

# NetBackup™ トラブルシュー ティングガイド

UNIX、Windows および Linux

リリース 10.0

**VERITAS™**

# NetBackup™ トラブルシューティングガイド

最終更新日: 2022-05-05

## 法的通知と登録商標

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、NetBackup は、Veritas Technologies LLC または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、Veritas 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Veritas製品に付属するサードパーティの法的通知文書は次の場所から入手できます。

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

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

本書は、現状のまま提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC 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、Veritas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。

Veritas Technologies LLC  
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 **Veritas 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](mailto:CustomerCare@veritas.com)

日本

[CustomerCare\\_Japan@veritas.com](mailto: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、**Veritas** の **Web** サイトで入手できます。

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

## マニュアルに対するご意見

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

[NB.docs@veritas.com](mailto:NB.docs@veritas.com)

次の **Veritas** コミュニティサイトでマニュアルの情報を参照したり、質問したりすることもできます。

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

## Veritas Services and Operations Readiness Tools (SORT)

**Veritas 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](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# 目次

第 1 章	概要 .....	9
	NetBackup のログと状態コード情報 .....	9
	問題のトラブルシューティング .....	9
	テクニカルサポートへの問題レポート .....	12
	NetBackup-Java アプリケーションの情報収集について .....	13
第 2 章	トラブルシューティングの手順 .....	16
	トラブルシューティング手順について .....	18
	NetBackup の問題のトラブルシューティング .....	20
	すべてのプロセスが UNIX サーバーで実行されていることの確認 .....	22
	すべてのプロセスが Windows サーバーで実行されていることの確認 .....	25
	インストールの問題のトラブルシューティング .....	28
	構成の問題のトラブルシューティング .....	29
	デバイス構成の問題の解決 .....	31
	マスターサーバーおよびクライアントの検証 .....	34
	メディアサーバーおよびクライアントの検証 .....	38
	UNIX クライアントとのネットワーク通信の問題の解決 .....	42
	Windows クライアントとのネットワーク通信の問題の解決 .....	46
	vnetd プロキシ接続のトラブルシューティング .....	49
	vnetd プロキシ接続の必要条件 .....	50
	vnetd プロキシ接続のトラブルシューティングの開始点 .....	51
	vnetd プロセスとプロキシがアクティブであることの確認 .....	52
	ホスト接続がプロキシされることの確認 .....	52
	vnetd プロキシ接続のテスト .....	53
	接続と受け入れのプロセスのログファイルの確認 .....	55
	vnetd プロキシログファイルの表示 .....	55
	セキュリティ証明書失効のトラブルシューティング .....	56
	クラウドプロバイダの無効化された SSL 証明書の問題のトラブルシュー ティング .....	57
	クラウドプロバイダの CRL のダウンロードに関する問題のトラブルシュー ティング .....	58
	ホストの CRL が証明書失効のトラブルシューティングに与える影響 .....	58

証明書が失効しているまたは CRL が使用できないため、NetBackup のジョブが失敗する .....	59
明らかなネットワークエラーが原因で NetBackup ジョブが失敗する .....	60
利用不能なリソースが原因で NetBackup ジョブが失敗する .....	61
マスターサーバーのセキュリティ証明書が失効している .....	62
NetBackup ホストの証明書の状態の確認 .....	63
外部 CA が署名した証明書の無効化に関する問題のトラブルシュー ティング .....	66
ネットワークとホスト名のトラブルシューティングについて .....	68
NetBackup のホスト名およびサービスエントリの検証 .....	72
UNIX マスターサーバーおよびクライアントのホスト名とサービスエント リの例 .....	76
UNIX マスターサーバーおよびメディアサーバーのホスト名とサービス エントリの例 .....	78
UNIX PC クライアントのホスト名とサービスエントリの例 .....	80
複数のネットワークに接続する UNIX サーバーのホスト名とサービスエ ントリの例 .....	81
bpplntcmd ユーティリティについて .....	83
[ホストプロパティ (Host Properties)] ウィンドウを使用した構成設定へのア クセス .....	86
空きがなくなったディスクの問題の解決 .....	87
凍結されたメディアのトラブルシューティングについての注意事項 .....	89
凍結されたメディアをトラブルシューティングする場合のログ .....	89
メディアが凍結される状況について .....	90
NetBackup Web サービスの問題のトラブルシューティング .....	93
NetBackup Web サービスのログの表示 .....	94
外部 CA の構成後の Web サービスの問題のトラブルシューティング .....	94
NetBackup Web サーバー証明書の問題のトラブルシューティング .....	97
PBX の問題の解決 .....	98
PBX インストールの確認 .....	98
PBX が実行中であるかどうかの確認 .....	99
PBX が正しく設定されているかどうかの確認 .....	99
PBX のログへのアクセス .....	100
PBX のセキュリティのトラブルシューティング .....	101
PBX デーモンかサービスが利用可能かどうかの判断 .....	103
リモートホストの検証に関する問題のトラブルシューティング .....	104
ホストの検証に関連するログの表示 .....	105
NetBackup 8.0 以前のホストとの安全でない通信の有効化 .....	106
保留中のホスト ID からホスト名へのマッピングの承認 .....	106
ホストキャッシュの消去 .....	108
自動イメージレプリケーションのトラブルシューティング .....	108

自動イメージレプリケーションと SLP で使用されるマスターサーバー のルール .....	117
外部証明書の構成で、ターゲットの AIR の信頼できるマスターサー バーの操作に失敗した .....	118
SLP コンポーネントが管理する自動インポートジョブのトラブルシュー ティングについて .....	120
ネットワークインターフェースカードのパフォーマンスのトラブルシューティ ング .....	124
bp.conf ファイルの SERVER エントリについて .....	125
使用できないストレージユニットの問題について .....	126
Windows での NetBackup 管理操作のエラーの解決 .....	126
UNIX コンピュータの NetBackup 管理コンソールに表示されるテキストの 文字化けの解決 .....	127
NetBackup 管理コンソールのエラーメッセージのトラブルシューティング .....	127
NetBackup 管理コンソールでのログと一時ファイルの保存に必要な追加 のディスク容量 .....	128
外部 CA の構成後に NetBackup 管理コンソールにログオンできない .....	129
ファイルベースの外部証明書の問題のトラブルシューティング .....	134
Windows 証明書ストアの問題のトラブルシューティング .....	141
バックアップエラーのトラブルシューティング .....	145
NAT クライアントまたは NAT サーバーのバックアップエラーの問題のトラ ブルシューティング .....	146
NetBackup Messaging Broker (または nbmqbroker) サービスに関する 問題のトラブルシューティング .....	150
Windows システムの電子メール通知に関する問題 .....	158
KMS 構成に関する問題 .....	158
キーサイズが大きいことによる NetBackup CA の移行を開始するときの問 題 .....	163
特権のないユーザー (サービスユーザー) アカウントに関する問題 .....	164
auth.conf ファイルのグループ名の形式に関する問題 .....	169
VxUpdate パッケージ追加処理のトラブルシューティング .....	171
FIPS モードの問題 .....	173
マルウェアスキャンの問題 .....	175
移動中のデータの暗号化が有効になっている NetBackup ジョブの問題 .....	178
<b>第 3 章</b> <b>NetBackup ユーティリティの使用</b> .....	182
NetBackup のトラブルシューティングユーティリティについて .....	182
NetBackup デバッグログの分析ユーティリティについて .....	184
ログアシスタントについて .....	187
ネットワークトラブルシューティングユーティリティについて .....	188

NetBackup サポートユーティリティ (nbsu) について .....	189
NetBackup サポートユーティリティ (nbsu) の出力 .....	191
NetBackup サポートユーティリティ (nbsu) の進捗状況の表示の例 .....	193
NetBackup の一貫性チェックユーティリティ (NBCC) について .....	193
NetBackup の一貫性チェックユーティリティ (NBCC) の出力 .....	195
NBCC の進捗状況の表示の例 .....	196
NetBackup の一貫性チェックの修復 (NBCCR) ユーティリティについて .....	203
nbcpllogs ユーティリティについて .....	205
ロボットテストユーティリティについて .....	206
UNIX でのロボットテスト .....	206
Windows でのロボットテスト .....	207
NetBackup Smart Diagnosis (nbsmartdiag) ユーティリティについて .....	208
NetBackup ホストの通信に nbsmartdiag ユーティリティを使用する ワークフロー .....	210
<b>第 4 章</b> <b>ディザスタリカバリ</b> .....	<b>212</b>
ディザスタリカバリについて .....	212
ディザスタリカバリの要件について .....	214
ディザスタリカバリパッケージ .....	215
ディザスタリカバリ設定について .....	216
バックアップに関する推奨事項 .....	217
UNIX および Linux のディスクリカバリ手順について .....	220
UNIX および Linux のマスターサーバーのディスクリカバリ .....	220
UNIX の NetBackup メディアサーバーのディスクリカバリについて .....	227
UNIX クライアントワークステーションのシステムディスクのリカバリ .....	227
UNIX および Linux のクラスタ化された NetBackup サーバーのリカバリに ついて .....	227
UNIX クラスタまたは Linux クラスタでの障害が発生したノードの置き 換え .....	228
UNIX クラスタまたは Linux クラスタ全体のリカバリ .....	230
Windows のディスクリカバリ手順について .....	231
Windows のマスターサーバーのディスクリカバリについて .....	232
Windows の NetBackup メディアサーバーのディスクリカバリについ て .....	238
Windows クライアントのディスクリカバリ .....	238
Windows のクラスタ化された NetBackup サーバーのリカバリについて .....	241
Windows VCS クラスタでの障害が発生したノードの置き換え .....	242
Windows VCS クラスタでの共有ディスクのリカバリ .....	243

Windows VCS クラスタ全体のリカバリ .....	244
ディザスタリカバリインストール後にクラスタマスターサーバーで証明書を生 成する .....	245
ディザスタリカバリパッケージのリストアについて .....	246
DR_PKG_MARKER_FILE 環境変数について .....	247
Windows でのディザスタリカバリパッケージのリストア .....	248
UNIX でのディザスタリカバリパッケージのリストア .....	250
NetBackup カタログのリカバリについて .....	254
Windows コンピュータでの NetBackup カタログリカバリについて .....	256
ディスクデバイスからの NetBackup カタログリカバリについて .....	256
NetBackup のカタログリカバリとシンボリックリンクについて .....	256
NetBackup カタログのリカバリと OpsCenter について .....	257
NetBackup ディザスタリカバリ電子メールの例 .....	258
NetBackup カタログ全体のリカバリについて .....	262
カタログリカバリ前の NAT メディアサーバーとの接続の確立 .....	277
NetBackup カタログイメージファイルのリカバリについて .....	277
NetBackup リレーショナルデータベースのリカバリについて .....	294
NetBackup アクセス制御が構成されている場合の NetBackup カタロ グのリカバリ .....	306
カタログバックアップのプライマリコピー以外からのカタログのリカバリ .....	308
ディザスタリカバリファイルを使用しない NetBackup カタログのリカバ リ .....	309
コマンドラインからの NetBackup のユーザー主導オンラインカタログ バックアップのリカバリ .....	310
NetBackup オンラインカタログバックアップからのファイルのリストア .....	315
NetBackup オンラインカタログリカバリメディアの凍結の解除 .....	315
カタログバックアップ中に終了状態 5988 が表示されたときに実行す る手順 .....	315
索引 .....	319

# 概要

この章では以下の項目について説明しています。

- **NetBackup** のログと状態コード情報
- 問題のトラブルシューティング
- テクニカルサポートへの問題レポート
- **NetBackup-Java** アプリケーションの情報収集について

## NetBackup のログと状態コード情報

次の情報は『**NetBackup** ログリファレンスガイド』に移動しました。

- ログ記録に関する章
- 付録「バックアップ機能およびリストア機能の概要」
- 付録「メディアおよびデバイス管理の機能の説明」

次のサイトにアクセスして『**NetBackup** ログリファレンスガイド』でこれらのトピックを参照してください。

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

**NetBackup** の状態コードに関する説明と推奨事項について詳しくは、『**NetBackup** 状態コードリファレンスガイド』を参照してください。

## 問題のトラブルシューティング

次の手順では、**NetBackup** を使う間に発生する可能性がある問題の解決に役立つ一般的なガイドラインを示します。手順では、特定のトラブルシューティングの詳細へのリンクを提供します。

表 1-1 NetBackup の問題をトラブルシューティングする手順

手順	処理	説明
手順 1	エラーメッセージの確認	<p>通常、エラーメッセージは、適切に行われなかった処理を示すため、インターフェースにエラーメッセージが表示されていなくても問題が発生している可能性がある場合、レポートおよびログを確認します。<b>NetBackup</b> には、拡張レポートおよびログ機能があります。これらの機能は、問題の解決に直接役立つエラーメッセージを提供します。</p> <p>ログには、適切に行われた処理とともに問題の発生時に <b>NetBackup</b> によって行われていた操作も表示されます。たとえば、リストア操作ではメディアをマウントする必要があるが、要求されたメディアが別のバックアップで使用中等であることが表示されます。ログとレポートは、トラブルシューティングの不可欠な手段です。</p> <p>『<a href="#">NetBackup ログリファレンスガイド</a>』を参照してください。</p>
手順 2	問題発生時に実行していた操作の確認	<p>次について質問します。</p> <ul style="list-style-type: none"> <li>■ 試行された操作。</li> <li>■ 使用した方法。          たとえば、クライアントにソフトウェアをインストールするには、複数の方法があります。また、多くの操作において使用可能なインターフェースは複数存在します。操作によっては、スクリプトを使用して実行することもできます。</li> <li>■ 使用していたサーバープラットフォームおよびオペレーティングシステムの種類。</li> <li>■ マスターサーバーとメディアサーバーのどちらで問題が発生したか (サイトでマスターサーバーとメディアサーバーの両方が使用されている場合)。</li> <li>■ クライアントの種類 (クライアントが関連する場合)。</li> <li>■ 過去にその操作が正常に実行されたことがあるかどうか。正常に実行されたことがある場合、現在との相違点。</li> <li>■ <b>Service Pack</b> のバージョン。</li> <li>■ 最新の、特に <b>NetBackup</b> を使用する際に必要な修正が行われたオペレーティングシステムソフトウェアを使用しているかどうか。</li> <li>■ デバイスのファームウェアのバージョン。公式のデバイス互換性リストに示されているバージョン以上かどうか。</li> </ul>

手順	処理	説明
手順 3	すべての情報の記録	<p>重要になる可能性がある情報を入手します。</p> <ul style="list-style-type: none"> <li>■ NetBackup の進捗ログ</li> <li>■ NetBackup のレポート</li> <li>■ NetBackup ユーティリティのレポート</li> <li>■ NetBackup のデバッグログ</li> <li>■ メディアおよびデバイスの管理のデバッグログ</li> <li>■ システムログまたは標準出力内のエラーメッセージまたは状態メッセージ (UNIX 版 NetBackup サーバーの場合)。</li> <li>■ ダイアログボックス内のエラーメッセージまたは状態メッセージ</li> <li>■ イベントビューアのアプリケーションログおよびシステムログ内のエラー情報または状態情報 (Windows 版 NetBackup サーバーの場合)。</li> </ul> <p>これらの情報を操作の試行ごとに記録します。複数の試行の結果を比較します。また、ユーザーが解決できないような問題が発生した場合に、サイト内の他のユーザーや、ベリタステクニカルサポートが解決のお手伝いをする際にも役立ちます。ログとレポートについて、より多くの情報を手に入れることができます。</p> <p>『<a href="#">NetBackup ログリファレンスガイド</a>』を参照してください。</p>
手順 4	問題の修正	<p>問題を定義した後、次の情報を使って問題を修正します。</p> <ul style="list-style-type: none"> <li>■ 状態コードまたはメッセージが推奨する修正措置を実行します。 『<a href="#">状態コードリファレンスガイド</a>』を参照してください。</li> <li>■ 状態コードまたはメッセージが存在しないか、状態コードの処置で問題が解決しない場合は、これらの追加のトラブルシューティングの手順を試みてください。 p.20 の「<a href="#">NetBackup の問題のトラブルシューティング</a>」を参照してください。</li> </ul>
手順 5	ベリタステクニカルサポートの問題レポートへの入力	<p>トラブルシューティングに失敗した場合は、問題レポートに入力してベリタステクニカルサポートに連絡する準備をします。</p> <p>p.12 の「<a href="#">テクニカルサポートへの問題レポート</a>」を参照してください。</p> <p>p.13 の「<a href="#">NetBackup-Java アプリケーションの情報収集について</a>」を参照してください。</p> <p>UNIX システムの場合、/usr/opensv/netbackup/bin/goodies/support スクリプトによって、発生した問題のデバッグをベリタステクニカルサポートで行うために必要なデータが含まれるファイルが作成されます。詳しくは、コマンド support -h を実行して、スクリプトの使用方法を参照してください。</p>
手順 6	ベリタステクニカルサポートへのお問い合わせ	<p>ベリタステクニカルサポート Web サイトでは、NetBackup の問題を解決するためのさまざまな情報を参照できます。</p> <p>次の URL のベリタステクニカルサポートにアクセスします。</p> <p><a href="https://www.veritas.com/support/en_US.html">https://www.veritas.com/support/en_US.html</a></p>

---

**メモ:** メディアサーバーという用語は NetBackup サーバー製品に使用されないことがあります。使用されるかどうかは文脈によって決まります。サーバーのインストールをトラブルシューティングする場合は、1 つのホストのみが存在することに注意してください。異なるホストのメディアサーバーについての説明は無視してください。

---

## テクニカルサポートへの問題レポート

サポートに連絡して問題を報告する前に、次の情報を記入します。

日付: \_\_\_\_\_

製品、プラットフォームおよびデバイスに関する次の情報を記録します。

- 製品およびそのリリース番号。
- サーバーハードウェアの種類およびオペレーティングシステムのバージョン。
- クライアントハードウェアの種類およびオペレーティングシステムのバージョン (クライアントが関連する場合)。
- 使用していたストレージユニット (ストレージユニットが関連する可能性がある場合)。
- ロボット形式やドライブ形式などのデバイス情報やバージョン、メディアおよびデバイスの管理の構成情報およびシステム構成情報 (デバイスに問題が発生している可能性がある場合)。
- インストールされている製品のソフトウェアパッチ。
- インストールされている Service Pack と Hotfix。

---

---

---

---

---

---

---

問題の定義

---

---

---

---

問題発生時に実行していた操作(Windows クライアント上でのバックアップなど)

---

---

エラーの表示(状態コードやエラーダイアログボックスなど)

---



---



---

問題が次の操作の実行中またはその直後に発生したかどうか:

- 初期インストール
  - 構成の変更 (具体的な内容)
  - システムの変更または問題 (具体的な内容)
  - 過去に問題が発生したかどうか(発生した場合、そのときに行った操作)
- 
- 

ログまたは問題についての他の保存済みデータ:

- [すべてのログエントリ (All Log Entries)]レポート
- メディアおよびデバイスの管理のデバッグログ
- NetBackup** のデバッグログ
- システムログ (UNIX の場合)
- イベントビューアのアプリケーションログおよびシステムログ (Windows の場合)

連絡方法:

- [MyVeritas.com](http://www.veritas.com) - ケース管理ポータル
- [mft.veritas.com](https://mft.veritas.com) - https アップロードのファイル転送ポータル
- [sftp.veritas.com](https://sftp.veritas.com) - sftp 転送のファイル転送サーバー

詳しくは、次を参照してください。

<http://www.veritas.com/docs/000097935>

- 電子メール
- WebEx

## NetBackup-Java アプリケーションの情報収集について

NetBackup-Java アプリケーションに問題が発生した場合、テクニカルサポートが必要とするデータを次のようにして収集します。

次のスクリプトおよびアプリケーションを使用して情報を収集できます。

<p>jnbSA  <b>(NetBackup-Java 管理アプリケーションの起動スクリプト)</b></p>	<p><code>/usr/opensv/netbackup/logs/user_ops/nbjlogs</code> のログファイルにデータを書き込みます。スクリプトを開始すると、このディレクトリ内のログを記録するファイルが示されます。通常、このファイルサイズは大きくありません (通常は 2 KB 未満)。<code>/usr/opensv/java/Debug.properties</code> ファイルを参照して、このログファイルの内容に影響するオプションを調べます。</p>
<p><b>Windows の NetBackup-Java 管理アプリケーション</b></p>	<p>アプリケーションが起動されているコンピュータ上に <b>NetBackup</b> がインストールされている場合、スクリプトは <code>install_path¥NetBackup¥logs¥user_ops¥nbjlogs</code> でログファイルにデータを書き込みます。</p> <p><b>NetBackup</b> がこのコンピュータ上にインストールされていない場合、ログファイルは作成されません。ログファイルを作成するには、<code>install_path¥java¥nbjava.bat</code> の最後の "java.exe" の行を変更し、ファイルへの出力を指定します。</p> <p><b>NetBackup</b> がこのコンピュータ上にインストールされていない場合、スクリプトは <code>install_path¥Veritas¥Java¥logs</code> でログファイルにデータを書き込みます。</p> <p><b>メモ:</b> アプリケーションが起動されているコンピュータ上に <b>NetBackup</b> がインストールされていて、<code>install_path</code> が <code>setconf.bat</code> ファイルで設定されていない場合、スクリプトは <code>install_path¥Veritas¥Java¥logs</code> のログファイルにデータを書き込みます。</p>
<p><code>/usr/opensv/java/get_trace</code></p>	<p><b>UNIX/Linux</b> のみ。</p> <p>テクニカルサポートが分析するための <b>Java Virtual Machine</b> のスタックトレースを提供します。このスタックトレースは、実行インスタンスに関連付けられたログファイルに書き込まれます。</p>
<p><b>UNIX または Linux の場合:</b>  <code>/usr/opensv/netbackup/bin/support/nbsu</code></p>	<p>ホストに問い合わせ、<b>NetBackup</b> とオペレーティングシステムに関する適切な診断情報を収集します。</p>
<p><b>Windows の場合:</b>  <code>install_path¥NetBackup¥bin¥support¥nbsu.exe</code></p>	<p>p.189 の「<b>NetBackup サポートユーティリティ (nbsu) について</b>」を参照してください。</p>

次の例では、Veritas 社のテクニカルサポートが分析するトラブルシューティングデータを集める方法を示します。

アプリケーションが応答しませんが、

操作がハングアップしているかどうかは、数分間様子を見てから判断します。操作によっては、完了するまで時間のかかるものもあります。特に、アクティビティモニターおよびレポートアプリケーションでは時間がかかります。

UNIX/Linux のみ:

数分後にもまだ応答がありません。

Javaアプリケーションを開始したアカウントで

`/usr/opensv/java/get_trace` を実行します。このスクリプトによって、ログファイルにスタックトレースが書き込まれます。

具体的には、**root** ユーザーアカウントで `jnbSA` を起動した場合、**root** ユーザーアカウントで

`/usr/opensv/java/get_trace` を実行します。これ以外のアカウントの場合、コマンドを実行してもエラーは発生しませんが、スタックトレースはデバッグログに追加されません。これは、**root** ユーザーアカウントだけが、スタックトレースを出力するコマンドの実行権限を所有しているためです。

構成についてのデータを取得します。

このトピックのリストに含まれる `nbsu` コマンドを実行します。

**NetBackup** のインストールが完了した後、**NetBackup** の構成を変更するたびに、このコマンドを実行します。

Veritas 社のテクニカルサポートへの連絡

分析用にログファイルと `nbsu` コマンドの出力を提供します。

# トラブルシューティングの手順

この章では以下の項目について説明しています。

- [トラブルシューティング手順について](#)
- [NetBackup の問題のトラブルシューティング](#)
- [インストールの問題のトラブルシューティング](#)
- [構成の問題のトラブルシューティング](#)
- [デバイス構成の問題の解決](#)
- [マスターサーバーおよびクライアントの検証](#)
- [メディアサーバーおよびクライアントの検証](#)
- [UNIX クライアントとのネットワーク通信の問題の解決](#)
- [Windows クライアントとのネットワーク通信の問題の解決](#)
- [vnetd プロキシ接続のトラブルシューティング](#)
- [セキュリティ証明書失効のトラブルシューティング](#)
- [ネットワークとホスト名のトラブルシューティングについて](#)
- [NetBackup のホスト名およびサービスエントリの検証](#)
- [bpclntcmd ユーティリティについて](#)
- [\[ホストプロパティ \(Host Properties\)\]ウィンドウを使用した構成設定へのアクセス](#)
- [空きがなくなったディスクの問題の解決](#)

- 凍結されたメディアのトラブルシューティングについての注意事項
- [NetBackup Web](#) サービスの問題のトラブルシューティング
- [NetBackup Web](#) サーバー証明書の問題のトラブルシューティング
- [PBX](#) の問題の解決
- リモートホストの検証に関する問題のトラブルシューティング
- 自動イメージレプリケーションのトラブルシューティング
- ネットワークインターフェースカードのパフォーマンスのトラブルシューティング
- `bp.conf` ファイルの `SERVER` エントリについて
- 使用できないストレージユニットの問題について
- [Windows](#) での [NetBackup](#) 管理操作のエラーの解決
- [UNIX](#) コンピュータの [NetBackup](#) 管理コンソールに表示されるテキストの文字化けの解決
- [NetBackup](#) 管理コンソールのエラーメッセージのトラブルシューティング
- [NetBackup](#) 管理コンソールでのログと一時ファイルの保存に必要な追加のディスク容量
- 外部 `CA` の構成後に [NetBackup](#) 管理コンソールにログオンできない
- ファイルベースの外部証明書の問題のトラブルシューティング
- [Windows](#) 証明書ストアの問題のトラブルシューティング
- バックアップエラーのトラブルシューティング
- [NAT](#) クライアントまたは [NAT](#) サーバーのバックアップエラーの問題のトラブルシューティング
- [NetBackup Messaging Broker](#) (または `nbmqbroker`) サービスに関する問題のトラブルシューティング
- [Windows](#) システムの電子メール通知に関する問題
- [KMS](#) 構成に関する問題
- キーサイズが大きいことによる [NetBackup CA](#) の移行を開始するときの問題
- 特権のないユーザー (サービスユーザー) アカウントに関する問題
- `auth.conf` ファイルのグループ名の形式に関する問題

- **VxUpdate** パッケージ追加処理のトラブルシューティング
- **FIPS** モードの問題
- マルウェアスキャンの問題
- 移動中のデータの暗号化が有効になっている **NetBackup** ジョブの問題

## トラブルシューティング手順について

**NetBackup** エラーの原因を発見するためのこれらの手順は一般的なものであり、発生する可能性があるすべての問題に対して適用できるとは限りません。ここでは、通常、問題を正常に解決可能な推奨方法が記載されています。

**Veritas** のテクニカルサポート Web サイトでは、**NetBackup** の問題を解決するための様々な情報を参照できます。トラブルシューティングについて詳しくは、次のサイトを参照してください。

[https://www.veritas.com/support/ja\\_JP.html](https://www.veritas.com/support/ja_JP.html)

これらの手順を実行する場合、各手順を順序どおり実行します。操作が実行済みであるか、または該当しない場合、その手順をスキップして次の手順に進みます。他の項を参照するように記載されている場合、その項で推奨されている解決方法を実行します。問題が解決しない場合、次の手順に進むか、もしくは構成や今までに試行済みの操作に応じて別の解決方法を模索することになります。

トラブルシューティング手順は、次のカテゴリに分類されます。

予備的なトラブルシューティング	次の手順では最初に調べるものについて説明します。次に、状況に応じた他の手順について説明します。  p.20 の「 <b>NetBackup</b> の問題のトラブルシューティング」を参照してください。  p.22 の「すべてのプロセスが <b>UNIX</b> サーバーで実行されていることの確認」を参照してください。  p.25 の「すべてのプロセスが <b>Windows</b> サーバーで実行されていることの確認」を参照してください。
インストールのトラブルシューティング	インストールに特に適用される問題。  p.28 の「インストールの問題のトラブルシューティング」を参照してください。
構成のトラブルシューティング	構成に特に適用される問題。  p.29 の「構成の問題のトラブルシューティング」を参照してください。

全般的なテストおよびトラブルシューティング これらの手順では、サーバーおよびクライアントの問題を検出する一般的な方法を定義します。この項は、最後に読んでください。

p.34 の「[マスターサーバーおよびクライアントの検証](#)」を参照してください。

p.38 の「[メディアサーバーおよびクライアントの検証](#)」を参照してください。

p.42 の「[UNIX クライアントとのネットワーク通信の問題の解決](#)」を参照してください。

p.46 の「[Windows クライアントとのネットワーク通信の問題の解決](#)」を参照してください。

p.72 の「[NetBackup のホスト名およびサービスエントリの検証](#)」を参照してください。

p.83 の「[bpclntcmd ユーティリティについて](#)」を参照してください。

p.72 の「[NetBackup のホスト名およびサービスエントリの検証](#)」を参照してください。

その他のトラブルシューティングの手順 p.87 の「[空きがなくなったディスクの問題の解決](#)」を参照してください。

p.89 の「[凍結されたメディアのトラブルシューティングについての注意事項](#)」を参照してください。

p.90 の「[メディアが凍結される状況について](#)」を参照してください。

p.124 の「[ネットワークインターフェースカードのパフォーマンスのトラブルシューティング](#)」を参照してください。

UNIX システムのホスト名とサービスエントリを示す一連の例も利用可能です。

- p.76 の「[UNIX マスターサーバーおよびクライアントのホスト名とサービスエントリの例](#)」を参照してください。
- p.78 の「[UNIX マスターサーバーおよびメディアサーバーのホスト名とサービスエントリの例](#)」を参照してください。
- p.80 の「[UNIX PC クライアントのホスト名とサービスエントリの例](#)」を参照してください。
- p.81 の「[複数のネットワークに接続する UNIX サーバーのホスト名とサービスエントリの例](#)」を参照してください。

# NetBackup の問題のトラブルシューティング

NetBackup に問題がある場合は、次の操作を最初に実行します。

この予備的な NetBackup のトラブルシューティングに関する項では、最初に確認する項目について説明し、次に状況に応じた他の手順について説明します。この章で説明している手順は、発生する可能性があるすべての問題に対して適用できるとはかぎりません。ここでは、通常、問題を正常に解決可能な推奨方法が記載されています。

これらの手順を実行する場合、各手順を順序どおり実行します。操作が実行済みであるか、または該当しない場合、その手順をスキップして次の手順に進みます。他の項を参照する場合、その項で推奨されている解決方法を実行します。問題が解決しない場合、次の手順に進むか、もしくは構成や今までに試行済みの操作に応じて別の解決方法を模索することになります。

