NetBackup™ ログリファレンスガイド

リリース 11.1

VERITAS
now part of Cohesity

NetBackup™ ログリファレンスガイド

最終更新日: 2026-01-22

法的通知と登録商標

Cohesity、Veritas、Cohesity ロゴ、Veritas ロゴ、Veritas Alta、Cohesity Alta、NetBackup は、Cohesity, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、Cohesity 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア(「サードパーティ製プログラム」)が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このCohesity製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

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

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

本書は、現状のまま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。Cohesity, Inc. およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Cohesityがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じてFAR 52.227-19「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

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

http://www.veritas.com

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サ

ポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Cohesity Account の情報を管理できます。

https://my.veritas.com

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

世界共通 (日本を除く)	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

マニュアル

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

Cohesity Services and Operations Readiness Tools (SORT)

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

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

目次

1

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

NetBackup で使用される様々なログは、発生した問題のトラブルシューティングに役立ちます。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。すべての NetBackup 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。

p.17 の「統合ログについて」を参照してください。

p.40 の「レガシーログについて」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。

[ログ (Logging)]プロパティ

[ログ (Logging)]プロパティにアクセスするには、Web UI で[ホスト (Host)]、[ホストプロパティ (Host properties)]の順に選択します。必要に応じて、[接続 (Connect)]をクリックし、[プライマリサーバーの編集 (Edit primary server)]、[メディアサーバーの編集 (Edit media server)]、または[クライアントの編集 (Edit client)]をクリックします。[ログ (Logging)]をクリックします。

ログの設定によって、プライマリサーバー、メディアサーバー、クライアントでの NetBackup によるログ記録の動作が決まります。

- NetBackup のすべてのプロセスに対する全体的なログレベルまたはグローバルログレベル
- レガシーログを使用する特定のプロセスの上書き
- 統合ログ機能を使用するサービスのログレベル
- 重要なプロセスのログ
- クライアントの場合は、データベースアプリケーションのログレベル
- NetBackup と NetBackup Vault (インストールされている場合) のログ保持の設定

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。特定のプロセスとサービスに対して、グローバルまたは一意のログレベルを設定できます。保持レベルにより、ログファイルのサイズや (プライマリサーバーの場合は) ログの保持日数を制限できます。NetBackup Vault を使用する場合は、そのオプションのログ保持の設定を個別に選択できます。

p.17 の「統合ログについて」を参照してください。

p.40 の「レガシーログについて」を参照してください。

p.14 の「ログの保持とログサイズ」を参照してください。

表 1-1 [ログ (Logging)]プロパティ

プロパティ	説明
グローバルログレベル (Global logging level)	この設定は、[グローバルと同じ (Same as global)]に設定されているすべてのプロセスのグローバルログレベルを確立します。 [グローバルログレベル (Global logging level)]は、サーバーまたはクライアントのすべての NetBackup プロセスのレガシーおよび統合ログレベルに影響します。この設定は、次のログプロセスには影響しません。 ■ 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.48 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。
プロセス固有の上書き (Process-specific overrides)	これらの設定により、レガシーログを使用する特定のプロセスのログレベルを上書きできます。
NetBackup サービスのデバッグログレベル (Debug logging levels for NetBackup services)	これらの設定により、統合ログを使用する特定のサービスのログレベルを管理できます。
重要なプロセスのログ (Logging for critical processes)	このオプションでは、重要なプロセスのログを有効化できます。 ■ プライマリサーバープロセス: bprd および bpdbm。 ■ メディアサーバープロセス: bpbrm、bptm、bpdm。 ■ クライアントプロセス: bpfis 次の点に注意してください。 ■ [重要なプロセスのログ (Logging for critical processes)]を有効にする場合は、[最大ログサイズ (Maximum log size)]オプションも有効にします。このオプションを無効にすると、NetBackup の操作に悪影響を及ぼす可能性があります。 ■ このオプションを指定すると、ログの保持がデフォルトのログサイズに設定されます。 ■ [デフォルトに戻す (Restore to defaults)]をクリックしても、[重要なプロセスのログ (Logging for critical processes)]または[最大ログサイズ (Maximum log size)]オプションは変更されません。 ■ 重要なプロセスのログを無効にするには、これらのプロセスのログレベルを変更します。

プロパティ	説明
保持期間 (Retention period)	NetBackup が、エラーカタログ、ジョブカタログおよびデバッグログの情報を保持する期間 (日数) を指定します。NetBackup はエラーカタログからレポートを生成する点に注意してください。 ログは大量のディスク領域を使用するため、ログを必要以上に保持しないでください。デフォルトは 28 日です。 注意: この設定は、Cloud Scale には適用できません。
最大ログサイズ (Maximum log size)	保持する NetBackup ログのサイズを指定します。NetBackup ログのサイズがこの値まで増加すると、古いログが削除されます。 ■ プライマリサーバーとメディアサーバーの場合、推奨値は 25 GB 以上です。 ■ クライアントの場合、推奨値は 5 GB 以上 注意: この設定は、Cloud Scale には適用できません。
Vault ログの保持期間 (Vault logs retention period)	NetBackup Vault がインストールされている場合、Vault セッションディレクトリを保存する日数を選択するか、[無期限 (Forever)]を選択します。

ログレベル

すべての NetBackup プロセスに同じログレベルを適用することを選択できます。または、特定のプロセスまたはサービスのログレベルを選択できます。

表 1-2　　ログレベルの説明

ログレベル	説明
グローバルと同じ	この処理では、グローバルログレベルと同じログレベルが使用されます。
[ログなし (No logging)]	プロセスに対してログは作成されません。
[最小ログ (Minimum logging)] (デフォルト)	プロセスに対して少量の情報が記録されます。 Cohesity Technical Supportから指示されないかぎり、この設定を使用してください。他の設定では、ログに大量の情報が蓄積される可能性があります。
レベル 1 から 4 まで	プロセスに対してレベルに合わせて情報が記録されます。
[5 (最大) (5 (Maximum))]	プロセスに対して最大量の情報が記録されます。

グローバルログレベル (Global logging level)

この設定は、すべてのプロセスと、[グローバルと同じ (Same as global)]に設定されているプロセスのログレベルを制御します。一部の NetBackup プロセスのログレベルは個別に制御できます。

p.13 の「レガシーログレベルの上書き」を参照してください。

p.13 の「プライマリサーバーの統合ログレベル」を参照してください。

レガシーログレベルの上書き

これらのログ記録レベルは、レガシープロセスのログに適用されます。表示されるログレベルは、ホストの種類 (プライマリ、メディア、クライアント) によって異なります。

表 1-3　　レガシープロセスに対するログレベルの上書き

サービス	説明	プライマリサーバー	メディアサーバー	クライアント
BPBRM のログレベル (BPBRM logging level)	NetBackup Backup Restore Manager。	X	X	
BPDM のログレベル (BPDM logging level)	NetBackup Disk Manager。	X	X	
BPTM のログレベル (BPTM logging level)	NetBackup Tape Manager。	X	X	
BPJOBD のログレベル (BPJOBD logging level)	NetBackup Jobs Database Management デーモン。この設定はプライマリサーバーでのみ利用可能です。	X		
BPDBM のログレベル (BPDBM logging level)	NetBackup Database Manager。	X		
BPRD のログレベル (BPRD logging level)	NetBackup Request デーモン。	X		
データベースログレベル (Database logging level)	データベースエージェントのログのログレベル。作成および参照するログについて詳しくは、特定のエージェントのマニュアルを参照してください。			X

プライマリサーバーの統合ログレベル

これらのログレベルは、NetBackup サービスログに適用され、プライマリサーバーでのみ利用可能です。

表 1-4 NetBackup サービスのログレベル

サービス	説明
Policy Execution Manager	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、ジョブの実行予定時間を決定します。ポリシーが変更されていたり、イメージの期限が切れていた場合は、NBPEM に通知され、適切なポリシーおよびクライアントタスクが更新されます。
Job Manager	Job Manager (NBJM) 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。
Resource Broker	Resource Broker (NBRB) は、ストレージユニット、テープドライブおよびクライアントを予約するための割り当てを行います。

レジストリ、bp.conf ファイル、統合ログのログの値

Windows レジストリ、bp.conf ファイル、または統合ログのログの値を設定することもできます。

表 1-5 ログレベルとその値

ログレベル	レガシーログ - Windows レジストリ	レガシーログ - bp.conf	統合ログ
最小のログ	0xffffffff の 16 進値。	VERBOSE = 0 (グローバル) *processname*_VERBOSE = 0 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 を指定します。	1
[ログなし (No logging)]	0xfffffffe の 16 進値。	VERBOSE=-2 (グローバル) *processname*_VERBOSE = -2	0

ログの保持とログサイズ

次のオプションを使用して、NetBackup でのログファイルの再利用と削除の方法を管理できます。

表 1-6 NetBackup のログの保持オプション

ログの保持オプション	説明	インターフェース
最大ログサイズ (Maximum log size)	統合ログとレガシーログのサイズを制限します。NetBackup サーバーの場合、推奨値は 25 GB 以上クライアントの場合、推奨値は 5 GB 以上 p.15 の「ログの削除」を参照してください。	このオプションは、ホストプロパティの[ログ (Logging)]設定にあります。
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。 p.30 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。	vxlogcfg
MaxLogFileSizeKB とその他の RolloverMode 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)。 p.29 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。	vxlogcfg
保持期間 (Retention period)	NetBackup が統合ログとレガシーログを保持する日数を制限します。 p.50 の「レガシーログのサイズと保持の制限」を参照してください。	このオプションは、ホストプロパティの[ログ (Logging)]設定にあります。
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。 p.50 の「レガシーログのサイズと保持の制限」を参照してください。	bpsetconfig

ログの削除

すべてのログはログサイズが高水準点、つまり、[最大ログサイズ (Maximum log size)]値の 95% に達するまで維持されます。NetBackup は 10 分ごとにログサイズを検証します。ログサイズが高水準に達すると、NetBackup は古いログの削除を開始します。ログサイズが低水準、つまり[最大ログサイズ (Maximum log size)]の値の 85% に達すると、NetBackup はログの削除を停止します。

[最大ログサイズ (Maximum log size)]と[保持期間 (Retention period)]の両方を選択した場合、ログは最初に起きる条件に基づいて削除されます。

次の場所にあるログを参照して、NetBackup のログ削除動作を確認できます。

install_path¥NetBackup¥logs¥nbutils

```
/usr/openv/logs/nbutils
```

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。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。

p.16 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.17 の「Windows クライアントのログレベルの変更」を参照してください。

グローバルログレベルの変更

グローバルログレベルは、[グローバルと同じ (Same as global)]に設定されているすべてのプロセスのログレベルを確立します。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。

グローバルログレベルを変更するには

1. NetBackup Web UI を開きます。
2. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host properties)]の順にクリックします。
3. サーバーまたはクライアントを選択します。必要に応じて、[接続 (Connect)]をクリックします。次に、[プライマリサーバーの編集 (Edit primary server)]、[メディアサーバーの編集 (Edit media server)]、または[クライアントの編集 (Edit client)]をクリックします。
4. [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)]リストから目的の値を選択します。
6. [保存 (Save)]をクリックします。

Media Manager のデバッグログを上位レベルに設定する

デバッグログを上位レベルに設定すると、多くのエラー状態を解決するために役立ちます。デバッグレベルを選択し、その後、操作を再試行して、デバッグログを調べます。

Media Manager のデバッグログを上位レベルに設定するには

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。

Windows クライアントのログレベルの変更

テクニカルサポートからアドバイスを受ける際に、トラブルシューティングを実行するため、クライアントプロセスのログレベルを上げることができます。それ以外の場合は、デフォルトレベルの 0 を使用してください。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。

メモ: `vxlogcfg` コマンドを使用して、Bare Metal Restore プロセス (`bmrsavecfg`) のログレベルを制御できます。

---

p.37 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。

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)]、[NetBackup クライアントのプロパティ (NetBackup Client Properties)]の順に選択し、[トラブルシューティング (Troubleshooting)]タブをクリックします。
3. [詳細 (Verbose)]設定には、推奨されたレベルを入力するか、トラブルシューティングが終了した場合は 0 を入力します。

統合ログについて

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

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 の場合　*install_path*¥NetBackup¥logs

UNIX の場合　/usr/openv/logs

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

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

vxlogcfg	統合ログ機能の構成設定を変更します。
vxlogmgr	統合ログをサポートする製品が生成するログファイルを管理します。
vxlogview	統合ログによって生成されたログを表示します。 p.33 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。

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。

の統合ログを収集する方法NetBackup

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/openv/logs/bmrsetup/51216-157-2202872032-050125-0000000.log

/usr/openv/logs/nbemm/51216-111-2202872032-050125-0000000.log
/usr/openv/logs/nbrb/51216-118-2202872032-050125-0000000.log
/usr/openv/logs/nbjm/51216-117-2202872032-050125-0000000.log
/usr/openv/logs/nbpem/51216-116-2202872032-050125-0000000.log
/usr/openv/logs/nbsl/51216-132-2202872032-050125-0000000.log
Total 6 file(s)
Copying
/usr/openv/logs/bmrsetup/51216-157-2202872032-050125-0000000.log
 ...
Copying
/usr/openv/logs/nbemm/51216-111-2202872032-050125-0000000.log ...

Copying
/usr/openv/logs/nbrb/51216-118-2202872032-050125-0000000.log ...

Copying
/usr/openv/logs/nbjm/51216-117-2202872032-050125-0000000.log ...

Copying
/usr/openv/logs/nbpem/51216-116-2202872032-050125-0000000.log ...

Copying
/usr/openv/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。

```
51216-111-2202872032-050125-0000000.log
51216-116-2202872032-050125-0000000.log
51216-117-2202872032-050125-0000000.log
51216-118-2202872032-050125-0000000.log
51216-132-2202872032-050125-0000000.log
51216-157-2202872032-050125-0000000.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す。

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。Cohesity 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/openv/logs/nbpem/51216-116-2201360136-041029-0000000000.log
```

表 1-7 に、ログファイル名の各部分の説明を示します。

表 1-7　統合ログのファイル名の形式の説明

例	説明	詳細
51216	製品 ID (Product 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、プロセス (Policy Execution Manager) のオリジネータ ID です。nbpemNetBackup
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.29 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.22 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/openv/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 1-8 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 1-8 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 SSL (Secure Sockets Layer) 通信で使用されます。 (nbatd) ディレクトリは /usr/netbackup/sec/at/bin ディレクトリ (UNIX の場合) または *install_path*¥NetBackup¥sec¥at¥bin 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、NetBackup 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 VRTSpbx です。ログは、/opt/VRTSpbx/log (UNIX の場合) または *install_path*¥VxPBX¥log (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。これはプライマリサーバー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。これはプライマリサーバー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。これはプライマリサーバー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。これはプライマリサーバーでのみ実行されます。
119	bmrd	NetBackup BMR (Bare Metal Restore) プライマリ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	bmrc	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 プライマリサーバーと通信します。
123	bmrs	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	bmrsrt	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 プライマリサーバーに Windows ドライバ、Service Pack、修正プログラムを追加します。
131	bmrrst	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。
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	libraries	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 Cohesity 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 外部プロシージャを管理します。
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。
144	da	EMM Device Allocator は共有ドライブのために使われます。

オリジネータ ID	エンティティ	説明
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、Cohesity の技術者が使用します。 Cohesity 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タ。
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。
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。

オリジネータ ID	エンティティ	説明
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	RDSM (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。
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、プライマリサーバーベースの対称キーマネージメントサービスです。
293	nbaudit	NetBackup Audit Manager。
294	nbauditmsgs	NetBackup 監査メッセージ。

オリジネータ ID	エンティティ	説明
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	root または管理者権限で実行されている NetBackup Client Service。
369	impmgr	NetBackup インポートマネージャ。
371	nbim	Indexing Manager。
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。

オリジネータ ID	エンティティ	説明
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。
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	ncfexchangepi	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。
495	NetBackup Web API	この OID は、NetBackup Web API を表します。
497	ncfcloudpi	NetBackup クラウド検出プラグイン。
528	ncfnbcs	サービスアカウントで実行されている NetBackup Client Service。
529	bmrbd	root または管理者権限で実行されている BMR ブートサーバーサービス。
530	bmrbd	サービスアカウントで実行されている BMR ブートサーバーサービス。

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。ただし、NFS または CIFS などのリモートファイルシステムにはログを保存しないでください。リモートで格納されたログはサイズが大きくなる場合があり、重大なパフォーマンスの問題につながる可能性があります。

