiles 37

O

OID

Web サービス 141

OID 486 145

OID 490 146

OpenStorage Technology (OST)

構成 125

構成と管理 128

originatorID

統合ログ 18

P

PBX

ログ 147

PBX (Private Branch Exchange)

ログ記録 147

PBX のログ 173

Private Branch Exchange (PBX) 122

productID

統合ログ 17

R

raw パーティション

リストア処理 91

reqlib のログ 173

robots のログ 174

RolloverMode 37

S

SAN クライアントのバックアッププロセスのフロー 98

SAN クライアントのバックアップ手順 98

SAN クライアントファイバートランスポートのバックアップ 97

SAN クライアントファイバートランスポートのリストア 100

Secure Sockets Layer (SSL) 178

Shared Storage Option の管理プロセス 74

Snapshot Client のバックアップ 151

Snapshot Client のバックアップ手順 152

SSO。「Shared Storage Option」を参照

stderr 58

stdout 58

syslogd 10～11

T

tar

Windows クライアントでのログ 43

ログ 174

ログファイル 16

TAR32 93

tl4d、説明 82

tl8cd、説明 83

tl8d、説明 82

tlcdc、説明 84

tlld、説明 83

tlhcd、説明 85

tlhd、説明 84

tlmd、説明 85

Tomcat

ログ記録 140

tpautoconf 47

tpconfig 47

tshd、概要 86

txxd および txxcd のログ記録 175

U

UNIX の NetBackup 管理コンソールのエラーメッセージ
のトラブルシューティング 58

UNIX クライアント

レガシーログを使うプロセス 39

UNIX システムログ 10

UNIX クライアントのリストア 91

upload ディレクトリ 16

user_ops ログ 41、43、46

V

VERBOSE 48

VERBOSE レベル 52

Veritas V-Ray 156

vm.conf 48

vm.conf の DAYS_TO_KEEP_LOGS 設定 49

vm.conf ファイル 80

vmd 46

デバッグログ 46

概要 86

vmscd 39

ログ 47

vmscd ディレクトリ 39

vmscd、概要 86

VMware バックアップ 153
VMware バックアップ手順 155
vnetd のログ 175
vnetd ログ 46
vSphere 155
vssat
 ログ記録 144
vxlogcfg 25
vxlogcfg コマンド 35、37、52
vxlogmgr コマンド 32、34
vxlogview コマンド 27
 ジョブ ID オプション 32
 問い合わせ文字列の概要 28

W

Web サービス
 オリジネータのログファイル 141
 ログ記録 141
Windows Open File Backup 157、159
Windows イベントビューア 55
Windows クライアント
 のリストア 93

X

XML 40

か

機能概要
 NetBackup
 リストア 91
キーワード
 ログ記録 123

は

ファイル
 リストア処理 91

ま

メディアサーバーの重複排除のログ記録と pdplugin ログ
 記録 122

ら

リストア処理
 UNIX クライアント 91
ログ記録
 Java ベースの管理コンソール 177
 キーワード 123