**表 2-1** NetBackup の問題をトラブルシューティングする手順

手順	処理	説明
手順 1	オペレーティングシステムと周辺機器を確認します。	<p>サーバーおよびクライアントが実行しているオペレーティングシステムのバージョンがサポートされているものであること、および使用している周辺機器がサポートされていることを確認します。</p> <p><a href="#">『NetBackup Master Compatibility List』</a>を参照してください。</p> <p>さらに、NetBackup リリースノートにある、NetBackup に必要なオペレーティングシステムパッチと更新に関するセクションもご確認ください。このリリース用のリリースノートは、次の場所から入手できます。</p> <p><a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></p>
手順 2	レポートを使用してエラーを確認します。	<p>[すべてのログエントリ (All Log Entries)]レポートを使用して、該当する期間の NetBackup のエラーを確認します。このレポートには、エラーが発生した状況が表示されます。さまざまな問題が原因で状態コードが表示されている場合、有効な特定情報が表示される場合があります。</p> <p><a href="#">『NetBackup 管理者ガイド Vol. 1』</a>のレポートに関する情報を参照してください。</p> <p>問題がバックアップまたはアーカイブに関連する場合、[バックアップの状態 (Status of Backups)]レポートを確認します。このレポートには、状態コードが表示されます。</p> <p>これらのいずれかのレポートに状態コードまたはメッセージが表示されている場合、推奨処置を実行します。</p> <p><a href="#">『状態コードリファレンスガイド』</a>を参照してください。</p>

手順	処理	説明
手順 3	オペレーティングシステムのログを確認します。	<p>問題がメディアまたはデバイスの管理に関するもので、次のいずれかに該当する場合は、システムログ (UNIX の場合) または [イベントビューア (Event Viewer)] アプリケーションログとシステムログ (Windows の場合) を確認します。</p> <ul style="list-style-type: none"> <li>■ NetBackup によって状態コードが表示されない。</li> <li>■ NetBackup の状態コードとメッセージに関する項で示されている手順を実行しても問題を修正できない。</li> <li>■ メディアおよびデバイスの管理の状態コードおよびメッセージに関する項で示されている手順を実行しても問題を修正できない。</li> </ul> <p>これらのログには、エラーが発生した状況が表示されます。通常、エラーメッセージに、問題の範囲を特定するために十分な説明が記載されています。</p>
手順 4	デバッグログを確認します。	<p>有効になっている適切なデバッグログを読み、検出された問題を修正します。これらのログが有効でない場合、失敗した操作を再試行する前に有効にします。</p> <p><a href="#">『NetBackup ログリファレンスガイド』</a>を参照してください。</p>
手順 5	操作を再試行します。	<p>処置を実行し、操作を再試行します。修正処置を実行していないか、または問題が解決しない場合は、次の手順を続行します。</p>
手順 6	インストールの問題についてより多くの情報を手に入れます。	<p>新規インストール中、アップグレードのインストール中、既存の構成を変更した後問題が起きた場合は、次の手順を参照してください。</p> <p>p.28 の「<a href="#">インストールの問題のトラブルシューティング</a>」を参照してください。</p> <p>p.29 の「<a href="#">構成の問題のトラブルシューティング</a>」を参照してください。</p>
手順 7	サーバーおよびクライアントが操作可能であることを確認します。	<p>サーバーまたはクライアントのディスククラッシュが発生している場合は、<b>NetBackup</b> 操作に重要なファイルのリカバリ手順を利用できます。</p> <p>p.220 の「<a href="#">UNIX および Linux のディスクリカバリ手順について</a>」を参照してください。</p> <p>p.231 の「<a href="#">Windows のディスクリカバリ手順について</a>」を参照してください。</p>

手順	処理	説明
手順 8	パーティションが十分なディスク領域を備えていることを確認します。	<p>ディスクパーティションに NetBackup で利用可能な領域が十分に存在するかどうかを検証します。1 つ以上のパーティションに空きがない場合、そのパーティションにアクセスする NetBackup プロセスは正常に実行されません。表示されるエラーメッセージはプロセスによって異なります。表示される可能性があるエラーメッセージは、[アクセスできません (unable to access)] や [ファイルを作成できないか、ファイルを開けません (unable to create or open a file)] などです。</p> <p>UNIX システムでは、df コマンドを実行してディスクパーティション情報を表示します。Windows システムでは、[ディスクの管理] またはエクスプローラを使用します。</p> <p>次のディスクパーティションを確認します。</p> <ul style="list-style-type: none"><li>■ NetBackup ソフトウェアがインストールされているパーティション。</li><li>■ NetBackup マスターサーバーまたはメディアサーバー上の、NetBackup データベースが存在するパーティション。</li><li>■ NetBackup プロセスによって一時ファイルが書き込まれるパーティション。</li><li>■ NetBackup ログが格納されているパーティション。</li><li>■ オペレーティングシステムがインストールされているパーティション。</li></ul>
手順 9	ログレベルを上げます。	<p>すべての領域に対して、または問題に関連する可能性がある領域のみに対して、詳細ログを有効にします。</p> <p>ログレベルの変更に関する情報について詳しくは、『NetBackup ログリファレンスガイド』を参照してください。</p>
手順 10	実行中のデーモンまたはプロセスを特定します。	<p>UNIX 版または Windows 版の NetBackup サーバーの手順に従います。</p> <p>p.22 の「すべてのプロセスが UNIX サーバーで実行されていることの確認」を参照してください。</p> <p>p.25 の「すべてのプロセスが Windows サーバーで実行されていることの確認」を参照してください。</p>

## すべてのプロセスが UNIX サーバーで実行されていることの確認

NetBackup が正しく動作するには、正しい一連のプロセス(デーモン)が UNIX サーバーで実行されている必要があります。この手順は、実行されているプロセスを判断し、実行されていない可能性があるプロセスを開始する方法を示します。

すべてのプロセスが **UNIX** サーバーで実行されていることを確認する方法

- 1 マスターサーバーとメディアサーバーで実行されているプロセス (デーモン) のリストを参照するために、次のコマンドを入力します。

```
/usr/opensv/netbackup/bin/bpps -x
```

## 2 NetBackup サーバーで、次のプロセスを実行していることを確認します。

マスターサーバー

bpcd -standalone	nbpem
bpcompatd	nbproxy
bpdbm	nbrb
bpjobd	nbrmms
bprd	nbsl
java	nbstserv
nbars	nbsvcmon
nbatd	nbwmc
nbdisco (discovery manager)	NB_dbsrv
nbemm	pbx_exchange
nbevtmgr	vmd
nbim (index manager)	vnetd -standalone
nbjm	

メディアサーバー (Media server)

avrd (automatic volume recognition, only if drives are configured

on the server)

bpcd -standalone  
ltid (needed only if tape devices are configured on the server)  
mtstrmd (if the system has data deduplication configured)  
nbrmms  
nbsl  
nbsvcmon  
pbx\_exchange  
spad (if the system has data deduplication configured)  
spoold (if the system has data deduplication configured)  
vmd (volume)  
vnetd -standalone  
Any tape or robotic processes, such as tldd, tldcd

---

**メモ:** 他のアドオン製品やデータベースエージェントなどがインストールされているとき、場合によっては、追加のプロセスも実行する必要があります。詳しくは、[https://www.veritas.com/support/en\\_US/article.100002166](https://www.veritas.com/support/en_US/article.100002166) を参照してください。

---

- 3 NetBackup Request デーモン (bprd) または NetBackup Database Manager デーモン (bpdbm) のいずれかが実行中でない場合、次のコマンドを実行して起動します。

```
/usr/opensv/netbackup/bin/initbprd
```

- 4 NetBackup Web Management Console (nbwmc) が実行されていない場合、次のコマンドで起動します。

```
/usr/opensv/netbackup/bin/nbwmc
```

- 5 メディアサーバープロセスのうちのどれかが実行中でない場合は、次のコマンドを実行してデバイスプロセス ltid を停止します。

```
/usr/opensv/volmgr/bin/stopltd
```

- 6 ltid、avrd およびロボット制御の各プロセスが停止していることを検証するには、次のコマンドを実行します。

```
/usr/opensv/volmgr/bin/vmps
```

- 7 ACS ロボット制御を使用している場合、ltid を終了しても、acsssi デーモンおよび acsssl プロセスは実行されたままのことがあります。個別にそれらのロボット制御プロセスを停止するには、UNIX kill コマンドを使用します。

- 8 その後、次のコマンドを実行し、すべてのデバイスプロセスを起動します。

```
/usr/opensv/volmgr/bin/ltid
```

デバッグを行うには、`-v` (詳細) オプションを指定して ltid を起動します。

- 9 必要に応じて、次を利用し、すべての NetBackup サーバープロセスを停止し、再起動します。

```
/usr/opensv/netbackup/bin/bp.kill_all  
/usr/opensv/netbackup/bin/bp.start_all
```

## すべてのプロセスが Windows サーバーで実行されていることの確認

Windows サーバーで実行されている必要があるすべてのプロセスが実行されていることを確認するには、次の手順を使います。

**表 2-2**                    すべての必要なプロセスが Windows サーバーで実行されていることを確認する手順

手順	処理	説明
手順 1	<p>マスターサーバーのすべてのサービスを起動します。</p>	<p>次のサービスは、典型的なバックアップおよびリストア操作 (この表のステップ 1、2、3) の場合、動作している必要があります。実行されていない場合、<b>NetBackup</b> アクティビティモニターまたは <b>Windows</b> の [管理ツール] の [サービス] を使用して、これらのサービスを起動します。</p> <p>すべてのサービスを起動するには、<code>install_path\NetBackup\bin\bpup.exe</code> を実行します。</p> <p>マスターサーバー上のサービス:</p> <ul style="list-style-type: none"> <li>■ NetBackup 認証</li> <li>■ NetBackup Client Service</li> <li>■ NetBackup Compatibility Service</li> <li>■ NetBackup Database Manager</li> <li>■ NetBackup Discovery Framework</li> <li>■ NetBackup Enterprise Media Manager</li> <li>■ NetBackup Event Manager</li> <li>■ NetBackup Indexing Manager</li> <li>■ NetBackup Job Manager</li> <li>■ NetBackup Policy Execution Manager</li> <li>■ NetBackup Relational Database Manager</li> <li>■ NetBackup Remote Manager and Monitor Service</li> <li>■ NetBackup Request デーモン</li> <li>■ NetBackup Resource Broker</li> <li>■ NetBackup Service Layer</li> <li>■ NetBackup Service Monitor</li> <li>■ NetBackup Storage Lifecycle Manager</li> <li>■ NetBackup Vault Manager</li> <li>■ NetBackup Volume Manager</li> <li>■ NetBackup Web 管理コンソール</li> <li>■ Veritas Private Branch Exchange</li> </ul> <p><b>メモ:</b> 他のアドオン製品やデータベースエージェントなどがインストールされているとき、場合によっては、追加のプロセスも実行する必要があります。詳しくは、<a href="https://www.veritas.com/support/en_US/article.100002166">https://www.veritas.com/support/en_US/article.100002166</a> を参照してください。</p>

手順	処理	説明
手順 2	メディアサーバーのすべてのサービスを起動します。	<p>メディアサーバー上のサービス:</p> <ul style="list-style-type: none"> <li>■ NetBackup Client Service</li> <li>■ NetBackup Deduplication Engine (システムにデータ重複排除が構成されている場合)</li> <li>■ NetBackup Deduplication Manager (システムにデータ重複排除が構成されている場合)</li> <li>■ NetBackup Deduplication Multi-Threaded Agent (システムにデータ重複排除が構成されている場合)</li> <li>■ NetBackup Device Manager サービス (システムにデバイスが構成されている場合)</li> <li>■ NetBackup Remote Manager and Monitor Service (システムにデータ重複排除が構成されている場合)</li> <li>■ NetBackup Volume Manager サービス</li> </ul>
手順 3	クライアントのすべてのサービスを起動します。	<p>クライアントのサービス:</p> <ul style="list-style-type: none"> <li>■ NetBackup Client Service</li> <li>■ NetBackup Legacy Client Service</li> <li>■ Veritas Private Branch Exchange</li> </ul>
手順 4	avrd およびロボットのプロセスを起動します。	<p><b>NetBackup</b> アクティビティモニターを使用して、次のプロセスが実行中であるかどうかを確認します。</p> <ul style="list-style-type: none"> <li>■ avrd (自動メディア認識。サーバー上でドライブが構成されている場合のみ)</li> <li>■ すべての構成済みロボットに対するプロセス。</li> </ul> <p>『<a href="#">NetBackup 管理者ガイド Vol. 1</a>』を参照してください。</p> <p>これらのプロセスが実行中でない場合、<b>NetBackup Device Manager</b> サービスを停止してから再起動します。<b>NetBackup</b> アクティビティモニターまたは <b>Windows</b> の [管理ツール] の [サービス] を使用します。</p>

手順	処理	説明
手順 5	操作をやりなおすか、または追加のトラブルシューティングを実行します。	<p>前述の手順に記載されているプロセスまたはサービスのいずれかを起動する必要がある場合、操作を再試行します。</p> <p>プロセスとサービスが実行中であるか、または問題が解決しない場合は、サーバーとクライアントのテストを試みることができます。</p> <p>p.34 の「<a href="#">マスターサーバーおよびクライアントの検証</a>」を参照してください。</p> <p>p.38 の「<a href="#">メディアサーバーおよびクライアントの検証</a>」を参照してください。</p> <p>これらのプロセスまたはサービスのいずれかを起動できない場合、該当するデバッグログに <b>NetBackup</b> の問題が示されていないかどうかを確認します。</p> <p>『<a href="#">NetBackup ログリファレンスガイド</a>』を参照してください。</p> <p>これらのプロセスおよびサービスが起動されると、手動で停止するか、またはシステムに問題が発生しないかぎり、継続して実行されます。Windows システムでは、起動スクリプトにこれらのプロセスを起動するためのコマンドを追加し、システムを再ブートする場合に、これらのプロセスが再起動されるようにすることをお勧めします。</p>

## インストールの問題のトラブルシューティング

インストールの問題をトラブルシューティングするには、次の手順を使います。

表 2-3 インストールの問題をトラブルシューティングする手順

手順	処理	説明
手順 1	リリースメディアを使用して、マスターサーバーおよびメディアサーバーにソフトウェアをインストールできるかどうかを判断します。	<p>失敗の原因として、次のことが考えられます。</p> <ul style="list-style-type: none"> <li>■ Windows システムの場合、管理者 (<b>Administrator</b>) 以外でのログオン (サービスをシステムにインストールするための権限が必要です)</li> <li>■ 許可権限が無効 (デバイスの使用権限、およびインストールするディレクトリおよびファイルの書き込み権限を所有していることを確認します)</li> <li>■ 不適切なメディア ((日本にてご購入の場合は、ご購入先を通じて)テクニカルサポートに連絡してください)</li> <li>■ ドライブの不良 (ドライブを交換するか、または各ベンダーが提供するハードウェアマニュアルを参照してください)</li> <li>■ ドライブの構成が不適切 (システムマニュアルおよび各ベンダーが提供するマニュアルを参照してください)</li> </ul>

手順	処理	説明
手順 2	クライアントに NetBackup クライアントソフトウェアをインストールできるかどうかを判断します。	<p><b>メモ:</b> NetBackup を Linux クライアント上でインストールまたは使用する前に、<code>bpcd -standalone</code> サービスと <code>vnetd -standalone</code> サービスがそのコンピュータ上で起動していることを確認します。これらのサービスによって、NetBackup マスターサーバーと Linux クライアントの間で適切な通信が行われます。</p> <p><b>メモ:</b> NetBackup の UNIX または Linux サーバーは、UNIX クライアントと Linux クライアントにクライアントソフトウェアをプッシュできます。Windows サーバーは、Windows クライアントにクライアントソフトウェアをプッシュできます。また、NetBackup アプライアンスからクライアントソフトウェアをダウンロードして、クライアント上でインストールを実行することもできます。</p> <p><b>メモ:</b> 『NetBackup Appliance 管理者ガイド』を参照してください。</p> <p>次の手順を実行します。</p> <ul style="list-style-type: none"> <li>■ 信頼できる UNIX クライアントへのインストールの場合、次を確認します。 <ul style="list-style-type: none"> <li>■ 正しいクライアント名がポリシー構成にある。</li> <li>■ 正しいサーバー名がクライアントの <code>.rhosts</code> ファイルにある。</li> </ul> </li> </ul> <p>インストールがハングアップした場合、クライアントで <code>root</code> ユーザーのシェルまたは環境変数に問題があるかどうかを確認します。確認するファイルは、使用しているプラットフォーム、オペレーティングシステムおよびシェルによって異なります。たとえば、Sun 社のシステムでは、<code>.login</code> によって、端末の種類が定義される前に <code>stty(stty ^erase など)</code> が実行されます。この操作によってインストール処理がハングアップする場合、<code>.login</code> ファイルを変更して、<code>stty</code> を実行する前に端末を定義します。または、インストールが完了するまでクライアントの <code>.login</code> ファイルを他のファイル名に変更しておきます。</p> <ul style="list-style-type: none"> <li>■ セキュリティ保護された UNIX クライアントへのインストールの場合、<code>ftp</code> の構成を確認します。たとえば、クライアント上で有効なユーザー名およびパスワードを使用する必要があります。</li> </ul>
手順 3	ネットワークの問題を解決します。	<p>問題が一般のネットワーク通信と関連しているかどうかを判断します。</p> <p>p.42 の「UNIX クライアントとのネットワーク通信の問題の解決」を参照してください。</p> <p>p.46 の「Windows クライアントとのネットワーク通信の問題の解決」を参照してください。</p>

## 構成の問題のトラブルシューティング

初期インストールの後または構成に変更が行われた後に問題があるかどうかを確認するには、次の手順を使います。

表 2-4 構成の問題をトラブルシューティングする手順

手順	処理	説明
手順 1	デバイス構成の問題があるかどうかを確認します。	デバイス構成に次の問題があるかどうかを確認します。 <ul style="list-style-type: none"> <li>■ ロボットドライブの構成で、ロボットが指定されていない。</li> <li>■ ドライブが不正な形式または密度で構成されている。</li> <li>■ ロボットドライブ番号が不適切である。</li> <li>■ ロボットに割り当てられた論理的なロボット番号ではなく、ロボット制御の SCSI ID が指定されている。</li> <li>■ 複数のロボットに同じロボット番号が使用されている。</li> <li>■ 一意のドライブインデックス番号ではなく、ドライブの SCSI ID が指定されている。</li> <li>■ プラットフォームでデバイスがサポートされていないか、またはそのデバイスを認識するようにプラットフォームが構成されていない。</li> <li>■ ロボットデバイスで LUN 1 (一部のロボットハードウェアが必要) を使用するように構成されていない。</li> <li>■ UNIX の場合、ドライブの非巻き戻しデバイスのパスが、巻き戻しデバイスのパスとして指定されている。</li> <li>■ UNIX では、テープデバイスは「Berkeley 形式のクローズ」で構成されません。NetBackup は、一部のプラットフォームで構成可能であるこの機能を必要とします。詳細な説明を参照できます。</li> <li>■ UNIX では、QIC 以外のテープデバイスは「変数モード」で構成されません。NetBackup は、一部のプラットフォームで構成可能であるこの機能を必要とします。この場合、バックアップは通常どおり行うことができますが、リストアは行うことができません。詳しくは、『状態コードリファレンスガイド』を参照してください。</li> <li>■ UNIX の場合、テープドライブへのパススルーパスが設定されていない。</li> </ul> デバイス構成の問題に関する詳しい説明を参照できます。 『NetBackup デバイス構成ガイド』を参照してください。
手順 2	デーモンまたはサービスを再確認します。	デーモンまたはサービスに次の問題があるかどうかを確認します。 <ul style="list-style-type: none"> <li>■ 再ブート中にデーモンまたはサービスが再起動しない(起動するようにシステムを構成します)。</li> <li>■ 不適切なデーモンまたはサービスが起動する(メディアサーバーの起動スクリプトの問題)。</li> <li>■ デーモンまたはサービスの実行中に構成が変更された。</li> <li>■ Windows の場合、%SystemRoot%\System32\drivers\etc\services ファイルに vmd、bprd、bpdbm および bpcd のエントリが存在しない。また、構成しているロボット用のエントリがプロセスに存在することも確認します。これらのプロセスのリストを利用できます。                      『NetBackup 管理者ガイド Vol. 1』を参照してください。</li> <li>■ UNIX の場合、/etc/services ファイル (または、NIS または DNS) に vmd、bprd、bpdbm またはロボットデーモンが存在しない。</li> </ul>

手順	処理	説明
手順 3	操作を再試行し、状態コードとメッセージを確認します。	<p>構成の問題が検出され、これらの問題を修正した場合、操作を再試行して、次のうち、<b>NetBackup</b> の状態コードまたはメッセージを確認します。</p> <ul style="list-style-type: none"> <li>■ [すべてのログエントリ (<b>All Log Entries</b>)]レポートに、該当する期間の <b>NetBackup</b> エラーが表示されていないかどうかを確認します。このレポートには、エラーが発生した状況が表示されます。さまざまな問題が原因でエラーが発生している場合、有効な特定情報が表示される場合があります。問題がバックアップまたはアーカイブに関連する場合、[アクティビティモニター (<b>Activity Monitor</b>)]でジョブの[状態の詳細 (<b>Detailed Status</b>)]を確認します。[バックアップの状態 (<b>Status of Backups</b>)]レポートも確認してください。これらのいずれかのレポートに状態コードまたはメッセージが表示されている場合、推奨処置を実行します。 『<b>状態コードリファレンスガイド</b>』を参照してください。</li> <li>■ 問題がメディアまたはデバイスの管理に関するものであり、<b>NetBackup</b> が状態コードを示さない場合は、システムログ (<b>UNIX</b> の場合) またはイベントビューアのアプリケーションログとシステムログ (<b>Windows</b> の場合)を確認します。そうしないと、状態コードで示される手順に従っても問題を修正できません。</li> <li>■ 有効になっている適切なデバッグログを確認します。検出された問題を修正します。これらのログが有効でない場合、再試行する前に有効にします。 『<b>NetBackup</b> ログリファレンスガイド』を参照してください。</li> </ul>
手順 4	操作を再試行し、追加のトラブルシューティングを実行します。	<p>処置を実行し、操作を再試行します。推奨処置を実行していないか、または問題が解決しない場合、次のいずれかの手順に進みます。</p> <p>p.87 の「<b>空きがなくなったディスクの問題の解決</b>」を参照してください。</p> <p>p.89 の「<b>凍結されたメディアのトラブルシューティングについての注意事項</b>」を参照してください。</p> <p>p.90 の「<b>メディアが凍結される状況について</b>」を参照してください。</p> <p>p.124 の「<b>ネットワークインターフェースカードのパフォーマンスのトラブルシューティング</b>」を参照してください。</p>

## デバイス構成の問題の解決

選択されたデバイスが次のいずれかの条件に該当する場合、デバイスの構成ウィザードの 2 番目のパネルに自動構成警告メッセージが表示されます。

- **NetBackup** サーバーのライセンスを入手していない。
- ライセンスの制限を超えている。
- 自動構成が困難になる固有の性質がいくつかある。

次のメッセージはデバイス構成に関連します。メッセージの説明および推奨処置も示します。

表 2-5 デバイス構成メッセージの推奨処置

メッセージ	説明	推奨処置
(Drive does not support serialization.)	ドライブからシリアル番号が戻されません。いくつかの製造元の製品ではシリアル番号がサポートされていないことに注意してください。ドライブは、シリアル番号を使用しなくても手動で構成して操作できます。ただし、デバイスの自動構成は最適な状態で動作しません。	シリアル番号が戻される新しいバージョンのファームウェアを製造元から入手するか(可能な場合)、シリアル番号を使用せずにドライブを手動で構成して操作します。
(Robot does not support serialization.)	ロボットから、ロボットのシリアル番号またはロボットに存在するドライブのシリアル番号が戻されません。いくつかの製造元の製品ではシリアル番号がサポートされていないことに注意してください。ロボットおよびドライブは、シリアル番号を使用しなくても手動で構成して操作できます。ただし、デバイスの自動構成は最適な状態で動作しません。	シリアル番号が戻される新しいバージョンのファームウェアを製造元から入手します(可能な場合)。または、シリアル番号を使用せずにロボットおよびドライブを手動で構成して操作します。
このロボット形式用のライセンスがありません。(No license for this robot type.)	<b>NetBackup Server</b> では、このロボットに定義されているロボット形式はサポートされていません。	別のロボット形式を定義します。 <b>NetBackup Server</b> でサポートされているロボットライブラリだけを使います。
このドライブ形式用のライセンスがありません。(No license for this drive type.)	このドライブに定義されているドライブ形式は、 <b>NetBackup Server</b> でサポートされていません。	別のドライブ形式を定義します。 <b>NetBackup</b> でサポートされているドライブだけを使います。
ロボット形式を判断できません。(Unable to determine robot type)	<b>NetBackup</b> でロボットライブラリが認識されません。ロボットライブラリを自動構成できません。	次の手順を実行します。 <ul style="list-style-type: none"> <li>■ 新しいデバイスマッピングファイルをベリタスのサポート Web サイトからダウンロードし、再試行します。<b>Veritas</b></li> <li>■ ロボットライブラリを手動で構成します。</li> <li>■ <b>NetBackup</b> でサポートされているロボットライブラリだけを使います。</li> </ul>
(Drive is standalone or in unknown robot)	ドライブがスタンドアロンであるか、またはドライブとロボットのいずれかからシリアル番号が戻されません。いくつかの製造元の製品ではシリアル番号がサポートされていないことに注意してください。ドライブまたはロボットは、シリアル番号を使用しなくても手動で構成して操作できます。ただし、デバイスの自動構成は最適な状態で動作しません。	シリアル番号が戻される新しいバージョンのファームウェアを製造元から入手するか(可能な場合)、シリアル番号を使用せずにドライブまたはロボットを手動で構成して操作します。

メッセージ	説明	推奨処置
ロボットドライブ番号が不明です。(Robot drive number is unknown)	ドライブまたはロボットのいずれかからシリアル番号が戻されません。いくつかの製造元の製品ではシリアル番号がサポートされていないことに注意してください。ドライブまたはロボットは、シリアル番号を使用しなくても手動で構成して操作できます。ただし、デバイスの自動構成は最適な状態で動作しません。	シリアル番号が戻される新しいバージョンのファームウェアを製造元から入手します (可能な場合)。または、シリアル番号を使用せずにドライブおよびロボットを手動で構成して操作します。
(Drive is in an unlicensed robot.)	ドライブが、NetBackup Server のライセンスで使用できないロボットライブラリ内に存在しています。NetBackup Server のライセンスでロボットを使用できないため、そのロボットに構成されているいずれのドライブも使用できません。	ドライブがライセンスを所有しないロボットに存在しないように構成します。
ドライブの SCSI アダプタがパススルーをサポートしていません (またはバススルーのパスが存在しません)。(Drive's SCSI adapter does not support pass-thru (or pass-thru path does not exist).)	ドライブに SCSI パススルーパスが構成されていないことが検出されました。考えられる原因は、次のとおりです。 <ul style="list-style-type: none"> <li>■ SCSI パススルー機能がサポートされていないアダプタにドライブが接続されている。</li> <li>■ このドライブにパススルーパスが定義されていない。</li> </ul>	ドライブのアダプタを変更するか、またはドライブにバススルーパスを定義します。SCSI アダプタのバススルーについて詳しくは、『NetBackup デバイス構成ガイド』を参照してください。
デバイス構成ファイルが存在しません。(No configuration device file exists)	デバイスを構成するために必要な、関連付けられたデバイスファイルが存在しないことが検出されました。	デバイスファイルを作成する方法については、『NetBackup デバイス構成ガイド』を参照してください。
ドライブ形式を判断できません。(Unable to determine drive type)	NetBackup Server でドライブが認識されません。ドライブを自動構成できません。	次の手順を実行します。 <ul style="list-style-type: none"> <li>■ 新しいデバイスマッピングファイルをベリタス社のサポート Web サイトからダウンロードし、再試行します。Veritas</li> <li>■ ドライブを手動で構成します。</li> <li>■ NetBackup でサポートされているドライブだけを使用します。</li> </ul>

メッセージ	説明	推奨処置
圧縮デバイスファイルを判断できません。 (Unable to determine compression device file)	デバイスの構成に使用される、想定された圧縮デバイスファイルが存在しないドライブが検出されました。デバイスの自動構成では、ハードウェアによるデータ圧縮をサポートするデバイスファイルが使用されます。1台のドライブに対して複数の圧縮デバイスファイルが存在する場合、デバイスの自動構成では、最適な圧縮デバイスファイルが判断されません。代わりに、非圧縮デバイスファイルが使用されます。	ハードウェアによるデータ圧縮が必要でない場合、処置は必要ありません。ドライブは、ハードウェアによるデータ圧縮を行わなくても操作可能です。ハードウェアによるデータ圧縮およびテープドライブの構成のヘルプを利用できます。  デバイスファイルを作成する方法については、『 <a href="#">NetBackup デバイス構成ガイド</a> 』を参照してください。

## マスターサーバーおよびクライアントの検証

NetBackup、インストールおよび構成のトラブルシューティング手順で問題が判明しない場合は、次の手順を実行します。実行済みの手順はスキップします。

次の手順では、ソフトウェアは正常にインストールされているが、必ずしも正しく構成されていないと想定しています。NetBackup が一度も正常に働かない場合には、おそらく設定に問題があります。特に、デバイス構成に問題があるかどうかを確認します。

バックアップおよびリストアを2回ずつ実行する場合もあります。UNIX では、最初に root ユーザーで実行し、次に root 以外のユーザーで実行します。Windows では、最初に管理者 (Administrators) グループのメンバーであるユーザーで実行します。次に、管理者 (Administrators) グループのメンバー以外のユーザーで実行します。いずれの場合も、テストファイルに対する読み込み権限および書き込み権限を所有していることを確認します。

これらの手順についての説明では、読者がバックアッププロセスとリストアプロセスに精通していることを前提としています。詳しくは、『[NetBackup ログリファレンスガイド](#)』を参照してください。

次の手順のいくつかで、[すべてのログエントリ (All Log Entries)] レポートについて述べています。このレポートと他のレポートについて詳しくは、次を参照してください。

『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

表 2-6 マスターサーバーとクライアントをテストする手順

手順	処理	説明
手順 1	デバッグログを有効にします。	マスターサーバー上で該当するデバッグログを有効にします。  ログについて詳しくは、『 <a href="#">NetBackup ログリファレンスガイド</a> 』を参照してください。  該当するログが不明な場合、問題が解決するまですべてのログを有効にします。問題が解決したら、デバッグログディレクトリを削除します。