UNIX の場合

```
/usr/openv/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.14 の「ログの保持とログサイズ」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。vxlogcfgvxlogcfg表 1-9コマンドを使用して、条件を設定します。

表 1-9　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/openv/logs/nbpem/51216-116-2201360136-041029-0000000000.log

/usr/openv/logs/nbpem/51216-116-2201360136-041029-0000000001.log

/usr/openv/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.22 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.14 の「ログの保持とログサイズ」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.37 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

[保持期間 (Retention period)]プロパティを使用して、ログを保持す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。

p.10 の「[ログ (Logging)]プロパティ」を参照してください。

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 でファイルを手動で削除または移動できない場合は、[保持期間 (Retention period)]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.35 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[保持期間 (Retention period)]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 コマンドを使用した場合だけ、統合ログの情報を正しく収集して表示することができます。統合ログファイルは、バイナリ形式のファイルで、一部の情報は関連するリソースファイルに含まれています。これらのログは次のディレクトリに保存されます。特定プロセスのファイルに検索を制限することによって vxlogview の結果をより速く表示することができます。

UNIX の場合　　/usr/openv/logs

Windows の場合　*install_path*¥NetBackup¥logs

表 1-10　vxlogview 問い合わせ文字列のフィールド

フィールド名	形式	説明	例
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 = '04/27/11 10:01:00 AM'
PREVTIME	文字列	hh:mm:ss の形式で、時間を指定します。このフィールドには、=、<、>、>= および <= の演算子だけを使用できます。	PREVTIME = '2:34:00'
SEV	整数	次の使用可能な重大度の種類のうちのいずれかを指定します。 0 = INFO 1 = WARNING 2 = ERR 3 = CRIT 4 = EMERG	SEV = 0 SEV = INFO

フィールド名	形式	説明	例
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'

表 1-11　日付を含む問い合わせ文字列の例

例	説明
(PRODID == 51216) && ((PID == 178964)|| ((STDATE == '2/5/15 09:00:00 AM') && (ENDATE == '2/5/15 12:00:00 PM'))	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。
((prodid = 'NBU') && ((stdate >= '11/18/14 00:00:00 AM') && (endate <= '12/13/14 12:00:00 PM'))) || ((prodid = 'BENT') && ((stdate >= '12/12/14 00:00:00 AM') && (endate <= '12/25/14 12:00:00 PM')))	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。
(STDATE <= '04/05/15 0:0:0 AM')	2015 年 4 月 5 日、またはその前に記録されたすべてのインストール済み Cohesity 製品のログメッセージを取得します。

vxlogview を使用した統合ログの表示の例

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

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

表 1-12 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	`vxlogview -p 51216 -d all`
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。 `vxlogview --prodid 51216 --display D,T,m,x`
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。 `# vxlogview -o 116 -t 00:20:00`

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。
	`# vxlogview -o nbpem -b "05/03/15 06:51:48 AM"`
	`-e "05/03/15 06:52:48 AM"`

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 `-i` オプションを使うことができます。 `# vxlogview -i nbpem` `vxlogview -i` オプションは、指定したプロセス (nbpem) が作成するログファイルのみを検索します。検索するログファイルを制限することで、vxlogview の結果が速く戻されます。一方、`vxlogview -o` 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 `-i` オプションを使用すると、vxlogview によってメッセージ [ログファイルが見つかりません。(No log files found)] が戻されます。サービスではないプロセスには、ファイル名にオリジネータ ID がありません。この場合、`-i` オプションの代わりに `-o` オプションを使用します。 -i 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。

項目	例
ジョブ ID の検索	特定のジョブ ID のログを検索できます。 `# vxlogview -i nbpem | grep "jobid=job_ID"` jobid=という検索キーは、スペースを含めず、すべて小文字で入力します。 ジョブ ID の検索には、任意の vxlogview コマンドオプションを指定できます。この例では、-i オプションを使用してプロセスの名前 (nbpem) を指定しています。このコマンドはジョブ ID を含むログエントリのみを返します。jobid=*job_ID* を明示的に含まないジョブの関連エントリは欠落します。

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 1-13 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。
	
	`# vxlogmgr -s -o nbrb`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050503-00.log`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050504-00.log`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050505-00.log`
	`Total 3 file(s)`

最も古いログファイルの削除	vxlogcfg 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。
	
	`# vxlogcfg -a -p 51216 -o nbrb -s NumberOfLogFiles=1`
	`# vxlogmgr -d -o nbrb -a`
	`Following are the files that were found:`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050504-00.log`
	`/usr/openv/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/openv/logs/nbrb/51216-118-1342895976-050504-00.log ...`
	`Deleting`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050503-00.log ...`

項目	例
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。 `# vxlogmgr -d --prodid 51216 -n 15` 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。 `# vxlogmgr -d -o nbrb` 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。 `# vxlogmgr -d -p NB` 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。

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。
	`# vxlogmgr -a -d`
	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。
	`# vxlogmgr -a -d -p ics`
	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。
	`# vxlogmgr -a -d -o nbrb`

項目	例
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実行することで、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 NumberOfLogFiles * オリジネータの MaxLogFileSizeKB 統合ログ機能が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 NumberOfLogFiles 設定および MaxLogFileSizeKB 設定が変更されていない場合、統合ログ機能が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 NumberOfLogFiles 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 NumberOfLogFiles が、デフォルト設定のままで変更されていない。 ■ 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 プライマリサーバーに特有) ■ MaxLogFileSizeKB のデフォルトが 51200 である。 ■ NumberOfLogFiles のデフォルトが 3 である。 統合ログ機能が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。

vxlogcfg を使用した統合ログの設定の例

次の点に注意してください。

- 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。
- 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。

表 1-14 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。
	
	`# vxlogcfg -a -p 51216 -o Default -s MaxLogFileSizeKB=100000`
	
	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。
	
	`# vxlogcfg -a --prodid 51216 --orgid Default -s RolloverMode=FileSize`
	
	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。
	
	`# vxlogcfg -a -p 51216 -o nbrb -s MaxLogFileSizeKB=1024000`

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。 `# vxlogcfg -a --prodid 51216 --orgid 111 -s RolloverMode=FileSize MaxLogFileSizeKB=512000 NumberOfLogFiles=999 LogRecycle=TRUE` 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。 `# vxlogcfg -a --prodid 51216 --orgid Default -s DebugLevel=1 DiagnosticLevel=6`

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、RolloverMode が含まれていることに注意してください。
	
	`# vxlogcfg -l -o nbrb -p NB`
	
	`Configuration settings for originator 118,`
	`of product 51,216...`
	`LogDirectory = /usr/openv/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/openv/lib/libvxexticu`
	`L10nResource = nbrb`
	`L10nResourceDir = /usr/openv/resources`
	`SyslogIdent = VRTS-NB`
	`SyslogOpt = 0`
	`SyslogFacility = LOG_LOCAL5`
	`LogFilePermissions = 600`

統合ログのアクセス設定

NetBackup では、統合ログディレクトリに対する権限が限定的かつ構成可能なレベルに設定されます。この変更は、機密情報が含まれている可能性のある NetBackup ログへの不正アクセスを防止することを目的としています。

統合ログのアクセス設定の変更

デフォルトのログファイル権限を変更して、制限を少なくできます。ログファイルまたはフォルダの権限を変更するには、vxlogcfg コマンドを使用します。特定のオリジネータ ID (OID) の権限を変更することも、すべての OID に適用されるデフォルトの権限を変更することもできます。フォルダ権限については、Default.LogFilePermissions が考慮されます。

フォルダとファイルの権限は、vxlogcfg コマンドの実行後すぐには変更されません。権限をすぐに適用するには、NetBackup サービスを再起動します。サービスの再起動について詳しくは、こちらの記事を参照してください。ファイルとフォルダの権限は、次のログロールオーバーサイクルの間に適用されます。このサイクルは、ログの長さと設定済みのログファイルサイズによって異なります。ロールオーバー期間は最大で 1 日です。したがって、この場合、ファイル権限を変更した 1 日後に新しい権限が反映されます。システム内の既存のログファイルの権限は変更されません。

デフォルトのログ権限を変更する例をいくつか示します。

- この 2 つのコマンド例では、すべてのコンポーネントのファイル権限を 644 に変更します。このフォルダに実行権限 (755) を追加します。
  - `/usr/openv/netbackup/bin/vxlogcfg -a --prodid 51216 -o ALL -s LogFilePermissions=644`
  - `/usr/openv/netbackup/bin/vxlogcfg -a --prodid 51216 -o ALL -s DynaReloadInSec=120`
- 任意のオリジネータ ID の権限を変更するには、次のコマンド例を使用します。
  `/usr/openv/netbackup/bin/vxlogcfg -a --prodid 51216 --orgid 111 -s LogFilePermissions=644`
  このコマンドでは、nbemm を表すオリジネータ ID *111* に *644* 権限を適用します。他のすべてのコンポーネントの orgid については、/usr/openv/netbackup/nblog.conf を参照してください。

  メモ: デフォルトでは、すべてのフォルダ権限に対して nblog.conf ファイル内のパラメータ Default.LogFilePermissions が適用されます。OID 固有の権限を使用する場合、<*OID*>.LogFilePermissions パラメータが使用されます。
- icsul.conf ファイルで PBX ログに対する権限を変更するには、次のコマンド例を使用します。
  `/usr/openv/netbackup/bin/vxlogcfg -a --prodid 50936 -o 103 -s LogFilePermissions=644`
  権限をすぐに適用するには、PBX サービスを再起動します。サービスの再起動について詳しくは、こちらの記事を参照してください。

レガシーログについて

NetBackup レガシーデバッグログの場合、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。デフォルトでは、NetBackup は次の場所にログディレクトリのサブセットのみを作成します。

Windows	*install_path*¥NetBackup¥logs *install_path*¥Volmgr¥debug
UNIX	/usr/openv/netbackup/logs /usr/openv/volmgr/debug

レガシーログを使用するには、プロセスのログファイルディレクトリが存在している必要があります。ディレクトリがデフォルトで作成されていない場合は、mklogdir ユーティリティを使用してディレクトリを作成できます。または、手動でディレクトリを作成することもできます。プロセスのログ記録を有効にすると、プロセスの開始時にログファイルが作成されます。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。

メモ: レガシーログディレクトリに適切な権限を付与するために、Windows と Linux に存在する mklogdir ユーティリティを常に使用して各プラットフォームのレガシーログディレクトリを作成します。

次のユーティリティを使用して、すべてのログディレクトリを作成できます。

- Windows の場合: *install_path*¥NetBackup¥Logs¥mklogdir.bat
- UNIX の場合: /usr/openv/netbackup/logs/mklogdir

レガシーログフォルダを作成して使用する場合は、次の推奨事項に従います。

- レガシーログフォルダ内でシンボリックリンクまたはハードリンクを使用しないでください。
- root 以外のユーザーまたは管理者以外のユーザーに対してプロセスが実行された場合、レガシーログフォルダにログが記録されない場合があります。その場合は、mklogdir コマンドを使用して、必要なユーザーのフォルダを作成します。
- root 以外のユーザーまたは管理者以外のユーザー用にコマンドラインを実行するには (NetBackup サービスが実行されていない場合のトラブルシューティング)、特定のコマンドライン用のユーザーフォルダを作成します。フォルダは、mklogdir コマンドを使用して、または root 以外のユーザーや管理者以外のユーザー権限で手動で作成します。

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/openv/netbackup/logs/mklogdir

表 1-15　　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
bmrbd	BMR ブートサーバーデーモン。これらのログには、bmrbd プロセスの情報が含まれます。
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。
bpbkar	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 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、クライアント上のコマンドラインユーティリティ。
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システム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。
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。

ディレクトリ	関連するプロセス
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 製品に付属のマニュアルを参照してください。
nbpas	NetBackup 特権アクセスサービス。これらのログには nbpas プロセスに関する情報が含まれます。このプロセスは、サービスユーザーが要求するルート固有のタスクを実行します。
ncfnbcs	NetBackup Client Service。これらのログには、nbcs プロセスの情報が含まれます。
tar	リストア操作中の nbtar の処理。
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。Java インターフェースログファイルを除いて、user_ops ディレクトリにあるログファイルは、KEEP_LOGS_DAYS 構成オプションの設定に従って削除されます。 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。管理者は、組織の要件に従って nbjlogs ディレクトリに存在するこれらのログをクリーンアップできます。

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¥

表 1-16　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
bmrbd	すべての Windows	BMR ブートサーバーデーモン。これらのログには、bmrbd プロセスの情報が含まれます。
bpinetd	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、bpinetd32 プロセスの情報が含まれます。
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 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 Services サービス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。
nbpas	すべての Windows クライアント	NetBackup 特権アクセスサービス。これらのログには nbpas プロセスに関する情報が含まれます。このプロセスは、サービスユーザーが要求するルート固有のタスクを実行します。
ncfnbcs	すべての Windows クライアント	NetBackup Client Service。これらのログには、nbcs プロセスの情報が含まれます。
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。Java インターフェースログファイルを除いて、user_ops ディレクトリにあるログファイルは、KEEP_LOGS_DAYS 構成オプションの設定に従って削除されます。 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。管理者は、組織の要件に従って nbjlogs ディレクトリに存在するこれらのログをクリーンアップできます。

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

ファイル名には次の要素が含まれます。

user_name これはプロセスを実行するユーザーの名前で、のようになります。

- UNIX の root ユーザーの場合、*user_name* は root です。
- UNIX の root ユーザー以外のユーザーの場合、*user_name* 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、*user_name* は ALL_ADMINS です。
- Windows のユーザーの場合、*user_name* は username@domain_name または username@machine_name です。

mmddyy これは NetBackup がログファイルを作成した月、日、年です。

nnnnn 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。

root 以外または非管理呼び出しプロセスログの新しいフォルダ構造は、プロセスログディレクトリ名の下に作成されます。

次に例を示します。

```
/usr/openv/netbackup/logs/tar/root.031020_00001.log
```

```
/usr/openv/netbackup/log/tar/usr1/usr1.031020_00001.log
```

root 以外のユーザー usr1 の場合、ルート以外のユーザー名のディレクトリは、それぞれの NetBackup プロセスの下に作成されます。

サーバーのレガシーデバッグログのディレクトリ名

NetBackup はサーバーのレガシーログ用に特定のディレクトリを作成します。各ディレクトリはプロセスに対応します。指定しない場合、各ディレクトリは次のディレクトリの下に作成されます。

Windows の場合 *install_path*¥NetBackup¥logs

UNIX の場合 /usr/openv/netbackup/logs

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

表 1-17 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。

表 1-17　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 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 ディスクマネージャ
bpdbm	NetBackup Database Manager。このプロセスは、プライマリ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 プライマリ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。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 はプライマリ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	認証デーモン (UNIX と Linux) またはサービス (Windows)。nbazd 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。Java インターフェースログファイルを除いて、user_ops ディレクトリにあるログファイルは、KEEP_LOGS_DAYS 構成オプションの設定に従って削除されます。 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。管理者は、組織の要件に従って nbjlogs ディレクトリに存在するこれらのログをクリーンアップできます。
vnetd	Cohesity 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/openv/logs ディレクトリまたは /usr/openv/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/openv/netbackup/logs/vnetd だけにログが記録されます。

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

次のディレクトリは、メディア管理プロセスとデバイス管理プロセスのレガシーログを有効にします。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。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　*install_path*¥Volmgr¥debug

UNIX　/usr/openv/volmgr/debug

表 1-18　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 のみ。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。
daemon	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 (oprd 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	tldcd 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 などのコマンド、および NetBackup Web UI によるデバイス構成のデバッグ情報。
vmscd	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 vmscd を停止して再起動します。

メディアおよびデバイスの管理ログの無効化

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 Volume Manager サービス　*install_path*¥Volmgr¥debug¥daemon

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

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を上げると、統合ログ機能にも影響します。
- UNIX の場合、/usr/openv/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 (またはそれ以上の値) 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)]設定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。

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、VERBOSE ファイルに vm.conf 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。vm.conf ファイルは、次のディレクトリに存在します。

Windows	*install_path*¥Cohesity¥Volmgr¥
UNIX	/usr/openv/volmgr/

レガシーログのサイズと保持の制限

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ので、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。

[ログを保持する日数 (Keep logs for days)]

NetBackup が NetBackup プロセスログを保持する時間を制限します (メディアおよびデバイスの管理ログを除く)。デフォルトは 28 日です。

vm.conf の DAYS_TO_KEEP_LOGS 設定

メディアおよびデバイス管理のレガシーログのログファイルのローテーションを制御します。デフォルトは 30 日です。vm.conf ファイルは *install_path*¥Volmgr¥ または /usr/openv/volmgr/ にあります。

MAX_LOGFILE_SIZE と MAX_NUM_LOGFILES の設定

レガシーのログ記録の場合には、NetBackup は設定ファイル (Windows のレジストリ、UNIX の場合には bp.conf 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次の bp.conf パラメータを構成します。

- MAX_LOGFILE_SIZE パラメータはログファイルの最大サイズを示します。NetBackup のログファイルのサイズが MAX_LOGFILE_SIZE の設定と一致すると、その次のログは新しいログファイルに格納されます。デフォルトは 500 MB です。

- MAX_NUM_LOGFILES パラメータは NetBackup で作成できるログファイルの最大数を示します。ログファイル数が MAX_NUM_LOGFILES 設定と一致すると、古いログファイルはパージされます。デフォルトは 0 (無制限) です。

レガシーログのアクセス設定

NetBackup では、レガシーログディレクトリの権限を制限が厳しくも構成可能なレベルに設定します。この変更は、機密情報が含まれている可能性のある NetBackup ログへの不正アクセスを防止することを目的としています。

nbsetconfig コマンドを使用して ALLOW_WORLD_READABLE_LOGS パラメータの値を構成することで、ログへのアクセスを制御できます。

構成可能な値は次のとおりです。

- ALLOW_WORLD_READABLE_LOGS=YES を指定すると、デバッグログに誰でも読み取り可能な権限が付与されます。
- ALLOW_WORLD_READABLE_LOGS=NO (デフォルトの状態) を指定すると、デバッグログに誰でも読み取り可能な権限が付与されません。

メモ: user_ops (user_ops/nbjlogs を除く) と dbagents のログは、誰でも読み取り可能で、誰でも書き込み不可です。

---

nbsetconfig 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。

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。

クライアントでログの保持制限を設定する方法

1. NetBackup Web UI を開きます。
2. 左側で、[ホスト (Host)]、[ホストプロパティ (Host Properties)]の順に選択します。
3. クライアントを選択します。必要に応じて、[接続 (Connect)]を選択します。次に、[クライアントの編集 (Edit client)]を選択します。
4. UNIX クライアントまたは Windows クライアントのいずれかから該当するノードを展開します。次に、[クライアントの設定 (Client settings)]を選択します。

5 [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)]フィールドを見つけます。

6 ログファイルを保持する日数を入力し、[保存 (Save)]を選択します。

syslogd を使用した UNIX のログ記録

UNIX では、NetBackup は syslogd を使用して、ロボットエラー、ネットワークエラー、ロボットで制御されたドライブの状態変更を記録します。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。

この追加のログ記録を有効にするには、次のいずれかの方法を使用します。

- デバイス管理プロセスを起動する ltid コマンドと -v オプションを使用します。このオプションを指定すると、ロボットデーモンおよび vmd が詳細モードで起動されます。
- 特定のデーモンを起動するコマンドと -v オプションを使用します (例: acsd -v)。

エラーは LOG_ERR、警告は LOG_WARNING、デバッグ情報は LOG_NOTICE と記録されます。facility の形式は[daemon]です。

Windows のイベントビューアのログオプション

Windows のイベントビューアのアプリケーションイベントログに、ログアプリケーションと診断メッセージを書き込むように、NetBackup Windows プライマリサーバーを構成することもできます。

vxlogcfg 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。

オリジネータの Windows イベントビューアに統合ログメッセージを書き込むには

1 vxlogcfg コマンドを使用して、オリジネータの LogToOslog の値を true に設定します。

次に例を示します。

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

2 NetBackup サービスを再起動します。

Windows イベントビューアにレガシーログメッセージを書き込むには

1 NetBackup プライマリサーバー上に eventlog ファイルを作成します。

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

2 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
```

「56」を指定すると、重大度が警告 (Warning)、エラー (Error)、重要 (Critical) のメッセージを記載したログを生成します (56 = 8 + 16 + 32)。「255」を指定すると、すべての種類のメッセージがあるログを生成します (255 = 1 + 2 + 4 + 8 + 16 + 32 + 64 +128)。

3 NetBackup サービスを再起動します。

イベントログのパラメータ

eventlog のパラメータは重大度と種類を表します。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 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。	1 = 不明 2 = デバッグ 4 = 情報 8 = 警告 16 = エラー 32 = 重要
形式	■ 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。	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

ログ内のメッセージの形式は次のとおりです。

```
<Severity>  <Job type>  <Job ID>  <Job group ID>  <Server>  <Client>  <Process>  <Text>
```

次に例を示します。

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

2

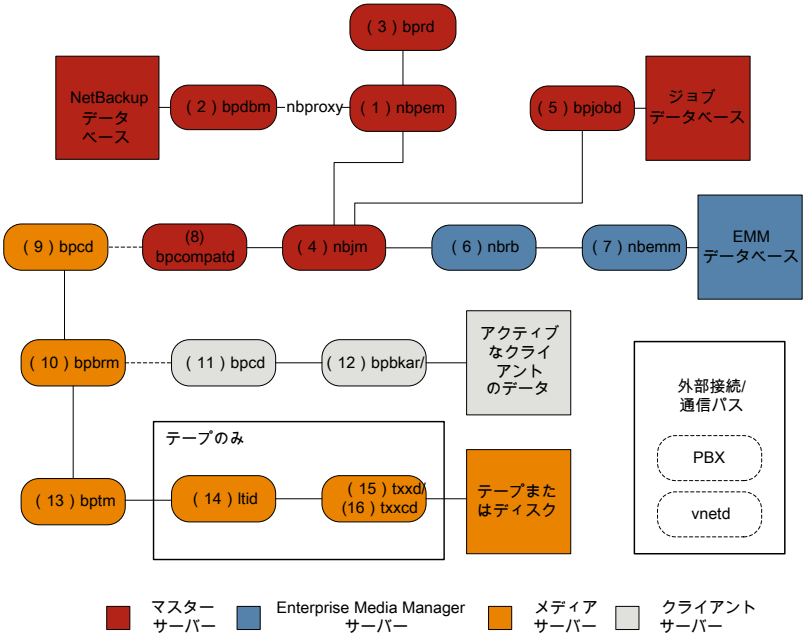
バックアッププロセスおよびログ記録

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

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. (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 デーモン (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。

2. 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。

3. 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。

4. 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。

5. 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 (tx*xx*d、*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。tx*xx*d 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 (tx*xx*cd) 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 サービスは、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。

バックアップに関係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.58 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.58 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.59 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.60 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 プライマリ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スポート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スポートガイド』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、`bpinetd` 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 プライマリサーバーと 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。

プライマリサーバーは 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、プライマリ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、開始するとサーバー上で同じデーモンやプログラムが実行されるという点で似ています。

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。これは、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検証します。

- 即時手動バックアップは、管理者が NetBackup Web UI でこのオプションを選択した場合、または bpbackup -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 bpbackup 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 bpbackup プログラムまたは bparchive プログラムが起動され、要求がプライマリサーバーの Request デーモン bprd に送信されます。bprd は、ユーザー要求を受信すると nbpem と通信し、スケジュールのポリシー構成を検証します。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。

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 bpbrm 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

次のログファイルは、メディアサーバーおよびプライマリサーバーのバックアップ失敗を確認する際に使用されます。

p.150 の「nbpem のログ」を参照してください。

p.150 の「nbproxy のログ」を参照してください。

p.146 の「bpdbm のログ」を参照してください。

p.147 の「bprd のログ」を参照してください。

p.149 の「nbjm のログ」を参照してください。

p.146 の「bpjobd のログ」を参照してください。

p.150 の「nbrb のログ」を参照してください。

p.149 の「nbemm のログ」を参照してください。

p.146 の「bpcompatd のログ」を参照してください。

p.152 の「PBX のログ」を参照してください。

p.155 の「vnetd のログ」を参照してください。

p.146 の「bpcd のログ」を参照してください。

p.145 の「bpbrm のログ」を参照してください。

p.145 の「bpbkar のログ」を参照してください。

p.148 の「bptm のログ」を参照してください。

p.149 の「ltid のログ」を参照してください。

p.154 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。

p.144 の「acsssi のログ」を参照してください。

p.145 の「bpbackup のログ」を参照してください。

p.148 の「daemon のログ」を参照してください。

p.153 の「reqlib のログ」を参照してください。

p.153 の「robots のログ」を参照してください。

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テクニカルサポートに送信して支援を依頼できます。

p.60 の「バックアップログについて」を参照してください。

p.95 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。

メモ: 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。

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。

問題の種類	収集するログ
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。
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bpdbm ログ ■ 詳細 5 の bpbrm 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)

3

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。

p.64 の 図 3-1 を参照してください。

`acsls` 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構成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。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。

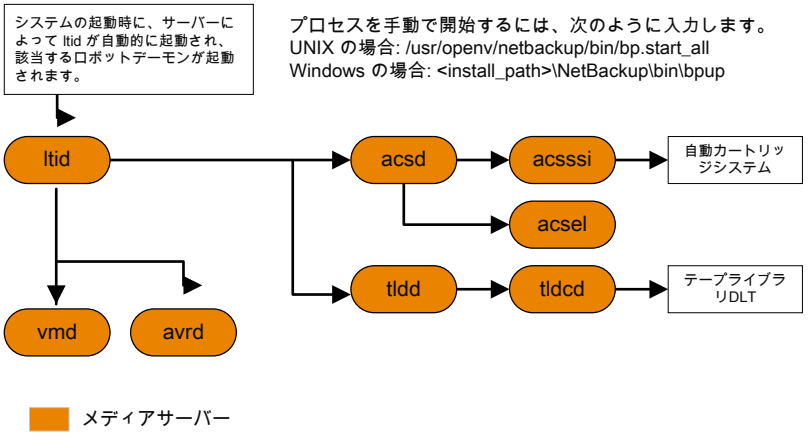
p.70 の 表 3-1 を参照してください。

ACSLS には、次の形式のデーモンが必要です。

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。

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.58 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.65 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。

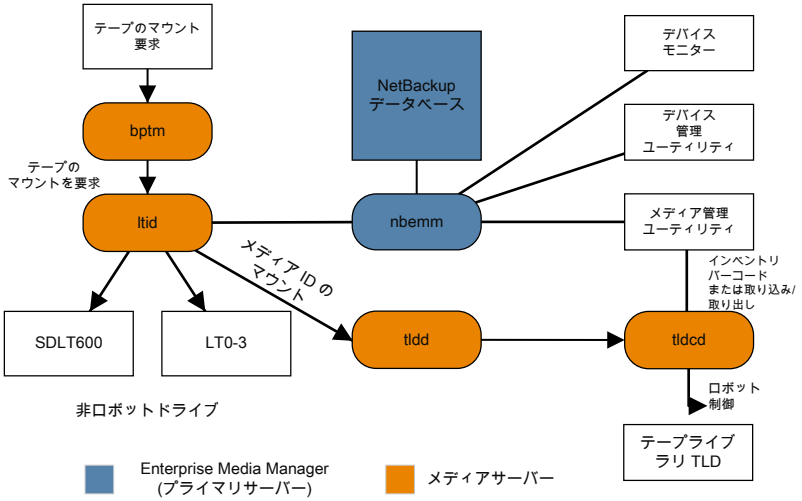
非ロボットドライブ用 NetBackup のメディアの選択について詳しくは、『NetBackup 管理者ガイド Vol. 2』を参照してください。

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/openv/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用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。

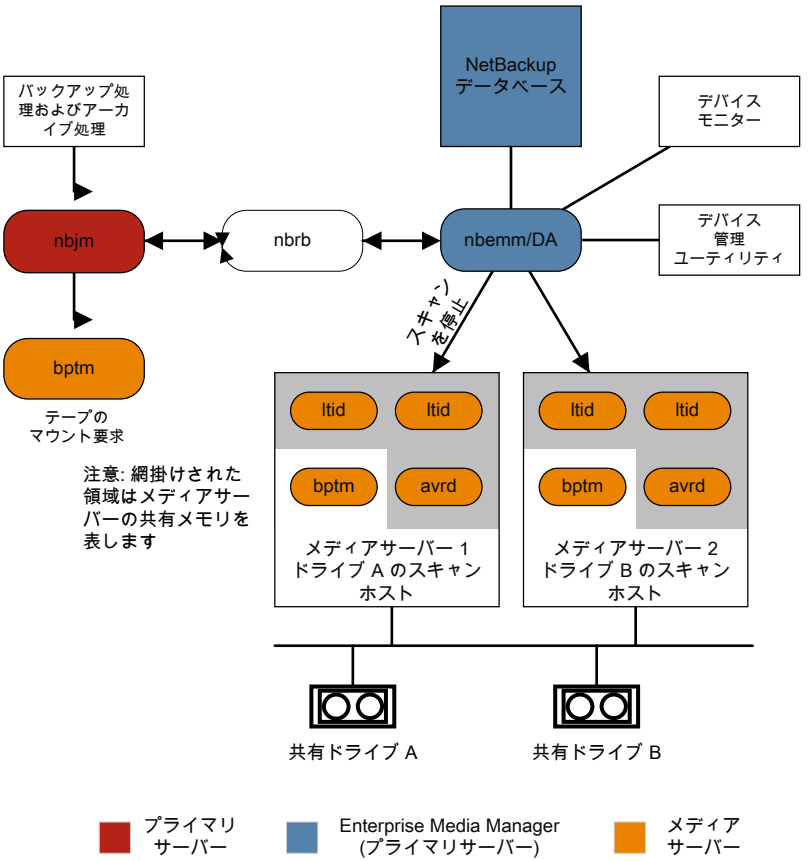
Shared Storage Option について詳しくは、『NetBackup 管理者ガイド Vol. 2』を参照してください。

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。ltidメディアサーバーの共有メモリで oprd、avrd、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。

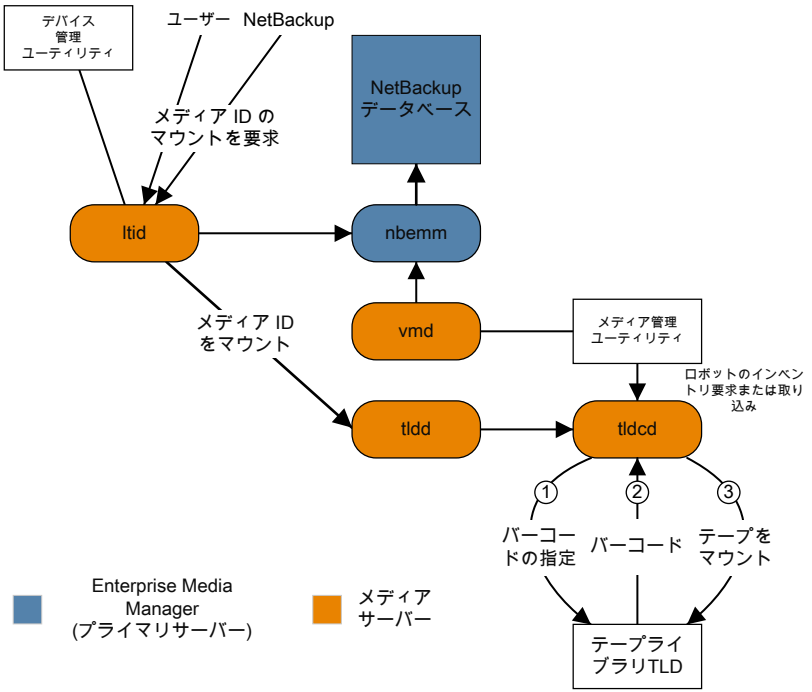
p.69 の 図 3-4 を参照してください。

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

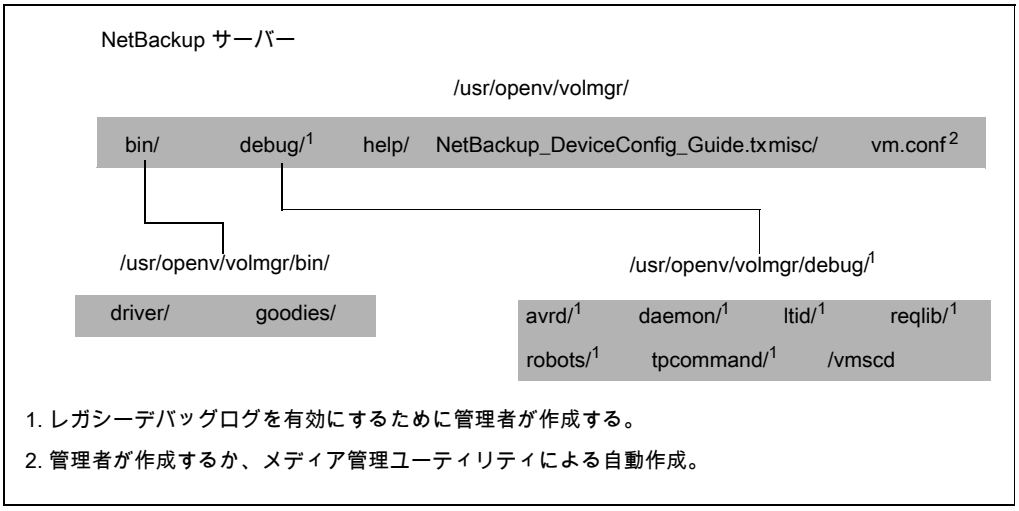


表 3-1 メディアおよびデバイスの管理のディレクトリおよびファイル

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、およびすべての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が含まれています。
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。 サービスユーザーが構成されている場合は、デバッグディレクトリとそのサブディレクトリにアクセスする権限をサービスユーザーに割り当てます。
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。
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。コンポーネントは、次のディレクトリに存在します。

/usr/openv/volmgr/bin

install_path¥volmgr¥bin.