手順	処理	説明
手順 2	テストポリシーを構成します。	<p>ベーシックディスクのストレージユニットを使うためのテストポリシーを設定します。</p> <p>テストする時間がバックアップ処理時間帯に含まれるようにテストポリシーを設定します。マスターサーバーをクライアントとして指定し、マスターサーバー上のストレージユニットを指定します (非ロボットドライブが望ましい)。NetBackup ボリュームプールでボリュームを設定してドライブにボリュームを挿入します。bp1abel コマンドを実行してボリュームにラベル付けしないと、NetBackup は未使用のメディア ID を自動的に割り当てます。</p>
手順 3	デーモンとサービスを検証します。	<p>マスターサーバー上で NetBackup デーモンまたはサービスが実行中であるかどうかを検証するには、次を実行します。</p> <ul style="list-style-type: none"> <li>■ UNIX システム上でデーモンを確認するには、次のコマンドを入力します。  <pre>/usr/openv/netbackup/bin/bpps -x</pre></li> <li>■ Windows システム上でサービスを確認するには、NetBackup アクティビティモニターまたは Windows の [管理ツール] の [サービス] を使用します。</li> </ul>
手順 4	ポリシーをバックアップおよびリストアします。	<p>NetBackup 管理インターフェースで手動バックアップオプションを使用して、ポリシーの手動バックアップを開始します。次に、バックアップのリストアを行います。</p> <p>これらの操作によって、次のことが検証されます。</p> <ul style="list-style-type: none"> <li>■ NetBackup サーバーソフトウェア (すべてのデーモンまたはサービス、プログラム、データベースを含む) が機能するかどうか。</li> <li>■ NetBackup によるメディアのマウントと構成済みのドライブの使用が可能かどうか。</li> </ul>
手順 5	エラーを確認します。	<p>エラーが起きた場合は、[アクティビティモニター (Activity Monitor)] でジョブの [詳細の状態 (Detailed Status)] を確認します。</p> <p>NetBackup の [すべてのログエントリ (All Log Entries)] レポートも確認してみてください。ドライブまたはメディアに関連する障害の場合、ドライブが起動状態で、ハードウェアが機能しているかどうかを検証します。</p> <p>問題をさらに特定するには、デバッグログを使用します。</p> <p>一連のプロセスの概要については、『NetBackup ログリファレンスガイド』にあるバックアッププロセスとリストアプロセスの情報を参照してください。</p>
手順 6	デバッグログ以外の情報を確認します。	<p>デバッグログで問題の原因が判明しない場合、次のログを確認します。</p> <ul style="list-style-type: none"> <li>■ システムログ (UNIX システムの場合)</li> <li>■ イベントビューアログとシステムログ (Windows システムの場合)</li> <li>■ バックアップ、リストア、複製を実行したメディアサーバー上にある Media Manager のデバッグログ</li> <li>■ バックアップ、リストア、複製を実行したメディアサーバー上にある bpdm と bptm のデバッグログ</li> </ul> <p>ハードウェア障害については、各ベンダーが提供するマニュアルを参照してください。</p>

手順	処理	説明
手順 7	ロボットドライブを検証します。	<p>ロボットを使用しており、初めて構成を行う場合、ロボットドライブを適切に構成しているかどうかを検証します。</p> <p>特に、次を検証します。</p> <ul style="list-style-type: none"> <li>■ メディアおよびデバイスの管理とストレージユニットの構成の両方で同じロボット番号が使用されているかどうか。</li> <li>■ 各ロボットに一意のロボット番号が割り当てられているかどうか。</li> </ul> <p>UNIX 版 <b>NetBackup</b> サーバーでは、設定に含まれるメディアとデバイスの管理部分のみを検証できます。検証するには、<code>tpreq</code> コマンドを実行してメディアのマウントを要求します。マウントが完了したことを検証して、メディアがマウントされたドライブを確認します。問題が発生したホストからこの処理を繰り返し、すべてのドライブに対してメディアのマウントおよびマウント解除を行います。この操作が正常に実行される場合、ポリシーまたはストレージユニットの構成に問題がある可能性が高くなります。操作が完了したら、メディアに対して <code>tpunmount</code> コマンドを実行します。</p>
手順 8	テストポリシーにロボットを含めます。	<p>以前に非ロボットドライブを構成しており、システムにロボットが含まれている場合、テストポリシーを変更してロボットを指定します。ロボットにボリュームを追加します。ボリュームは、ロボットの <b>EMM</b> データベースホスト上の <b>NetBackup</b> ボリュームプールに存在する必要があります。</p> <p>手順 3 に戻り、ロボットに対してこの手順を繰り返します。この手順によって、<b>NetBackup</b> によるボリュームの検出、そのボリュームのマウントおよびロボットドライブの使用が可能かどうかを検証できます。</p>
手順 9	ロボットテストユーティリティを使います。	<p>ロボットに問題がある場合は、テストユーティリティを試行します。</p> <p>p.206 の「<b>ロボットテストユーティリティについて</b>」を参照してください。</p> <p>バックアップまたはリストアの実行中は、ロボットテストユーティリティを使用しないでください。これらのユーティリティを使用すると、対応するロボットプロセスによるメディアのロードやアンロードなどのロボット操作が実行されません。そのため、メディアのマウントでタイムアウトが発生し、ロボットのインベントリや取り込み、取り出しなどの他のロボット操作が実行されなくなる場合があります。</p>
手順 10	テストポリシーを拡張します。	<p>テストポリシーにユーザースケジュールを追加します (テストする時間がバックアップ処理時間帯に含まれるようにする必要があります)。前述の手順で検証済みのストレージユニットおよびメディアを使用します。</p>

手順	処理	説明
手順 11	<p>ファイルをバックアップおよびリストアします。</p>	<p>マスターサーバー上でクライアントユーザーインターフェースを使用して、ファイルのユーザーバックアップおよびリストアを開始します。状態および進捗ログで操作を監視します。操作が正常に実行される場合、マスターサーバー上でクライアントソフトウェアが機能していることが検証されます。</p> <p>失敗した場合、<b>NetBackup</b> の [すべてのログエントリ (All Log Entries)] レポートを確認します。問題をさらに特定するには、次に示すデバッグログのうち、該当するデバッグログを確認します。</p> <p>UNIX システムでは、デバッグログは /usr/opensv/netbackup/logs/ ディレクトリに存在します。Windows コンピュータでは、デバッグログは <code>install_path¥NetBackup¥logs¥</code> ディレクトリに存在します。</p> <p>次のプロセス用のデバッグログディレクトリが存在します。</p> <ul style="list-style-type: none"> <li>■ bparchive (UNIX の場合のみ)</li> <li>■ bpbackup (UNIX の場合のみ)</li> <li>■ bpbkar</li> <li>■ bpcd</li> <li>■ bplist</li> <li>■ bprd</li> <li>■ bprestore</li> <li>■ nbwin (Windows の場合のみ)</li> <li>■ bpinetd (Windows の場合のみ)</li> </ul> <p>特定のクライアント形式に適用されるログに関する説明を参照できます。</p> <p>ログについて詳しくは、『<b>NetBackup</b> ログリファレンスガイド』を参照してください。</p>
手順 12	<p>テストポリシーを再構成します。</p>	<p>テストポリシーを再構成して、ネットワークの他の位置に存在するクライアントを指定します。前述の手順で検証済みのストレージユニットおよびメディアを使用します。必要に応じて、<b>NetBackup</b> クライアントソフトウェアをインストールします。</p>
手順 13	<p>デバッグログディレクトリを作成します。</p>	<p>次に示すプロセスのデバッグログディレクトリを作成します。</p> <ul style="list-style-type: none"> <li>■ サーバー上の bprd</li> <li>■ クライアント上の bpcd</li> <li>■ クライアント上の bpbkar</li> <li>■ クライアント上の nbwin (Windows の場合のみ)</li> <li>■ クライアント上の bpbackup (Windows クライアント以外の場合)</li> <li>■ bpinetd (Windows の場合のみ)</li> <li>■ tar</li> <li>■ メディアサーバー: bpbbrm、bpdm、bptm</li> </ul> <p>特定のクライアント形式に適用されるログに関する説明を参照できます。</p> <p>ログについて詳しくは、『<b>NetBackup</b> ログリファレンスガイド』を参照してください。</p>

手順	処理	説明
手順 14	クライアントとマスターサーバーの間の通信を検証します。	<p>手順 8 で指定したクライアントからユーザーバックアップを行い、次にリストアを行います。これらの操作はクライアントとマスターサーバー間の通信、クライアントの NetBackup ソフトウェアを検証します。</p> <p>エラーが起きた場合は、[アクティビティモニター (Activity Monitor)] でジョブの [詳細の状態 (Detailed Status)] を確認します。</p> <p>[すべてのログエントリ (All Log Entries)] レポートと、前の手順で作成したデバッグログを調べます。エラーが発生した場合、原因は、サーバーとクライアントの間の通信の問題である可能性が高くなります。</p>
手順 15	他のクライアントまたはストレージユニットをテストします。	テストポリシーが正常に動作した場合、必要に応じて特定の手順を繰り返し、他のクライアントおよびストレージユニットを検証します。
手順 16	残りのポリシーとスケジュールをテストします。	すべてのクライアントおよびストレージユニットが機能する場合、マスターサーバー上のストレージユニットを使用する、残りのポリシーおよびスケジュールをテストします。スケジュールバックアップが失敗した場合、[すべてのログエントリ (All Log Entries)] レポートにエラーが表示されていないかどうかを確認します。それから、エラー状態コードの一部に示される推奨処置に従います。

## メディアサーバーおよびクライアントの検証

メディアサーバーを使う場合は、次の手順を使用して実行可能な状態であることを検証します。メディアサーバーをテストする前に、マスターサーバー上のすべての問題を解決します。

p.34 の「[マスターサーバーおよびクライアントの検証](#)」を参照してください。

表 2-7                   メディアサーバーとクライアントをテストする手順

手順	処理	説明
手順 1	レガシーデバッグログを有効にします。	<p>次を入力することにより、サーバー上の適切なレガシーデバッグログを有効にします。</p> <p>UNIX と Linux の場合: <code>/usr/opensv/netbackup/logs/mklogdir</code></p> <p>Windows の場合: <code>install_path¥NetBackup¥logs¥mklogdir.bat</code></p> <p>『<a href="#">NetBackup ログリファレンスガイド</a>』を参照してください。</p> <p>該当するログが不明な場合、問題が解決するまですべてのログを有効にします。問題が解決したら、レガシーデバッグログディレクトリを削除します。</p>

手順	処理	説明
手順 2	テストポリシーを構成します。	<p>ユーザースケジュールを使用してテストポリシーを構成するには (テストする時間がバックアップ処理時間帯に含まれるように設定します)、次の手順を実行します。</p> <ul style="list-style-type: none"> <li>■ メディアサーバーをクライアントとして指定し、ストレージユニットを指定します (非ロボットドライブが望ましい)。</li> <li>■ ストレージユニット内のデバイスの EMM データベースホストにボリュームを追加します。ボリュームが NetBackup ボリュームプール内に存在することを確認します。</li> <li>■ ドライブにボリュームを挿入します。bp1abel コマンドを実行して事前にボリュームにラベル付けしない場合、使用されていないメディア ID が NetBackup によって自動的に割り当てられます。</li> </ul>
手順 3	デーモンとサービスを検証します。	<p>すべての NetBackup デーモンまたはサービスがマスターサーバーで実行されていることを検証します。また、すべてのメディアおよびデバイスの管理デーモンまたはサービスがメディアサーバーで実行されていることを検証します。</p> <p>この検証を実行するには、次のいずれかを行います。</p> <ul style="list-style-type: none"> <li>■ UNIX システムの場合は、次のコマンドを実行します。  <code>/usr/opensv/netbackup/bin/bpps -x</code></li> <li>■ Windows システムの場合は、Windows の [コントロールパネル] の [管理ツール] の [サービス] を使用します。</li> </ul>
手順 4	ファイルをバックアップおよびリストアします。	<p>マスターサーバーと問題なく動作することを検証済みのクライアントから、ユーザーバックアップを実行し、次にリストアを実行します。</p> <p>このテストによって、次のことが検証されます。</p> <ul style="list-style-type: none"> <li>■ NetBackup メディアサーバーソフトウェア。</li> <li>■ メディアサーバー上の NetBackup によるメディアのマウントと、構成したドライブの使用の可否。</li> <li>■ マスターサーバープロセス (nbpem、nbjm、nbrb)、EMM サーバープロセス (nbemm)、メディアサーバープロセス (bpcd、bpbrm、bpdm、bptm) の間の通信。</li> <li>■ メディアサーバープロセス (bpbrm、bpdm、bptm) とクライアントプロセス (bpcd と bpbkar) との間の通信。</li> </ul> <p>ドライブまたはメディアに関連する障害の場合、ドライブが起動状態で、ハードウェアが機能しているかどうかを確認します。</p>
手順 5	マスターサーバーとメディアサーバーの間の通信を確認します。	<p>マスターサーバーとメディアサーバーの間の通信に問題がある可能性がある場合、デバッグログで関連するプロセスを確認します。</p> <p>デバッグログを確認しても問題が解決しない場合、次のログを確認します。</p> <ul style="list-style-type: none"> <li>■ システムログ (UNIX サーバーの場合)</li> <li>■ イベントビューアのアプケーションログおよびシステムログ (Windows サーバーの場合)</li> <li>■ vmd のデバッグログ</li> </ul>

手順	処理	説明
手順 6	ハードウェアが正しく動作することを確認します。	<p>ドライブまたはメディアに関連する障害の場合、ドライブが実行中で、ハードウェアが正しく機能しているかどうかを確認します。</p> <p>ハードウェア障害については、各ベンダーが提供するマニュアルを参照してください。</p> <p>初期構成の状態でロボットを使用する場合は、ロボットドライブが適切に構成されているかどうかを検証します。</p> <p>特に、次を検証します。</p> <ul style="list-style-type: none"> <li>■ メディアおよびデバイスの管理とストレージユニットの構成の両方で同じロボット番号が使用されているかどうか。</li> <li>■ 各ロボットに一意のロボット番号が割り当てられているかどうか。</li> </ul> <p>UNIX サーバーでは、構成内のメディアおよびデバイスの管理部分だけを検証できます。検証するには、<code>tpreq</code> コマンドを実行してメディアのマウントを要求します。マウントが完了したことを検証して、メディアがマウントされたドライブを確認します。問題が発生したホストからこの処理を繰り返し、すべてのドライブに対してメディアのマウントおよびマウント解除を行います。これらの手順は、メディアサーバーから実行します。この操作が正常に実行される場合、ポリシーまたはメディアサーバーのストレージユニットの構成に問題がある可能性が高くなります。操作が完了したら、<code>tpunmount</code> コマンドを実行して、メディアのマウントを解除します。</p>

手順	処理	説明
手順 7	テストポリシーにロボットデバイスを含めます。	<p>以前に非ロボットドライブを構成しており、メディアサーバーにロボットが接続されている場合、テストポリシーを変更してロボットを指定します。また、EMM サーバーにロボットのボリュームを追加します。ボリュームが NetBackup ボリュームプールおよびロボットに存在するかどうかを検証します。</p> <p>ロボットに対して、手順 3 以降を繰り返します。この手順によって、NetBackup によるボリュームの検出、そのボリュームのマウントおよびロボットドライブの使用が可能かどうかを検証できます。</p> <p>失敗した場合、NetBackup の[すべてのログエントリ (All Log Entries)]レポートを確認します。デバイスまたはメディアに関連するエラーが表示されていないかどうかを確認します。</p> <p>『NetBackup 管理者ガイド Vol. 1』を参照してください。</p> <p>[すべてのログエントリ (All Log Entries)]レポートを使用しても問題が解決しない場合、次のログを確認します。</p> <ul style="list-style-type: none"> <li>■ メディアサーバー上のシステムログ (UNIX サーバーの場合)</li> <li>■ ロボットの EMM サーバー上に存在する vmd のデバッグログ</li> <li>■ イベントビューアのアプリケーションログおよびシステムログ (Windows システムの場合)</li> </ul> <p>初めて構成を行う場合、ロボットドライブを適切に構成しているかどうかを検証します。他のサーバーで構成済みのロボット番号は使用しないでください。</p> <p>テストユーティリティを試行します。</p> <p>p.206 の「ロボットテストユーティリティについて」を参照してください。</p> <p>バックアップまたはリストアの実行中は、ロボットテストユーティリティを使用しないでください。これらのユーティリティを使用すると、対応するロボットプロセスによるメディアのロードやアンロードなどのロボット操作が実行されません。そのため、メディアのマウントでタイムアウトが発生し、ロボットのインベントリや取り込み、取り出しなどの他のロボット操作が実行されなくなる場合があります。</p>
手順 8	他のクライアントまたはストレージユニットをテストします。	<p>テストポリシーが正常に動作した場合、必要に応じて特定の手順を繰り返し、他のクライアントおよびストレージユニットを検証します。</p>
手順 9	残りのポリシーとスケジュールをテストします。	<p>すべてのクライアントおよびストレージユニットが機能する場合、メディアサーバー上のストレージユニットを使用する、残りのポリシーおよびスケジュールをテストします。スケジュールバックアップが失敗した場合、[すべてのログエントリ (All Log Entries)]レポートにエラーが表示されていないかどうかを確認します。次に、該当する状態コードに記載されている推奨処置を実行します。</p>

# UNIX クライアントとのネットワーク通信の問題の解決

次の手順では、NetBackup 状態コード 25、54、57、58 に関連付けられた NetBackup の通信の問題を解決します。この手順には、UNIX クライアント用と Windows クライアント用があります。

**メモ:** NetBackup の問題の解決を試行する前に、NetBackup とは関係のないネットワーク構成が正常に機能していることを常に確認します。

UNIX クライアントの場合、次の手順を実行します。この手順を実行する前に、`/usr/opensv/netbackup/bp.conf` ファイルに `VERBOSE=5` オプションを追加します。

**表 2-8** UNIX クライアントとのネットワーク通信の問題を解決する手順

手順	処理	説明
手順 1	デバッグログディレクトリを作成します。	<p>通信の再試行時、デバッグログには、問題の分析に有効なデバッグの詳細情報が表示されません。</p> <p>次のディレクトリを作成します。</p> <ul style="list-style-type: none"> <li>■ <code>bpcd</code> (マスターサーバーとクライアントに)</li> <li>■ <code>vnetd</code> (マスターサーバーとクライアントに)</li> <li>■ <code>bprd</code> (マスターサーバーに)</li> </ul> <p>クライアントとメディアサーバーの通信ではなくクライアントとマスターサーバーの通信の問題をデバッグするには、<code>bprd</code> ログディレクトリを使います。</p>
手順 2	新しい構成または変更を行った構成をテストします。	<p>新しい構成または変更を行った構成の場合、次の手順を実行します。</p> <ul style="list-style-type: none"> <li>■ 最新の変更を確認し、これらの変更によって問題が発生していないことを確認します。</li> <li>■ クライアントソフトウェアがインストールされており、クライアントのオペレーティングシステムをサポートすることを確認します。</li> <li>■ 次の項の説明に従って、NetBackup 構成内のクライアント名、サーバー名およびサービスのエントリを確認します。</li> </ul> <p><b>p.72</b> の「<a href="#">NetBackup のホスト名およびサービスエントリの検証</a>」を参照してください。</p> <p>クライアント上で <code>hostname</code> コマンドを実行して、クライアントがマスターサーバーに要求を送信するときのホスト名を判断することもできます。マスターサーバー上の <code>bprd</code> のデバッグログを確認し、サーバーが要求を受信したときに発生するイベントを判断します。</p>

手順	処理	説明
手順 3	名前解決を検証します。	<p>名前解決を検証するには、マスターサーバーとメディアサーバーで次のコマンドを実行します。</p> <pre># bpclntcmd -hn client name</pre> <p>結果が予想外の場合、nsswitch.conf ファイル、hosts ファイル、ipnodes ファイル、resolv.conf ファイルの名前解決サービスの構成を見直します。</p> <p>また、クライアントで次を実行し、バックアップを実行するマスターサーバーとメディアサーバーの名前の正引き参照と逆引き参照を調べます。</p> <pre># bpclntcmd -hn server name</pre> <pre># bpclntcmd -ip IP address of server</pre>
手順 4	ネットワークの接続を検証します。	<p>サーバーからクライアントに対して ping を実行することによって、クライアントとサーバーの間でのネットワークの接続を検証します。</p> <pre># ping clientname</pre> <p>ここで、<i>clientname</i> は NetBackup のポリシー構成で構成されているクライアントの名前です。</p> <p>たとえば、ant という名前のポリシークライアントに ping を実行すると想定します。</p> <pre># ping ant ant.nul.nul.com: 64 byte packets 64 bytes from 199.199.199.24: icmp_seq=0. time=1. ms ----ant.nul.nul.com PING Statistics---- 2 packets transmitted, 2 packets received, 0% packet loss round-trip (ms)  min/avg/max = 1/1/1</pre> <p>ping の成功により、サーバーとクライアントの間の接続が検証されます。ping が失敗し、ICMP がホストの間でブロックされない場合は、続行する前に NetBackup に関係のないネットワークの問題を解決してください。</p> <p>ping コマンドの形式によっては、クライアント上の bpcd ポートに bpcd を実行できます。次にコマンドの例を示します。</p> <pre># ping ant 1556</pre> <p>1556 (PBX)、13724 (vnetd) の順 ( がデフォルトで試行する順序と同じ) で ping を実行します。[NBU-39038: New for 8.1. gary.nelson. 4/13/2017]NetBackup これにより、閉じているポートがわかるため、効率的にポートを開いて接続を試みることができます。</p>

手順	処理	説明
手順 5	クライアントが正しいポートで bpcd への接続を待機していることを確認します。	クライアントで、次のいずれかのコマンド (プラットフォームおよびオペレーティングシステムによって異なる) を実行します。 <pre>netstat -a   grep bpcd netstat -a   grep 13782 rpcinfo -p   grep 13782</pre> <p><b>1556 (PBX) と 13724 (vnetd)</b> で繰り返します。ポートに問題がない場合、想定される出力は次のとおりです。</p> <pre># netstat -a   egrep '1556 PBX 13724 vnetd 13782 bpcd'   grep LISTEN *.1556      *.*        0          0 49152      0 LISTEN *.13724     *.*        0          0 49152      0 LISTEN *.13782     *.*        0          0 49152      0 LISTEN</pre> <p><b>LISTEN</b> は、クライアントがポートで接続を待機していることを示します。</p> <p><b>NetBackup</b> プロセスを正しく実行している場合に想定される出力を以下に示します。</p> <pre># ps -ef   egrep 'pbx_exchange vnetd bpcd'   grep -v grep root    306  1  0 Jul 18 ? 13:52 /opt/VRTSspbx/bin/pbx_exchange root 10274  1  0 Sep 13 ?  0:11 /usr/opensv/netbackup/bin/vnetd -standalone root 10277  1  0 Sep 13 ?  0:45 /usr/opensv/netbackup/bin/bpcd -standalone</pre> <p>マスターサーバーとメディアサーバーで手順を繰り返し、クライアントに通信をテストします。</p>
手順 6	telnet によってクライアントに接続します。	クライアントで、telnet を使用して <b>1556 (PBX) と 13724 (vnetd)</b> に接続します。両方のポートを調べて、少なくともどちらかで接続が確立されていることを確認します。telnet 接続が成功した場合は、手順 8 の実行が終了するまで接続を保持します。手順を実行したら、 <b>Ctrl+C</b> を押して接続を切断します。 <pre>telnet clientname 1556 telnet clientname 13724</pre> <p>ここで、<b>clientname</b> は <b>NetBackup</b> のポリシー構成で構成されているクライアントの名前です。次に例を示します。</p> <pre># telnet ant vnetd Trying 199.999.999.24 ... Connected to ant.nul.nul.com. Escape character is '^]'.  この例では、telnet によってクライアント ant への接続を確立できます。 <p>マスターサーバーとメディアサーバーで手順を繰り返し、クライアントに通信をテストします。</p> </pre>

手順	処理	説明
手順 7	サーバーホストのアウトバウンドソケットを識別します。	マスターサーバーとメディアサーバーで: 手順 6 の telnet コマンドに使用されたアウトバウンドソケットを識別するには、次のコマンドを使用します。サーバーがポリシークライアントを解決する適切な IP アドレスを指定します。送信元 IP (10.82.105.11)、送信元ポート (45856)、送信先ポート (1556) に注意してください。 <pre># netstat -na   grep '&lt;client_IP_address&gt;'   egrep '1556 13724' 10.82.105.11.45856 10.82.104.99.1556 49152 0 49152 0 ESTABLISHED</pre> telnet がまだ接続されていて、ソケットが表示されていない場合は、ポート番号のフィルタを削除し、サイトがサービス名をマップしたポート番号を確認します。手順 5 のポート番号でプロセスが待機していることを確認します。 <pre>\$ netstat -na   grep '&lt;client_IP_address&gt;' 10.82.105.11.45856 10.82.104.99.1234 49152 0 49152 0 ESTABLISHED</pre> ソケットが ESTABLISHED 状態ではなく SYN_SENT 状態である場合、サーバーホストは接続を確立しようとしています。ただし、ファイアウォールにより、アウトバウンド TCP SYN のクライアントホストへの到達、または返す方向の TCP SYN+ACK のサーバーホストへの到達はブロックされます。
手順 8	telnet 接続がこのクライアントホストに到達することを確認します。	マスターサーバーとメディアサーバーで、telnet 接続がこのクライアントホストに到達することを確認するには、次のコマンドを実行します。 <pre>\$ netstat -na   grep '&lt;source_port&gt;' 10.82.104.99.1556 10.82.105.11.45856 49152 0 49152 0 ESTABLISHED</pre> 次のいずれかの状況が発生します。 <ul style="list-style-type: none"> <li>■ telnet が接続されていてもソケットが存在しない場合、telnet はクライアントホストと同じ IP アドレスを誤って共有している他のホストに到達しています。</li> <li>■ ソケットが ESTABLISHED ではなく SYN_RCVD 状態である場合、接続はこのクライアントホストに到達しました。ただし、ファイアウォールにより、TCP SYN+ACK のサーバーホストへの到達はブロックされます。</li> </ul>
手順 9	クライアントとマスターサーバーの間の通信を検証します。	bpclntcmd ユーティリティを使用して、クライアントからマスターサーバーへの通信を検証します。-pn および -sv を指定して NetBackup クライアント上で実行した場合、(クライアント上の bp.conf ファイルで構成されている) NetBackup マスターサーバーへの問い合わせが開始されます。その後、マスターサーバーから問い合わせ元のクライアントに情報が戻されます。bpclntcmd についての詳細情報を参照できます。 <p>p.83 の「bpclntcmd ユーティリティについて」を参照してください。</p> PBX、vnetd および bprd のデバッグログに、他のエラーの性質に関する詳細が示されます。

# Windows クライアントとのネットワーク通信の問題の解決

次の手順では、NetBackup 状態コード 54、57 および 58 に関連付けられた NetBackup の通信の問題を解決します。この手順には、UNIX クライアント用と Windows クライアント用があります。

---

**メモ:** NetBackup の問題の解決を試行する前に、NetBackup とは関係のないネットワーク構成が正常に機能していることを常に確認します。

---

この手順は、PC クライアントでのネットワーク通信の問題の解決に役立ちます。

## ネットワーク通信の問題を解決する方法

- 1 失敗した操作を再試行する前に、次の操作を実行します。
  - クライアントのログレベルを上げます (『NetBackup 管理者ガイド Vol I』の「クライアント設定のプロパティ」を参照)。
  - NetBackup マスターサーバー上に bprd のデバッグログディレクトリを作成し、クライアント上に bpcd のデバッグログを作成します。
  - NetBackup サーバーで、[詳細 (Verbose)]レベルを 1 に設定します。ログレベルの変更について詳しくは、『NetBackup ログリファレンスガイド』を参照してください。
- 2 新しいクライアントの場合、NetBackup 構成内のクライアントおよびサーバーの名前を検証します。

p.72 の「NetBackup のホスト名およびサービスエントリの検証」を参照してください。
- 3 サーバーからクライアントまたはクライアントからサーバーに ping を実行して、クライアントとサーバー間のネットワーク接続を検証します。次のコマンドを使用します。

```
# ping hostname
```

ここで、*hostname* は、次のものに構成されているホストの名前です。

- NetBackup ポリシー構成
- WINS
- DNS (該当する場合)
- システムディレクトリ %SystemRoot%\system32\drivers \etc\hosts の hosts ファイル

すべてのインスタンスで ping が正常に実行された場合、サーバーとクライアントの間の接続が検証されます。

ping が失敗した場合、NetBackup に関係のないネットワークの問題が存在します。次の手順に進む前にこの問題を解決する必要があります。最初に、ワークステーションが起動されているかどうかを確認します。ワークステーションに関連する接続の問題では、ワークステーションが起動されていないことが主な原因となるためです。

- 4 Microsoft Windows クライアントで、ログを確認して NetBackup Client サービスがアクティブであることを確認します。[コントロールパネル]の[管理ツール]の[サービス]を使用して、NetBackup Client Service が実行中であるかどうかを検証します。必要に応じて起動します。

- bpcd のデバッグログに問題またはエラーが表示されていないかどうかを確認します。これらのログを有効にして使用方法については、『NetBackup ログリファレンスガイド』を参照してください。
- NetBackup クライアントとサーバーの両方で、指定している NetBackup Client Service (bpcd) のポート番号が一致しているかどうかを検証します (デフォルトでは 13782)。次のいずれかを実行します。

Windows の場合

NetBackup Client Service のポート番号を調べます。

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インターフェースを起動します。[ファイル (File)]メニューから [NetBackup クライアントのプロパティ (Client Properties)] を選択します。[NetBackup クライアントのプロパティ (Client Properties)]ダイアログボックスの[ネットワーク (Network)]タブで NetBackup Client Service のポート番号を確認します。

[ネットワーク (Network)]タブの設定が services ファイルの設定と一致しているかどうかを検証します。services ファイルは次の位置に存在します。

```
%SystemRoot%\system32\drivers\etc\services
(Windows)
```

[ネットワーク (Network)]タブの値は、NetBackup Client Service が起動されると services ファイルに書き込まれます。

UNIX NetBackup サーバー

bpcd ポート番号は /etc/services ファイルにあります。Windows 版 NetBackup サーバーの場合、[ホストプロパティ (Host Properties)]の[クライアントプロパティ (Client Properties)]ダイアログボックスを参照します。

p.86 の「[ホストプロパティ (Host Properties)]ウィンドウを使用した構成設定へのアクセス」を参照してください。

必要に応じて、ポート番号を修正します。その後、Windows クライアントおよびサーバーの場合、NetBackup Client Service を停止し、再起動します。

NetBackup のポートの割り当ては、他のアプリケーションとの競合を解消するために変更する必要がある場合を除き、変更しないでください。ポートの割り当てを変更する場合、すべての NetBackup クライアントとサーバー上で同様に変更してください。これらの番号は、NetBackup 構成全体で同じである必要があります。

- 5** Microsoft Windows クライアント上の NetBackup Request サービス (bprd) のポート番号が、サーバー上の番号と一致しているかどうかを検証します (デフォルトは 13720)。次のいずれかを実行します。

Windows クライアント NetBackup Client Service のポート番号を調べます。

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インターフェースを起動します。[ファイル (File)]メニューから[NetBackup クライアントのプロパティ ( Client Properties)]を選択します。  
[NetBackup クライアントのプロパティ (Client Properties)]ダイアログボックスの[ネットワーク (Network)]タブで NetBackup Client Service のポート番号を確認します。

[ネットワーク (Network)]タブの設定が services ファイルの設定と一致しているかどうかを検証します。services ファイルは次の位置に存在します。

```
%SystemRoot%\system32\drivers\etc\services
(Windows)
```