メモ: UNIX では、syslog がシステムログを管理します (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連携して動作し、acsssi プロセス (UNIX の場合) または STK Libattach 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、acsssi プログラムおよび acssel プログラムの説明を参照してください。 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/ascd 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、ltid を介して、または vm.conf ファイルに VERBOSE を追加すると使用できます。
acssel	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。
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。

プログラムまたはデーモン	説明
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 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/stopltid 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 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。
tldd	DLT テープライブラリデーモンは、tldcd 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)。同じ TLD ロボット内の DLT 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。tldd 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。ホストに DLT ロボット内のドライブ用のデバイスパスが存在する場合、そのドライブに対するマウント要求およびマウント解除要求は、最初にローカル ltid に送信され、その後、ローカル tldd に送信されます (すべて同じホスト上)。その後、tldd が、その要求を、ロボットを制御しているホスト (別のホストである可能性があります) の tldcd に送信します。 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/openv/volmgr/bin/tldd 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。
tldcd	DLT テープライブラリ制御デーモンは、DLT 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。tldcdcd は、ドライブが接続されているホストの tldd 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 を開始します (UNIX の場合は、ltid を開始しなくても、/usr/openv/volmgr/bin/tldcd 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 tldcd -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。

プログラムまたはデーモン	説明
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は) デバッグログ。

4

リストアプロセスおよびログ記録

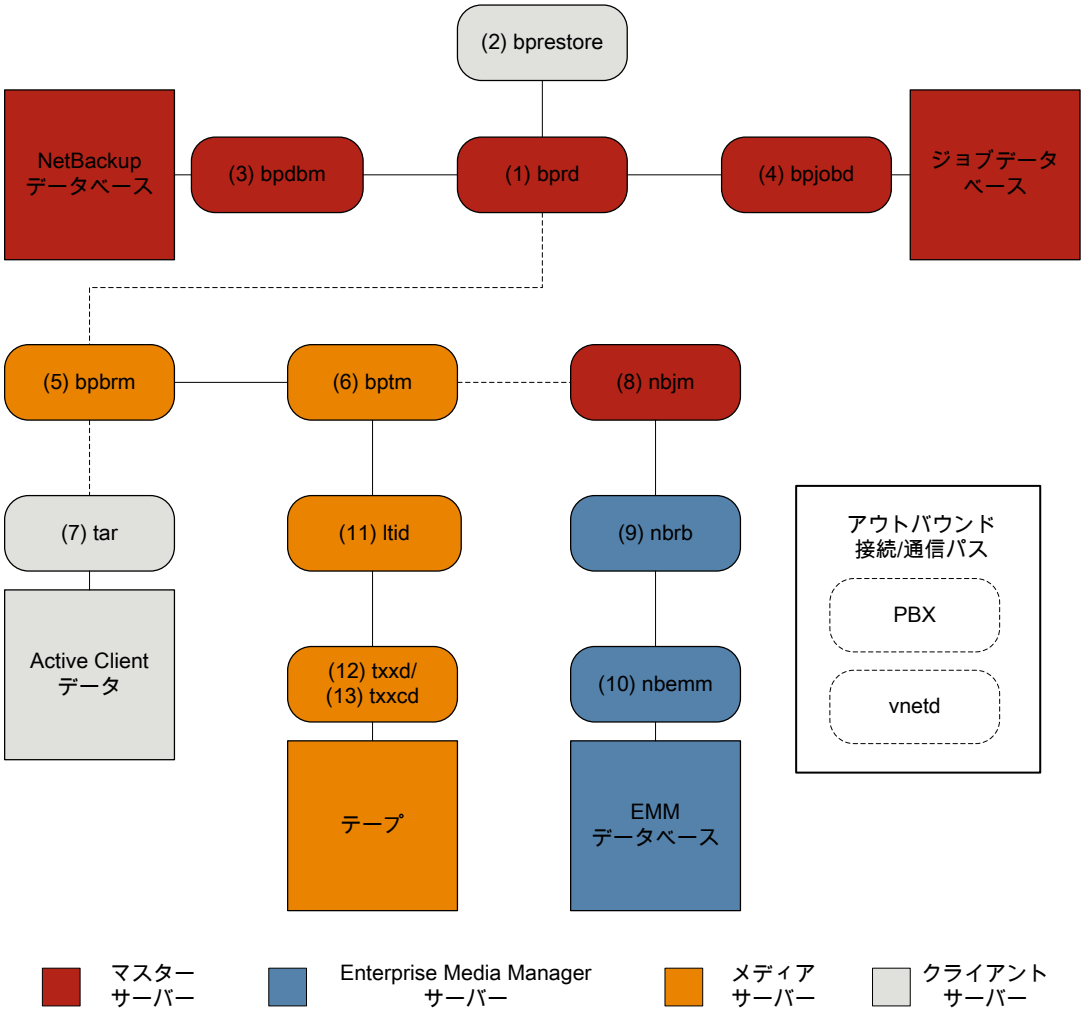
この章では以下の項目について説明しています。

リストアプロセス

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。イメージをテープからリストアするかディスクからリストア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を図示しています。

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 (bpbrm) を開始します。

6 bpbrm 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情報を提供します。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 (nbrb) に問い合わせを行う (9) NetBackup Resource Broker (nbemm) 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。

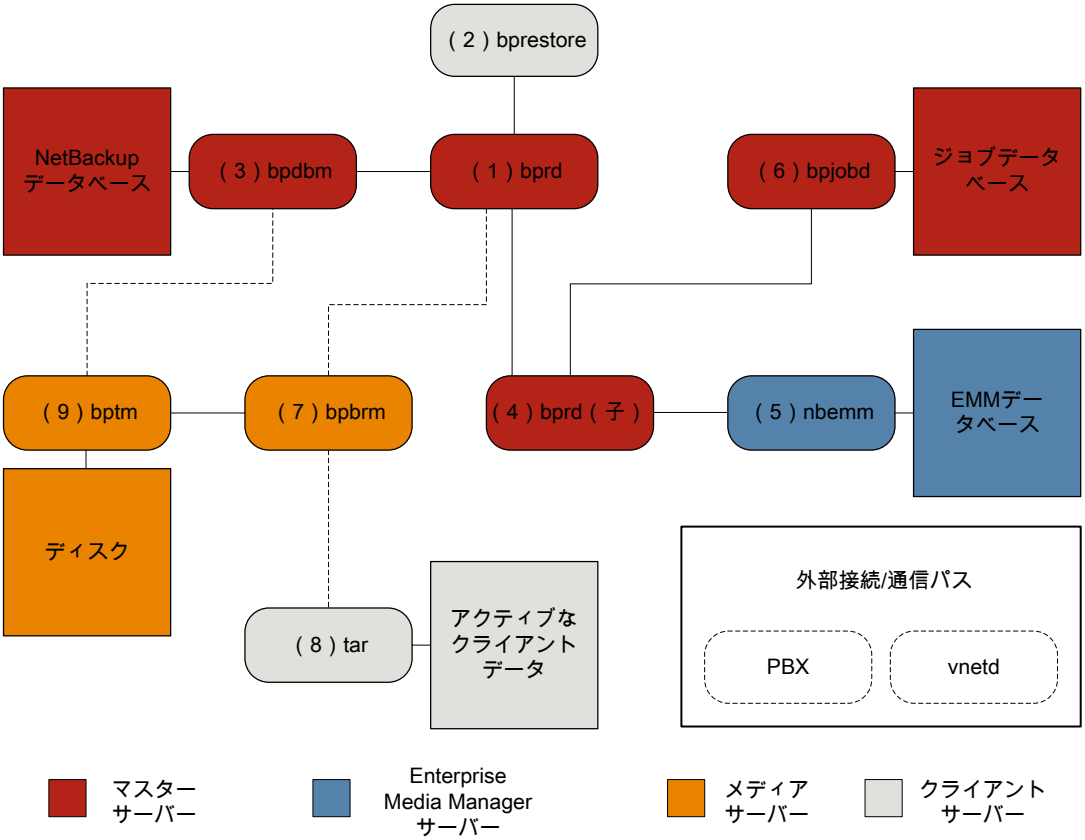
11 tar プロセスはクライアントディスクにデータを書き込みます。

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図示しています。

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` 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。
3. `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 (NetBackup) および bpbrm Legacy Network Service (PBX) を介して (7) メディアサーバーの NetBackup Backup Restore Manager (vnetd) 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 bpdbm 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。

リストアに関係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。

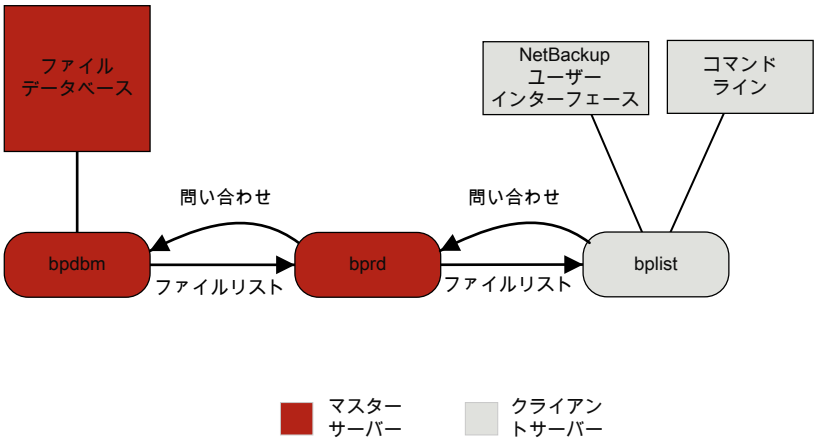
p.81 の「リストアログについて」を参照してください。

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これを使用できます。

ファイルリストを取り込むために、bplist は問い合わせをプライマリサーバーの 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 bpdbm に情報を問い合わせてクライアントの 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 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。
- 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プライマリサーバーに接続されている場合、プライマリサーバーで、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。
- 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 プロセスによって、イメージカタログに基づいて、リストアに必要なメディアが特定されます。その後、bptm によって、必要なメディアの nbrb からの割り当てが nbjm を介して要求されます。さらにその後、nbjm から mds (nbemm) の一部) へリソースが要求され、nbemm によってメディアが割り当てられ、適切なドライブ (テープメディア用) が選択されて割り当てられます。
  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同時アクセスをサポートするため、bptm は nbrb に対して割り当てを要求する必要はありません。bptm はシステムディスクマネージャに対する読み込み要求でファイルパスを使います。
- 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。

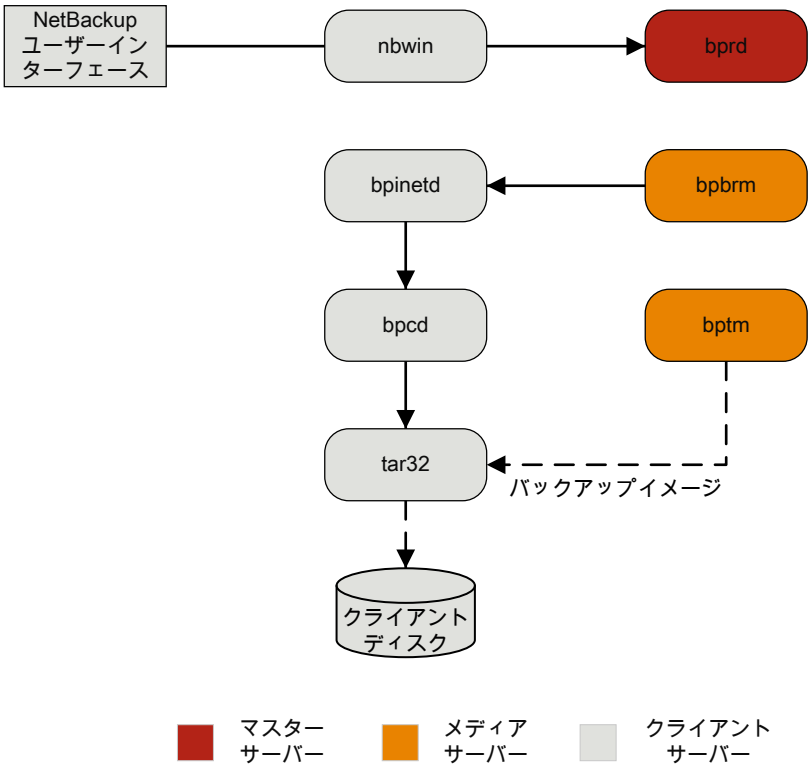
次に、リストア処理に関連する Windows プロセスを示します。

- 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 NetBackup nbtar 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、テクニカルサポートにログを送信してください。

p.82 の「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.147 の「bprd のログ」を参照してください。

p.147 の「bprestore のログ」を参照してください。

p.152 の「PBX のログ」を参照してください。

p.155 の「vnetd のログ」を参照してください。

p.146 の「bpdbm のログ」を参照してください。
p.146 の「bpjobd のログ」を参照してください。
p.145 の「bpbrm のログ」を参照してください。
p.148 の「bptm のログ」を参照してください。
p.154 の「tar ログ」を参照してください。
p.149 の「nbjm のログ」を参照してください。
p.150 の「nbrb のログ」を参照してください。
p.149 の「nbemm のログ」を参照してください。
p.149 の「ltid のログ」を参照してください。
p.153 の「reqlib のログ」を参照してください。
p.153 の「robots のログ」を参照してください。
p.144 の「acsssi のログ」を参照してください。

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テクニカルサポートに送信して支援を依頼できます。

p.95 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。

メモ: 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。

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

5

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。

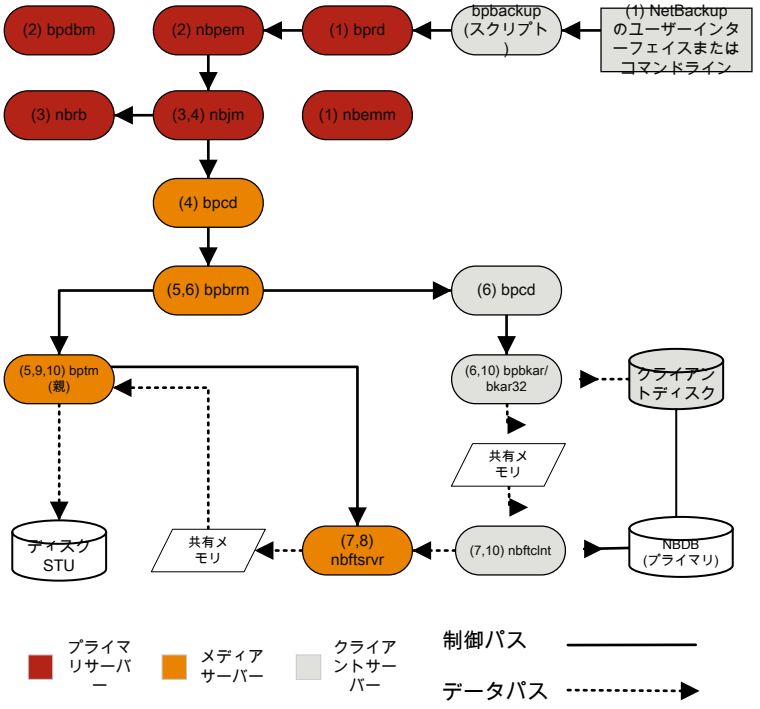
SAN クライアントファイバートランスポートのバックアップ

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。

FSM (FT Service Manager) は、SAN クライアントの一部としてプライマリ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 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、`nbftclnt` クライアント上の NetBackup 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 プライマリ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) は、NetBackup Policy Execution Manager (nbpem) にバックアップ要求を送信します。nbpem はポリシー構成を処理します。

   nbpem、nbjm、nbrb、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 を使用して bpbkar を起動し、次を実行します。

- 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、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。

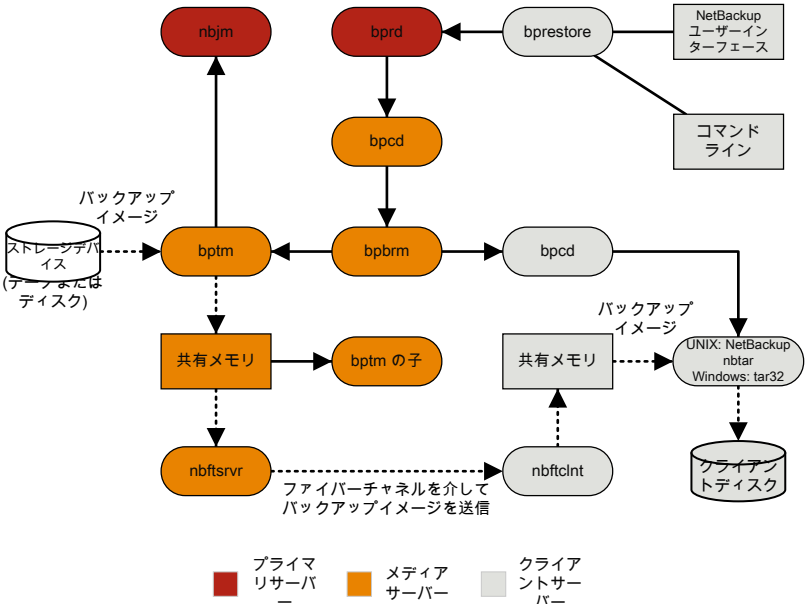
10 ジョブの最後に、次の処理が実行されます。

- bpbkar は bpbrm および bptm にジョブが完了したことを通知します。

- bptm は bpbrm にデータ書き込みの最終状態を送信します。
- 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 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。
- 対象のデータが存在するディスクまたはテープがプライマリサーバーに接続されている場合、プライマリサーバーで、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 (nbjm)。
  - FT サーバープロセスにリストア要求を送信します (nbftsrvr)。
  - リストア要求が、クライアント上の FT クライアントプロセス (nbftclnt) に送信されます。nbftclnt によって、メディアサーバー上の nbftsrvr へのファイバーチャネル接続がオープンされ、共有メモリが割り当てられて、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。
- 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 からのデータを待機し、その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、nbftclnt が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 は tar および bpbrm にジョブが完了したことを通知します。
- 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。