[ネットワーク (Network)]タブの値は、NetBackup Client Service が起動されると services ファイルに書き込まれます。

UNIX NetBackup サーバー bprd ポート番号は /etc/services ファイルにあります。

p.86 の「[ホストプロパティ (Host Properties)]ウィンドウを使用した構成設定へのアクセス」を参照してください。

Windows NetBackup サーバー [ホストプロパティ (Host Properties)]ウィンドウの[クライアントプロパティ (Client Properties)]ダイアログボックスでこれらの番号を設定します。

p.86 の「[ホストプロパティ (Host Properties)]ウィンドウを使用した構成設定へのアクセス」を参照してください。

- 6** hosts ファイルまたは同等のファイルに NetBackup サーバー名が含まれているかどうかを検証します。hosts ファイルを次に示します。

Windows の場合 %SystemRoot%\system32\drivers\etc\hosts

UNIX の場合 /etc/hosts

- 7 クライアント上で ping または同等のコマンドを実行して、クライアントからサーバーへの接続を検証します (サーバーからクライアントへの接続は、手順 3 で検証済みです)。
- 8 クライアントの TCP/IP プロトコルスタックでサーバーからの telnet 接続および ftp 接続が許可されている場合、これらのサービスの接続の確認も試行します。
- 9 bpcIntcmd ユーティリティを使用して、クライアントからマスターサーバーへの通信を検証します。-pn および -sv オプションを指定してクライアント上で実行した場合、(クライアント上のサーバーリストに構成されている) マスターサーバーへの問い合わせが開始されます。その後、マスターサーバーから問い合わせ元のクライアントに情報が戻されます。

p.83 の「[bpcIntcmd ユーティリティについて](#)」を参照してください。

- 10 bptestbpcd ユーティリティを使用して、NetBackup サーバーから別の NetBackup システムの bpcd デーモンへの接続の確立を試行します。成功すると、確立されているソケットに関する情報がレポートされます。

bptestbpcd 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。

- 11 クライアントのオペレーティングシステムがクライアントソフトウェアによってサポートされているかどうかを検証します。

## vnetd プロキシ接続のトラブルシューティング

Veritas ネットワークデーモンの vnetd プロセスとそのプロキシプロセスは、NetBackup ホストとリモートホスト間の通信を可能にします。

セキュリティ証明書失効のトラブルシューティング情報は次のトピックを参照してください。

p.50 の「[vnetd プロキシ接続の必要条件](#)」を参照してください。

p.51 の「[vnetd プロキシ接続のトラブルシューティングの開始点](#)」を参照してください。

p.52 の「[vnetd プロセスとプロキシがアクティブであることの確認](#)」を参照してください。

p.52 の「[ホスト接続がプロキシされることの確認](#)」を参照してください。

p.53 の「[vnetd プロキシ接続のテスト](#)」を参照してください。

p.55 の「[接続と受け入れのプロセスのログファイルの確認](#)」を参照してください。

p.55 の「[vnetd プロキシログファイルの表示](#)」を参照してください。

接続の問題の原因を特定できない場合は、Veritas のサポート担当者にお問い合わせください。

## vnetd プロキシ接続の必要条件

同じ NetBackup ドメイン内での通信の場合:

- ホスト ID ベースの証明書と証明書失効リストは、NetBackup 8.1 以降のホストに存在する必要があります。

NetBackup のグローバルセキュリティ設定では、NetBackup が証明書をプロビジョニングする方法を構成します。

NetBackup 管理コンソールの[セキュリティ管理 (Security Management)]でグローバル設定を確認します。

NetBackup がホスト間で使用する証明書を確認するには、`-verbose` オプションとともに `bptestbpcd -host` コマンドとオプションを使用し、`bpcIntcmd -pn` コマンドとオプションを使用します。

- ホスト ID は、NetBackup 8.1 以降のすべてのホストでホスト名に対してマッピングする必要があります。

NetBackup のグローバルセキュリティ設定では、NetBackup がホスト ID を名前にマッピングする方法を構成します。

NetBackup 管理コンソールの[セキュリティ管理 (Security Management)]でグローバル設定を確認します。代わりに、次のコマンドとオプションを使用することもできます。

Windows の場合:

```
install_path\Veritas\NetBackup\bin\admincmd\nbseccmd  
-getsecurityconfig -autoaddhostmapping
```

UNIX の場合:

```
/usr/opensv/netbackup/bin/admincmd/nbseccmd -getsecurityconfig  
-autoaddhostmapping
```

- 8.1 より前の NetBackup ホストでは、安全でない通信を許可する必要があります。NetBackup のグローバルセキュリティ設定では、NetBackup が 8.1 より前のホストと通信できるようにするかどうかを構成します。

NetBackup 管理コンソールの[セキュリティ管理 (Security Management)]でグローバル設定を確認します。代わりに、次のコマンドとオプションを使用することもできます。

Windows の場合:

```
install_path\Veritas\NetBackup\bin\admincmd\nbseccmd  
-getsecurityconfig -insecurecommunication
```

UNIX の場合:

```
/usr/opensv/netbackup/bin/admincmd/nbseccmd -getsecurityconfig  
-insecurecommunication
```

- マスターサーバー上の NetBackup Web サービスはアクティブである必要があります。それらがアクティブであることを確認するには、次の NetBackup コマンドとオプションを使用します。

Windows の場合: `install_path\Veritas\NetBackup\bin\NBCertcmd -ping`

UNIX の場合: `/usr/opensv/netbackup/bin/nbcertcmd -ping`

- 外部 CA が署名した証明書を使用するようにマスターサーバーが構成されている場合、ホストは外部 CA が署名した証明書を適切なマスターサーバーのドメインに登録する必要があります。

外部 CA のサポートと証明書の登録については、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

自動イメージレプリケーションでは、宛先ドメインの信頼できるマスターサーバーすべてで、ソースマスターサーバーからのホスト ID ベースの証明書が必要です。

外部 CA が署名した証明書を使用するようにマスターサーバーが構成されている場合、外部 CA が署名した証明書を使用するソースとターゲットのマスターサーバー間で信頼が確立されていることを確認します。

詳しくは、『Deduplication ガイド』を参照してください。NetBackup

## vnetd プロキシ接続のトラブルシューティングの開始点

NetBackup 状態コード 61 および 76xx の範囲の状態コードは、vnetd プロキシ通信に関連しています。

NetBackup ジョブが vnetd プロキシ接続の問題のため失敗する場合は、ジョブの詳細で該当する状態コードを調べます。状態コードの説明については NetBackup のマニュアルを参照してください。次の形式の接続 ID をすべて書き留めます。これらは、追加のトラブルシューティングに役立ちます。

```
{23FAD260-7D2F-11E7-91C6-2EB679166937}:OUTBOUND
```

NetBackup ジョブ中にエラーがない場合は、対象の状態コードの操作の終了状態を調べます。また、操作に関連するプロセスのデバッグログを調べます。最初に、要求を実行した操作またはサービスを開始したコマンドを確認します。

次で説明されている状態コードを見つけることができます。

- [NetBackup 状態コードリファレンスガイド](#)。
- NetBackup 管理コンソールヘルプ。
- NetBackup 管理コンソールのトラブルシューター。
- NetBackup OpsCenter のヘルプ。

ジョブが実行されなかった場合は、vnetd プロセスとそのプロキシがアクティブであることを確認します。

## vnetd プロセスとプロキシがアクティブであることの確認

Windows の場合は、[タスク マネージャー]の[プロセス]タブ ([コマンド ライン]列の表示が必要) を使用して、プロキシがアクティブかどうかを確認できます。UNIX と Linux の場合は、次のように **NetBackup bpps** コマンドを使用できます。

```
$ bpps
...output shortened...
root 13577 1 0 Jun27 ? 00:00:04 /usr/opensv/netbackup/bin/vnetd -standalone
root 13606 1 0 Jun27 ? 00:01:55 /usr/opensv/netbackup/bin/vnetd -proxy inbound_proxy

-number 0
root 13608 1 0 Jun27 ? 00:00:06 /usr/opensv/netbackup/bin/vnetd -proxy outbound_proxy

-number 0
root 13610 1 0 Jun27 ? 00:00:06 /usr/opensv/netbackup/bin/vnetd -proxy http_tunnel
```

vnetd プロセスまたはプロキシが実行中かどうかに応じて、次を実行します。

- vnetd プロセス (-standalone) を実行していない場合は起動します。
- vnetd プロセスが実行中の場合は、vnetd のデバッグログで、vnetd がプロキシを起動しようとしていることを確認します。
- vnetd プロセスがインバウンドとアウトバウンドのプロキシを起動しようとしている場合は、プロキシログファイルで、プロキシが接続を待機しない理由を確認します。nbpxyhelper の短いコンポーネント名またはそのオリジネータ ID 486 を vxlogview コマンドとともに使用します。
- vnetd プロセスが HTTP トンネルプロキシを起動しようとする場合は、HTTP トンネルプロキシログを調べます。nbpxytn1 の短いコンポーネント名またはそのオリジネータ ID 490 を vxlogview コマンドとともに使用します。

vnetd プロセスとそのプロキシがアクティブである場合、接続がプロキシされたかどうかを確認します。

## ホスト接続がプロキシされることの確認

NetBackup 8.1 以降のサーバーで **NetBackup bptestbpcd** コマンドを使用すると、次のように、リモートホストへの接続がプロキシされることを確認できます。

Windows の場合: `install_path\Veritas\NetBackup\bin\admincmd\bptestbpcd -host remote_host`

UNIX の場合: `/usr/opensv/netbackup/bin/admincmd/bptestbpcd -host remote_host`

次のコマンドの出力例の PROXY は、接続がプロキシされることを示します。

```
1 1 0
127.0.0.1:42553 -> 127.0.0.1:52236 PROXY 10.81.41.245:895 -> 10.81.40.148:1556
127.0.0.1:35386 -> 127.0.0.1:49429 PROXY 10.81.41.245:51325 -> 10.81.40.148:1556
```

接続がプロキシされる場合は、プロキシ接続をテストします。

## vnetd プロキシ接続のテスト

vnetd プロキシ接続をテストするために使う **NetBackup** コマンドは、サーバーとクライアントで異なります。

### vnet プロキシ接続をサーバーからテストする

**NetBackup 8.1** 以降のサーバーから **NetBackup 8.1** 以降のホストへの接続をテストするには、**NetBackup** `bptestbpcd` コマンドとともに `-verbose` オプションを使用することができます。コマンド出力で、状態コードやエラーの兆候を調べます。状態コードの説明については **NetBackup** のマニュアルを参照してください。

次の例では、`connect-host.example.com` という名前の **NetBackup** メディアサーバーから `accept-host.example.com` という名前のメディアサーバーへの接続テストの成功を示しています。

```
# bptestbpcd -host accept-host.example.com -verbose
1 1 1
127.0.0.1:43697 -> 127.0.0.1:58089 PROXY 10.80.97.186:47054 -> 10.80.97.140:1556
127.0.0.1:52061 -> 127.0.0.1:58379 PROXY 10.80.97.186:37522 -> 10.80.97.140:1556
LOCAL_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = a753da9b-b1ff-4a5f-b57d-69a4e2b47e29
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
PEER_CERT_SUBJECT_COMMON_NAME = b900a238-d7be-4c6e-8af6-19b5c1d1dec4
PEER_NAME = connect-host.example.com
HOST_NAME = accept-host.example.com
CLIENT_NAME = accept-host.example.com
VERSION = 0x08100000
PLATFORM = linuxR_x86_2.6.18
PATCH_VERSION = 8.1.0.0
SERVER_PATCH_VERSION = 8.1.0.0
MASTER_SERVER = master.example.com
EMM_SERVER = master.example.com
NB_MACHINE_TYPE = MEDIA_SERVER
SERVICE_TYPE = VNET_DOMAIN_CLIENT_TYPE
PROCESS_HINT = 7157d866-8eb2-45bb-bde8-486790c0b40c
```

次の例は、反対に、セキュリティ証明書が失効した後に失敗する、同じメディアサーバーに対する接続テストを示します。

```
# bptestbpcd -host accept-host.example.com -verbose
<16>bptestbpcd main: Function ConnectToBPCD(accept-host.example.com) failed: 7653
<16>bptestbpcd main: The Peer Certificate is revoked
<16>bptestbpcd main: The certificate of the host that you want to connect to is revoked.
Revocation Reason Code : 0 Revocation Time : 1502637798: 7653
The Peer Certificate is revoked
```

NetBackup ホストは、その他の NetBackup ホストと通信できるように、有効なホスト ID ベースのセキュリティ証明書と有効な証明書失効リストが必要です。いずれかが欠けていると、通信できません。この場合、状態コード **7653** を探し、エラーから回復するための説明および推奨処置を確認します。

## vnetd プロキシ接続をクライアントからテストする

NetBackup 8.1 以降のクライアントでは、NetBackup `bpcIntcmd` コマンドを使用してマスターサーバーへの接続をテストできます。コマンド出力で、状態コードやエラーの兆候を調べます。状態コードの説明については NetBackup のマニュアルを参照してください。コマンドの構文は次のとおりです。

Windows の場合:

```
install_path¥Veritas¥NetBackup¥bin¥bpcIntcmd -pn -verbose
```

UNIX の場合:

```
/usr/opensv/netbackup/bin/bpcIntcmd -pn -verbose
```

次に、`bpcIntcmd` コマンドに対する正常な応答の例を示します。

```
# bpcIntcmd -pn -verbose
expecting response from server master.example.com
127.0.0.1:52704 -> 127.0.0.1:33510 PROXY 10.80.97.186:40348 -> 10.80.97.157:1556
LOCAL_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = 7157d866-8eb2-45bb-bde8-486790c0b40c
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
PEER_CERT_SUBJECT_COMMON_NAME = b900a238-d7be-4c6e-8af6-19b5c1d1dec4
PEER_IP = 10.80.97.186
PEER_PORT = 40348
PEER_NAME = connect-host.example.com
POLICY_CLIENT = *NULL*
Old Domain Service Type VNET_DOMAIN_SERVER_TYPE and Hint
New Domain Service Type VNET_DOMAIN_SERVER_TYPE and Hint
7157d866-8eb2-45bb-bde8-486790c0b40c
```

次の例では、反対に、失効した証明書がある `bpcIntcmd` クライアントでの NetBackup コマンドに対する応答を示します。

```
# bpcIntcmd -pn -verbose
Unable to perform peer host name validation. Curl error has occurred for peer name:
master.example.com, self name: connect-host: 0
    [PROXY] Encountered error (VALIDATE_PEER_HOST_PROTOCOL_RUNNING) while processing
        (ValidatePeerHostProtocol).: 1
Can't connect to host master.example.com: cannot connect on socket (25)
```

vnetd プロキシ接続がアクティブである場合、接続と受け入れのプロセスのログファイルを調べます。

## 接続と受け入れのプロセスのログファイルの確認

接続を開始する **NetBackup** プロセスが接続プロセスであり、その接続のターゲットが受け入れプロセスです。接続と受け入れのプロセスでは、それぞれ、アウトバウンドとインバウンドの vnetd プロキシプロセスと通信します。各プロキシプロセスでは、接続が許可されているかどうかを確認します。

接続プロセスと受け入れたプロセスのデバッグログでは、プロキシとの対話が表示されます。状態コードおよび状態メッセージについてログを調べます。また、一意のインバウンドとアウトバウンドの接続 ID のログを調べます。vnetd プロキシプロセスログを調べる必要がある場合、これらの ID を使用できます。ほとんどの接続はいずれかのホストからデバッグすることができます。

たとえば、次の接続プロセスログファイルの抜粋では、ホストの検証エラーによって接続できなかったことが示されています。

```
Peer host validation failed for SECURE connection; Peer host:
accepting-host.example.com, Error: 8618, Message: Connection is
dropped, because the host ID-to-hostname mapping is not yet
approved., nbu status = 7648, severity = 1
```

**NetBackup** ホストの名前は、そのホスト ID にマッピングされている必要があります。ホスト名が **NetBackup** で適切にマッピングされていない場合、通信に失敗します。この場合、状態コード **7648** を探し、エラーから回復するための説明および推奨処置を確認します。

接続プロセスと受け入れプロセスのログファイルを調べても問題の兆候が見つからない場合は、vnetd プロキシログファイルを調べます。接続 ID を使用して関連情報を見つけることができます。

## vnetd プロキシログファイルの表示

vnetd プロキシプロセスは、vnetd 自体とは別のファイルにログ記録されます。次の表に、vnetd プロキシの統合ログの短いコンポーネント名とのオリジネータ ID を示します。

表 2-9 vnetd プロキシログファイル

プロキシ	コンポーネント名	オリジネータ ID
インバウンドとアウトバウンドのプロキシ	nbpxyhelper	486
HTTP トンネル	nbpxytnl	490

次に、短いコンポーネント名を使用してインバウンドとアウトバウンドのプロキシログファイルを表示する **NetBackup vxlogview** コマンド構文を示します。

**Windows** の場合: `install_path\Veritas\NetBackup\bin\vxlogview -p NB -i nbpxyhelper`

**UNIX** の場合: `/usr/openv/netbackup/bin/vxlogview -p NB -i nbpxyhelper`  
`vxlogview` コマンドには、ログファイルの表示を調整するためのオプションが含まれています。たとえば、`vnetd` プロキシ接続をトラブルシューティングするには、次のように接続 ID を使用することができます。

```
vxlogview -p NB -i nbpxyhelper -X  
'{23FAD260-7D2F-11E7-91C6-2EB679166937}:OUTBOUND'
```

---

**メモ:** **Windows** の場合、接続 ID 文字列から一重引用符の記号を省略します。

---

『[NetBackup コマンドリファレンスガイド](#)』では、`vxlogview` コマンドとそのオプションについて説明しています。

『[NetBackup ログリファレンスガイド](#)』では、統合ログとログファイルの表示方法について説明しています。

## セキュリティ証明書失効のトラブルシューティング

ジョブでは、**NetBackup** は [ジョブの詳細 (Job Details)] にエラーの原因を書き込みます。ジョブとは、バックアップ、リストア、複製、およびレプリケーションです。ホスト証明書に関連するエラーをトラブルシューティングするには、ジョブの詳細でメッセージと状態コードを調べます。証明書、失効、および **CRL** に関連するメッセージを探します。メッセージに付随する状態コードはすぐ横にあります。問題を解決するための説明と推奨される操作について、状態コードの説明を確認します。

`vnetd` プロキシプロセスログファイルを調べる必要があることもあります。ジョブの詳細と同様に、証明書、失効、および **CRL** に関連するメッセージと状態コードについてログを調べます。メッセージに付随する状態コードはすぐ横にあります。

p.55 の「[vnetd プロキシログファイルの表示](#)」を参照してください。

次で説明されている状態コードを見つけることができます。

- [NetBackup 状態コードリファレンスガイド](#)。
- [NetBackup 管理コンソールヘルプ](#)。
- [NetBackup 管理コンソールのトラブルシューター](#)。
- [NetBackup OpsCenter のヘルプ](#)。

ホストの CRL は、トラブルシューティングに影響する可能性があります。

p.58 の「[ホストの CRL が証明書失効のトラブルシューティングに与える影響](#)」を参照してください。

次のトピックでは、いくつかのセキュリティ証明書失効シナリオのトラブルシューティングについて説明します。

p.59 の「[証明書が失効しているまたは CRL が使用できないため、NetBackup のジョブが失敗する](#)」を参照してください。

p.60 の「[明らかなネットワークエラーが原因で NetBackup ジョブが失敗する](#)」を参照してください。

p.61 の「[利用不能なリソースが原因で NetBackup ジョブが失敗する](#)」を参照してください。

p.62 の「[マスターサーバーのセキュリティ証明書が失効している](#)」を参照してください。

問題の原因を特定できない場合は、Veritas のテクニカルサポート担当者にお問い合わせください。

## クラウドプロバイダの無効化された SSL 証明書の問題のトラブルシューティング

SSL が有効で CRL オプションが有効になっている場合、CRL に対して、それぞれの非自己署名 SSL 証明書が検証されます。証明書が無効である場合、NetBackup はクラウドプロバイダに接続しません。

クラウドストレージの CRL 検証の問題をトラブルシューティングするには、次のログで cURL エラー 60 を参照します。

- `tpcommand` ログで、構成の問題を確認します。
- `bpptm` ログで、バックアップおよびリストアの問題を確認します。
- クラウドストレージサーバーが停止している場合は、`nbrmms` ログを確認します。

現象:

- クラウドストレージの作成が失敗する。
- クラウドストレージサーバーが停止しているため、バックアップジョブが失敗する。

原因:

- 証明書が無効であるため、NetBackup がクラウドプロバイダに接続しない。
- CRL ファイルのダウンロードに失敗した。

解決方法:

- CRL 検証エラーが問題である場合は、セキュリティ管理者にお問い合わせください。
- ダウンロードエラーが問題である場合は、ファイアウォールの設定を確認します。  
『NetBackup クラウド管理者ガイド』を参照し、CRL のすべての要件を満たしていることを確認します。

## クラウドプロバイダの CRL のダウンロードに関する問題のトラブルシューティング

メディアサーバーで、ポート 80 に対する HTTP 接続がすべて遮断されているため、ダウンロードが失敗します。

現象:

- クラウドストレージの作成が失敗する。
- クラウドストレージサーバーが停止しているため、バックアップジョブが失敗する。

原因:

- NetBackup が宛先ポート 80 に接続できない。
- ファイアウォールの設定で、不明な URL への接続が許可されていない。

解決方法:

- ポート 80 に接続するようにファイアウォールの設定を更新します。それができない場合は、CRL チェックをオフにします。
- CRL をオフにするには、クラウドストレージのホストプロパティを変更します。詳しくは、『NetBackup クラウド管理者ガイド』を参照してください。

## ホストの CRL が証明書失効のトラブルシューティングに与える影響

各 NetBackup ホストは定期的に最新の証明書失効リストを取得します。ホストの証明書失効リストが最新の場合、ジョブのエラーメッセージと状態コードは正確であり、信頼できます。同様に、NetBackup 監査メッセージは正確であり、信頼できます。

しかし、CRL が最新でない場合は、ジョブのエラーがネットワークエラーとして表示されることがあります。NetBackup のジョブの詳細を確認するだけでなく、コマンド出力を確認してエラーを特定する必要があることがあります。

各 NetBackup ホストは、CRL が更新されたときにのみ、新しい証明書の失効について学習します。

## NetBackup CA が署名した証明書が使用されている場合

マスターサーバーの CRL は 60 分ごと、または失効後 5 分以内に生成されます。裏を返せば、他の NetBackup ホストがマスターサーバーから新しい CRL を要求する間隔はより長い場合があります。

[証明書配備のセキュリティレベル (Security level for certificate deployment)] の設定は、すべての NetBackup ホストの CRL 更新間隔を決定します。すべてのホストは同じ時間間隔で CRL を更新しますが、各ホストが新しい CRL を要求するタイミングはさまざまです。NetBackup

NetBackup 管理コンソールの [セキュリティ管理 (Security Management)] でセキュリティ設定を確認します。

## 外部 CA が署名した証明書が使用されている場合

ECA\_CRL\_PATH 構成オプションで指定されている CRL を使用するように NetBackup ホストが構成されている場合、CRL は ECA\_CRL\_PATH\_SYNC\_HOURS に従って更新されます。

CDP から CRL をダウンロードするように NetBackup ホストが構成されている場合、CRL は ECA\_CRL\_REFRESH\_HOURS に従って更新されます。

CRL の外部証明書構成オプションとグローバルセキュリティ設定について詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

## 証明書が失効しているまたは CRL が使用できないため、NetBackup のジョブが失敗する

### 現象

NetBackup ジョブが失敗します。

### 原因

次のいずれかの原因があります。

- クライアントのセキュリティ証明書が失効している。
- クライアントをバックアップするメディアサーバーのセキュリティ証明書が失効している。
- マスターサーバーのセキュリティ証明書が失効している。
- クライアント、メディアサーバー、またはマスターサーバーの CRL が破損または欠落している。

### 解決方法

1. 次のメッセージの文字列と隣接する状態コードをジョブの詳細で確認します。

- 証明書失効の場合、certificate と revoked を含むメッセージの文字列を探します。
  - CRL の場合、certificate revocation list または CRL および missing、corrupted、または unavailable を含むメッセージの文字列を探します。
2. 必要に応じて、クライアントまたはメディアサーバー証明書が失効しているかどうかを確認します。  
p.63 の「[NetBackup ホストの証明書の状態の確認](#)」を参照してください。
  3. 外部 CA が署名した証明書が使用されている場合、外部証明書のセクションを参照してください。  
p.66 の「[外部 CA が署名した証明書の無効化に関する問題のトラブルシューティング](#)」を参照してください。
  4. 状態コードとリカバリのための推奨される操作の説明については、**NetBackup** のマニュアルを参照してください。可能な場合は、問題を解決します。
  5. 適切なタイミングで問題を解決できない場合は、バックアップポリシーから失効したホストを削除するか、ポリシーを非アクティブ化します。失効したホストがメディアサーバーの場合は、非アクティブ化します。(ホストを非アクティブ化すると、「NetBackup バージョン」エラーを無視できます。)
  6. **NetBackup CA** が署名した証明書の場合、セキュリティの問題を解決した後で、失効したホストの証明書を再発行します。証明書の再発行については『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。
  7. 必要に応じて、クライアントをバックアップポリシーに再度追加し、バックアップポリシーをアクティブ化するか、メディアサーバーをアクティブ化します。

## 明らかなネットワークエラーが原因で NetBackup ジョブが失敗する

### 現象

ネットワークエラー 23、25、59 などによりジョブが失敗することがあります。

### 原因

**NetBackup** クライアントまたはクライアントをバックアップするメディアサーバーのホスト証明書が失効している可能性があります。また、クライアントまたはメディアサーバーの CRL が古い、見つからない、または破損していることもあります。この場合、クライアントまたはメディアサーバーがホスト証明書が失効していることを判別できません。ジョブは実行されますが、通信が失敗し、ネットワークエラーとして表示されます。

### 解決方法

1. クライアントまたはメディアサーバー証明書が失効しているかどうかを確認します。  
p.63 の「[NetBackup ホストの証明書の状態の確認](#)」を参照してください。

2. 必要に応じて、次のいずれかを実行して原因を確認します。
  - 失効したホストにログオンし、vnetd プロキシログファイルを確認します。次を含むメッセージの文字列を探します。
    - PEER\_HOST\_PROTOCOL\_ERROR
    - certificate revocation list
    - CRL および missing または corrupted

p.55 の「[vnetd プロキシログファイルの表示](#)」を参照してください。
  - NetBackup bptestbpcd コマンドを使用し、ホスト証明書が失効しているかどうかを確認します。

p.63 の「[NetBackup ホストの証明書の状態の確認](#)」を参照してください。
3. 問題の解決方法:
  - ホストの CRL が見つからないか破損している場合、そのホストで CRL を更新します。

ホストの CRL を更新する方法については『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。
  - 外部 CA が署名した証明書が使用されている場合、外部証明書のセクションを参照してください。

p.66 の「[外部 CA が署名した証明書の無効化に関する問題のトラブルシューティング](#)」を参照してください。
  - NetBackup CA が署名したホスト証明書が失効している場合は、セキュリティの問題を解決し、証明書を再発行します。

証明書を再発行する方法については『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

## 利用不能なリソースが原因で NetBackup ジョブが失敗する

### 現象

証明書または CRL の問題が、利用不能なリソースとして表示されることがあります。たとえば、ジョブの詳細に、ストレージサーバーが停止または利用不能であることが表示される場合があります。ジョブは、タイムアウトになるまで延長された時間の間実行できることがあります。

### 原因

クライアントをバックアップまたはリストアするメディアサーバーのセキュリティ証明書が無効化されています。または、ディスクベースのストレージの場合、ストレージサーバーの証明書が無効化されていることがあります。

## 解決方法

1. クライアントおよびメディアサーバーまたはストレージサーバーでセキュリティ証明書の状態を確認します。  
  
p.63 の「[NetBackup ホストの証明書の状態の確認](#)」を参照してください。
2. どのホストに失効した証明書があるかによって、次のいずれかの操作を行います。
  - 失効したホストがクライアントの場合は、バックアップポリシーから削除するか、ポリシーを非アクティブ化します。
  - 失効したホストがメディアサーバーまたはストレージサーバーの場合は、非アクティブ化します。(ホストを非アクティブ化すると、「[NetBackup バージョン](#)」エラーを無視できます。)  
可能な場合は、異なるメディアサーバーまたはストレージサーバーを使用するようにストレージユニットを変更します。
3. 失効したホストを調査してセキュリティの問題を判別し、問題を解決します。  
外部 CA が署名した証明書が使用されている場合、外部証明書のセクションを参照してください。  
  
p.66 の「[外部 CA が署名した証明書の無効化に関する問題のトラブルシューティング](#)」を参照してください。
4. [NetBackup CA](#) が署名したホスト証明書が失効している場合は、セキュリティの問題を解決し、証明書を再発行します。証明書の再発行については『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。
5. 失効したホストを稼働状態に戻したら、クライアントのジョブを防ぐために加えたポリシーの変更を元に戻すか、メディアサーバーを再アクティブ化します。

## マスターサーバーのセキュリティ証明書が失効している

[NetBackup](#) マスターサーバーのセキュリティ証明書が失効していることは、[NetBackup](#) セキュリティにとって最悪のシナリオです。次の現象は、マスターサーバー証明書の失効を示している可能性があります。

- ジョブがネットワークエラーで失敗する。
- メディアサーバーが自動的に非アクティブ化される。
- ホストの `vnetd` プロキシプロセスログファイルで、マスターサーバーの証明書が失効していることが示されている。  
p.55 の「[vnetd プロキシログファイルの表示](#)」を参照してください。
- `bptestbpcd -host master_server` コマンド出力は、マスターサーバーの証明書が失効していることを示す場合があります。  
p.63 の「[NetBackup ホストの証明書の状態の確認](#)」を参照してください。

マスターサーバーが不正にアクセスされたままになっている場合は、次の操作を行います。

#### NetBackup CA が署名した証明書が使用されている場合

1. ホストの証明書失効リストを信頼しません。
2. 問題を解決し、マスターサーバーのセキュリティ証明書を再発行してから、マスターサーバーを稼働状態に戻します。
3. 問題を解決してマスターサーバーを稼働状態に戻すことができない場合は、交換します。その後、すべてのホスト証明書を再発行する必要があります。

外部 CA が署名した証明書が使用されている場合、マスターサーバーの証明書の無効化を元に戻すか、マスターサーバーの新しい証明書を登録できます。

p.66 の「外部 CA が署名した証明書の無効化に関する問題のトラブルシューティング」を参照してください。

## NetBackup ホストの証明書の状態の確認

### NetBackup CA が署名した証明書を使用する場合

NetBackup 証明書の状態が有効か無効化済みかを確認できます。これは、接続と通信の問題のトラブルシューティングに役立つことがあります。証明書の状態を確認する方法には、次の 3 つの方法があります。

- |  |  |
|--|--|
| <p>ホスト自体からホスト証明書を<br/>確認する</p>             | <p>この方法では、NetBackup <code>nbcertcmd</code> コマンドを使用します。</p> <p>p.64 の「ホストからホストの証明書の状態を確認するには」を参照してください。</p>                               |
| <p>NetBackup サーバーからホス<br/>ト証明書を確認する</p>    | <p>この方法では、NetBackup <code>bptestbpcd</code> コマンドを使用しま<br/>す。</p> <p>p.64 の「別のホストの証明書が失効している場合に NetBackup<br/>サーバーから確認する方法」を参照してください。</p> |
| <p>NetBackup 管理コンソールか<br/>らホスト証明書を確認する</p> | <p>p.65 の「NetBackup 管理コンソールを使用してホストの証明書<br/>を確認する方法」を参照してください。</p>   |