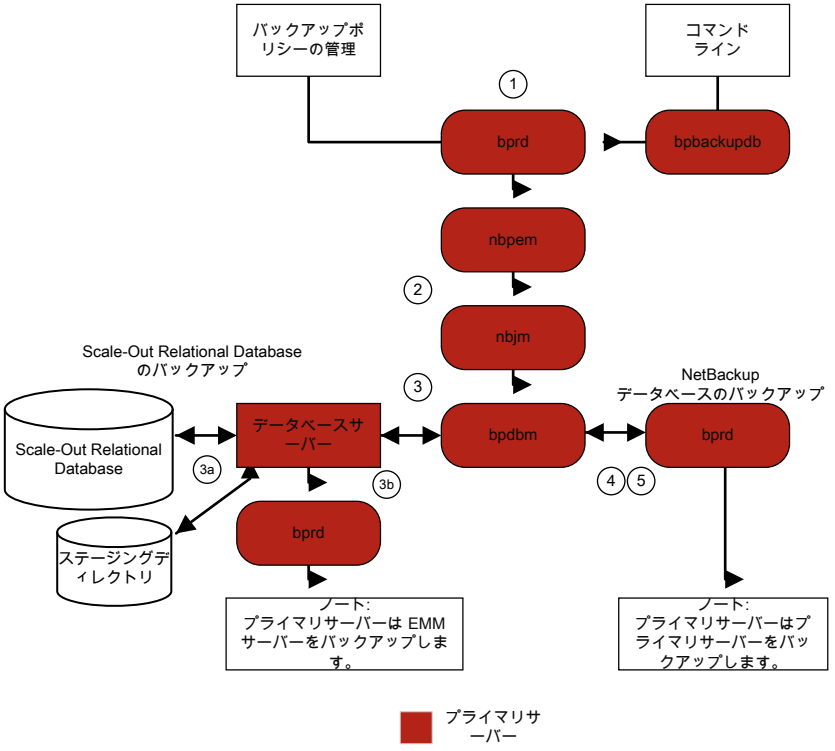
ホットカタログバックアップ

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 カタログの手動バックアップを開始できます。または、カタログが自動的にバックアップされるようにポリシーを構成できます。

図 5-3では、ホットカタログバックアップ処理が表示されます。

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。
- プライマリサーバーの 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。ステージングの前に、同じ子ジョブは次のディレクトリへの NetBackup データベースのオンラインバックアップを実行します。
  UNIX の場合: /usr/openv/db/staging
  Windows の場合: *install_path*¥NetBackupDB¥staging
- NBDB データベースのバックアップを行う子ジョブ。
  データベースがステージング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、これがバックアップされます。
- NetBackup データベースをバックアップする子ジョブ。
  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、NetBackup によってディザスタリカバリファイルが作成され、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。

- bpdbm、bpbkar、bpbrm、bpcd、bpbackup、bprd

NetBackup データベースのみに関係するメッセージについては、次のディレクトリにある bpdbm ログファイルを参照してください。

- UNIX の場合: /usr/openv/netbackup/logs/bpdbm
- Windows の場合: *install_path*¥NetBackup¥logs¥bpdbm

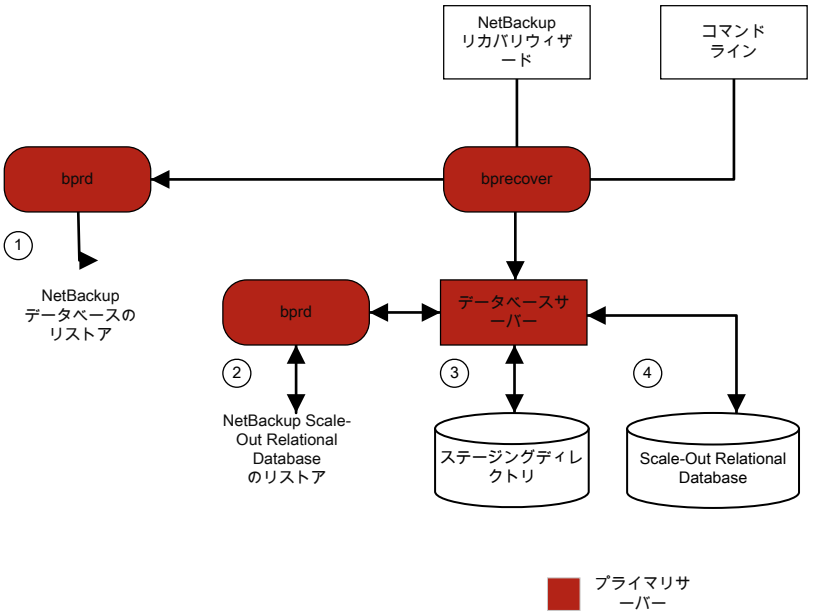
ホットカタログのリストア

カタログのリストアは、[設定 (Settings)]の[NetBackup カタログリカバリ (NetBackup catalog recovery)]オプションを使用するか、bprecover コマンドを使用して開始できます。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、プライマリサーバーの 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 データベースのリストアは、次の手順で構成されます (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 データベースは次の場所にリストアされます。
  `/usr/openv/db/staging` (UNIX) *`install_path`*`¥NetBackupDB¥staging` (Windows)
- NBDB がリカバリされます。
- NBDB データベースがステージングディレクトリからターゲットの場所に移動されます。この場所は、`VXDBMS_NB_DATA` 設定によって設定されます。(UNIX の場合 `bp.conf` ファイル内、Windows の場合対応するレジストリキー。) デフォルトの場所は `/usr/openv/db/data` と *`install_path`*`¥NetBackupDB¥data` です。
  データベースが再配置されると、ステージングディレクトリから、`vxdbms.conf` で示されるディレクトリに移動されます。
  `/usr/openv/db/data/vxdbms.conf` (UNIX)
  `install_path``¥NetBackupDB¥data¥vxdbms.conf` (Windows)

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。

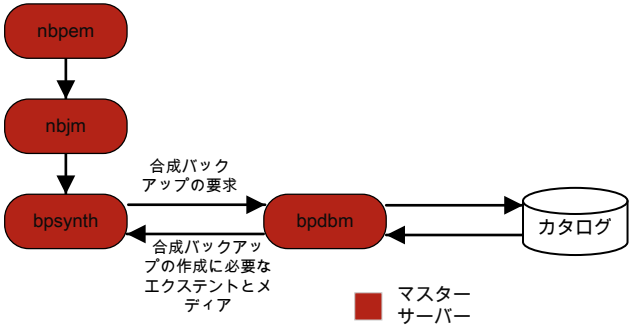
メモ: 合成アーカイブは存在しません。

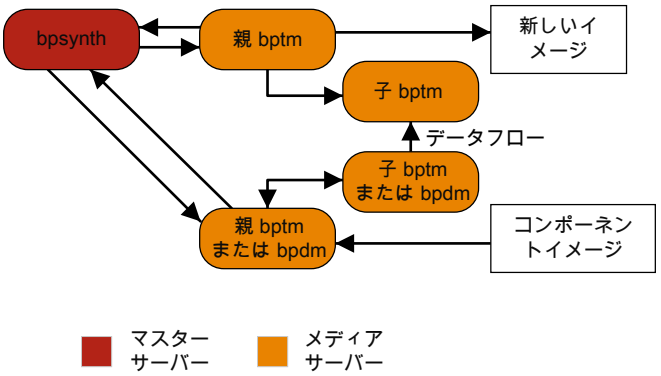
たとえば、既存の完全イメージとその後の差分増分イメージを合成して、新しい完全イメージを作成できます。以前の完全イメージと増分イメージが、コンポーネントイメージです。新しく作成された合成完全イメージは、従来の処理で作成されたバックアップと同様に動作します。またこの合成完全イメージは、最新の増分と同時期のクライアントのバックアップになります。合成イメージは、ファイルを含む最新のコンポーネントイメージから各ファイルの最新バージョンをコピーすることによって作成されます。合成バックアップは[True Image Restore]と[移動検出 (Move Detection)]オプションを選択したポリシーを使用し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。これは nbjm に要求を送信して合成バックアップを開始し、その後で nbjm がプライマリ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 情報を使用し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。(エクステントは、開始ブロック番号と、特定のコンポーネントイメージ内の連続したブロック数を示します)。エクステントのセットは、通常、新しい合成イメージに各コンポーネントイメージからコピーされます。 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。  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。
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ことが必要です。

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。次のログの形式を Cohesity テクニカルサポートに送信します。

- 統合ログ機能によって作成されるログファイル
  p.18 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.95 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

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。

p.95 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 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	プライマリ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。 *install_path*/netbackup/logs/bpsynth *install_path*/netbackup/logs/bpdbm *install_path*/netbackup/logs/vnetd
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。 *install_path*/netbackup/logs/bpcd *install_path*/netbackup/logs/bptm
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、プライマリサーバーを選択し、[グローバルログレベル (Global logging level)]を 5 に設定します。 ホストプロパティを使用して構成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。
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。

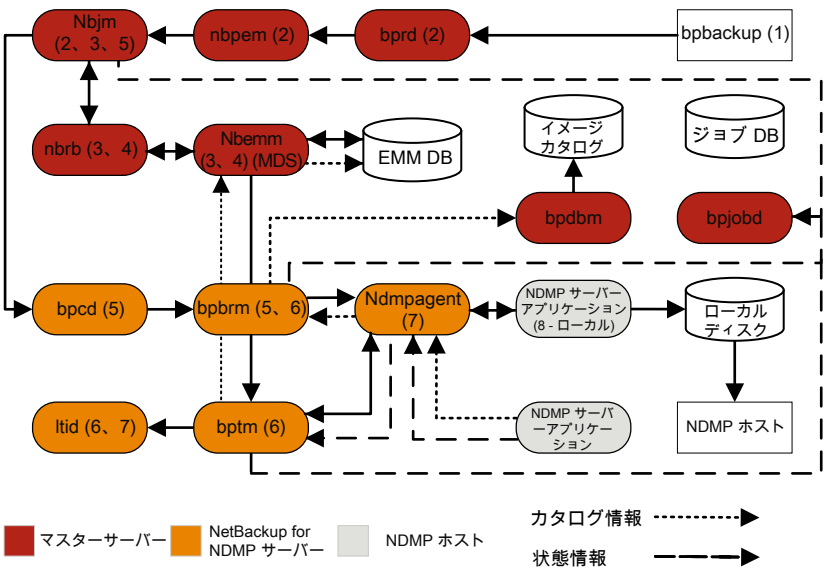
6

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

図 6-1 NDMP バックアップ処理



NDMP バックアップ操作の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 bpbackup 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、スケジュール設定されたポリシーがジョブを開始できます。
2. bpbackup 処理はプライマリサーバーに接続してバックアップ要求を作成します。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) に送信します。
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 (bpbrm) を開始します。
6. bpbrm 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用する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。

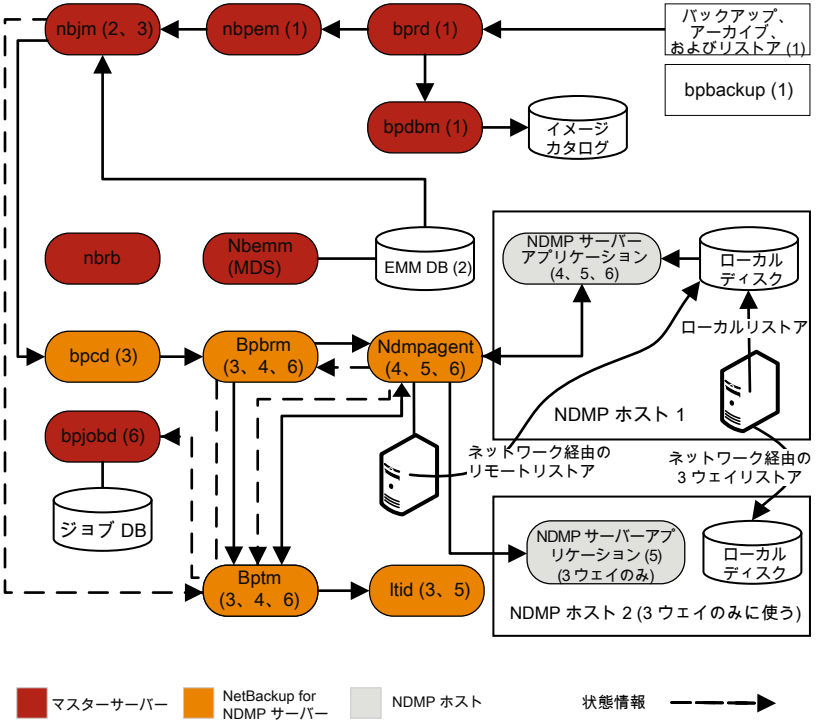
- リモートバックアップ (プロセスの流れ図には表示されない)。バックアップの書き込みに使用するデバイスは NetBackup ストレージユニットに関連付けられます。NetBackup メディアサーバーの bptm はテープドライブにテープをマウントします。NetBackup は NDMP サーバーに NDMP コマンドを送信して NDMP 以外のメディアマネージャストレージユニットのバックアップを開始します。NDMP ホストから NetBackup メディアサーバーにネットワークを経由してデータを移動すると、メディアサーバーは選択したストレージユニットにデータを書き込みます。

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 bpjobd に送信し、bpjobd はこの情報を使用して 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

図 6-2 NDMP リストア処理



NDMP リストア操作の処理手順は次のとおりです。

NDMP リストア手順

1. リストアジョブを開始するため、NetBackup のプライマリサーバーまたはメディアサーバーの管理者は、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 プライマリ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. プライマリサーバーは、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. プライマリ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 が Tape Manager プロセス (bptm) を開始して、nbjm にテープボリュームを問い合わせます。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ます。直接接続されているテープをマウントする NDMP コマンドが発行されます。その後、ltid から NDMP コマンドが送信され、要求されたテープがストレージデバイスにマウントされます。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) はプライマリサーバーにジョブの状態情報を送信します。プライマリサーバーの Jobs Database Manager (bpjobd) 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。

7

NetBackup 重複排除ログ

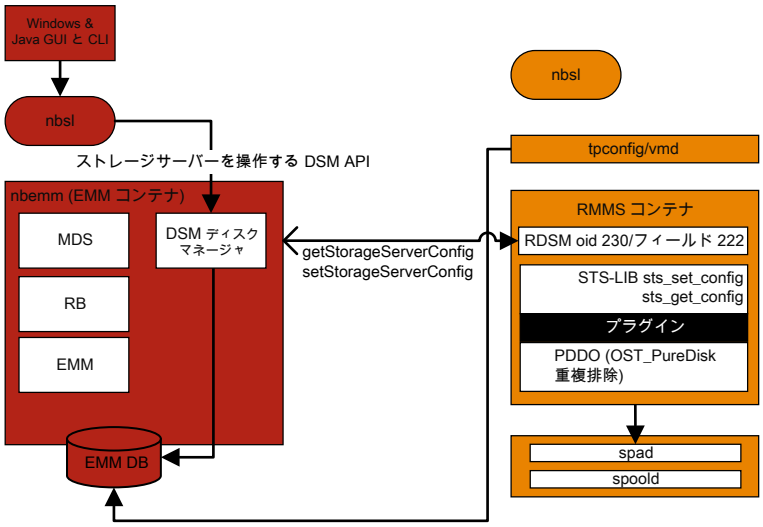
この章では以下の項目について説明しています。

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

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 は (プロキシとして bptm を使用して) NetBackup 重複排除マネージャ (spad) に接続し、spadbミニカタログにメタデータ (イメージレコード) を記録します。これは、NetBackup 重複排除エンジン (spoold) に接続し、イメージデータをデータディレクトリ (*dedup_path*¥data) の .bhd/.bin ファイルに格納します。
- 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。

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。クライアントが正しいメディアサーバーを使用し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` ログ:

   - `/usr/openv/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。
   - `bptm` のログ詳細度を 5 に設定します。メディアサーバーで[ホスト (Hosts)]、[ホストプロパティ (Host properties)]、[ログ記録 (Logging)]の順にクリックします。
   - 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`
     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。ログ情報 (PDVFS デバッグログ) は、bptm および 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 は Logging=full,thread に変更されます。
   - 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. [アクティビティモニター (Activity monitor)]>[ジョブ (Jobs)]で、ジョブの詳細を開いて[詳細 (Details)]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. 手順 3 で見つかった bptm PID をメディアサーバーの bptm ログから抽出します。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/openv/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)
- tpcommand の tpconfig 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/openv/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/openv/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
  ```

- tpcommand (...¥volmgr¥debug¥tpcommand)
- *storage_directory*¥log¥msdp-config.log

ユニバーサル共有のログ

ユニバーサル共有の設定ログを次に示します。

ストレージサーバーの場合:

- /var/log/vpfs/ia_byo_precheck.log
  インスタントアクセス自社構築 (BYO) プリコンディション検査の結果
- /var/log/vpfs/vpfs-config.log
  Velocity Provisioning File System (VPFS) の設定ログ
- /var/log/vpfs/spws/spws.log
  ストレージプラットフォーム Web サービス (spws) ログ
- /var/log/vpfs/spws_backend/spws_backend.log
  ストレージプラットフォーム Web サービス (spws) spws_backend ログ

プライマリサーバー上:

- /usr/openv/logs/nbwebservice/
  NetBackup Web サービス (nbwmc) 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

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、プライマリ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
get_plugin_version	libstspipd.dll (pdplugin バージョン)

キーワード	説明
get_agent_cfg_file_path_for_mount	PureDisk エージェントの構成ファイルを使う (.cfg のファイル名に注目)、省略名または FQDN を判断。
emmlib_NdmpUserIdQuery	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
tag_nbu_dsid 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
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

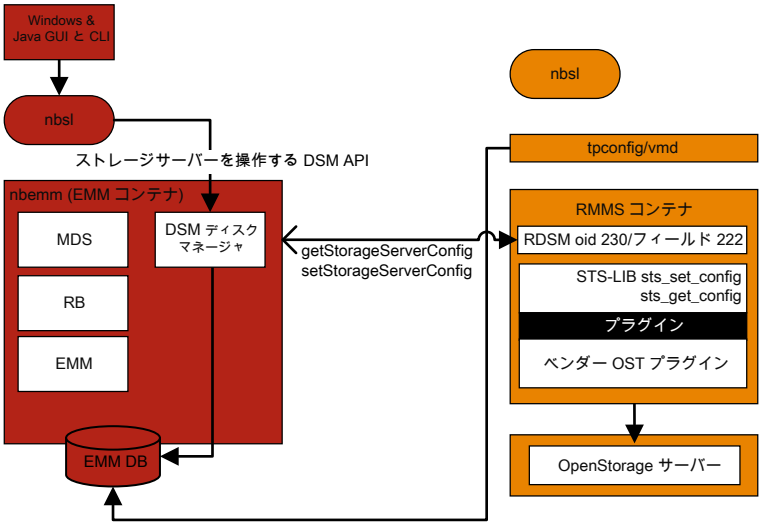
8

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

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.49 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。
5. 次のプロセスに対して DebugLevel=6 および DiagnosticLevel=6 を設定します。
   - OID 178 (ディスクマネージャサービスまたは dsm)
   - OID 202 (ストレージサービスまたは stssvc)
   - OID 220 (ディスクポーリングサービスまたは 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 または rdsm)
   - OID 395 (STS Event Manager または 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. [アクティビティモニター (Activity monitor)]>[ジョブ (Jobs)]で、ジョブの詳細を開いて[詳細 (Details)]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 および Linux の場合: `/usr/openv/netbackup/bin/admincmd/bpstsinfo -pi`
- Windows の場合: *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 および Linux の場合: `/usr/openv/netbackup/bin/admincmd/bpstsinfo -li -storage_server` *storage server name* `-stype` *OST_TYPE*
- Windows の場合: *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 および Linux の場合: `/usr/openv/netbackup/bin/admincmd/nbdevquery -liststs -stype` *OST_TYPE* `-U`
- Windows の場合: *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 および Linux の場合: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdp -stype` *OST_TYPE* `-U`
- Windows の場合: *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 および Linux の場合: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype` *OST_TYPE* `-U`
- Windows の場合: *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 および Linux の場合: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -updatedp -stype OST_TYPE -dp diskpool -M master`
- Windows の場合: `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 および Linux の場合: `/usr/openv/volmgr/bin/tpconfig -dsh -all_hosts`
- Windows の場合: `install dir¥volmgr¥bin¥tpconfig -dsh -all_hosts`

9

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) 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。ベリタスは、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。

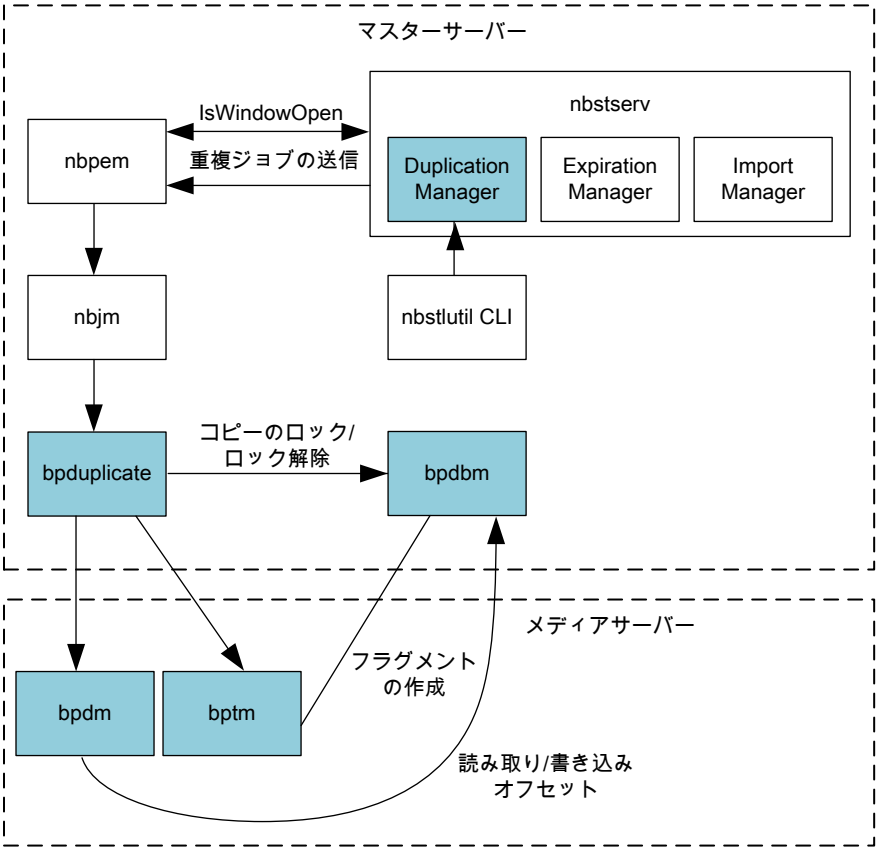
ストレージライフサイクルポリシー (SLP) の操作 (バックアップ、複製、レプリケーション、インポート、スナップショットなど) について理解することは、問題のトラブルシューティングに役立つログを判断するために役立ちます。このトピックでは、主に自動イメージレプリケーション (A.I.R.) と複製のプロセスフローに焦点を当てます。バックアップやスナップショットなどの他の操作のプロセスフローについては、このガイドの他のトピックで説明しています。

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。

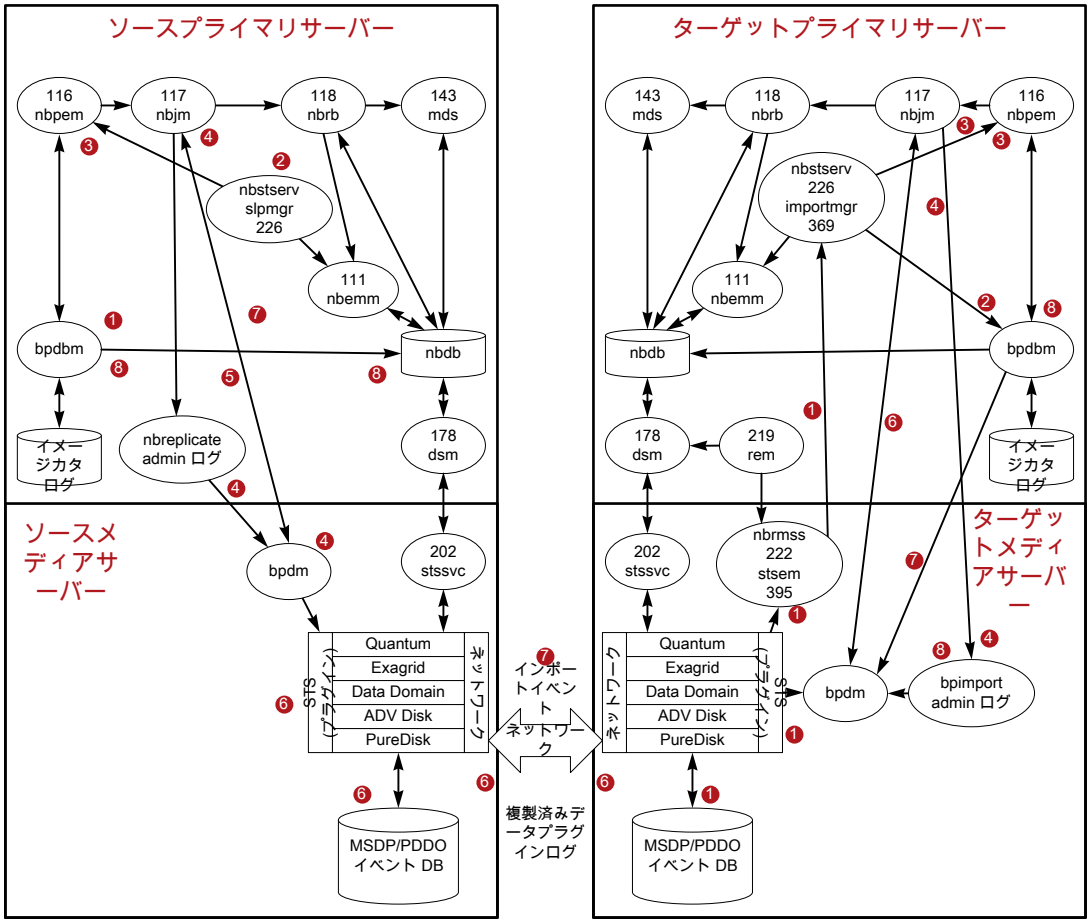
1. SLP マネージャ (nbstserv) が、複製ジョブを送信するために複製ウィンドウが開いているかどうかを確認します。複製ジョブを送信するために開いている SLP ウィンドウが見つかると、SLP ポリシーによって管理されている関連イメージの処理とバッチ処理が行われ、さらに処理するために nbpem に送信されます。
2. nbpem も、複製操作のために SLP ウィンドウがまだ開いているかどうかを確認します。ウィンドウが開いている場合、nbpem は複製ジョブ構造を作成して nbjm に送信します。
3. nbjm がバックアップ用のリソースを要求して (図には示されていません)、bpduplicate 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 nbpem にバッチを送信します。nbpemは、nbrb と nbemm からのリソースを確認する nbjm にジョブを渡します。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 ログに記録され)、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チェックが実行され、レプリケーションを開始します。bpdm はレプリケーションを開始するタイミングをソースストレージサーバーに通知します。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、プライマリサーバー上の (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て、要求を nbpem に送信します。nbpem は nbjm にジョブを渡してから、nbrb と nbemm からのリソースを確認します。
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、その情報をプライマリサーバーの bpdbm に送信します。
8. イメージのインポートが完了し、bpdbm により検証されます。

SLP および A.I.R. のログ記録

nbstserv (プライマリサーバー):

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

importmgr (プライマリサーバー、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。

プライマリサーバーでは、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 コマンドをプライマリ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`

A.I.R. を使用して (ソースプライマリサーバー上で) レプリケート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 repllist
```

ターゲット環境への A.I.R. のインポートが (ターゲットプライマリサーバー上で) 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
```

10

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 の安全な通信ログ記録について

NetBackup は、NetBackup ホスト間における制御型機能の安全な通信に関する情報をログに記録します。これらの機能には、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プロセスの起動が含まれます。現在、これらのプロセスに `bpbkar` または `tar` データ転送は含まれません。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。

プライマリサーバーは CA として動作します。プライマリサーバーは、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。

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、NetBackup 証明書が配備されます。証明書の配備が失敗した場合、バックアップとリストアは実行できません。次の場合に配備が失敗します。

- pbx、nbatd、または nbwmc プロセスがプライマリサーバーで実行されていない。
- インストールまたはアップグレード中に、ホストがプライマリサーバーから CA 証明書とホスト ID ベースの証明書の両方を取得できない。

安全な通信や証明書に関する問題を診断するとき、通常、プライマリ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、問題を特定するためにログファイルが役立つ場合があります。

Tomcat のログ記録

Tomcat ログファイルは、次の場所にあります (プライマリ サーバー上のみ)。

UNIX の場合: `usr/openv/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 (プライマリサーバー上のみ)。

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

Windows の場合: *install path*¥netbackup¥logs¥nbwebservice

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	nbwebservice¥nbwebservice	NetBackup Web サービス
466	nbwebservice¥security	NetBackup セキュリティサービス (セキュリティ Web アプリ)
482	nbwebservice¥hosts	NetBackup ホスト Web サービス (ホスト Web アプリ)
483	nbwebservice¥nbconfigmgmt	NetBackup 構成管理サービス (Web アプリ)
484	nbwebservice¥nbgateway	NetBackup ゲートウェイサービス (Web アプリ)
485	nbwebservice¥nbwss	NetBackup WebSocket サービス (NBWSS) (Web アプリ)
487	nbwebservice¥nbcatalogws	NetBackup カタログ Web サービス (Web アプリ)
488	nbwebservice¥nbrbac	NetBackup の役割に基づくアクセス制御 (RBAC) Web サービス (Web アプリ)
489	nbwebservice¥nbadminws	NetBackup 管理 Web サービス (Web アプリ)
495	nbwebservice¥nbwebservice	NetBackup Web API

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なことがあります。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.127 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 (任意のプライマリ、メディア、またはクライアントサーバ

UNIX の場合: /usr/openv/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、問題を解決するために、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、すべてのプライマリ、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プライマリ、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 やプライマリサーバー上など、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.169 の「NetBackup 管理コンソール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、プライマリサーバーでのみ発生します。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。AT ログが有効な場合に、NetBackup 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 (プライマリサーバー上のみ)。

UNIX の場合: `/usr/openv/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/openv/netbackup/sec/at/bin/vssat setloglevel -l 4 -f /usr/openv/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¥NetBackup¥sec¥at¥bin¥vssat setloglevel -l 4
  -f install_path¥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/openv/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¥NetBackup¥sec¥at¥bin¥vssat setloglevel -l 0
```

FIPS モードで vssat コマンドを実行するには、-F, --enable_fips オプションを使用します。デフォルトでは、FIPS モードは無効になっています。

UNIX の場合に FIPS モードでの vssat のログ作成を無効にするには、次のコマンドを使用します。

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

Windows の場合に FIPS モードでの vssat のログ作成を無効にするには、次のコマンドを使用します。

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

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、プライマリ、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/openv/logs/nbpxyhelper

UNIX の起動とシャットダウンの問題の場合: /usr/openv/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/TSL 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/openv/netbackup/bin/vnetd -proxy inbound_proxy -number 0

/usr/openv/netbackup/bin/vnetd -proxy outbound_proxy -number 0

/usr/openv/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

プライマリ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。ログファイルのサイズと数を、51,200 KB ごとにログファイル 5 つ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。

PBX のログは、すべてのプライマリ、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/VRTSpbx/log`

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

ログファイルの最大サイズと数を増やす方法

1. ログの最大サイズとログファイル数を増やすには、次のコマンドを実行します。

   次の例では、10 個のログファイルが最大サイズ 102,400 KB で作成されます。

   Windows の場合:

```
C:¥Program Files (x86)¥VERITAS¥VxPBX¥bin¥vxlogcfg -a -p 50936 -s
"MaxLogFileSizeKB=102400" -o 103

C:¥Program Files (x86)¥VERITAS¥VxPBX¥bin¥¥vxlogcfg -a -p 50936 -s
"NumberOfLogFiles=10" -o 103
```

   UNIX の場合:

```
/opt/VRTSpbx/bin/vxlogcfg -a -p 50936 -s "MaxLogFileSizeKB=102400" -o 103
/opt/VRTSpbx/bin/vxlogcfg -a -p 50936 -s "NumberOfLogFiles=10" -o 103
```

2. PBX ログディレクトリを開きます。

   UNIX の場合: /opt/VRTSpbx/log

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

3. ログファイルのサイズが増えて 51,200 KB を超えたかどうかを確認します。
4. PBX のログ設定を確認します。

   Windows の場合:

   HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Veritas¥VxICS¥logcfg¥103

   UNIX の場合:

   - ディレクトリ /etc/vx/VxICS に移動します。
   - 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。

   例:

```
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/VRTSpbx/
103.L10nResourceDir=/opt/VRTSpbx/resources
```

```
103.L10nLib=/optVRTSpbx/lib/libvxexticu.so.3
103.L10nResource=VxPBX
103.MaxLogFileSizeKB=102400
103.RolloverMode=FileSize
103.NumberOfLogFiles=10
103.LogRecycle=true
```

11

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

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 プライマリ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 Request デーモン (bprd) がバックアップ要求を NetBackup Policy Execution Manager (nbpem) に送信します。nbpem はポリシー構成を処理します。
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ます。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プライマリサーバーにコピーします。
8. bpfis は、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。
9. 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。
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、プライマリサーバー上の NetBackup ファイルデータベース (bpdbm) 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。