## ホストからホストの証明書の状態を確認するには

- 1 必要に応じて、NetBackup ホストで最新の証明書失効リストを取得するため、管理者として次のコマンドを実行します。

UNIX の場合: `/usr/opensv/netbackup/bin/nbcertcmd -getCRL [-server master_server_name]`

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -getCRL [-server master_server_name]`

デフォルト以外の NetBackup ドメインから CRL を取得するには、`-servermaster_server_name` オプションおよび引数を指定します。

- 2 NetBackup ホストで、管理者として次のコマンドを実行します。

UNIX の場合: `/usr/opensv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster] [-server master_server_name]`

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -hostSelfCheck [-cluster] [-server master_server_name]`

必要に応じて、次のオプションのいずれかまたは両方を使用します。

`-cluster` 仮想ホストの証明書を確認するには、NetBackup マスターサーバークラスターのアクティブノードでこのオプションを使用します。

`-server` デフォルト以外のマスターサーバーから証明書を確認するには、**Master\_server\_name** 引数を指定してこのオプションを使用します。

- 3 コマンドの出力を確認します。出力は、証明書が失効しているかいないかを示します。

## 別のホストの証明書が失効している場合に NetBackup サーバーから確認する方法

- 1 NetBackup マスターサーバーまたは NetBackup メディアサーバーで管理者として次のコマンドを実行します。

UNIX の場合: `/usr/opensv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

Windows の場合: `install_path¥NetBackup¥bin¥bptestbpcd -host hostname -verbose`

`-host hostname` には、証明書を確認するホストを指定します。

- 2 コマンドの出力を確認します。指定されたホストの証明書が失効している場合、コマンド出力には `The Peer Certificate is revoked` という文字列が含まれます。コマンド出力にこの文字列が含まれていない場合、証明書は有効です。

## NetBackup 管理コンソールを使用してホストの証明書を確認する方法

- 1 NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[証明書管理 (Certificate Management)]の順に展開します。
- 2 目的のホストの[証明書の状態 (Certificate State)]列で証明書の状態を調べます。

## 外部 CA が署名した証明書を使用する場合

外部 CA が署名したホスト証明書の状態が有効か無効化済みかを確認できます。これは、接続と通信の問題のトラブルシューティングに役立つことがあります。

証明書の状態を確認するには、次の 2 つの方法があります。

ホスト自体から p.65 の「[ホスト自体からホスト証明書を確認するには](#)」を参照してください。  
ホスト証明書を  
確認する

NetBackup p.66 の「[別のホストの証明書が失効している場合に NetBackup サーバーからサーバーからホスト証明書を確認する方法](#)」を参照してください。  
ホスト証明書を確認する

### ホスト自体からホスト証明書を確認するには

- 1 NetBackup CRL キャッシュ内の CRL を更新します。  
p.66 の「[外部 CA が署名した証明書の無効化に関する問題のトラブルシューティング](#)」を参照してください。
- 2 NetBackup ホストで、管理者として次のコマンドを実行します。  
UNIX の場合: `/usr/opensv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster]`  
Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -hostSelfCheck [-cluster]`  
仮想名の証明書を確認するには、クラスタマスターサーバーのアクティブノードで `-cluster` オプションを使用します。
- 3 コマンドの出力を確認します。出力は、証明書が無効化されているかいないかを示します。

別のホストの証明書が失効している場合に **NetBackup** サーバーから確認する方法

- 1 **NetBackup** マスターサーバーまたは **NetBackup** メディアサーバーで管理者として次のコマンドを実行します。

UNIX の場合: `/usr/opensv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

Windows の場合: `install_path¥NetBackup¥bin¥bptestbpcd -host hostname -verbose`

`-host hostname` には、証明書を確認するホストを指定します。

- 2 コマンドの出力を確認します。指定されたホストの証明書が無効化されている場合、コマンド出力には **The Peer Certificate is revoked** という文字列が含まれます。コマンド出力にこの文字列が含まれていない場合、証明書は有効です。

## 外部 CA が署名した証明書の無効化に関する問題のトラブルシューティング

**NetBackup CRL キャッシュ**は、`ECA_CRL_PATH` または `CDP` を使用して、必要な CRL で更新されます。

詳しくは、『**NetBackup セキュリティおよび暗号化ガイド**』の「外部 CA の証明書失効リストについて」の章を参照してください。

### 現象

証明書失効リストを使用できません (**NetBackup** 状態コード - 5982)

### 原因

- **NetBackup** が正しい CRL パスで構成されていない、または証明書に有効な CDP が含まれていない。
- ホストの **NetBackup CRL キャッシュ**に CRL がキャッシュされていない。

### 解決方法

- 1 `ECA_CRL_PATH` の設定が **NetBackup** 構成ファイルで指定されている場合、次を確認します。

- `ECA_CRL_PATH` に正しい CRL ディレクトリのパスが設定されている
- CRL ディレクトリに、すべての必要な証明書の発行者の CRL が含まれている (`ECA_CRL_CHECK` 設定に基づく)

CDP が使用されている (`ECA_CRL_PATH` が指定されていない) 場合

- あらゆる理由の証明書の無効化の情報を含む CRL を指す、1 つ以上の CDP (HTTP または HTTPS プロトコルを使用) が証明書にあることを確認します。

- CDP の URL がアクセス可能である。
- 2 ECA\_CRL\_PATH で指定されたディレクトリまたは CDP の場所で、CRL が有効であることを確認します。
    - CRL が PEM または DER 形式である。
    - CRL の期限が切れていない。
    - CRL が差分 CRL ではない。
    - CRL の最終更新日が将来の日付ではない。
  - 3 `bpclntcmd -crl_download` サービスが実行中の場合は、`bpclntcmd -terminate` コマンドを使用して終了させて、この操作を再試行します。
  - 4 次の場所にある NetBackup CRL キャッシュで、必要な CRL が利用可能であることを確認します。

UNIX の場合: `/usr/opensv/var/vxss/crl`

Windows の場合: `install_path¥NetBackup¥var¥vxss¥crl`

- 5 問題が解決しない場合は、次の場所にある `bpclntcmd` ログを調べます。

UNIX の場合: `/usr/opensv/netbackup/logs/bpclntcmd`

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

## 現象

証明書が失効している、または証明書は失効していないが「証明書が失効しています」エラーで NetBackup 操作が失敗する場合でも、NetBackup が正常に機能しています。

## 原因

NetBackup ホストの CRL キャッシュが更新されていません。

## 解決方法

- 1 次の場所にある CRL が更新されているかどうかを確認します。

UNIX の場合: `/usr/opensv/var/vxss/crl`

Windows の場合: `install_path\NetBackup\var\vxss\crl`

更新されていない場合は、ECA\_CRL\_CHECK 設定に従い、証明書チェーンの発行者のキャッシュされた CRL をクリーンアップします。

クリーンアップ操作では、`nbcertcmd -cleanupCRLCache -issuerHash SHA-1_hash_of_CRL_issuer_name` コマンドを使用します。

- 2 ECA\_CRL\_PATH の設定が NetBackup 構成ファイルで指定されている場合、必要なすべての発行者の最新の CRL が含まれていることを確認します。
- 3 `bpclntcmd -crl_download` サービスが実行中の場合は、`bpclntcmd -terminate` コマンドを使用して終了させて、この操作を再試行します。

## ネットワークとホスト名のトラブルシューティングについて

複数のネットワークと複数のホスト名があるクライアントを含む構成では、NetBackup 管理者はポリシーのエントリを慎重に構成する必要があります。管理者は、ネットワーク構成 (物理的な構成、ホスト名とエイリアス、NIS や DNS などのネームサービス、ルーティングテーブルなど) を考慮する必要があります。バックアップデータおよびリストアデータを特定のネットワークパスで送信する場合には、特にこれらを考慮する必要があります。

バックアップの場合、NetBackup は、ポリシーで構成されたホスト名に接続されます。オペレーティングシステムのネットワークコードでこの名前を解決し、システムのルーティングテーブルに定義されたネットワークパスでその接続を送信します。この判断には、`bp.conf` ファイルは関与しません。

クライアントからのリストアの場合、そのクライアントはマスターサーバーに接続されます。たとえば、UNIX コンピュータの場合、マスターサーバーは `/usr/opensv/netbackup/bp.conf` ファイルの先頭に指定されているサーバーです。Windows コンピュータの場合、マスターサーバーは、[NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)] ダイアログボックスの [バックアップおよびリストアに使用するサーバー (Server to use for backups and restores)] ドロップダウンメニューで指定します。このダイアログを開くには、のバックアップ、アーカイブおよびリストアインターフェースを起動し、[ファイル (File)] メニューから [NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)] を選択します。サーバー名を IP アドレスにマッピングする、クライアントのネットワークコードによってサーバーへのネットワークパスが決定されます。

接続を受信すると、ターゲットホストは接続しているホストのピアホスト名を判断します。ターゲットホストがマスターサーバーの場合は、ピアホスト名からクライアントの構成名も判断します。

ピアネームは、接続の IP アドレスから導出します。これは、(getnameinfo() ネットワークルーチンを使用して) アドレスがホスト名に変換される必要があることを意味します。接続が確立されると、次の行に示すとおり、この名前が bpcd または bprd のデバッグログに表示されます。

```
bpcd: Connection from host peername ipaddress ...
```

```
bprd: Connection from host peername ipaddress ...
```

クライアントでは、接続しているサーバーのピアホスト名は、ローカル NetBackup 構成内のサーバーまたはメディアサーバーのエントリと一致する必要があります (各サーバーエントリについて、文字列一致するか、getaddrinfo() の情報と比較)。

マスターサーバーでは、比較の方が複雑です。

その後、bpdbm プロセスの問い合わせ (UNIX/Linux ホストの場合) または NetBackup Database Manager サービス (Windows ホストの場合) によって、クライアントの構成名がピアネームから導出されます。

bpdbm プロセスは、次のクライアントが生成したクライアント名のリストとピアネームを比較します。

- バックアップが実行されたすべてのクライアント
- すべてのポリシー内に存在するすべてのクライアント

最初に文字列の比較が行われます。この比較は、ピアネームをクライアント名のリストと比較することで検証されます。

名前が一致しなかった場合、総あたりの方法が使用されます。この方法では、リスト内の各クライアント名について、getaddrinfo() を使用して見つかったすべての名前とエイリアスが比較されます。

最初に一致した名前が構成名になります。

比較が失敗すると、ほとんどの場合、要求内のホスト名がネットワークや NetBackup 構成などの管理制御下にないため、bprd が要求元クライアント (次に示す) をピアネームに置き換えます。

失敗した比較の例を次に示します。

クライアントに新しいネットワークインターフェースがあり、新しいネットワークを利用するために最初のサーバーエントリを変更したとします。マスターサーバーのネームサービスが、クライアントの新しいソース IP を、どのポリシーのクライアントのネットワークエイリアスでもないピアネームに解決します。

VERBOSE が設定されている場合、これらの比較は bpdbm のデバッグログに記録されます。クライアント上で bpcIntcmd コマンドを実行すると、クライアントの構成名を確認できます。たとえば、

```
# /usr/opensv/netbackup/bin/bpcIntcmd -pn (UNIX の場合)
```

```
# install_path¥NetBackup¥bin¥bpcIntcmd -pn (Windows の場合)
```

```
expecting response from server wind.abc.me.com  
danr.abc.me.com danr 194.133.172.3 4823
```

最初の出力行は、要求が送信されるサーバーを識別します。2 番目の出力行は、次の順序でサーバーの応答を示します。

- サーバーに接続するときに使うピアネーム
- クライアントの構成名
- サーバーへの接続の IP アドレス
- サーバーへの接続のソース IP アドレス

クライアントがサーバーに接続すると、クライアントからサーバーに次の 3 つの名前が送信されます。

- 参照クライアント
- 要求元のクライアント
- 宛先クライアント

**browse client** 名は、表示するクライアントファイル、またはリストア元のクライアントを識別するために使用されます。クライアント上のユーザーは、この名前を変更して、異なるクライアントからファイルのリストアを行うことができます。たとえば、**Windows** クライアントの場合、ユーザーはバックアップ、アーカイブおよびリストアインターフェースを使用してクライアント名を変更できます。(手順については、**NetBackup** のオンラインヘルプを参照)。ただし、この変更を有効にするには、管理者もそれに対応する変更をサーバーで行う必要があります。

『**NetBackup 管理者ガイド Vol. 1**』を参照してください。

要求元クライアントは、**CLIENT\_NAME** の値またはクライアントの `gethostname ()` 関数で取得された値です。

**destination client** 名は、管理者がサーバーからクライアントへのリストアを実行する場合だけ関連します。ユーザーリストアの場合、**destination client** と **requesting client** は同じです。管理者主導リストアの場合、管理者は **destination client** に異なる名前を指定できます。

これらの名前が `bprd` のデバッグログに表示されるまでに、**requesting client** 名はクライアントの構成名に変換されます。

リストアを完了するためにクライアントに接続し直すときに使う名前は、クライアントのピアネームまたは構成名のいずれかです。この処理は、リストア要求の種類(サーバーの **root** ユーザーからのリストア要求、クライアントからのリストア要求、異なるクライアントへのリストア要求など)によって影響を受けます。

特定のネットワークパスに対応するために **NetBackup** ポリシーのクライアント名を変更する場合、管理者は次のことを考慮する必要があります。

- クライアントで構成されたクライアント名。たとえば、**UNIX** の場合、クライアント名はクライアントの `bp.conf` ファイル内の `CLIENT_NAME` です。**Windows** クライアントの場合、この名前は[**NetBackup** クライアントのプロパティ (**NetBackup Client Properties**)]ダイアログボックスの[全般 (**General**)]タブに表示されます。このダイアログボックスを表示するには、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の[ファイル (**File**)]メニューから[**NetBackup** クライアントのプロパティ (**NetBackup Client Properties**)]を選択します。
- ポリシー構成で現在指定されているクライアント。
- マスターサーバーの `images` ディレクトリに記録されている既存のクライアントのバックアップイメージとアーカイブイメージ。**UNIX** サーバーの場合、`images` ディレクトリは `/usr/opensv/netbackup/db/images` です。**Windows** 版 **NetBackup** サーバーの場合、`images` ディレクトリは `install_path¥NetBackup¥db¥images` です。

クライアントが複数のネットワークでサーバーへ接続されているか、接続に関連する問題が原因でそのクライアントからのリストア要求が失敗した場合、これらのクライアント名について、管理者が手動で変更を加える必要がある可能性があります。

`tracert` (**UNIX**) および `tracert` (**Windows**) プログラムは通常、ネットワークの構成に関する有益な情報を提供します。

ドメインネームサービス (**DNS**) を使用している場合に、クライアントが `gethostname()` ライブラリを実行して取得した名前がマスターサーバーの **DNS** で認識されないと、マスターサーバーがクライアントの要求に応答できないことがあります。クライアントとサーバーの構成により、この状況が存在するかどうかを判断できます。クライアントで `gethostname()` 関数を使用すると、マスターサーバーの **DNS** で解決できない、修飾されていないホスト名が戻される場合があります。

ネームサービスを再構成する(ホストファイルを含む)ことも可能ですが、この解決方法が常に最適とはかぎりません。そのため、**NetBackup** では、マスターサーバーに特別なファイルが提供されています。このファイルは次のとおりです。

`/usr/opensv/netbackup/db/altnames/host.xlate` (**UNIX** の場合)

`install_path¥NetBackup¥db¥altnames¥host.xlate` (**Windows** の場合)

このファイルを作成および編集することで、**NetBackup** クライアントのホスト名を目的の名前に強制的に変換することができます。

`host.xlate` ファイルの各行には、数値キーと 2 つのホスト名の 3 つの要素が含まれます。各行は左揃えで、行内の各要素は空白文字で区切られます。

```
key peername client_as_known_by_server
```

次に、これらの変数について説明します。

- **key** は数値であり、NetBackup が変換を実行するケースの指定に使用します。現状では、この値は常に構成名の変換を示す 0 (ゼロ) とする必要があります。
- **peername** は変換する値です。これは、マスターサーバーの `getnameinfo()` が、クライアントによる接続元 IP アドレスを解決する値です。
- **client\_as\_known\_by\_server** は、クライアントが要求に応答するときに **peername** から置換される名前です。この名前は、マスターサーバーの NetBackup 構成で構成された名前である必要があります、通常はポリシー内のクライアントです。マスターサーバーによって使用されるネームサービスにも認識される必要があります、バックアップを実行するメディアサーバーのネットワークサービスによって認識される必要があります。

次に例を示します。

```
0 danr danr.eng.aaa.com
```

構成したクライアント名に対する要求 (数値キー 0 (ゼロ)) をマスターサーバーが受信した場合、名前は常にピアネームを置換します。

## NetBackup のホスト名およびサービスエントリの検証

この項では、ホスト名またはネットワーク接続に関連する問題が発生し、NetBackup 構成が適切であるかどうかを検証する必要がある場合に有効な手順を示します。手順の後にいくつかの例を示します。

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

p.68 の「ネットワークとホスト名のトラブルシューティングについて」を参照してください。

### NetBackup のホスト名およびサービスエントリを検証する方法

- 1 NetBackup でクライアントおよびサーバーのホスト名が正しく構成されているかどうかを検証します。実行する操作は調べるコンピュータによって異なります。

Windows サーバーと 次の手順を実行します。

Windows クライアントの  
 場合

- [バックアップおよびリストアに使用するサーバー (Server to use for backups and restores)] ドロップダウンリストで、マスターサーバーおよび各メディアサーバーの **SERVER** エントリが存在することを確認します。  
 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インターフェースを起動します。[ファイル (File)]メニューから[NetBackup マシンおよびポリシー形式の指定 (Specify Machines and Policy Type)]を選択します。[NetBackup マシンおよびポリシー形式の指定 (Specify Machines and Policy Type)]ダイアログボックスの[バックアップおよびリストアに使用するサーバー (Server to use for backups and restores)]ドロップダウンリストをクリックします。  
 Windows コンピュータでは、現在のマスターサーバーとして適切なサーバーがリストに表示されている必要があります。マスターサーバー上で **SERVER** エントリを追加または変更する場合は、**NetBackup Request** サービスと **NetBackup Database Manager** サービスを停止し、再起動します。
- [一般 (General)]タブで、正しいクライアントの名前を設定しており、マスターサーバー上のポリシーのクライアントリストで設定しているクライアント名と一致しているかどうかを検証します。  
 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インターフェースを起動します。[ファイル (File)]メニューから[NetBackup クライアントのプロパティ ( Client Properties)]を選択します。[NetBackup クライアントのプロパティ ( Client Properties)]ダイアログボックスで、[全般 (General)]タブをクリックします。
- マスターサーバーまたはメディアサーバー上で、そのサーバーを管理するための各 Windows 管理クライアントの **SERVER** エントリが存在することを確認します。
- マスターサーバーの `bp.conf` ファイル (UNIX の場合) またはサーバーリスト (Windows の場合) のホスト名に誤りがないことを確認します。ホスト名に誤りがあった場合、または `gethostbyname` によってホスト名を解決できない場合、次のエラーメッセージが **NetBackup** エラーログに記録されます。

```
Gethostbyname failed for
<host_name>:<h_errno_string> (<h_errno>)
One or more servers was excluded from the server
list because gethostby name() failed.
```

Windows 版 **NetBackup** サーバー上の[プロパティ (Properties)]ダイアログボックスの適切なタブでこれらの変更を加えることもできます。

p.86 の「[ホストプロパティ (Host Properties)]ウィンドウを使用した構成設定へのアクセス」を参照してください。

**UNIX NetBackup サーバーとクライアントの場合** bp.conf ファイルのサーバー名およびクライアント名のエントリを確認するには、次を実行します。

- 構成内のマスターサーバーおよび各メディアサーバーの SERVER エントリが存在することを確認します。マスターサーバーの名前が、リストの先頭に存在する必要があります。  
 マスターサーバー上で SERVER エントリを追加または変更する場合は、bprd と bpdbsm を停止してから再起動して変更を有効にします。
- マスターサーバーの bp.conf は、CLIENT\_NAME = *master server name* としてのマスターサーバー以外に他のクライアントの追加を必要としません。この名前はデフォルトで追加されます。

bp.conf ファイルは、UNIX クライアントでは /usr/opensv/netbackup ディレクトリに存在します。

UNIX クライアントのユーザーは、自分のホームディレクトリにユーザー固有の bp.conf ファイルを設定することもできます。\$HOME/bp.conf の CLIENT\_NAME オプションは、/usr/opensv/netbackup/bp.conf の同じオプションより優先されます。

マスターサーバー

次の必要なファイルのいずれかが作成済みかどうかを検証します。

- install\_path¥NetBackup¥db¥altnames ファイル (Windows の場合)
- /usr/opensv/netbackup/db/altnames ファイル (UNIX の場合)

host.xlate ファイルのエントリの要件に特に注意してください。

- 2 各サーバーおよびクライアントに NetBackup の予約済みポート番号についての必要なエントリを設定しているかどうかを検証します。

次の例では、デフォルトのポート番号を示します。

p.76 の「[UNIX マスターサーバーおよびクライアントのホスト名とサービスエントリの例](#)」を参照してください。

p.78 の「[UNIX マスターサーバーおよびメディアサーバーのホスト名とサービスエントリの例](#)」を参照してください。

p.80 の「[UNIX PC クライアントのホスト名とサービスエントリの例](#)」を参照してください。

p.81 の「[複数のネットワークに接続する UNIX サーバーのホスト名とサービスエントリの例](#)」を参照してください。

NetBackup のポートの割り当ては、他のアプリケーションとの競合を解消するために変更する必要がある場合を除き、変更しないでください。ポートの割り当てを変更する場合、すべての NetBackup クライアントとサーバー上で同様に変更してください。これらの番号は、NetBackup 構成全体で同じである必要があります。

- 3 NetBackup サーバー上で、services ファイルに次のエントリが含まれているかどうかを確認します。

- bpcd と bprd

- vmd
- bpdbm
- 構成済みロボットに対するプロセス。  
[『NetBackup デバイス構成ガイド』](#)を参照してください。

**NetBackup Client** デーモンまたはサービスの番号、**Request** デーモンまたはサービスのポート番号を検証します。実行する操作は、クライアントが **UNIX** か、**Microsoft Windows** によって異なります。

**UNIX** クライアントの場合 /etc/services ファイルの bprcd および bpcd エントリを確認します。

**Microsoft Windows** クライアントの場合 次を実行して、[NetBackup Client サービスポート (BPCD) (NetBackup client service port (BPCD))]と[NetBackup Request サービスポート (BPRD) (NetBackup request service port (BPRD))]の番号が、services ファイルの設定と一致しているかどうかを検証します。

クライアントのバックアップ、アーカイブおよびリストインターフェースを起動します。[ファイル (File)]メニューから[NetBackup クライアントのプロパティ (Client Properties)]を選択します。[NetBackup クライアントのプロパティ (NetBackup Client Properties)]ダイアログボックスの[ネットワーク (Network)]タブで[NetBackup Client サービスポート (BPCD) (NetBackup client service port (BPCD))]および[NetBackup Request サービスポート (BPRD) (NetBackup request service port (BPRD))]の番号を選択します。

[ネットワーク (Network)]タブの値は、NetBackup Client Service が起動されると services ファイルに書き込まれます。

services ファイルは次の場所にあります。

```
%SystemRoot%\system32\drivers\etc\services
```

- 4 UNIX サーバーとクライアントで、bpcd -standaloneのプロセスが動作していることを確認します。
- 5 Windows サーバーとクライアントで、NetBackup Client Service が実行中であるかどうかを検証します。
- 6 ネットワークで NIS を使っている場合、/etc/services ファイルに追加された NetBackup の情報をそれらのサービスに反映します。
- 7 NIS、WINS または DNS のホスト名の情報が、ポリシー構成、およびホスト名のエントリの設定に対応しているかどうかを確認します。Windows NetBackup サーバーと Microsoft Windows クライアントで、次を実行します。
  - [一般 (General)]タブを確認します。

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インターフェースを起動します。[ファイル (File)]メニューから[NetBackup クライアントのプロパティ (Client Properties)]を選択します。[NetBackup クライアントのプロパティ (Client Properties)]ダイアログボックスで、[全般 (General)]タブをクリックします。

- [バックアップおよびリストアに使用するサーバー (Server to use for backups and restores)]ド롭ダウンリストを確認します。  
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インターフェースを起動します。[ファイル (File)]メニューから[NetBackup マシンおよびポリシー形式の指定 (Specify Machines and Policy Type)]を選択します。[NetBackup マシンおよびポリシー形式の指定 (Specify Machines and Policy Type)]ダイアログボックスの[バックアップおよびリストアに使用するサーバー (Server to use for backups and restores)]ド롭ダウンリストをクリックします。
  - UNIX サーバーおよびクライアント上の `bp.conf` ファイルを確認します。
  - DNS の逆引きができるように構成しているかどうかを検証します。
- 8 `bpclntcmd` ユーティリティを使って各 NetBackup ノードの DNS、NIS、ローカルホストファイルの IP アドレスとホスト名設定を確認します。

---

**メモ:** FT (ファイバートランスポート) ターゲットデバイスはデバイスからのホスト名またはドメイン名の応答に基づいて名前が付きます。異なる VLAN ネットワークインターフェース名の代替コンピュータ名が DNS (Domain Name System) の `SERVER/MEDIA_SERVER` エントリやホストファイルに表示される場合にはプライマリ名が最初に表示されます。

---

p.83 の「[bpclntcmd ユーティリティについて](#)」を参照してください。

## UNIX マスターサーバーおよびクライアントのホスト名とサービスエントリの例

次の図には、1 つの UNIX クライアントを持つ UNIX マスターサーバーが示されています。

図 2-1 UNIX マスターサーバーおよびクライアント

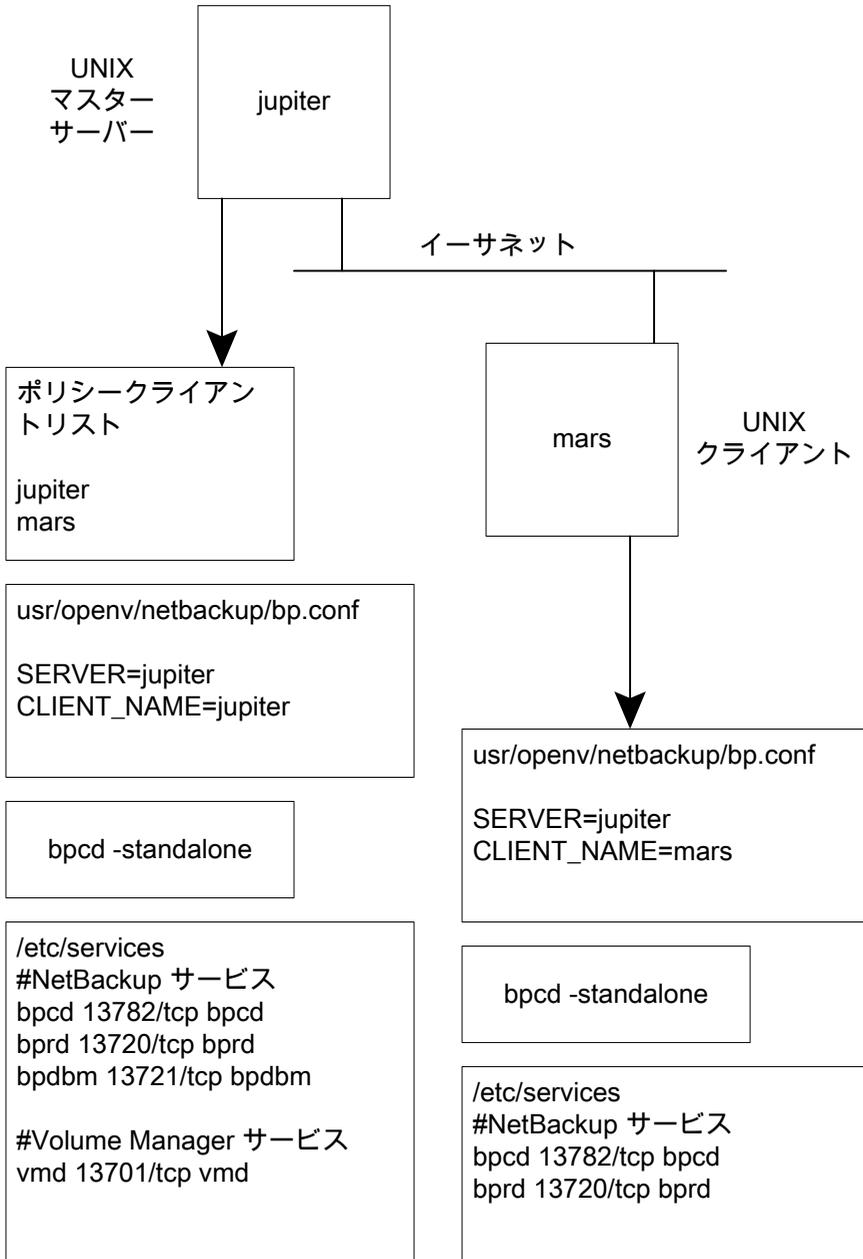


図 2-1については、次の点を考慮してください。

- 適用可能なすべてのネットワーク構成は NetBackup 情報を反映するように更新する必要があります。たとえば、この情報には /etc/hosts ファイル、NIS および DNS (使用されている場合) を含めることができます。

## UNIX マスターサーバーおよびメディアサーバーのホスト名とサービスエントリの例

次の図に、*saturn* という名前の UNIX 版 NetBackup メディアサーバーを示します。すべてのコンピュータ上の `bp.conf` ファイルに *saturn* の SERVER エントリが追加されていることに注意してください。これは 2 番目のエントリで、マスターサーバー *jupiter* の SERVER エントリの下に存在します。

図 2-2 UNIX マスターサーバーおよびメディアサーバー

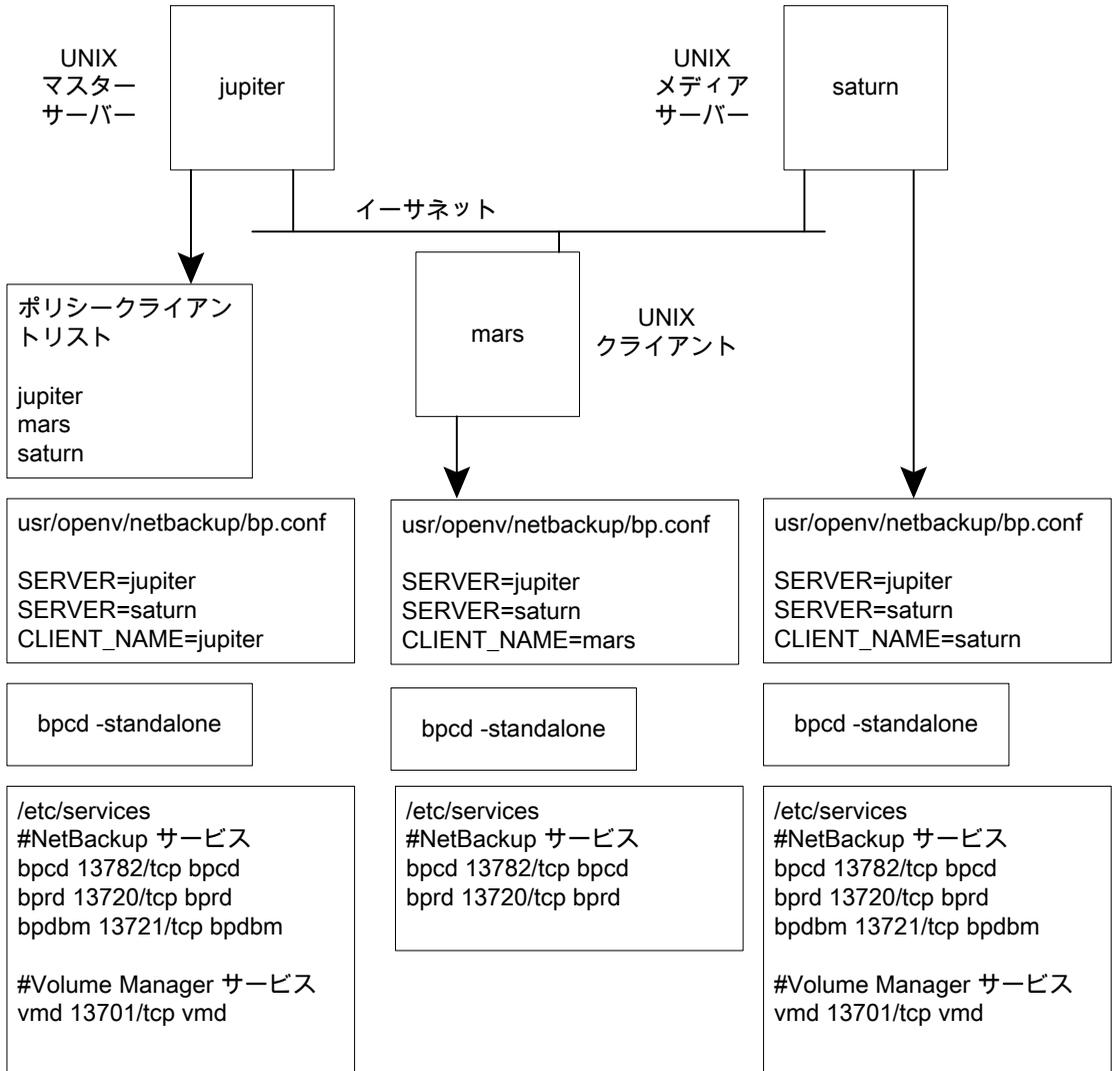


図 2-2については、次の点を考慮してください。

- 適用可能なすべてのネットワーク構成は **NetBackup** 情報を反映するように更新する必要があります。たとえば、この情報には `/etc/hosts` ファイル、NIS および DNS (使用されている場合) を含めることができます。

## UNIX PC クライアントのホスト名とサービスエントリの例

次の図には、PC (Windows) クライアントを持つ NetBackup マスターサーバーが示されています。UNIX クライアントが含まれる場合も、サーバー構成は次の図と同じです。これらのクライアントには、inetd.conf エントリは存在しません。

図 2-3 UNIX PC クライアント

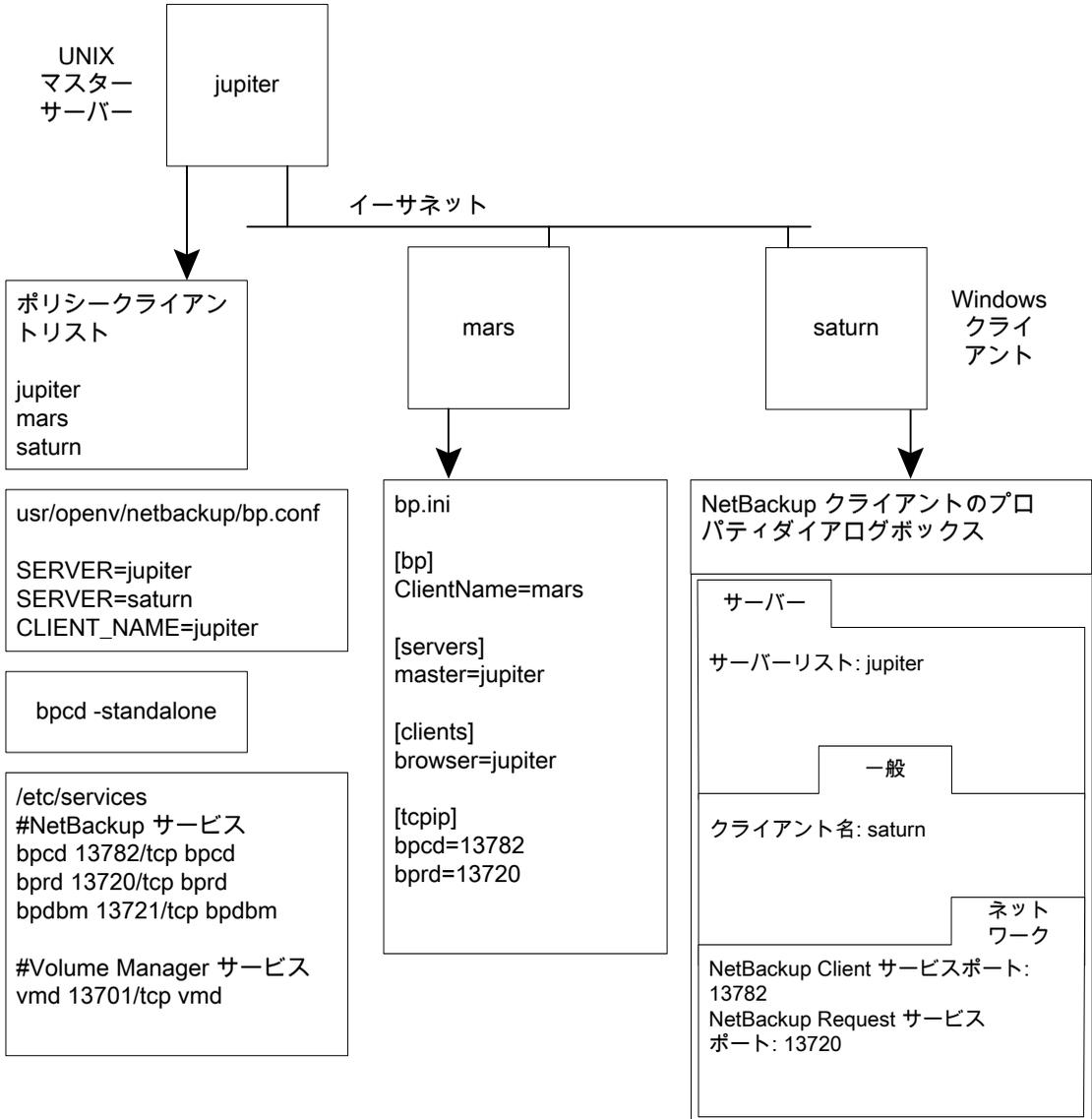


図 2-3 については、次の点を考慮してください。

- 適用可能なすべてのネットワーク構成は NetBackup 情報を反映するように更新する必要があります。たとえば、この情報には /etc/hosts ファイル、NIS および DNS (使用されている場合) を含めることができます。

## 複数のネットワークに接続する UNIX サーバーのホスト名とサービスエントリの例

次の図に、2 つのイーサネットに接続し、両方のネットワークにクライアントを持つ NetBackup サーバーを示します。サーバーのホスト名は、一方のネットワーク上では *jupiter* で、もう一方のネットワーク上では *meteor* です。

図 2-4 複数のネットワークに接続する UNIX サーバー

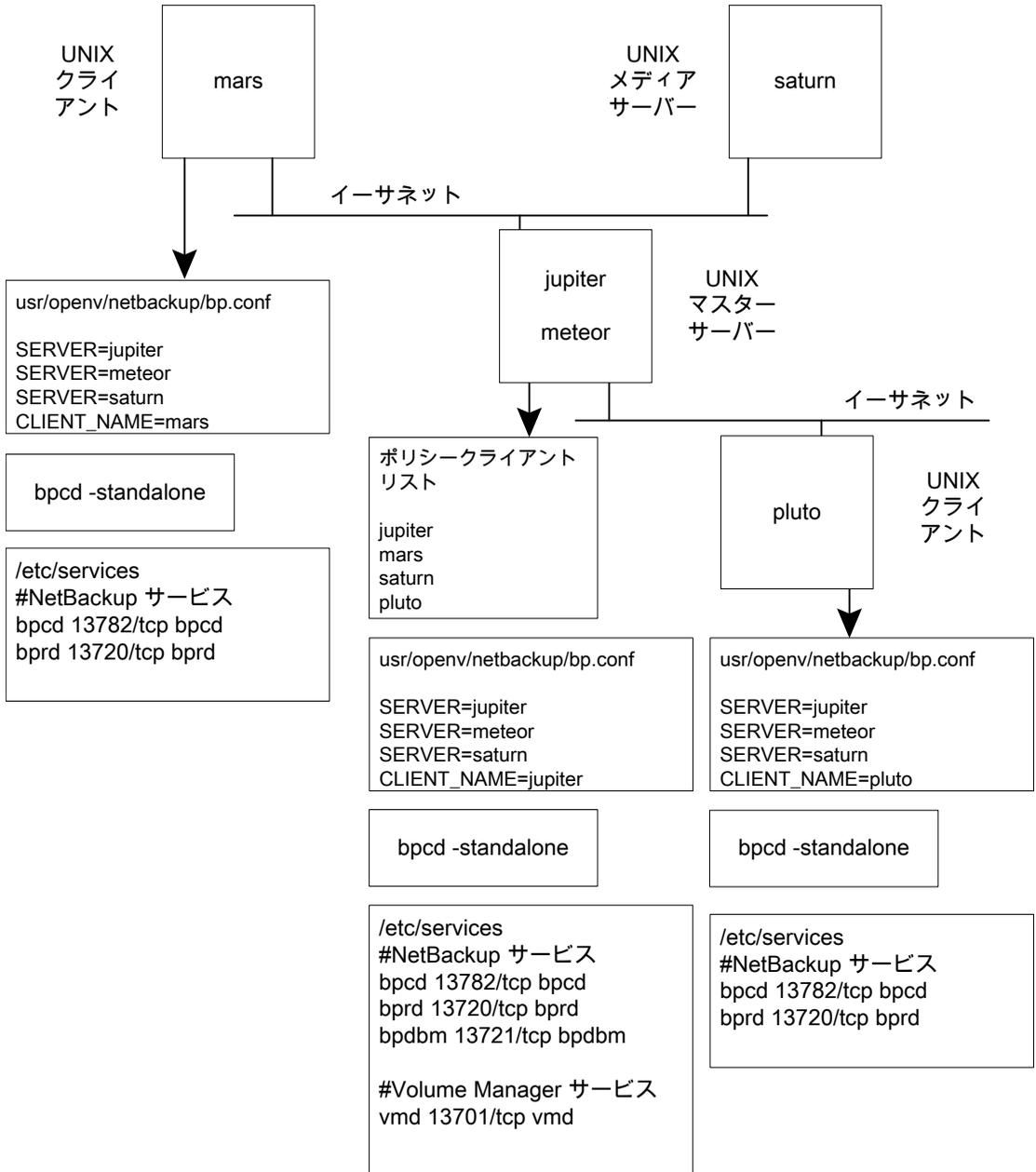


図 2-4 については、次の点を考慮してください。

- 適用可能なすべてのネットワーク構成は **NetBackup** 情報を反映するように更新する必要があります。たとえば、この情報には `/etc/hosts` ファイル、NIS および DNS (使用されている場合) を含めることができます。

この例は、複数のネットワークに接続する **UNIX** サーバーを示しています。NetBackup ポリシーのクライアントリストで、マスターサーバーのクライアント名として *jupiter* が指定されています。リストには *jupiter* または *meteor* のいずれかを表示できますが、両方を表示することはできません。

マスターサーバー上の NetBackup サーバーリストには、*jupiter* と *meteor* の両方のエントリが含まれます。両方が含まれるのは、サーバーによってバックアップが行われる場合、バックアップ対象のクライアントに関連付けられた名前が使用されるためです。たとえば、*pluto* のバックアップを行う場合は *meteor* のインターフェースが使用され、*mars* のバックアップを行う場合は *jupiter* のインターフェースが使用されます。最初の **SERVER** エントリ (マスターサーバーの名前) は *jupiter* です。これは、マスターサーバー上のクライアントのバックアップに使用される名前が *jupiter* であるためです。

他のコンピュータの NetBackup サーバーリストにも、*jupiter* と *meteor* の両方のインターフェースに対するエントリが含まれます。構成内のすべてのクライアントおよびサーバー上で同じ **SERVER** エントリを保持するには、この設定を使用することをお勧めします。クライアントコンピュータまたはメディアサーバーに対するローカルネットワークインターフェースの場合は、マスターサーバー名だけを表示することをお勧めします。(たとえば、*pluto* の場合は *meteor* を表示します。)

この図に示すネットワークの場合、ポリシーのクライアントリストとサーバーリストとの相違点は、唯一の構成が必要とされていることです。すべての標準のネットワークファイル (`hosts`、`WINS`、`NIS`、`DNS` およびルーティングテーブル) が適切に設定されていると、すべての必要なネットワーク接続を確立できます。

## bpcIntcmd ユーティリティについて

bpcIntcmd ユーティリティでは、IP アドレスがホスト名に、ホスト名が IP アドレスに解決されます。このユーティリティは NetBackup アプリケーションモジュールと同じシステムコールを使います。

`-pn` オプションを指定して bpcIntcmd でマスターサーバーに接続し、ソース IP アドレスとポート番号、IP が解決するホスト名およびそのホスト名のポリシークライアントなど、マスターサーバーが接続ホストを確認するために使用する項目を返します。`-verbose` オプションを追加すると、NetBackup がホストの認証に使用するホスト証明書など、追加の接続情報の詳細が表示されます。

次のディレクトリに、ユーティリティを起動するコマンドが存在します。

Windows の場合 `install_path¥NetBackup¥bin`

UNIX の場合 `/usr/opensv/netbackup/bin`

Windows の場合、MS-DOS コマンドウィンドウでこの bpcIntcmd コマンドを実行すると、結果が表示されます。

ホスト名および IP アドレスの解決の機能をテストするために有効な bpcIntcmd のオプションは、-ip、-hn、-sv および -pn です。次の項では、これらのオプションについて説明します。

**-ip**            bpcIntcmd -ip *IP\_Address*

-ip オプションを使用すると、IP アドレスを指定できます。bpcIntcmd によって NetBackup ノード上で gethostbyaddr () が使用され、gethostbyaddr () によって、ノードの DNS、WINS、NIS またはローカルホストファイルのエントリに定義されている IP アドレスに関連付けられたホスト名が戻されます。NetBackup サーバーとの接続は確立されません。

**-hn**            bpcIntcmd -hn *Hostname*

-hn オプションはホスト名を指定します。bpcIntcmd によって NetBackup ノード上で gethostbyname () が使用され、ノードの DNS、WINS、NIS またはローカルホストファイルのエントリに定義されているホスト名に関連付けられた IP アドレスが戻されます。NetBackup サーバーとの接続は確立されません。

**-sv**            bpcIntcmd -sv

-sv オプションを使うと、マスターサーバー上に NetBackup のバージョン番号が表示されます。

**-pn** `-pn` オプションを指定して **NetBackup** クライアント上で実行すると、**NetBackup** マスターサーバーへの問い合わせが開始されます。その後、サーバーから問い合わせ元のクライアントに情報が戻されます。最初は、サーバーリスト内の最初のサーバーです。次に、サーバーが戻す情報が表示されます。サーバーが返す情報は、マスターサーバーの観点からの情報で、マスターサーバーが接続クライアントを確認する方法について説明しています。次に例を示します。

```
bpclntcmd -pn
expecting response from server rabbit.friendlyanimals.com
dove.friendlyanimals.com dove 123.145.167.3 57141
```

このコマンド例では次のことが該当します。

- `expecting response from server`  
`rabbit.friendlyanimals.com` は、クライアント上のサーバーリストに含まれるマスターサーバーエントリです。
- `dove.friendlyanimals.com` は、マスターサーバーによって戻された接続名 (ピアネーム) です。マスターサーバーは、`getaddrinfo()` を使用してこの名前を取得します。
- `dove` は、**NetBackup** ポリシーのクライアントリストに構成されているクライアント名です。
- `123.145.167.3` は、マスターサーバーに接続している接続元クライアントの IP アドレスです。
- `57141` は、クライアントの接続元ポート番号です。

**-verbose** `-pn` オプションを指定して使用すると、使用している接続とホスト証明書に関する詳細が表示されます。次に、この出力の例を示します。

```
$ bpclntcmd -pn -verbose
expecting response from server rabbit.friendlyanimals.com
127.0.0.1:34923 -> 127.0.0.1:50464 PROXY
123.145.167.3:27082
-> 192.168.0.15:1556
LOCAL_CERT_ISSUER_NAME = /CN=broker/OU=root@
rabbit.friendlyanimals.com /O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME =
fad46a25-1fe2-4143-a62b-2dc0642d8c45
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@
rabbit.friendlyanimals.com /O=vx
PEER_CERT_SUBJECT_COMMON_NAME =
3ca8ab18-8eb3-4c8e-825d-faee9f9320d1
PEER_IP = 123.145.167.3
PEER_PORT = 27082
PEER_NAME = dove.friendlyanimals.com
POLICY_CLIENT = dove
```

-ip と -hn を使うと、NetBackup ノードで、他の NetBackup ノードの IP アドレスとホスト名を解決できるかどうかを検証できます。

たとえば、NetBackup サーバーがクライアントに接続できるかどうかを検証するには、次を実行します。

- NetBackup サーバー上で、`bpcplntcmd -hn` を使用して、オペレーティングシステムによってポリシーのクライアントリストに構成されている NetBackup クライアントのホスト名を解決して IP アドレスにできるかどうかを検証します。IP アドレスは、その後ノードのルーティングテーブルで使用され、NetBackup サーバーからのネットワークメッセージがルーティングされます。
- NetBackup クライアント上で、`bpcplntcmd -ip` を使用して、オペレーティングシステムによって NetBackup サーバーの IP アドレスを解決できるかどうかを検証します。(IP アドレスは、クライアントのネットワークインターフェースに送信されるメッセージに示されます。)

---

**メモ:** `bpcplntcmd` コマンドは `usr/opensv/netbackup/logs/bpcplntcmd` ディレクトリ (UNIX) または `install_path\NetBackup\logs\bpcplntcmd` (Windows) にメッセージを記録します。NetBackup の以前のバージョンでは、`bpcplntcmd` ログは `bpcplntcmd` ディレクトリではなく `bplist` ディレクトリに送信されます。

---

## [ホストプロパティ (Host Properties)] ウィンドウを使用した構成設定へのアクセス

NetBackup 管理コンソールに表示される [ホストプロパティ (Host Properties)] ウィンドウでは、NetBackup クライアントとサーバーに対する多くの構成を設定できます。たとえば、サーバーリスト、電子メール通知設定、サーバーとクライアントの様々なタイムアウトの値などを変更できます。このウィンドウを使用するための一般的な手順を次に示します。

Windows 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 (Backup, Archive, and Restore)] インターフェースの [NetBackup クライアントのプロパティ (NetBackup Client Properties)] ダイアログボックスを使うと、インターフェースを実行しているローカルコンピュータのみにこの構成設定を変更できます。[NetBackup クライアントのプロパティ (Client Properties)] ダイアログボックスの設定の多くは、[ホストプロパティ (Host Properties)] ウィンドウでも利用可能です。

[ホストプロパティ (Host Properties)] ウィンドウを使用して構成設定にアクセスする方法

- 1 NetBackup 管理コンソールの左ペインで、[ NetBackup の管理 ( Management) ] > [ホストプロパティ (Host Properties)] を展開します。
- 2 構成するホストに応じて、[マスターサーバー (Master Servers)]、[メディアサーバー (Media Servers)]、または [クライアント (Clients)] を選択します。

- 3 [処理 (Actions)]メニューから[プロパティ (Properties)]を選択します。
- 4 [プロパティ (Properties)]ダイアログボックスの左ペインで、適切なプロパティをクリックし、変更を行います。

## 空きがなくなったディスクの問題の解決

ログファイルの使用などで空きがなくなったディスクまたはファイルシステムに NetBackup をインストールすると、多くの問題が発生する可能性があります。NetBackup が応答しなくなる可能性があります。たとえば、NetBackup のすべてのプロセスおよびサービスが実行されていても、NetBackup ジョブが長時間キューに投入されたままになることがあります。

### NetBackup のログファイルが原因でディスクの空き領域が不足する問題を解決する方法

- 1 次を実行して、NetBackup がインストールされているディレクトリのディスク領域を整理して空き領域を増やします。
  - ログファイルを手動で削除し、ログレベルを下げて、ログファイルが短期間で自動的に削除されるようにログの保持を調整することが必要となる場合があります。ログレベル、ログファイルの保持、および統合ログの構成方法について詳しくは、『[NetBackup ログリファレンスガイド](#)』を参照してください。
  - NetBackup の統合ログファイルを別のファイルシステムに移動することを検討します。
- 2 アクティビティモニターを使用して、NetBackup リレーショナルデータベースサービスが実行されていることを確認します。

このサービスは、UNIX の デーモン、または Windows の NetBackup リレーショナルデータベースマネージャサービスです。NB\_dbdrv
- 3 NetBackup リレーショナルデータベースサービスが停止している場合は、次のことに注意してください。
  - nbrb サービスを停止しないでください。リレーショナルデータベースサービスが停止しているときに サービスを停止すると、エラーが起きることがあります。  
nbrbNetBackup
  - NetBackup リレーショナルデータベースサービスを再起動します。
- 4 NetBackup リレーショナルデータベースサービスが実行されていることを確認します。

実行されていない場合、ファイルを削除してディスク領域を解放しても問題を解決できない可能性があります。リレーショナルデータベースサービスを再起動して、NetBackup Resource Broker (nbrb) がジョブリソースを割り当てられるようにする必要があります。

## NBDB ファイルシステムでの空き領域不足を解決する方法

- 1 NetBackup デーモンを停止します。
- 2 ステージングディレクトリを圧縮し、コピーを安全な場所に置きます。  
 UNIX の場合: `/usr/opensv/db/staging`  
 Windows の場合: `install_path\VERITAS\NetBackupDB\staging`  
 このコピーは前回のカタログバックアップ時点でのデータベースのバックアップです。
- 3 データベースの検証を実行します。  
 UNIX の場合: `/usr/opensv/db/bin/nbdb_admin -validate -full -verbose`  
 Windows の場合: `install_path\VERITAS\NetBackup\bin\ nbdb_admin -validate -full -verbose`  
 検証が失敗した場合は、Veritas 社のサポートにお問い合わせください。
- 4 検証が成功した場合は、データベースの再構築を実行します。  
 UNIX の場合: `/usr/opensv/db/bin/ >nbdb_unload -rebuild -verbose`  
 Windows の場合: `install_path\VERITAS\NetBackup\bin\ >nbdb_unload -rebuild -verbose`  
 再構築が失敗した場合は、Veritas 社のサポートにお問い合わせください。
- 5 再構築が成功した場合は、データベースに対して再度検証を実行します (手順 3)。  
 この検証が失敗した場合は、Veritas 社のサポートにお問い合わせください。
- 6 NetBackup デーモンを起動します。
- 7 できるだけ早く、NBDB を含むファイルシステムに領域を追加します。

## 他のファイルシステムでの空き領域不足を解決する方法 (バイナリ、ルート、イメージカタログなど)

- 1 NetBackup デーモンを停止します。
- 2 ファイルシステムの空き領域不足の原因を特定し、修正措置を取ります。
- 3 NetBackup デーモンを起動します。
- 4 NetBackup デーモンが異常終了やエラーなく実行していることを確認します。  
 エラーが発生した場合は、Veritas 社のサポートにお問い合わせください。

## 凍結されたメディアのトラブルシューティングについての注意事項

凍結されたメディアは状態コード **84**、**85**、**86**、**87**、**96** のいずれかを含むさまざまな問題を引き起こす可能性があります。

凍結されたメディアをトラブルシューティングする場合は、次に注意してください。

- `bpmedialist` コマンドは、メディアの状態 ([凍結 (**Frozen**)]、[空きなし (**Full**)]、[有効 (**Active**)] を含む MediaDB の情報にアクセスするために使用します。
- メディアを解冻するには、`bpmedia` コマンドを使います。コマンドの構文に、その凍結されたレコードを含んでいるメディアサーバーを指定します。メディアを1つずつ解冻します。
- 凍結されたメディアは必ずしもメディアが不完全であることを意味しません。**NetBackup** はエラー、ドライブの損傷、またはデータ損失の拡大を防ぐ安全対策としてメディアを凍結することがあります。
- メディアが凍結されるときに関係するメディア ID、テープドライブ、またはメディアサーバーのパターンを調査します。

## 凍結されたメディアをトラブルシューティングする場合のログ

次のログは凍結されたメディアをトラブルシューティングするときに役に立ちます。

- |         |   |
|---------|---|
| UNIX    | <ul style="list-style-type: none"><li>■ メディアを凍結したメディアサーバーの <code>bptm</code> ログ。<br/><code>/usr/opensv/netbackup/logs/bptm</code></li><li>■ オペレーティングシステムの管理メッセージか、<b>syslog</b>。</li></ul>  |
| Windows | <ul style="list-style-type: none"><li>■ メディアを凍結したメディアサーバーの <code>bptm</code> ログ。<br/><code>install_dir\VERITAS\NetBackup\logs\bptm</code></li><li>■ <b>Windows</b> のイベントビューアのシステムログ。</li><li>■ <b>Windows</b> のイベントビューアのアプリケーションログ。</li></ul> |

メディアとドライブ関連の問題のトラブルシューティングを行うには、`bptm` 処理のログの詳細度を **5** に設定します。このログは高い詳細度でも過度のディスク容量またはリソースを使いません。メディアが凍結される時、`bptm` ログはアクティビティモニターまたは[問題 (**Problems**)]レポートより詳しい情報を含むことがあります。**NetBackup** 管理コンソールの[ホストプロパティ (**Host Properties**)]でログ記録レベルを変更することによって、個々のメディアサーバーの `bptm` に対して詳細度を設定します。

p.89 の「凍結されたメディアのトラブルシューティングについての注意事項」を参照してください。

p.90 の「メディアが凍結される状況について」を参照してください。

## メディアが凍結される状況について

次の状況では、メディアが凍結される可能性があります。

- バックアップの間に同じメディアに過度のエラーが発生しています。ログエントリの例は次のとおりです。

```
FREEZING media id E00109, it has had at least 3 errors in the last
12 hour(s)
```

この問題の原因と解決方法を次に示します。

**汚れたドライブ** 製造元の推奨事項に従ってメディアを凍結しているドライブをクリーニングします。凍結されたメディアは汚れたドライブの最初の症状の 1 つです。

**ドライブ自体** オペレーティングシステムがログに記録したりデバイスドライバが報告しているテープデバイスのエラーがないか確認します。あったら、この種類のエラーに関するハードウェア製造元の推奨事項に従います。

**SCSI またはホストバスアダプタ (HBA) レベルでの通信の問題** オペレーティングシステムがログに記録したりデバイスドライバが報告している SCSI や HBA デバイスのエラーがないか確認します。あったら、この種類のエラーに関するハードウェア製造元の推奨事項に従います。

**サポートされていないドライブ** テープドライブが **NetBackup** でサポート対象のドライブとしてハードウェア互換性リストに表示されていることを確認します。このリストは **Veritas** の次のサポート **Web** サイトにあります。

[www.veritas.com/docs/TECH59978](http://www.veritas.com/docs/TECH59978)

**サポートされていないメディア** メディアがテープドライブベンダーによるテープドライブとの使用に対してサポートされていることを確認してください。

- 予想外のメディアがドライブにあります。ログエントリの例は次のとおりです。

```
Incorrect media found in drive index 2, expected 30349,      ¥
found 20244, FREEZING 30349
```

次の状況がこのエラーを引き起こす可能性があります。

- **NetBackup** がメディア ID をドライブにマウントするように要求する。テープに物理的に記録されるメディア ID が **NetBackup** のメディア ID と異なっていれば、メディアは凍結します。このエラーは、ロボットにインベントリを実行する必要があるか、またはバーコードがメディアで物理的に変更された場合に発生します。
- 別の **NetBackup** インストールで以前に異なるバーコード規則でメディアに書き込みを行った。
- ロボットのドライブが **NetBackup** 内の順序で構成されていないか、または間違ったテープパスで構成されている。メディアを適切にマウントして使用するためには、正しいロボットドライブ番号が必要です。通常、ロボットドライブ番号は、ロボットライブラリからのドライブのシリアル番号の情報とドライブのシリアル番号の関係に基づいています。デバイス構成が完了しているとみなす前にこの番号を検証します。
- メディアは **NetBackup** 以外の形式を含んでいます。ログエントリの例は次のとおりです。

```
FREEZING media id 000438, it contains MTF1-format data and cannot
be used for backups
FREEZING media id 000414, it contains tar-format data and cannot
be used for backups
FREEZING media id 000199, it contains ANSI-format data and cannot
be used for backups
```

これらのライブラリテープは、**NetBackup** に関係なく書き込まれることがあります。デフォルトでは、**NetBackup** は未使用メディアまたは **NetBackup** の他のメディアにのみ書き込みます。他のメディア形式 (DBR、TAR、CPIO、ANSI、MTF1、再利用された **Backup Exec BE-MTF1** のメディア) は安全対策として凍結されます。次の手順を使用してこの動作を変更します。

**UNIX** の場合      **NetBackup** で異種メディアを上書きできるようにするために、関連メディアサーバーの `/usr/opensv/netbackup/bp.conf` にある `bp.conf` ファイルに次を追加します。

```
ALLOW_MEDIA_OVERWRITE = DBR
ALLOW_MEDIA_OVERWRITE = TAR
ALLOW_MEDIA_OVERWRITE = CPIO
ALLOW_MEDIA_OVERWRITE = ANSI
ALLOW_MEDIA_OVERWRITE = MTF1
ALLOW_MEDIA_OVERWRITE = BE-MTF1
```

変更を有効にするために **NetBackup** デーモンを停止し、再起動します。

Windows の場合 NetBackup 管理コンソールで、[ホストプロパティ (Host Properties)]> [メディアサーバー (Media Servers)] の順に進みます。

対象のメディアサーバーのプロパティを開きます。

[メディア (Media)] タブを選択します。

[メディアの上書きを許可 (Allow media overwrite)] プロパティによって特定のメディア形式に対する NetBackup の上書き保護が無効になります。上書き保護を無効にするには、表示されたメディア形式の 1 つ以上を選択します。次に、変更を有効にするために NetBackup サービスを停止し、再起動します。

異種メディア形式の上書きは、上書きする必要があることが確実でなければ選択しないでください。

各メディア形式について詳しくは、『NetBackup デバイス構成ガイド』を参照してください。

- メディアは、NetBackup カタログバックアップで以前使われたテープです。たとえば、ログエントリは次のようになることがあります。

```
FREEZING media id 000067: it contains Veritas NetBackup (tm)
database backup data and cannot be used for backups.
```