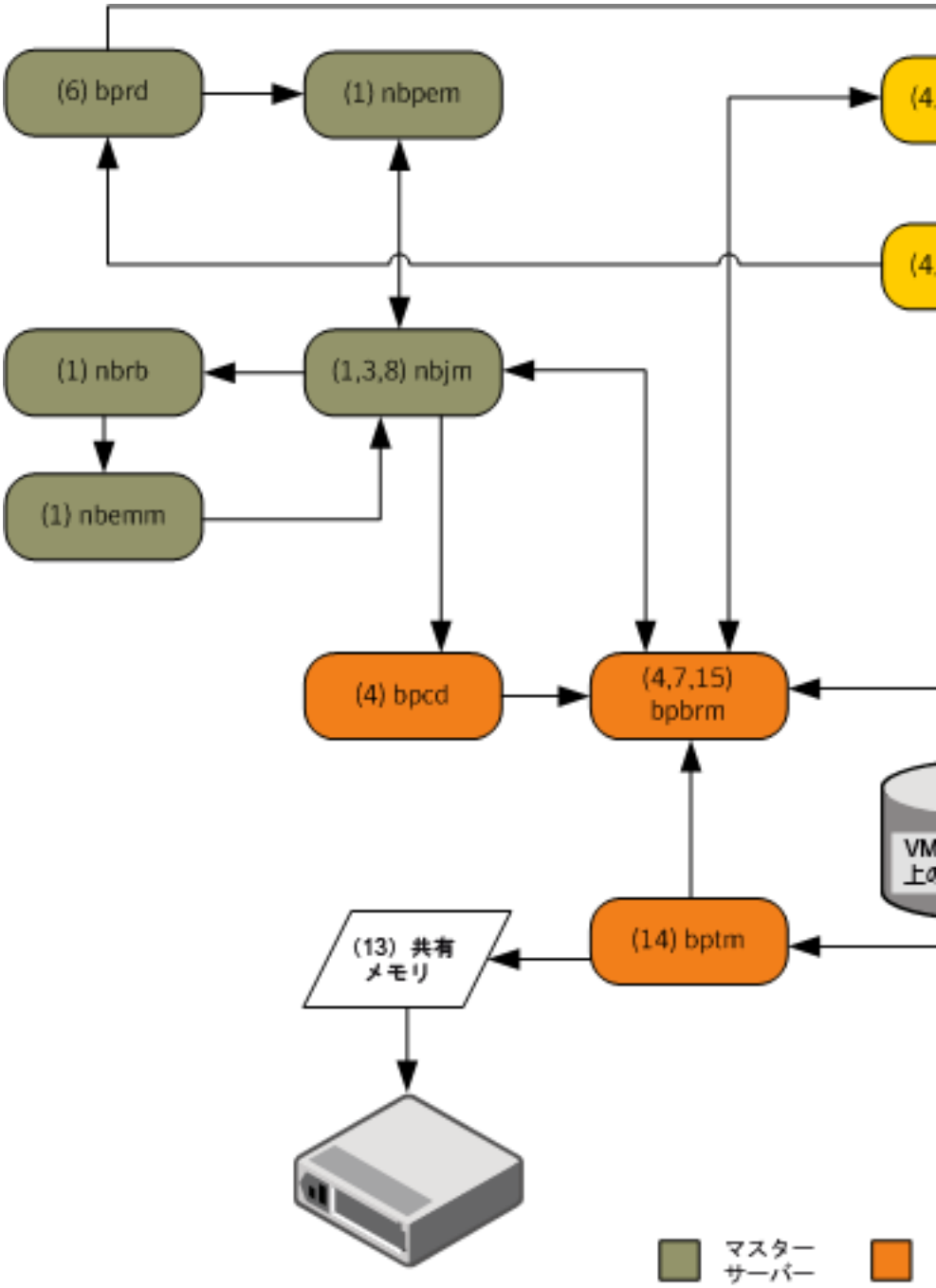
13 元の bptm プロセスによって、バックアップイメージが共有メモリから取り出され、ストレージデバイス (ディスクまたはテープ) に送信されます。

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。

VMware バックアップ

次に、VMware バックアップ処理を示します。


(6) bprd
(1) nbpem
(1) nbrb
(1,3,8) nbjm
(1) nbemm
(4) bpcd
(4,7,15)
bpbrm
(14) bptm
(13) 共有
メモリ
マスター
サーバー

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上でクライアントサービス (bpbrm) を介して bpcd のインスタンスを開始します。bpbrm は、VMware バックアップホスト上でクライアントサービス (bpcd) を使用して、Frozen Image Snapshot (bpfis) のスナップショットを開始します。bpfis は、構成済みのクレデンシャルクレデンシャルサーバーに応じて vCenter または ESX ホストを使用することで、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することで VIP の並行スナップショット数を制御できます。bpfis は、標準の SSL ポート (デフォルトは 443) を使用することで vSphere ホストと通信します。

5. bpfis は Request Manager (bprd) に接続して VMware バックアップホストからプライマリサーバーに 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、各状態ファイルを VMware バックアップホストからプライマリ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 にレポートします。nbjm から nbpem に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 bpbrm 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 (Cohesity 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ピングし、vmdk ファイルの内容を識別します。bpbkar は VxMS を使用してファイルカタログ情報を bpbrm に送信し、ここを中継してプライマリサーバーのデータベースマネージャ bpdbm にこの情報を送信します。

11 bpbrm 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 V-Ray 操作を示します。

- VxMS 内で 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処理中に実行されます。メディアサーバーの bpbrm では、このカタログ情報がプライマリサーバーに送信されます。
- 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。

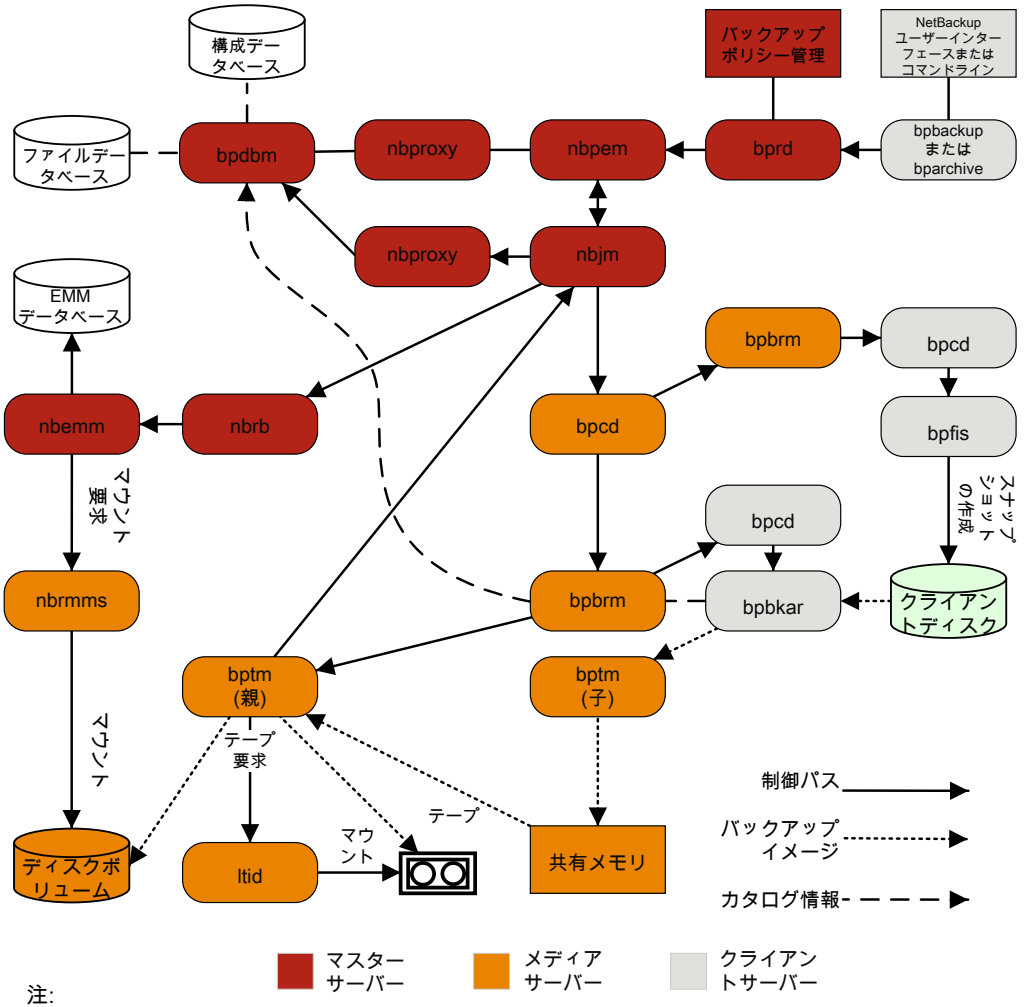
14 bptm は bpbrm にバックアップの完了状態を送信し、bpbrm から nbjmと nbpem に完了状態が渡されます。

15 nbpem は、スナップショットを削除するよう nbjm に通知します。nbjm は、メディアサーバーで bpbrm の新しいインスタンスを起動し、bpbrm は、VMware バックアップホストで bpfis の新しいインスタンスを起動します。bpfis は、vSphere 環境のスナップショットを削除します。bpfis と bpbrm は状態を報告して終了します。

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 プライマリ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 NetBackup Policy Execution Manager nbpem にバックアップ要求が送信されます。nbpem はポリシー構成を処理します。
- 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 bpbrm を介して bpcd 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 bpfis を介して bpcd 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 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、プライマリサーバー上の NetBackup ファイルデータベース bpdbm 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 bpbkar 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、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 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 Manager for Data Center 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。

12

ログの特定

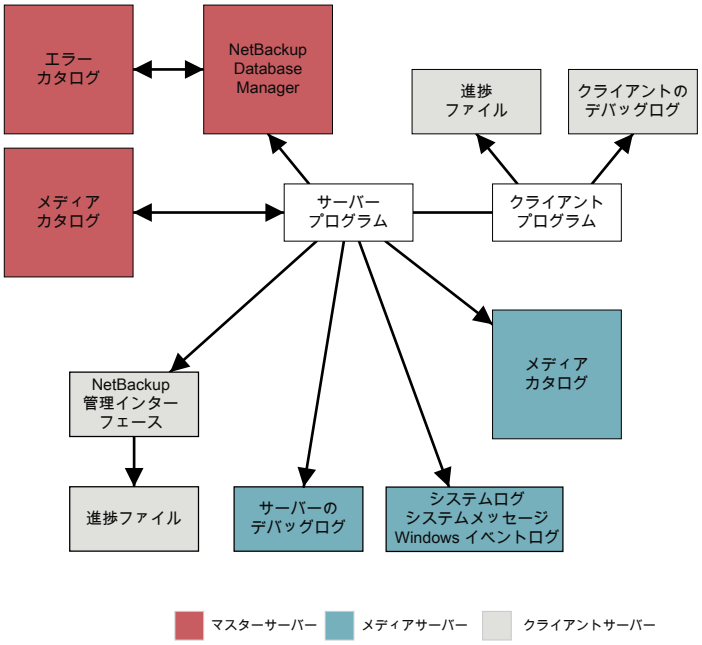
この章では以下の項目について説明しています。

- nbpem のログ
- nbproxy のログ
- nbrb のログ
- NetBackup Vault 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 txxcd のログ
- vnetd のログ

NetBackup ログの場所とプロセスの概要

図 12-1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 12-1 NetBackup エンタープライズシステムで利用可能なログ



NetBackup の各種レポートを利用し、ジョブアクティビティとメディアに関する情報を多種多様に表示できます。現在、[すべてのログエントリ (All log entries)]レポートのみを NetBackup Web UI で利用できます。その他のレポートは、NetBackup 管理コンソールで利用可能です。詳しくは『NetBackup 管理者ガイド Vol. 1』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。

acsssi のログ

UNIX システムでは、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	/usr/openv/volmgr/debug/acsssi
ログが存在するサーバー	メディア
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bpbackup /usr/openv/netbackup/logs/bpbackup
ログが存在するサーバー	クライアント
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bpbkar /usr/openv/netbackup/logs/bpbkar
ログが存在するサーバー	クライアント
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bpbrm /usr/openv/netbackup/logs/bpbrm
ログが存在するサーバー	メディア
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bpcd
	/usr/openv/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
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bpcompatd
	/usr/openv/netbackup/logs/bpcompatd
ログが存在するサーバー	プライマリ
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bpdbm
	/usr/openv/netbackup/logs/bpdbm
ログが存在するサーバー	プライマリ
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bpjobd /usr/openv/netbackup/logs/bpjobd
ログが存在するサーバー	プライマリ
ログ方式	レガシー

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	*install_path*¥NetBackup¥logs¥bprd /usr/openv/netbackup/logs/bprd
ログが存在するサーバー	プライマリ
ログ方式	レガシー

bprdproxy のログ

bprdproxy デーモンは、bprd と nbpem の中間のデーモンとして機能します。bprd 要求を nbpem にプロキシします。同様に、nbpem の応答を bprd に変換します。

ログの場所	*install_path*¥NetBackup¥logs¥bprdproxy /usr/openv/logs/bprdproxy
ログが存在するサーバー	プライマリ
ログ方式	統合

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。これは、プライマリサーバー上で bprd と通信します。

ログの場所	*install_path*¥NetBackup¥logs¥bprestore /usr/openv/netbackup/logs/bprestore
ログが存在するサーバー	クライアント

ログ方式	レガシー

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。コマンドで実行し 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	*install_path*¥Cohesity¥NetBackup¥logs¥nbutils /usr/openv/logs/nbutils
ログが存在するサーバー	プライマリ、クライアント、およびメディア
ログ方式	統合

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	*install_path*¥NetBackup¥logs¥bptm /usr/openv/netbackup/logs/bptm
ログが存在するサーバー	メディア
ログ方式	レガシー

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	*install_path*¥Volmgr¥debug¥daemon /usr/openv/volmgr/debug/daemon

ログが存在するサーバー	プライマリおよびメディア
ログ方式	レガシー

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 とも呼ばれ、テープの予約と割り当てを制御します。

ログの場所	*install_path*¥volmgr¥debug¥ltid /usr/openv/volmgr/debug/ltid
ログが存在するサーバー	メディア
ログ方式	レガシー

nbemm のログ

プライマリ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 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。nbrb

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/openv/volmgr/debug/vmscd

ログの場所	*install_path*¥NetBackup¥logs¥nbemm /usr/openv/logs/nbemm
ログが存在するサーバー	プライマリ
ログ方式	統合

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 bpjobd と通信し、必要に応じて bpbrm 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	*install_path*¥NetBackup¥logs¥nbjm
	/usr/openv/logs/nbjm
ログが存在するサーバー	プライマリ
ログ方式	統合

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	*install_path*¥NetBackup¥logs¥nbpem
	/usr/openv/logs/nbpem
ログが存在するサーバー	プライマリ
ログ方式	統合

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、プライマリサーバーのカタログに問い合わせます。

ログの場所	*install_path*¥NetBackup¥logs¥nbproxy
	/usr/openv/netbackup/logs/nbproxy
ログが存在するサーバー	プライマリ
ログ方式	レガシー

nbrb のログ

プライマリサーバーで、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	*install_path*¥NetBackup¥logs¥nbrb
	/usr/openv/logs/nbrb

ログが存在するサーバー	プライマリ
ログ方式	統合

NetBackup Vault のログ

Vault セッションディレクトリは、次の場所に存在します。

install_path¥NetBackup¥vault¥sessions¥vaultname¥*session_x*

ここで、*session_x* はセッション番号を示します。このディレクトリには、Vault ログファイル、一時作業ファイルおよびレポートファイルが格納されます。

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。

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* *install_path*¥NetBackup¥wmc¥webserver¥logs /usr/openv/wmc/webserver/logs *Web アプリケーションのログ* *install_path*¥NetBackup¥logs¥nbwebservice /usr/openv/logs/nbwebservice
ログが存在するサーバー	プライマリ
ログ方式	統合 NetBackup Web サーバーフレームワークは、標準の VxUL 形式を使いません。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。

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	*install_path*¥NetBackup¥logs¥nbatd *install_path*¥NetBackup¥logs¥nbcert C:¥ProgramData¥Cohesity¥NetBackup¥InstallLogs¥WMC_configureCerts_*yyyymmdd_timestamp*.txt /usr/openv/logs/nbatd /usr/openv/netbackup/logs/nbcert /usr/openv/wmc/webserver/logs/configureCerts.log
ログが存在するサーバー	プライマリ
ログ方式	nbatd ログは、統合ログを使用します。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。

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	*install_path*¥NetBackup¥logs¥nbatd *install_path*¥NetBackup¥logs¥nbwebservice C:¥ProgramData¥Cohesity¥NetBackup¥InstallLogs¥WMC_configureCerts_*yyyymmdd_timestamp*.txt /usr/openv/logs/nbatd /usr/openv/logs/nbwebservice /usr/openv/wmc/webserver/logs/configureCerts.log
ログが存在するサーバー	プライマリ
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。configureCerts.log は VxUL ではなく簡易的なログのスタイルを使います。

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

ログの場所	*install_path*¥VxPBX¥log /opt/VRTSpbx/log
ログが存在するサーバー	プライマリ、メディア、およびクライアント
ログ方式	統合 PBX のログを表示するには、PBX のプロダクト ID 50936 を使用する必要があります。root または管理者権限も必要です。

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。

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	*install_path*¥Volmgr¥debug¥reqlib¥ /usr/openv/volmgr/debug/reqlib
ログが存在するサーバー	プライマリおよびメディア
ログ方式	レガシー

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	*install_path*¥volmgr¥debug¥robots /usr/openv/volmgr/debug/robots
ログが存在するサーバー	メディア
ログ方式	レガシー

p.154 の「txxd および txxcd のログ」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	*install_path*¥NetBackup¥logs¥tar /usr/openv/netbackup/logs/tar
ログが存在するサーバー	クライアント
ログ方式	レガシー

p.81 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.52 の「syslogd を使用した UNIX のログ記録」を参照してください。 p.52 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。 p.153 の「robots のログ」を参照してください。
ログ方式	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.49 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。

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	*install_path*¥NetBackup¥logs¥vnetd /usr/openv/logs/vnetd または /usr/openv/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/openv/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	プライマリ、メディア、およびクライアント
ログ方式	レガシー

13

ログ収集ユーティリティの使用

この章では以下の項目について説明しています。

ログ収集ユーティリティについて

ログ収集ユーティリティは、デバッグログやその他の情報を収集するために必要な時間を短縮できる有用なツールです。

ログ収集ユーティリティは、デバッグログやその他の情報を設定および収集するために必要な時間を短縮できる有用なツールです。このユーティリティは、多くの機能を自動で実行するため、NetBackup ホストへの手動ログイン、ログディレクトリの作成、ログレベルの変更などに関連した問題を回避できます。

制限事項

ログ収集ユーティリティでは、次の制限事項に注意してください。

- ログ収集ユーティリティでは、Cloud Scale 環境がサポートされていません。
- NetBackup は、NetBackup クライアントがインストールされていないエージェントレスホストからログを収集しません。たとえば、VMware、クラウドオブジェクトストア、DBPaaS、BigData 作業負荷、NetBackup Snapshot Manager やマルウェアスキャンホストに対して使用されるエージェントレスホストです。ただし、「バックアップホスト」