このメディアは NetBackup がデフォルトでは上書きしない古いカタログバックアップテープなので凍結されます。bplabel コマンドはメディアヘッダーをリセットするためにメディアをラベル付けする必要があります。

- メディアは意図的に凍結されます。さまざまな管理上の理由でメディアを手動で凍結するために bpmedia コマンドを使うことができます。メディアを凍結する特定のジョブのレコードが存在しなければそのメディアは手動で凍結された可能性があります。
- メディアは物理的には書き込み禁止です。メディアに書き込み禁止のために設定される書き込み禁止ノッチがあれば、NetBackup はメディアを凍結します。

凍結されたメディアを解凍するには、次の bpmedia コマンドを入力します。

```
# bpmedia -unfreeze -m mediaID -h media_server
```

*media\_server* 変数はメディアを凍結したものです。この項目が不明の場合は、bpmedialist コマンドを実行し、出力に表示された「Server Host:」に注意してください。次の例はメディアサーバー denton がメディア div008 を凍結したことを示したものです。

```
# bpmedialist -m div008
```

```
Server Host = denton
```

```
ID      rl images  allocated      last updated      density  kbytes
```

```
restores
      vimages expiration      last read      <----- STATUS
----->
-----
DIV08 1      1      04/22/2014 10:12 04/22/2014 10:12 hcart      35
5
      1      05/06/2014 10:12 04/22/2014 10:25 FROZEN
```

## NetBackup Web サービスの問題のトラブルシューティング

NetBackup Web サービスの問題をトラブルシューティングするには、次の手順を実行します。

### NetBackup Web サービスの問題を解決する方法

- 1 NetBackup Web Management Console サービスが実行中であることを確認します。

- UNIX では、次のコマンドを入力します。

```
/usr/opensv/netbackup/bin/bpps -x
```

- Windows では、NetBackup アクティビティモニターを使うか、または Windows の[コントロールパネル]の[管理ツール]の[サービス]を使用します。

- 2 NetBackup Web Management Console サービスを停止して再起動します。

- UNIX の場合:

```
install_path/netbackup/bin/nbwmc -terminate
```

```
install_path/netbackup/bin/nbwmc
```

- Windows では、Windows の[コントロールパネル]の[管理ツール]の[サービス]を使用します。

- 3 NetBackup Web サーバーのログと Web アプリケーションのログを確認します。

p.94 の「[NetBackup Web サービスのログの表示](#)」を参照してください。

マスターサーバーをインストールする前に実行する必要がある Web サーバータスクについては、次の [TechNote](#) を参照してください。

[https://www.veritas.com/support/en\\_US/article.000081350](https://www.veritas.com/support/en_US/article.000081350)

## NetBackup Web サービスのログの表示

NetBackup は NetBackup Web サーバーのログと、Web サーバーアプリケーションのログを作成します。

- NetBackup Web サーバーフレームワークのログでは、統合ログをしません。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。これらのログは次の場所に書き込まれます。

```
usr/opencv/wmc/webserver/logs  
install_path¥NetBackup¥wmc¥webserver¥logs
```

- NetBackup Web アプリケーションのログは、統合ログを使います。これらのログは次の場所に書き込まれます。

```
usr/opencv/logs/nbwebsevice  
install_path¥NetBackup¥logs¥nbwebsevice
```

これらのログについて追加のサポートが必要な場合は、テクニカルサポートにお問い合わせください。

## 外部 CA の構成後の Web サービスの問題のトラブルシューティング

### 問題

外部証明書 (ECA) の構成後に Web サービスが起動または応答しません。

### 原因

次の場所にある Web サーバーのログを確認します。

```
install_path/wmc/webserver/logs/catalina.log
```

ログに次のいずれかの文字列が含まれていないかどうかを確認します。

```
SEVERE [main] org.apache.tomcat.util.net.SSLUtilBase.getStore Failed  
to load keystore type [JKS] with path [C:¥Program  
Files¥Veritas¥NetBackup¥var¥global¥wsl¥credentials¥tpcredentials¥nbwebsevice.jks]  
due to [Illegal character in opaque part at index 2: C:¥Program  
Files¥Veritas¥NetBackup¥var¥global¥wsl¥credentials¥tpcredentials¥nbwebsevice.jks]  
Caused by: java.lang.IllegalArgumentException: Keystore was tampered  
with, or password was incorrect
```

考えられる根本原因: NetBackup Web サービスによって使用される外部 CA のキーストアが変更または削除された。

## 解決方法

- NetBackup Web 管理コンソールサービスが実行中であることを確認します。  
次のコマンドを実行します。  
UNIX の場合: `/usr/opensv/netbackup/bin/bpps -x`  
Windows の場合: NetBackup アクティビティモニターを使用するか、Windows の [コントロールパネル] の [サービス] アプリケーションを使用します。

- 状態が失敗である場合は、次のコマンドを実行して、外部証明書を再構成します。

Windows の場合: `Install`

```
path%netbackup%wmc%bin%configureWebServerCerts -addExternalCert  
-nbHost -certPath file_path -privateKeyPath file_path  
-trustStorePath file_path
```

UNIX の場合: `/usr/opensv/netbackup/bin/configureWebServerCerts  
-addExternalCert -nbHost -certPath file_path -privateKeyPath  
file_path -trustStorePath file_path`

- NetBackup Web サービスの起動を試みます。

Windows の場合: `Install path%netbackup%wmc%bin%nbwmc.exe -start  
-srvname "NetBackup Web Management Console"`

UNIX の場合: `/usr/opensv/netbackup/bin/nbwmc start`

## 問題

外部証明書が構成されていません。

## 原因

この問題は、次の原因で発生する場合があります。

- 無効な証明書、秘密鍵、またはトラストストア。  
エラーメッセージ: 証明書を追加できませんでした。configureWebServerCerts ログを確認してください。
- 証明書のサブジェクトの別名 (SAN) にサーバー名が含まれていない。

## 次が原因である場合の解決方法: 無効な証明書、秘密鍵、またはトラストストア

- Web サーバーの構成ログを開きます。  
場所: `<install dir>/NetBackup/wmc/webserver/logs/configureWebServerCerts.log`
- ログに次のメッセージが存在する場合:
  - ログに次のメッセージが存在する場合:  
`unable to load private key 22308:error:0906D06C:PEM  
routines:PEM_read_bio:no start`

```
line:.%crypto%pem%pem_lib.c:697:Expecting: ANY PRIVATE KEY Could
not export certificates in PKCS#12 format, 1.
```

秘密鍵が、指定された証明書の秘密鍵と一致していません。

適切な秘密鍵を指定します。

- ログに次のメッセージが存在する場合:

```
Error occurred while adding certificate to keystore. Exception:
java.security.cert.CertificateParsingException: signed overrun,
bytes = 918 Exiting.. Could not import CA certificates in JAVA
keystore, -1.
```

-trustStorePath オプションに指定されたファイルパスが有効なファイルパスではないか、指定されたファイルパスに有効なトラストストアの CA 証明書が存在しません。

-trustStorePath オプションにトラストストアバンドルパスを指定します。

## 次が原因である場合の解決方法: 証明書のサブジェクトの別名 (SAN) にサーバー名が含まれていない

次のエラーメッセージが表示されます。

```
The server name server_name was not found in the web service
certificate.
```

証明書を追加できませんでした。configureWebServerCerts ログを確認してください。

正常に構成するには、次の項目を確認します。

- サブジェクト名の一般名と SAN 名は、同時に空にすることはできません。
- SAN が空でない場合は、SAN エントリにホスト名が存在する必要があります。
- SAN が空の場合、サブジェクト名の一般名はホスト名にする必要があります。PEM 形式の証明書のみが許可されています。

---

**メモ:** ホスト名は、インストール時に指定されるマスターサーバーの名前です。ホスト名は、setenv ファイルの NB\_HOSTNAME プロパティに記載されています。

ファイルの場所:

**UNIX の場合:** /usr/opensv/wmc/bin/setenv

**Windows の場合:** install\_path\Veritas\NetBackup\wmc\bin\setenv

---

次のシナリオで正常に通信できます。

- マスターサーバーが認識されるすべてのホスト名 (ドメイン内の他のホストの SERVER エントリに記載されているホスト名) が証明書の SAN フィールドに含まれている。
- 証明書でサーバーの認証属性が設定されている。

- ログで不足しているエントリがないかを確認します。  
証明書の SAN で不足しているホスト名を追加します。

## NetBackup Web サーバー証明書の問題のトラブルシューティング

NetBackup はインストール時に NetBackup Web Management Console (nbwmc) または NetBackup Web サーバーのための X509 証明書を生成して配備します。この証明書は NetBackup マスターサーバーを認証して、クライアントがマスターサーバーに接続されていることを検証します。この証明書は定期的に更新されます。

### NetBackup Web サーバー証明書の生成

NetBackup Web サーバー証明書は NetBackup のインストール時に生成されます。この証明書の生成についてトラブルシューティングを実行するには、次のログを参照します。nbcert と nbatd 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。

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

```
install_path¥NetBackup¥logs¥nbcert  
C:¥ProgramData¥Veritas¥NetBackup¥InstallLogs¥WMC_configureCerts_¥¥¥¥mmdd_timestamp.txt  
install_path¥NetBackup¥logs¥nbatd
```

### NetBackup Web 証明書の更新

Web サーバー証明書は 1 年間の有効期限があります。NetBackup は 6 カ月ごとに自動的に証明書の更新を試みます。更新された証明書は自動的に配備されます。証明書を更新できない場合は、情報が監査されて、エラーが NetBackup エラーログに記録されます。このような場合、NetBackup は 24 時間ごとに証明書の更新を試みます。証明書の更新の失敗が解決しない場合は、テクニカルサポートにお問い合わせください。

nbauditreport コマンドを使用して、監査レコードを表示できます。

この証明書の更新についてトラブルシューティングを実行するには、次のログを参照します。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。

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

```
install_path¥NetBackup¥logs¥nbwebservice
```

```
C:\ProgramData\Veritas\NetBackup\InstallLogs\WMC_configureCerts_YYYYMMDD_timestamp.txt  
install_path\NetBackup\logs\nbatd
```

## PBX の問題の解決

Enterprise Media Manager (EMM) サービスおよび NetBackup の他のサービスを使用するには、Private Branch Exchange (PBX) と呼ばれる共通のサービスフレームワークが必要です。PBX を使用すると、と同様に、の CORBA サービスが使用する TCP/IP ポートの数を制限できます。vnetdNetBackup

### PBX の問題を解決する方法

- 1 PBX が適切にインストールされていることを確認します。PBX がインストールされていない場合、NetBackup は応答しません。次の手順を参照してください。  
p.98 の「[PBX インストールの確認](#)」を参照してください。
- 2 PBX が実行されていることを確認し、必要に応じて次の手順に従って PBX を開始します。  
p.99 の「[PBX が実行中であるかどうかの確認](#)」を参照してください。
- 3 PBX が正しく構成されていることを確認します。PBX が不正確に構成されている場合、NetBackup は応答しません。次の手順を参照してください。  
p.99 の「[PBX が正しく設定されているかどうかの確認](#)」を参照してください。
- 4 次の手順に従って PBX のログにアクセスし、確認を行います。  
p.100 の「[PBX のログへのアクセス](#)」を参照してください。
- 5 次の手順に従って PBX のセキュリティを確認し、問題を修正します。  
p.101 の「[PBX のセキュリティのトラブルシューティング](#)」を参照してください。
- 6 必要な NetBackup デーモンまたはサービスが実行中であることを確認します。必要に応じて、次の手順に従って必要なデーモンまたはサービスを開始します。  
p.103 の「[PBX デーモンかサービスが利用可能かどうかの判断](#)」を参照してください。

## PBX インストールの確認

NetBackup を使用するには、Veritas Private Branch Exchange サービス (PBX) が必要です。PBX は、NetBackup をインストールする前または NetBackup インストール中にインストールできます。

『[NetBackup インストールガイド](#)』を参照してください。

PBX をアンインストールした場合は、再インストールする必要があります。

### PBX インストールを確認する方法

- 1 NetBackup マスターサーバーで次のディレクトリを確認します。
  - Windows の場合: `install_path¥VxPBX`
  - UNIX の場合: `/opt/VRTSspb`
- 2 PBX のバージョンを確認するには、次のコマンドを入力します。
  - Windows の場合: `install_path¥VxPBX¥bin¥pbxcfg -v`
  - UNIX の場合: `/opt/VRTSspb/bin/pbxcfg -v`

## PBX が実行中であるかどうかの確認

PBX が NetBackup マスターサーバーにインストールされたことを確認した後に、そのサーバーが実行されていることを確認する必要があります。

### PBX が実行中であるかどうかを確認する方法

- 1 UNIX の場合、次のコマンドを実行して、PBX プロセスを確認します。

```
ps | grep pbx_exchange
```

- 2 PBX を UNIX で起動するには、次を入力します。

```
/opt/VRTSspb/bin/vxpbx_exchanged start
```

Windows では、Private Branch Exchange サービスが起動していることを確認します。([スタート]>[ファイル名を指定して実行]を選択して、`services.msc` と入力します)。

## PBX が正しく設定されているかどうかの確認

PBX が正常に動作するには、認証ユーザーとセキュアモードの 2 つの設定が重要です。これらの設定は、PBX のインストール時に、必要に応じて自動的に設定されます。

### PBX が正しく設定されているかどうかを確認する方法

- 1 PBX の現在の設定を表示するには、次のいずれかを実行します。
  - Windows では、次を入力します。

```
install_path¥VxPBX¥bin¥pbxcfg -p
```

出力例は次のとおりです。

```
Auth User:0 : localsystem
Secure Mode: false
Debug Level: 10
Port Number: 1556
PBX service is not cluster configured
```

Auth Userが localsystem、Secure Modeが false である必要があります。

- UNIX の場合、次のコマンドを入力します。

```
/opt/VRTSspbx/bin/pbxcfg -p
```

出力例は次のとおりです。

```
Auth User:0 : root
Secure Mode: false
Debug Level: 10
Port Number: 1556
PBX service is not cluster configured
```

Auth Userが root、Secure Modeが false である必要があります。

## 2 必要に応じて、またはをリセットします。Auth UserSecure Mode

- 認証ユーザーリストに適切なユーザーを追加する場合 (UNIX の例):

```
/opt/VRTSspbx/bin/pbxcfg -a -u root
```

- Secure Modeを false に設定する場合:

```
/opt/VRTSspbx/bin/pbxcfg -d -m
```

pbxcfg コマンドについて詳しくは、pbxcfg のマニュアルページを参照してください。

## PBX のログへのアクセス

PBX は統合ログ機能を使用します。PBX のログは、次の場所書き込まれます。

- /opt/VRTSspbx/log (UNIX の場合)
- `install_path¥VxPBX¥log` (Windows の場合)

PBX の統合ログのオリジネータ番号は 103 です。統合ログ機能について詳しくは、『[NetBackup ログリファレンスガイド](#)』を参照してください。

PBXに関するエラーメッセージは、PBX のログ、または統合ログの nbemm、nbpem、nbrb または nbjm のログに記録されます。PBX に関連するエラーの例を次に示します。

```
05/11/10 10:36:37.368 [Critical] V-137-6 failed to initialize ORB:
check to see if PBX is running or if service has permissions to
connect to PBX. Check PBX logs for details
```

### PBX のログにアクセスする方法

- 1 PBX およびその他の統合ログを表示するには、`vxlogview` コマンドを使用します。PBX のオリジネータ ID は 103 です。詳しくは、`vxlogview` のマニュアルページを参照してください。

統合ログ機能のトピックについては、『[NetBackup ログリファレンスガイド](#)』も参照してください。

- 2 PBX のログレベルを変更するには、次のコマンドを入力します。

```
pbxcfg -s -l debug_level
```

ここで、`debug_level` には 0 から 10 までの数値を指定します。10 (デフォルト値) が最も詳細なレベルです。

現在のレベルを調べるには、次を入力してください。

```
pbxcfg -p
```

PBX では、UNIX のシステムログ (`/var/adm/messages` や `/var/adm/syslog`) または Windows イベントログにデフォルトでメッセージが記録されます。その結果、システムログが不要な PBX ログメッセージで一杯になる場合があります。これは、メッセージが PBX ログにも書き込まれるためです。

UNIX の場合: `/opt/VRTSpx/log`

Windows の場合: `<install_path>%VxPBX%log`

- 3 システムログまたはイベントログへの PBX ログを無効にするには、次のコマンドを入力します。

```
# vxlogcfg -a -p 50936 -o 103 -s LogToOslog=false
```

設定を有効にするために PBX を再起動する必要はありません。

## PBX のセキュリティのトラブルシューティング

PBX の Secure Mode には `false` を設定する必要があります。Secure Mode が `true` の場合、`NetBackup` コマンド (`bplabel` や `vmopr cmd` など) は正しく機能しません。(UNIX の場合) または (Windows の場合) に、次のような PBX のメッセージが表示されず、`/opt/VRTSpx/log/install_path%VxPBX%log`

```
5/12/2008 16:32:17.477 [Error] V-103-11 User MINOV%Administrator
not authorized to register servers
5/12/2008 16:32:17.477 [Error] Unauthorized Server
```

## PBX のセキュリティをトラブルシューティングする方法

1 PBX の Secure Mode が false (デフォルト値) に設定されていることを確認します。

- Windows の場合:

```
install_path%VxPBX%bin%pbxcfg -p
```

- UNIX の場合:

```
/opt/VRTSpx/bin/pbxcfg -p
```

2 必要に応じ、次を入力して Secure Mode を false に設定します。

- Windows の場合:

```
install_path%VxPBX%bin%pbxcfg -d -m
```

- UNIX の場合:

```
/opt/VRTSpx/bin/pbxcfg -d -m
```

3 NetBackup を停止します。

- Windows の場合:

```
install_path%NetBackup%bin%bpdown
```

- UNIX の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all
```

4 PBX を停止します。

- Windows の場合: [スタート]>[ファイル名を指定して実行]を選択して、`services.msc` と入力します。次に、Veritas Private Branch Exchange サービスを停止します。

- UNIX の場合:

```
/opt/VRTSpx/bin/vxpbx_exchanged stop
```

5 PBX を起動します。

- UNIX の場合:

```
/opt/VRTSpx/bin/vxpbx_exchanged start
```

- Windows の場合: [スタート]>[ファイル名を指定して実行]を選択して、`services.msc`と入力します。次に、Veritas Private Branch Exchange サービスを起動します。
- 6 NetBackup を起動します。

- Windows の場合:

```
install_path¥NetBackup¥bin¥bpup
```

- UNIX の場合:

```
/usr/opensv/netbackup/bin/bp.start_all
```

## PBX デーモンかサービスが利用可能かどうかの判断

NetBackup が構成しているとおりに動作しない場合、必要な NetBackup サービスが停止している可能性があります。たとえば、バックアップがスケジュールされていない場合や、スケジュールされていても実行されない場合があります。発生する問題の種類は、どのプロセスが実行されていないかによって異なります。

NetBackup サービスが動作しておらず、別のプロセスがそれに接続しようとする、次に類似したメッセージが `/opt/VRTSspbx/log (UNIX)` または `install_path¥VxPBX¥log (Windows)` に表示されます。PBX の統合ログ機能オリジネータは 103 であり、製品 ID は 50936 です。

```
05/17/10 9:00:47.79 [Info] PBX_Manager:: handle_input with fd = 4
05/17/10 9:00:47.79 [Info] PBX_Client_Proxy::parse_line, line = ack=1
05/17/10 9:00:47.79 [Info] PBX_Client_Proxy::parse_line, line =
extension=EMM
05/17/10 9:00:47.80 [Info] hand_off looking for proxy for = EMM
05/17/10 9:00:47.80 [Error] No proxy found.
05/17/10 9:00:47.80 [Info] PBX_Client_Proxy::handle_close
```

### PBX デーモンかサービスが利用可能かどうかを判断する方法

- 1 必要なサービスを起動します。

この例では、足りない NetBackup サービスは EMM です。必要なサービスを起動するには、`nbemm` コマンドを入力するか (UNIX の場合)、NetBackup Enterprise Media Manager サービスを起動します (Windows の場合、[スタート]>[ファイル名を指定して実行]を選択し、`services.msc`と入力します)。

- 2 必要に応じて、NetBackup のすべてのサービスを停止し、再起動します。
  - Windows の場合:

```
install_path¥NetBackup¥bin¥bpdown  
install_path¥NetBackup¥bin¥bpup
```

- UNIX の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all  
/usr/opensv/netbackup/bin/bp.start_all
```

## リモートホストの検証に関する問題のトラブルシューティング

NetBackup は Secure Socket Layer (SSL) を使用して他の NetBackup ホストと安全に通信します。その他のホストが 8.0 以前の場合を除き、NetBackup 8.1 では常に通信が安全に行われる必要があります。この目的のため、接続を設定したり受け入れたりするすべてのホストは、マスターサーバーで利用可能な詳細に対してリモートホストを検証します。ホストの検証が失敗すると接続が切断されるため、特定の操作 (バックアップまたはリストアなど) が失敗します。

ホスト検証の失敗のために発生した問題を解決するには、次の操作を行います。

- ホスト検証の失敗に関連するログを調べます。  
p.105 の「[ホストの検証に関連するログの表示](#)」を参照してください。
- すべての NetBackup Web サービスがマスターサーバーで実行されていることを検証します。  
p.93 の「[NetBackup Web サービスの問題のトラブルシューティング](#)」を参照してください。
- NetBackup Web サーバー証明書が正しく配備されていることを検証します。  
p.97 の「[NetBackup Web サーバー証明書の問題のトラブルシューティング](#)」を参照してください。
- ホストがマスターサーバー上の NetBackup Web サービスに接続できることを検証します。  
『NetBackup セキュリティおよび暗号化ガイド』の「非武装地帯の NetBackup クライアントと HTTP トンネルを経由するマスターサーバー間の通信について」のトピックを参照してください。
- リモートホストが 8.0 以前の場合は、このようなホストとの安全でない通信が有効になっていることを検証します。  
p.106 の「[NetBackup 8.0 以前のホストとの安全でない通信の有効化](#)」を参照してください。
- マスターサーバー上で承認が保留されているホスト ID からホスト名へのマッピングがないかどうかを検証します。

- p.106 の「[保留中のホストIDからホスト名へのマッピングの承認](#)」を参照してください。
- リモートホストの **NetBackup** ソフトウェアが 8.1 から旧バージョンに最近ダウングレードされた場合は、マスターサーバーのホスト情報を必ず再設定します。  
『**NetBackup セキュリティおよび暗号化ガイド**』の「**Resetting a NetBackup host attributes** (ホスト属性のリセット)」のトピックを参照してください。
  - ホストのキャッシュにリモートホストについての情報が反映されていることを検証します。  
p.108 の「[ホストキャッシュの消去](#)」を参照してください。
  - 外部 **CA** が署名した証明書を使用するように **NetBackup Web** サーバーが構成されている場合、ホスト証明書が適切なマスターサーバーのドメインに正常に登録されていることを確認します。  
外部 **CA** のサポートと証明書の登録について詳しくは、『**NetBackup セキュリティおよび暗号化ガイド**』を参照してください。

## ホストの検証に関連するログの表示

プロキシからのホスト検証のログは次の場所にあります。

Windows の場合: `Install_Path\NetBackup\logs\nbpxyhelper`

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

プロキシは統合ログ機能を使用します。

また、着信接続の場合、ホスト検証のログ記録は個々のプロセスのログファイルにも出力されます。このログファイルには **NetBackup** ホストの認可も出力されます。

たとえば、`bpcd` の認可中にホストの検証が失敗した場合は、以下の場所にある関連ログを参照してください。

Windows の場合: `Install_Path\NetBackup\logs\bpcd`

UNIX の場合: `/usr/opensv/NetBackup/logs/bpcd`

ホスト接続が切断されるときに記録されるログメッセージの例:

```
Connection is to be dropped for peer host: examplemaster with error  
code:8618 error message: Connection is dropped, because the host  
ID-to-hostname mapping is not yet approved.
```

```
Connection is to be dropped for peer host: 10.10.10.10 with error  
code:8620 error message: Connection is dropped, because insecure  
communication with hosts is not allowed.
```

---

メモ: ホスト検証エラーは、**NetBackup 8.0** 以前のホストでは接続失敗エラーとして表示されます。

---

## NetBackup 8.0 以前のホストとの安全でない通信の有効化

マスターサーバーで NetBackup 8.0 以前のホストとの安全でない通信が有効になっていないかどうかを調べます。

次のコマンドを実行します。

- Windows の場合: `Install_Path¥NetBackup¥bin¥admincmd¥nbseccmd -getsecurityconfig -insecurecommunication`
- UNIX の場合: `/usr/opensv/netbackup/bin/admincmd/nbsecmd -getsecurityconfig -insecurecommunication`

`insecurecommunication` オプションを「off」に設定すると、NetBackup 8.0 以前のホストとの安全でない通信が有効になります。

次のコマンドを実行します。

- Windows の場合: `Install_Path¥NetBackup¥bin¥admincmd¥nbseccmd -setsecurityconfig -insecurecommunication on`
- UNIX の場合: `/usr/opensv/netbackup/bin/admincmd/nbsecmd -setsecurityconfig -insecurecommunication on`

---

**メモ:** OpsCenter がマスターサーバーと通信できるようにするには、安全でない通信を有効にする必要があります。

---

## 保留中のホスト ID からホスト名へのマッピングの承認

次のコマンドを実行して、ホスト ID からホスト名へのマッピングの保留中の承認要求の一覧を調べます。

- Windows の場合: `Install_Path¥NetBackup¥bin¥admincmd¥nbhostmgmt -list -pending`

出力例は次のとおりです。

ホスト ID: `zzzzzz-1271-4ea4-zzzz-5281a4f760e6`

ホスト: `example1.com`

マスターサーバー: `example1.com`

OS タイプ: `Windows`

オペレーティングシステム: `Microsoft Windows Server yyyy Rn 64 ビット Service Pack n、ビルド nnn(nnnnnn)`

NetBackup EEB:

ハードウェアの説明: `GenuineIntel Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz、4 基の CPU`

CPU アーキテクチャ: `Intel x64`

バージョン: `NetBackup_8.1`

セキュア: はい

コメント:

マッピングされた ホスト名	承認済み	競合	自動検出済み	共有	作成日時	最終更新日時
example1.com	なし	なし	はい	なし	2017 年 7 月 28 日午後 03 時 53 分 30 秒	2017 年 7 月 28 日午後 03 時 53 分 30 秒

- UNIX の場合: `/usr/opensv/netbackup/bin/admincmd/nbhostmgmt -list -pending`

出力例は次のとおりです。

ホスト ID: xxxxx-52e8-xxxx-ba92-7be20c6dceb9

ホスト: example2.com

マスターサーバー: example2.com

OS タイプ: UNIX

オペレーティングシステム: RedHat Linux(2.6.32-642.el6.x86\_64)

NetBackup EEB:

ハードウェアの説明: AuthenticAMD AMD Opteron(tm) プロセッサ 6366 HE、16  
基の CPU

CPU アーキテクチャ: x86\_64

バージョン: NetBackup\_8.1

セキュア: はい

コメント:

マッピングされた ホスト名	承認済み	競合	自動検出済み	共有	作成日時	最終更新日時
example2.com	なし	なし	はい	なし	2017 年 7 月 28 日午後 02 時 52 分 20 秒	2017 年 7 月 28 日午後 02 時 52 分 20 秒

次のコマンドを実行して、ホスト ID からホスト名へのマッピングを承認します。

- Windows の場合: `Install_Path¥NetBackup¥bin¥admincmd¥nbhostmgmt -add -hostid zzzzzz-1271-4ea4-zzzz-5281a4f760e6 -mappingname mymaster`  
出力例: example1.com is successfully updated.
- UNIX の場合: `/usr/opensv/netbackup/bin/admincmd/nbhostmgmt -add -hostid xxxxx-52e8-xxxx-ba92-7be20c6dceb9 -mappingname mymaster`  
出力例: example2.com is successfully updated.