や「アクセスホスト」など、バックアップに使用するサーバーまたはホストとして指定されたホストのログは利用できます。

- NetBackup では、マルウェアスキャンジョブのログは収集されません。ログはプライマリサーバー (選択されている場合) または選択したメディアサーバーからのみ収集され、クライアントからは収集されません。
- NetBackup Web UI では、Web UI のログレコードのみを利用できます。Alta View と管理コンソールのログレコードは、NetBackup Web UI には表示されません。

要件

ログ収集ユーティリティを使用する場合は、次の要件と操作上の注意事項に留意してください。

- ログ収集ユーティリティは、Cohesity Technical Support の指示に従って使用してください。
- ログ収集ユーティリティを使用するには、RBAC 管理者の役割が必要です。または、ログを収集する権限を持つ役割が必要です。特定のジョブのログを収集するには、ジョブを表示する権限も必要になります。
  p.157 の「ログ収集管理者向けの RBAC の役割の構成」を参照してください。
- 一度に収集できるログは 1 つのログレコードのみです。別のログ収集プロセスが実行されている場合、そのプロセスが終了するまで待機してください。その後、別のログレコードを選択し、[ログの収集 (Collect logs)]を選択できます。
- NetBackup11.1 では、NetBackup でログディレクトリの作成やログレベルの詳細度の調整は行われません。

ログ収集管理者向けの RBAC の役割の構成

NetBackup では、役割ベースのアクセス制御 (RBAC) を使用して、どのユーザーがログ収集を実行できるかを制御できます。管理者の役割を持つすべての NetBackup に対して、RBAC アクセス権を付与できます。または、ログ収集操作のみを許可するカスタム役割を作成し、ユーザーが特定のジョブのログを収集できるように、必要に応じてジョブの表示を許可できます。

次の点に注意してください。

- RBAC の役割を作成するには、RBAC 管理者の役割、または役割を作成する権限が必要です。
- 役割の作成と役割のユーザーへの追加については、NetBackup 管理者にお問い合わせください。

RBAC の権限とデフォルトの役割について詳しくは、NetBackup API のマニュアル (http://sort.veritas.com/) を参照してください。

ログ収集管理者用のカスタム役割の作成

カスタム役割を使用すると、ログ収集管理者が、アクセス制限付きで NetBackup Web UI にサインインできます。管理者に RBAC 管理者の役割は必要ない場合、この役割を使用します。このカスタム役割が割り当てられたこの種類の管理者は、ログ収集処理と、(必要に応じて) 特定のジョブのログを収集できるよう、アクティビティモニターおよび NetBackup ジョブの表示のみを行うことができます。

ログ収集管理者用にカスタム役割を作成するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]を選択します。
2. [カスタム役割 (Custom role)]を選択し、[次へ (Next)]をクリックします。
3. [役割名 (Role name)]と説明を指定します。

   たとえば、管理者にログ収集の実行を許可する役割であることを示す説明を含めます。
4. [アクセス権 (Permissions)]で、[割り当て (Assign)]を選択します。
5. [グローバル (Global)]タブで[NetBackup の管理 (NetBackup management)]を展開します。
6. (オプション) [ジョブ (Jobs)]に移動します。[表示 (View)]を選択します。

   アクティビティモニターでジョブを表示したり、特定のジョブのログを収集したりするには、ユーザーにこの権限を割り当てる必要があります。
7. [トラブルシューティング (Troubleshooting)]、[ログの収集 (Log collection)]の順に移動します。
8. [表示 (View)]、[削除 (Delete)]、[ログの管理 (Manage logs)]を選択します。

   [表示 (View)]権限では、ユーザーはログをダウンロードすることもできることに注意してください。
9. [割り当て (Assign)]を選択します。
10. [ユーザー (Users)]で、[割り当て (Assign)]を選択します。次に、この RBAC の役割を付与するユーザーを追加します。
11. [割り当て (Assign)]を選択します。
12. 役割の構成が完了したら、[役割の追加 (Add role)]を選択します。

レコードの追加とログの収集

ログ収集ユーティリティを使用して、Cohesity Technical Support に対する新しいログレコードを追加し、ログを収集します。すでにレコードを作成しており、追加情報を収集する場合は、同じサポート ID を使用して新しいレコードを作成します。

メモ: 選択したホストのそれぞれに、選択したデバッグログに使用できる容量が十分にあることを確認してください。

レコードを追加して、ログを収集する方法

1. Cohesity Technical Support にログファイルをアップロードする場合は、サポートケース ID が必要です。Cohesity Technical Support に連絡してサポートケースを開設してください。
2. NetBackup Web UI を開きます。
3. 次のオプションから選択します。
   - アクティビティモニターで特定のジョブのログを収集します。
     [ジョブ (Jobs)]タブでジョブを選択してから、[ログの収集 (Collect logs)]を選択します。
   - ログ収集ユーティリティで新しいログレコードを作成します。
     右上で[ヘルプ (Help)]、[ログの収集 (Log collection)]の順に選択します。次に、[レコードの追加 (Add record)]または[新しいレコードの追加 (Add new record)] を選択します。
4. (オプション)[ジョブ ID (Job ID)]を指定します。

   アクティビティモニターからログを収集することを選択すると、このジョブ ID が自動的に入力されます。

   ジョブ ID を追加して、その ID のホストおよびログが NetBackup で自動的に選択されるようにします。

   次の場合は、ジョブ ID を指定しないでください。
   - 問題が特定の NetBackup ジョブとは関係ない場合。
   - 有効にするホストがすでに分かっている場合。
5. (オプション)[サポートケース ID (Support Case ID)]を指定します。
6. (オプション) ログの記録の説明を入力します。
7. [次へ (Next)]を選択します。
8. データ収集オプションのいずれかを選択します。
   - NBSU 診断情報とデバッグログの両方の収集
   - NBSU 診デバッグログの収集断情報の収集
   - デバッグログの収集

9 (該当する場合)[デバッグログの収集 (Collect debug logs)]を選択した場合、ログを収集する日時を選択します。

ジョブ ID を指定しなかった場合、日時はデフォルトで過去 24 時間になります。ジョブ ID を指定した場合、日時にはジョブが実行された時間が反映されます。

10 次の 1 つ以上を実行します。

ジョブ ID を追加した場合、その ID のホストおよびログが NetBackup で自動的に選択されます。

- [プライマリサーバーのログの収集 (Collect logs for primary server)]を選択して、プライマリサーバーのログを収集します。
- [メディアサーバー (Media Servers)]に移動し、メディアサーバーを追加します。
- [クライアント (Clients)]に移動し、クライアントを追加します。

11 [次へ (Next)]を選択します。

12 ログ収集の構成の詳細を確認します。

ページの上部には、NetBackup がログを保存する場所が表示されます。

13 [収集 (Collect)]を選択します。

NetBackup では、指定したジョブ ID または条件に従ってログが収集されます。

14 Cohesity Technical Support に送信する情報を確認します。

15 [ログの収集 (Log collection)]ページで、作成したログレコードを見つけます。[収集状態 (Collection Status)]列に進捗状況が表示されます。

16 ログ収集が完了したら、処理を続行してログをダウンロードします。

p.161 の「ログレコードのログのダウンロード」を参照してください。

ログレコードとログ収集状態の表示

作成したログレコードと、(該当する場合) 各レコードのログ収集状態を表示できます。状態が[未開始 (Not Started)]のログレコードでは、ログ収集が自動的に開始されないことに注意してください。進行中のログ収集が完了したら、手動で [処理 (Actions)]、[収集 (Collect)]の順に選択して、そのレコードの収集を開始する必要があります。

ログレコードとログ収集状態を表示する方法

1. NetBackup Web UI を開きます。
2. 右上で[ヘルプ (Help)]、[ログの収集 (Log collection)]の順に選択します。
3. ログレコードのリンクを見つけて選択します。

   値は[ID] と[説明 (description)]列で検索できます。

   レコードについての追加の詳細を表示するには、[詳細 (More)]を選択します。[進捗ログ (Progress log)]セクションには、ログ収集プロセスの詳細が表示されます。

ログレコードのログのダウンロード

ログレコードのログ収集が完了したら、ログをダウンロードし、それらのログを Cohesity Technical Support にアップロードできます。

ログレコードのログをダウンロードする方法

1. NetBackup Web UI を開きます。
2. 右上で[ヘルプ (Help)]、[ログの収集 (Log collection)]の順に選択します。
3. ログレコードを見つけて選択します。
4. [ダウンロード (Download)]を選択します。

   NetBackup で、選択したホストのログ収集情報を含むアーカイブファイルが作成されます。選択する収集オプションに応じて、アーカイブファイルには `nbsu` 情報、デバッグログ情報、またはその両方が含まれます。

ログレコードの削除

不要になったログレコードと収集した証拠を削除できます。

ログレコードを削除する方法

1. NetBackup Web UI を開きます。
2. 右上で[ヘルプ (Help)]、[ログの収集 (Log collection)]の順に選択します。
3. レコードを見つけて、[処理 (Actions)]、[レコードの削除 (Delete record)]の順に選択します。

NetBackup で、プライマリサーバー上のレコードと関連する証拠が削除されます。

14

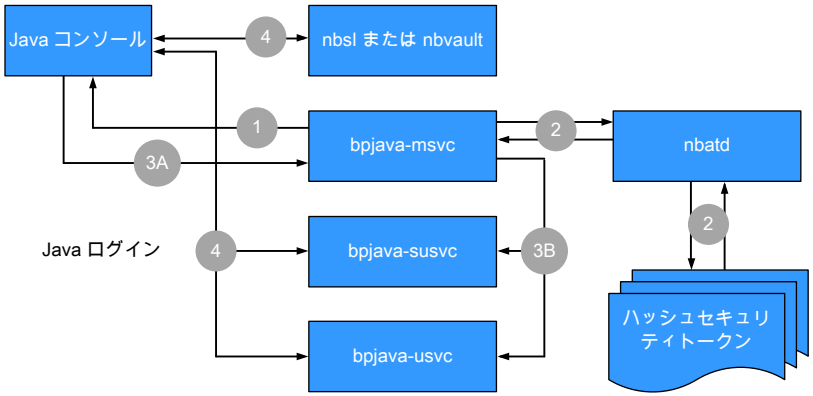
NetBackup 管理コンソールのログ記録

この章では以下の項目について説明しています。

NetBackup 管理コンソールのログ記録プロセスフロー

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。

NetBackup 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、NetBackup 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 NetBackup 管理コンソールへのログイン要求を開始します。クレデンシャルは、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 `bjava-usvc`
4. NetBackup 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。

NetBackup 管理コンソールの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、認証サービスとユーザーサービスがある、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。ログオン要求が認証サービスに

送信されます。ユーザー名とパスワードが有効である場合、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。

表 14-1に、NetBackup 管理コンソールの詳細なデバッグログの作成方法を示します。

表 14-1　詳細なデバッグログの有効化

手順	説明
手順 1	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 (認証サービス) ■ bpjava-susvc (サーバー上のユーザーサービス) ■ bpjava-usvc (クライアント上のユーザーサービス) 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/openv/netbackup/logs (UNIX の場合)
手順 2	Debug.properties ファイルに次の行を追加します。 debugMask=0x00040000 UNIX の場合、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。 NetBackup リモート管理コンソールを使用する場合、次の場所でファイルを変更します。 /usr/openv/java *install_path*¥VERITAS¥java
手順 3	リモート管理コンソールを使用している場合、次のファイルに出力をリダイレクトするように nbjava.bat を編集します。 *install_path*¥VERITAS¥java¥nbjava.bat

NetBackup 管理コンソールと bpjava-* 間のセキュアなチャネルの設定

次の手順では、NetBackup 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、管理者の制御プロセスである 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 のプロセスが使用されます。

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 を介してクレデンシャルが 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クレデンシャル情報を使用し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 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。NetBackup 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用します。このコンソールは、bpjava-*usvc プロセスへの接続時にクレデンシャルを使用しません。NetBackup 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用します。

   - セッショントークンとセッション証明書の指紋を NetBackup 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/openv/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 NetBackup 管理コンソールを認証するときに使用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、NetBackup 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。NetBackup 管理コンソール側からの証明書は存在しません。)

5. NetBackup 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)。NetBackup 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、NetBackup 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 NetBackup 管理コンソール間に信頼が確立されます。
9. bpjava-*usvc と NetBackup 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 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、NetBackup 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. NetBackup 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、次のような名前で所定の場所にすでに存在します。

   hash(session token)_susvc_pid

   p.164 の「NetBackup 管理コンソールと bpjava-* 間のセキュアなチャネルの設定」を参照してください。
2. NetBackup 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向の認証済みの 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。NetBackup 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。

- NetBackup 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。
- NetBackup 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. NetBackup 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.164 の「NetBackup 管理コンソールと bpjava-* 間の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 NetBackup 管理コンソールの間に信頼が確立されます。
9. `nbsl/nbvault` と NetBackup 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 NetBackup 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 Java GUI オプションとともにインストールされているシステムで Java コンソール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。

ルートユーザーおよび管理者ユーザーの場合、Java GUI のログは次のログディレクトリに配置されます。

- UNIX の場合: `/usr/openv/netbackup/logs/user_ops/nbjlogs/`
- Windows の場合: *`install_directory`*`¥netbackup¥logs¥user_ops¥nbjlogs¥`

ルート以外のユーザーおよび管理者以外のユーザーの場合、Java GUI のログは次のログディレクトリに配置されます。

- UNIX の場合:
  `/usr/openv/netbackup/logs/user_ops/nbjlogs/<`*`non-root-username`*`>`

- Windows の場合:

  install_directory¥netbackup¥logs¥user_ops¥nbjlogs¥<*non-admin-username*>

管理者は、NetBackup レガシーログフォルダ内に存在する mklogdir -user *username* -group *groupname* コマンドを使用して、nbjlogs ディレクトリ内にルート以外のユーザー名のディレクトリを作成する必要があります。これらのユーザー名のディレクトリが、そのユーザーに対する適切な書き込み権限を付与して作成されていない場合、ユーザーのホームディレクトリがログ記録に使用されます。nbjlogs フォルダは最初にユーザーのホームディレクトリに作成され、すべてのログはこのフォルダに出力されます。ホームディレクトリにアクセスできない場合、ログはコンソールにリダイレクトされます。管理者は、mklogdir コマンドを使用して特定のユーザーの特定のログディレクトリを作成することもできます。たとえば、mklogdir -create user_ops/nbjlogs -user *username* -group *groupname* コマンドを使用してこのディレクトリを作成します。

NetBackup リモート管理コンソールの Java 操作のログ記録

NetBackup リモート管理コンソールを使用するホストの Java 操作をログに記録するには、setconf.bat ファイルを更新する必要があります。

1. 次のディレクトリを作成します。

   install_path¥NetBackup¥logs¥user_ops¥nbjlogs

2. 次のファイルを編集します。

   install_path¥Cohesity¥Java¥setconf.bat

3. 次の行を追加します。

   ```
   SET NB_INSTALL_PATH=C:¥¥Program Files¥¥Cohesity
   NetBackup¥NetBackup
   ```

4. ファイルを保存します。
5. 次回コンソールを開いたときに、次のログが作成されます。

   install_path¥NetBackup¥logs¥user_ops¥nbjlogs

NetBackup 管理コンソール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

NetBackup 管理コンソールをインストールした後、ログの詳細なセットを収集するようにログレベルが設定されます。

NetBackup 管理コンソールは、使用するログ記録レベルを決定するために Debug.properties ファイルを使用します。

/usr/openv/java/Debug.properties

install_dir¥VERITAS¥Java¥Debug.properties

追加のログ記録を有効にするには、次の設定を調整します。

```
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. コンソール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 NetBackup 管理コンソールログを収集します。

   ルートユーザーおよび管理者ユーザーの場合、Java GUI のログは次のログディレクトリに配置されます。

   - UNIX の場合: /usr/openv/netbackup/logs/user_ops/nbjlogs/
   - Windows の場合:
     install_directory¥netbackup¥logs¥user_ops¥nbjlogs¥

   ルート以外および管理者以外のユーザーの場合、Java GUI のログは次のログディレクトリに配置されます。

   - UNIX の場合:
     /usr/openv/netbackup/logs/user_ops/nbjlogs/<*non-root-username*>
   - Windows の場合:
     install_directory¥netbackup¥logs¥user_ops¥nbjlogs¥<*non-admin-username*>

   管理者は、NetBackup レガシーログフォルダ内に存在する mklogdir -user *username* -group *groupname* コマンドを使用して、nbjlogs ディレクトリ内に root 以外のユーザー名のディレクトリを作成する必要があります。これらのユーザー名のディレクトリが、そのユーザーに対する適切な書き込み権限を付与して作成されていない場合、ユーザーのホームディレクトリがログ記録に使用されます。nbjlogs フォルダは最初にユーザーのホームディレクトリに作成され、すべてのログはこのフォルダに出力されます。ホームディレクトリにアクセスできない場合、ログはコンソールにリダイレクトされます。

2. プライマリサーバーで NetBackup 管理コンソールにログインし、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/openv/netbackup/logs/admin
   - /usr/openv/netbackup/logs/bpjava-msvc
   - /usr/openv/netbackup/logs/bpjava-susvc
   - /usr/openv/netbackup/logs/bpjava-usvc

3. /usr/openv/netbackup/bp.conf ファイルに、次の行を追加します。

```
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 > CurrentVersion > 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) 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/openv/logs/nbsl
   - /usr/openv/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/VRTSpbx/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
```

プライマリサーバーで、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