## ホストキャッシュの消去

ホストキャッシュの消去により、ホストの検証に関連するすべての変更 (ホスト ID からホスト名へのマッピングの承認や、グローバルセキュリティ設定の変更など) がホストですぐに反映されます。

ホストキャッシュを消去するには、次のコマンドを実行します。

- **Windows** の場合: `Install_Path\NetBackup\bin\bpcIntcmd -clear_host_cache`
- **UNIX** の場合: `/usr/opensv/netbackup/bin/bpcIntcmd -clear_host_cache`

出力例は次のとおりです。

```
Successfully cleared host cache
```

```
Successfully cleared peer validation cache
```

## 自動イメージレプリケーションのトラブルシューティング

自動イメージレプリケーションは、1 つの **NetBackup** ドメインで作成したバックアップを 1 つ以上の **NetBackup** ドメインにある別のメディアサーバーにレプリケートします。

---

**メモ:** 複数のマスターサーバードメインにわたるレプリケーションは、自動イメージレプリケーションではサポートされていますが、**Replication Director** では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は、ジョブに書き込み側が含まれない点を除いてはあらゆる複製ジョブと同じように動作します。ジョブでは、ソースイメージが存在するディスクボリュームから読み込んだリソースを使用する必要があります。メディアサーバーが利用できない場合、このジョブは状態 **800** で失敗します。

自動イメージレプリケーションジョブは、ディスクボリュームレベルで動作します。ソースコピーのストレージライフサイクルポリシーで指定したストレージユニット内では、一部のディスクボリュームがレプリケーションをサポートしないことがあります。**NetBackup** 管理コンソールの [ディスクプール (Disk Pools)] インターフェースを使用して、イメージがレプリケーションをサポートするディスクボリュームにあることを検証します。ディスクボリュームがレプリケーションソースではないことをインターフェースが示す場合は、[ディスクボリュームの更新 (Update Disk Volume)] または [更新 (Refresh)] をクリックしてディスクプールのディスクボリュームを更新します。問題が解決しない場合は、ディスクデバイスの構成を調べます。

自動レプリケーションジョブでの処理は、次の表に示すように複数の条件によって決まります。

処理	条件
AIR レプリケーションジョブが開始されなかった	次のことを検証します。 <ul style="list-style-type: none"> <li>■ SLP がアクティブか</li> <li>■ nbstserv デーモンが実行中か</li> <li>■ イメージの再試行回数が増やした回数を超えていないか</li> </ul>
AIR レプリケーションジョブがキューに投入されているが開始されていない	利用できるメディアサーバーまたは I/O ストリームがありません。
AIR レプリケーションジョブが状態 191 などですぐ失敗した	エラーについて詳しくはジョブの詳細を参照してください。  詳しくは、レプリケーションジョブを処理したメディアサーバーの bpdm ログを参照してください。

次の手順は **OpenStorage** 構成で動作する **NetBackup** に基づいています。この構成では自動イメージレプリケーションを使うメディアサーバーの重複排除プール (MSDP) と通信します。

## 自動イメージレプリケーションジョブをトラブルシューティングする方法

- 1 次のコマンドを使用してストレージサーバーの情報を表示します。

```
# bpstsinfo -lsuinfo -stype PureDisk -storage_server  
storage_server_name
```

出力例は次のとおりです。

```
LSU Info:  
Server Name: PureDisk:ssl.acme.com  
LSU Name: PureDiskVolume  
Allocation : STS_LSU_AT_STATIC  
Storage: STS_LSU_ST_NONE  
Description: PureDisk storage unit (/ssl.acme.com#1/2)  
Configuration:  
Media: (STS_LSUF_DISK | STS_LSUF_ACTIVE |  
STS_LSUF_STORAGE_NOT_FREED  
| STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE)  
Save As : (STS_SA_CLEARF | STS_SA_OPAQUEF | STS_SA_IMAGE)  
Replication Sources: 0 ( )  
Replication Targets: 1 ( PureDisk:bayside:PureDiskVolume )  
...
```

この出力には、PureDiskVolume の論理ストレージユニット (LSU) フラグ **STS\_LSUF\_REP\_ENABLED** と **STS\_LSUF\_REP\_SOURCE** が示されています。PureDiskVolume は自動イメージレプリケーションに対して有効になっているレプリケーションソースです。

- 2 NetBackup がこれら 2 つのフラグを認識することを検証するために、次のコマンドを実行します。

```
# nbdevconfig -previewdv -stype PureDisk -storage_server  
storage_server_name -media_server media_server_name -U  
Disk Pool Name      :  
Disk Type           : PureDisk  
Disk Volume Name    : PureDiskVolume  
...  
Flag                : ReplicationSource  
...
```

ReplicationSource フラグで NetBackup が LSU フラグを認識することを確認します。

- 3 raw 出力を使用してレプリケーションターゲットを表示するために、次のコマンドを実行します。

```
# nbdevconfig -previewdv -stypе PureDisk -storage_server
storage_server_name -media_server media_server_name

V_5_ DiskVolume < "PureDiskVolume" "PureDiskVolume" 46068048064

46058373120 0 0 0 16 1 >
V_5_ ReplicationTarget < "bayside:PureDiskVolume" >
```

この表示には、レプリケーションターゲットが `bayside` と呼ばれるストレージサーバーであり、LSU (ボリューム) 名が `PureDiskVolume` であることが示されています。

- 4 NetBackup がこの設定を正しく取得したことを確認するために、次のコマンドを実行します。

```
# nbdevquery -listdv -stypе PureDisk -U
Disk Pool Name      : PDpool
Disk Type           : PureDisk
Disk Volume Name    : PureDiskVolume
...
Flag                : AdminUp
Flag                : InternalUp
Flag                : ReplicationSource
Num Read Mounts     : 0
...
```

このリストには、ディスクボリューム `PureDiskVolume` をディスクプール `PDpool` に設定し、NetBackup がソース側のレプリケーション機能を認識することが示されています。ターゲット側の同様の `nbdevquery` コマンドにそのディスクボリュームの `ReplicationTarget` が表示されるはずですが。

- 5 NetBackup がレプリケーション機能を認識しない場合は、次のコマンドを実行します。

```
# nbdevconfig -updatedv -stypе PureDisk -dp PDpool
```

- 6 このディスクプールを使うストレージユニットがあることを確認するために、次のコマンドを実行します。

```
# bpstulist
PDstu 0 _STU_NO_DEV_HOST_ 0 -1 -1 1 0 "*NULL*"
      1 1 51200 *NULL* 2 6 0 0 0 PDpool *NULL*
```

この出力には、ストレージユニット PDstu がディスクプール PDpool を使うことが示されています。

- 7 次のコマンドを実行してディスクプールの設定を調べます。

```
nbdevquery -listdp -stype PureDisk -dp PDpool -U
Disk Pool Name   : PDpool
Disk Pool Id    : PDpool
Disk Type       : PureDisk
Status          : UP
Flag            : Patchwork
...
Flag            : OptimizedImage
Flag            : ReplicationTarget
Raw Size (GB)   : 42.88
Usable Size (GB) : 42.88
Num Volumes     : 1
High Watermark  : 98
Low Watermark   : 80
Max IO Streams  : -1
Comment         :
Storage Server  : ss1.acme.com (UP)
```

Max IO Streams は -1 に設定されます。これは、ディスクプールの入出力ストリーム数が無制限であることを意味します。

- 8 ストレージサーバーとそのディスクプールにアクセスする資格証明済みのメディアサーバーのリストを確認するには、次のコマンドを実行します。

```
# tpconfig -dsh -all_hosts
```

```
=====
Media Server:                ssl.acme.com
Storage Server:              ssl.acme.com
User Id:                      root
    Storage Server Type:      BasicDisk
    Storage Server Type:      SnapVault
    Storage Server Type:      PureDisk
=====
```

このディスクプールには 1 つのメディアサーバー `ssl.acme.com` のみがあります。ストレージ構成の検証が完了しました。

- 9 検証の最後のフェーズは、ストレージライフサイクルポリシー構成です。自動イメージレプリケーションを実行するには、ソースコピーはストレージユニット PDstu 上にある必要があります。たとえば、次のコマンドを実行します。

```
nbstl woodridge2bayside -L
                                Name: woodridge2bayside
                                Data Classification: (none specified)
                                Duplication job priority: 0
                                State: active
                                Version: 0
Destination 1                   Use for: backup
                                Storage: PDstu
                                Volume Pool: (none specified)
                                Server Group: (none specified)
                                Retention Type: Fixed
                                Retention Level: 1 (2 weeks)
                                Alternate Read Server: (none specified)
                                Preserve Multiplexing: false
                                Enable Automatic Remote Import: true
                                State: active
                                Source: (client)
                                Destination ID: 0
Destination 2                   Use for: 3 (replication to remote
master)
                                Storage: Remote Master
                                Volume Pool: (none specified)
                                Server Group: (none specified)
                                ...
                                Preserve Multiplexing: false
                                Enable Automatic Remote Import: false
                                State: active
                                Source: Destination 1 (backup:PDstu)
                                Destination ID: 0
```

自動イメージレプリケーションジョブのフローをトラブルシューティングするには、他のストレージライフサイクルポリシーによって管理されるジョブに使うのと同じコマンドラインを使用してください。たとえば、リモートマスターに複製されたイメージをリストするには、次のコマンドを実行します。

```
nbstlutil list -copy_type replica -U -copy_state 3
```

リモートマスターに複製されなかった (保留中または失敗した) イメージをリストするには、次のコマンドを実行します。

```
nbstlutil list -copy_type replica -U -copy_incomplete
```

**10** 完了したレプリケーションの複製の状態を表示するには、次のコマンドを実行します。

```

nbstlutil repllist -U
Image:
Master Server           : ssl.acme.com
Backup ID               : woodridge_1287610477
Client                  : woodridge
Backup Time             : 1287610477 (Wed Oct 20 16:34:37 2010)

Policy                  : two-hop-with-dup
Client Type             : 0
Schedule Type          : 0
Storage Lifecycle Policy : woodridge2bayside2pearl_withdup
Storage Lifecycle State : 3 (COMPLETE)
Time In Process         : 1287610545 (Wed Oct 20 16:35:45 2010)

Data Classification ID  : (none specified)
Version Number          : 0
OriginMasterServer     : (none specified)
OriginMasterServerID   : 00000000-0000-0000-0000-000000000000

Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
Created Date Time       : 1287610496 (Wed Oct 20 16:34:56 2010)

Copy:
Master Server           : ssl.acme.com
Backup ID               : woodridge_1287610477
Copy Number             : 102
Copy Type               : 3
Expire Time             : 1290288877 (Sat Nov 20 15:34:37 2010)
Expire LC Time          : 1290288877 (Sat Nov 20 15:34:37 2010)
Try To Keep Time        : 1290288877 (Sat Nov 20 15:34:37 2010)
Residence               : Remote Master
Copy State              : 3 (COMPLETE)
Job ID                  : 25
Retention Type          : 0 (FIXED)
MPX State               : 0 (FALSE)
Source                  : 1
Destination ID          :
Last Retry Time         : 1287610614
    
```

```
Replication Destination:  
Source Master Server: ssl.acme.com  
Backup ID           : woodridge_1287610477  
Copy Number        : 102  
Target Machine     : bayside  
Target Info        : PureDiskVolume  
Remote Master      : (none specified)
```

## 自動イメージレプリケーションと SLP で使用されるマスターサーバーのルール

自動イメージレプリケーション操作は、少なくとも 2 つの NetBackup マスターサーバードメインのストレージライフサイクルポリシー (SLP) を使用します。2 つのマスターサーバーが次の規則に従っていることを検証します。

- 特定のターゲットに複製する場合 (対象設定された AIR)、元のドメインで自動イメージレプリケーションの SLP を作成する前にインポート SLP を作成します。その後、適切なインポート SLP を選択できます。

---

**メモ:** インポート SLP の名前が 113 文字未満であることを確認します。

---

- ソースマスターサーバードメインのストレージライフサイクルポリシーのデータ分類は、ターゲットマスターサーバードメインの SLP ポリシーのデータ分類と一致している必要があります。
- ソースストレージライフサイクルポリシー内のリモートマスターへの複製コピーでは、階層的な複製を使い、レプリケーションが可能な位置情報が付いているソースコピーを指定する必要があります。(ディスクプールのレプリケーション列は[ソース (Source)]を示す必要があります。)
- ターゲットドメインのストレージライフサイクルポリシーは、最初のコピーのためにインポートを指定する必要があります。インポートの位置情報には、ソースストレージライフサイクルポリシーのソースコピーのレプリケーションパートナーであるデバイスを含める必要があります。インポートコピーではストレージユニットグループかストレージユニットを指定できますが、[任意 (Any Available)]は指定できません。
- ターゲットドメインのストレージライフサイクルポリシーには、リモート保持形式を指定する少なくとも 1 つのコピーが必要です。

## 外部証明書の構成で、ターゲットの AIR の信頼できるマスターサーバーの操作に失敗した

### 信頼の追加または更新

#### 問題

ソースマスターサーバーとターゲットマスターサーバー間の信頼の追加または更新に失敗しました。

#### 原因

この問題は、次の原因で発生する場合があります。

- 原因 1: ターゲットマスターサーバーへのソースマスターサーバーの登録に失敗した。
- 原因 2: 信頼できるマスターサーバーデータベースおよび構成ファイルにターゲットマスターサーバーを `TRUSTED_MASTER` として追加することに失敗した。

#### 原因 1 (ターゲットマスターサーバーへのソースマスターサーバーの外部証明書の登録に失敗した) の解決方法

p.141 の「[Windows 証明書ストアの問題のトラブルシューティング](#)」を参照してください。

#### 原因 2 (信頼できるマスターサーバーデータベースおよび構成ファイルにターゲットマスターサーバーを `TRUSTED_MASTER` として追加することに失敗した) の解決方法

- 1 エラーメッセージ (「終了状態 5630: リモートマスターサーバーのバージョンの取得に失敗しました。」) を確認します。

`vnetd` プロキシサービスが停止している場合、またはソースマスターサーバーで `vnetd` がプロキシへの接続に失敗した場合は、次の順序でログを確認します。

- リモートマスターサーバーの `vnetd` プロキシへの接続を確認します。  
リモートマスターサーバーの `vnetd` プロキシへの接続を確認するには、  
`bptestbpcd -host remote_master_server_name` コマンドを実行します。

- プロキシのログを確認します。

**Windows** の場合: `C:\Program`

`Files\Veritas\NetBackup\logs\nbpxyhelper\log_file`

**Unix** の場合: `/usr/openv/logs/nbpxyhelper/log_file`

- 2 エラーメッセージ (「終了状態 5616: ローカルマスターサーバーにアクセスできません。現在、信頼が単方向になっています。リモートマスターサーバーはローカルマスターサーバーを信頼していますが、ローカルマスターサーバーはリモートマスターサーバーを信頼していません。信頼を除去してください。」) を確認します。

ソースマスターサーバーで bprd プロキシサービスが停止している場合は、次の順序でログを確認します。

- bprd ログを確認します。  
Windows の場合: C:\Program Files\Veritas\NetBackup\logs\bprd\log\_file  
UNIX の場合: /usr/opensv/netbackup/logs/bprd/log\_file
- プロキシのログを確認します。  
Windows の場合: C:\Program Files\Veritas\NetBackup\logs\nbpxyhelper\log\_file  
UNIX の場合: /usr/opensv/logs/nbpxyhelper/log\_file
- EMM データベースログを確認します。  
Windows の場合: C:\Program Files\Veritas\NetBackup\logs\nbemm\log\_file  
UNIX の場合: /usr/opensv/logs/nbemm/log\_file

## 信頼の削除

### 問題

信頼の削除操作に失敗しました

### 原因

信頼できるマスターサーバーデータベースと、構成ファイルの TRUSTED\_MASTER からターゲットマスターサーバーを削除できませんでした。

### 解決方法

- エラーメッセージ (「終了状態 5616: ローカルマスターサーバーにアクセスできません。現在、信頼が単方向になっています。リモートマスターサーバーはローカルマスターサーバーを信頼していますが、ローカルマスターサーバーはリモートマスターサーバーを信頼していません。信頼を除去してください。」)を確認します。  
ソースマスターサーバーで bprd サービスが停止しています。  
ログを次の順序で確認します。
  - bprd ログを確認します。  
Windows の場合: C:\Program Files\Veritas\NetBackup\logs\bprd\log\_file  
UNIX の場合: /usr/opensv/netbackup/logs/bprd/log\_file
  - プロキシのログを確認します。  
Windows の場合: C:\Program Files\Veritas\NetBackup\logs\nbpxyhelper\log\_file

UNIX の場合: /usr/opensv/logs/nbpxyhelper/log\_file

- EMM データベースログを確認します。

Windows の場合: C:¥Program

Files¥Veritas¥NetBackup¥logs¥nbemm¥log\_file

UNIX の場合: /usr/opensv/logs/nbemmm/log\_file

## SLP コンポーネントが管理する自動インポートジョブのトラブルシューティングについて

ストレージライフサイクルポリシー (SLP) コンポーネントによって管理される自動インポートジョブは、レガシーのインポートジョブと異なっています。自動インポートジョブはイメージのインポートが必要であることを非同期的に **NetBackup** に通知します。また、自動イメージレプリケーションジョブでは、カタログエントリをストレージデバイスに渡すため、このジョブでイメージ全体を読み込む必要はありません。自動インポートジョブはストレージデバイスからカタログレコードを読み込み、自身のカタログに追加します。この処理は高速であるため、**NetBackup** はイメージをまとめて効率よくインポートできます。インポート保留中とは、**NetBackup** が通知されていてもインポートがまだ実行されていない状態をいいます。

SLP でのインポート操作、およびインポートマネージャプロセスのバッチ間隔の調整方法について詳しくは、次のマニュアルで説明しています。

『**NetBackup 管理者ガイド Vol. 1**』を参照してください。

ストレージサーバーからの通知イベントによって、イメージ名、このイメージのカタログを読み込むストレージサーバーの場所、そのイメージを処理する SLP の名前が提供されます。自動インポートジョブのイメージはストレージライフサイクルポリシーの名前とディスクボリュームごとにバッチ処理されます。インポートジョブはディスクボリュームの入出力ストリームを消費します。

インポート保留中のイメージを表示するには、次のコマンドを実行します。

```
# nbstlutil pendimplist -U
Image:
Master Server      : bayside.example.com
Backup ID          : gdwinlin04_1280299412
Client             : gdwinlin04
Backup Time        : 1280299412 (Wed Jul 28 01:43:32 2010)
Policy             : (none specified)
Client Type        : 0
Schedule Type      : 0
Storage Lifecycle Policy : (none specified)
Storage Lifecycle State : 1 (NOT_STARTED)
Time In Process    : 0 (Wed Dec 31 18:00:00 1969)
Data Classification ID : (none specified)
```

```
Version Number           : 0
OriginMasterServer      : master_tlk
OriginMasterServerID    : 00000000-0000-0000-0000-000000000000
Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
Created Date Time       : 1287678771 (Thu Oct 21 11:32:51 2010)
```

Copy:

```
Master Server           : bayside.example.com
Backup ID               : gdwinlin04_1280299412
Copy Number            : 1
Copy Type              : 4
Expire Time            : 0 (Wed Dec 31 18:00:00 1969)
Expire LC Time         : 0 (Wed Dec 31 18:00:00 1969)
Try To Keep Time       : 0 (Wed Dec 31 18:00:00 1969)
Residence              : (none specified)
Copy State              : 1 (NOT_STARTED)
Job ID                 : 0
Retention Type         : 0 (FIXED)
MPX State              : 0 (FALSE)
Source                 : 0
Destination ID         :
Last Retry Time        : 0
```

Fragment:

```
Master Server           : bayside.example.com
Backup ID               : gdwinlin04_1280299412
Copy Number            : 1
Fragment Number        : -2147482648
Resume Count           : 0
Media ID               : @aaaab
Media Server           : bayside.example.com
Storage Server         : bayside.example.com
Media Type             : 0 (DISK)
Media Sub-Type         : 0 (DEFAULT)
Fragment State         : 1 (ACTIVE)
Fragment Size          : 0
Delete Header          : 1
Fragment ID            : gdwinlin04_1280299412_C1_IM
```

自動インポートジョブと自動インポートイベントでの処理は、次の表に示すように複数の条件によって決まります。

## 処理

## 条件

自動インポートジョブがキューに投入される

メディアサーバーか I/O ストリームがこのディスクボリュームで無効になっています。

自動インポートジョブが開始しない(ストレージライフサイクル状態 1 でコピーが停止している)

- ストレージライフサイクルポリシーが非アクティブです。
- ストレージライフサイクルポリシーのインポートの宛先が非アクティブです。
- ストレージライフサイクルポリシーはセッションとセッションの間にあります。
- イメージは拡張再試行回数を超過しましたが、拡張再試行時間は経過していません。

自動インポートイベントが破棄され、イメージが無視される

- このイベントは、このマスターサーバーカタログにすでに存在するバックアップ ID を指定します。
- イベントはこのストレージサーバーの **NetBackup** で設定していないディスクボリュームを指定します。

自動インポートジョブは開始されるが、イメージが期限切れであるために削除され、ディスク領域がクリーンアップされることがある。イベントは[問題 (Problems)]レポートまたは bpererror 出力に記録されます。インポートジョブは実行されましたが、範囲 1532–1535 の状態コードを表示してこのイメージのインポートに失敗しました。

- イベントで指定されているストレージライフサイクルポリシーはインポートの宛先を含んでいません。
- イベントに指定されているストレージライフサイクルポリシーのインポート先の位置情報に、イベントによって指定されているディスクボリュームが含まれていません。
- 指定されているストレージライフサイクルポリシーは存在しません。デフォルトでは、[ストレージライフサイクルポリシー (Storage Lifecycle Policies)]ユーティリティは自動的に正しい名前でストレージライフサイクルポリシーを作成します。名前の大文字/小文字の使い方が同じストレージライフサイクルポリシーがターゲットマスターサーバーに存在することを確認します。  
ストレージライフサイクルポリシーの設定オプションについて、詳細情報が利用可能です。  
『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

このような状況が発生した場合は、[問題 (Problems)]レポートまたは bpererror リストで確認してください。

自動インポートジョブのジョブの流れをトラブルシューティングするには、他の **Storage Lifecycle Policy (SLP)** の管理ジョブで使うコマンドと同じコマンドを使います。NetBackup でストレージからの通知は受信しているがまだインポートを開始していない (保留中または失敗の) イメージをリストするには、前述のコマンドを使うか、または次のコマンドを実行します。

```
# nbstlutil list -copy_type import -U -copy_incomplete
```

自動的にインポートされたイメージをリストするには、次のコマンドを実行します。

```
# nbstlutil list -copy_type import -U -copy_state 3 -U
Master Server           : bayside.example.com
Backup ID               : woodridge_1287610477
Client                  : woodridge
Backup Time             : 1287610477 (Wed Oct 20 16:34:37 2010)
Policy                  : two-hop-with-dup
Client Type             : 0
Schedule Type          : 0
Storage Lifecycle Policy : woodridge2bayside2pearl_withdup
Storage Lifecycle State : 3 (COMPLETE)
Time In Process         : 1287610714 (Wed Oct 20 16:38:34 2010)
Data Classification ID  : (none specified)
Version Number          : 0
OriginMasterServer      : woodridge.example.com
OriginMasterServerID    : f5cec09a-da74-11df-8000-f5b3612d8988
Import From Replica Time : 1287610672 (Wed Oct 20 16:37:52 2010)
Required Expiration Date : 1290288877 (Sat Nov 20 15:34:37 2010)
Created Date Time       : 1287610652 (Wed Oct 20 16:37:32 2010)
```

OriginMasterServer、OriginMasterServerID、Import From Replica Time、Required Expiration Date はイメージがインポートされるまで不明であるため、保留中のレコードは次のように表示される場合があります。

Image:

```
Master Server           : bayside.example.com
Backup ID               : gdwinlin04_1280299412
Client                  : gdwinlin04
Backup Time             : 1280299412 (Wed Jul 28 01:43:32 2010)
Policy                  : (none specified)
Client Type             : 0
Schedule Type          : 0
Storage Lifecycle Policy : (none specified)
Storage Lifecycle State : 1 (NOT_STARTED)
Time In Process         : 0 (Wed Dec 31 18:00:00 1969)
Data Classification ID  : (none specified)
Version Number          : 0
OriginMasterServer      : master_tlk
OriginMasterServerID    : 00000000-0000-0000-0000-000000000000
Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
```

Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)  
Created Date Time : 1287680533 (Thu Oct 21 12:02:13 2010)

この例では OriginMasterServer は空ではありませんが、空の場合もあります。自動イメージレプリケーションのカスケード時に、マスターサーバーは通知を送信します。

## ネットワークインターフェースカードのパフォーマンスのトラブルシューティング

バックアップジョブまたはリストアジョブに時間がかかる場合は、ネットワークインターフェースカード (NIC) が全二重モードに設定されていることを確認します。多くの場合、半二重モードが設定されていると、パフォーマンスが低下します。

---

**メモ:** NetBackup マスターサーバーまたはメディアサーバーの NIC を変更したり、サーバーの IP アドレスを変更した場合、CORBA の通信が中断される可能性があります。この問題を解決するには、NetBackup を停止してから再起動します。

---

特定のホストまたはデバイスで二重モードを確認および再設定する場合は、各製造元のマニュアルを参照してください。マニュアルが役に立たない場合は、次の手順を実行します。

## ネットワークインターフェースカードのパフォーマンスをトラブルシューティングする方法

- 1 二重モードを調べるネットワークインターフェースカードを含んでいるホストにログオンします。
- 2 次のコマンドを入力し、現在の二重モードの設定を表示します。

```
ifconfig -a
```

オペレーティングシステムによっては、ipconfig コマンドを使用します。

次に NAS ファイラからの出力例を示します。

```
e0: flags=1948043<UP,BROADCAST,RUNNING,MULTICAST,TCPCSUM> mtu
1500
inet 10.80.90.91 netmask 0xfffff800 broadcast 10.80.95.255
ether 00:a0:98:01:3c:61 (100tx-fd-up) flowcontrol full
e9a: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCSUM> mtu 1500
ether 00:07:e9:3e:ca:b4 (auto-unknown-cfg_down) flowcontrol full
e9b: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCSUM> mtu 1500
ether 00:07:e9:3e:ca:b5 (auto-unknown-cfg_down) flowcontrol full
```

この例では、ネットワークインターフェース **100tx-fd-up** が全二重モードで動作しています。(リストの最初の)インターフェース **e0** だけが、全二重モードで動作しています。

[**auto**]の設定では、デバイスが自動的に半二重モードに設定されることがあるため、[**auto**]に設定しないことをお勧めします。

- 3 二重モードをリセットするには、ifconfig (または ipconfig) コマンドを実行します。次に例を示します。

```
ifconfig e0 mediatype 100tx-fd
```

- 4 多くのホストでは、ホストの /etc/rc ファイルなどで、全二重モードを永続的に設定できます。詳しくは、各ホストのマニュアルを参照してください。

## bp.conf ファイルの SERVER エントリについて

UNIX コンピュータと Linux コンピュータでは、クライアントの bp.conf ファイル内のすべての SERVER エントリが **NetBackup** マスターサーバーまたはメディアサーバーである必要があります。すなわち、SERVERとして表示されている各コンピュータには、**NetBackup** マスターまたはメディアのサーバーソフトウェアがインストールされている必要があります。クライアント名が誤ってサーバーとしてリストに表示されている場合、そのクライアント上のクライアントサービスは起動されません。

bp.conf の SERVER エントリに **NetBackup** クライアントだけがインストールされているコンピュータが指定されている場合、ファイバーチャネルを介した **SAN** クライアントのバックアップまたはリストアが開始されない可能性があります。この場合、クライアント上で nbftclnt プロセスが実行されているかどうかを判断します。実行されていない場合、nbftclnt の統合ログファイル (**OID 200**) にエラーが表示されていないかどうかを確認します。nbftclnt ログに次のようなエラーが表示されている可能性があります。

```
The license is expired or this is not a NBU server. Please check
your configuration. Note: unless NBU server, the host name can't be
listed as server in NBU configuration.
```

bp.conf ファイル内の SERVER エントリを削除または修正し、クライアント上の nbftclnt を再起動して、操作を再試行します。

---

**メモ:** クライアント上の nbftclnt プロセスは、ファイバーチャネルを介した **SAN** クライアントのバックアップまたはリストアを開始する前に実行しておく必要があります。

---

## 使用できないストレージユニットの問題について

**NetBackup** ジョブは、ディスクドライブまたはテープドライブの停止または構成エラーに起因してストレージユニットが利用不可になったことで失敗することがあります。このような問題を特定して解決するために、**NetBackup** プロセスにより **NetBackup** エラーログにメッセージが記録されます。

また、アクティビティ 모니터の[ジョブの詳細 (**Job Details**)]ダイアログボックスには、次のようなリソースを示すメッセージが表示されます。

- ジョブが要求しているリソース
- 付与された (割り当てられた) リソース

ジョブがキューに投入され、リソースを待機している場合、[ジョブの詳細 (**Job Details**)]ダイアログボックスにはジョブが待機しているリソースが表示されます。次のように始まる 3 種類のメッセージが表示されます。

```
requesting resource ...
awaiting resource ...
granted resource ...
```

## Windows での NetBackup 管理操作のエラーの解決

管理者グループのメンバーに対する操作は、次のエラーで失敗する可能性があります。コマンドは **NetBackup** 管理者コマンドです。

command: terminating - cannot open debug file: Permission denied (13)

### Windows での NetBackup 管理操作のエラーの解決方法

- 1 [ローカルセキュリティポリシー (Local Security Policy)]を開きます。
- 2 [ローカルポリシー (Local Policies)]、[セキュリティの設定 (Security Settings)]の順に展開します。
- 3 [ユーザーアカウント制御: 管理者承認モードですべての管理者を実行する (User Account Control: Run All administrators in Admin Approval Mode)]設定を無効にします。

## UNIX コンピュータの NetBackup 管理コンソールに表示されるテキストの文字化けの解決

文字化けしたテキストが表示されるか、英語以外のテキストが UNIX コンピュータの NetBackup 管理コンソールに表示できない場合には、次の手順を実行します。

- 1 コマンドプロンプトで、`locale` と入力します。
- 2 `LC_CTYPE` が、表示したいロケールに対応する値に設定されていることを確認します。

たとえば、`LC_CTYPE` が `en_US.UTF-8` に設定されている場合、コンソール内のテキストは US 英語で表示されます。

`LC_CTYPE` が `fr_FR.UTF8` に設定されている場合、コンソール内のテキストはフランス語で表示されます。

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

NetBackup に表示されるエラーメッセージの種類は次のとおりです。

表 2-10 エラーメッセージの種類

エラーの種類	説明
NetBackup の状態コードおよびメッセージ	<p>NetBackup 管理コンソールで実行される操作によって、NetBackup の他の部分でエラーが検出される場合があります。これらのエラーは、通常、NetBackup の状態コードおよびメッセージの章に記載されているとおりに表示されます。</p> <p><b>メモ:</b> エラーメッセージには、状態コードが付かない場合もあります。</p>

エラーの種類	説明
NetBackup 管理コンソール: アプリケーションサーバーの状態コードおよびメッセージ	これらのメッセージには、500 番台の状態コードが付きま <b>メモ:</b> エラーメッセージには、状態コードが付かない場合もあります。
Java の例外	これらの例外は、Java API または NetBackup 管理 API によって生成されます。 Java の例外は、通常、次のいずれかの位置に表示されます。 <ul style="list-style-type: none"> <li>■ NetBackup 管理コンソールのステータスバー</li> <li>■ jnbSA コマンドまたは jbpSA コマンドで生成されるログファイル</li> </ul>

## NetBackup 管理コンソールでのログと一時ファイルの保存に必要な追加のディスク容量

NetBackup 管理コンソールはログと一時ファイルを保存する追加のディスク容量を必要とします。

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

利用可能な領域がない場合、次の問題が発生することがあります。

- アプリケーションの応答に時間がかかる
- データが不完全になる
- ログイン中に応答がない
- NetBackup インターフェースの機能が低下する (ツリーにはバックアップ、アーカイブ、リストアノードおよびファイルシステムの分析ノードしか表示されないなど)
- 予想外のエラーメッセージ:
  - NetBackup-Java アプリケーションサーバーへのログオン中に、"ソケットに接続できない"というエラーが発生する
  - [ログインできません。状態: 35 要求されたディレクトリを作成できません (Unable to login, status: 35 cannot make required directory)]
  - [/bin/sh: null: not found (1)]

- [An exception occurred: vrts.nbu.admin.bpmgmt.CommandOutputException: Invalid or unexpected class configuration data: <the rest of the message will vary>]
- 空白の警告ダイアログボックスが表示される

## 外部 CA の構成後に NetBackup 管理コンソールにログオンできない

次のシナリオのトラブルシューティングを確認します。

NetBackup での外部 CA のサポートについて詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

### シナリオ

NetBackup 管理コンソールの接続先となるホストで vnetd サービスが停止している場合

### 推奨処置

ホストでサービスが起動しているかどうかを確認し、ログインを再試行します。

### シナリオ

外部証明書の秘密鍵が使用できないか、不正な形式で、エラー VRTS-28678 が表示される場合

### 推奨処置

- ECA\_PRIVATE\_KEY\_PATH 構成オプションで指定されたパスが有効であるかどうかを確認します (このパスは空にできません)。
- ECA\_PRIVATE\_KEY\_PATH で指定されたパスがアクセス可能で、秘密鍵ファイルに必要なアクセス許可があるかどうかを確認します。
- 有効な秘密鍵を指定して、ログインを再試行してください。

Windows 証明書ストアの場合は、次の操作を行います。

- certlm.msc コマンドを実行します。  
certlm.msc が動作しない場合は、mmc.exe コマンドを実行して Windows 証明書ストアにアクセスできます。[ファイル (File)]、[スナップインの追加と削除 (Add Remove Snap in)]の順に移動します。
- 証明書をダブルクリックして開きます。  
秘密鍵付きの証明書では、この証明書に対応する秘密鍵があることを示すメッセージが表示されます。

## シナリオ

NetBackup 管理コンソールとの信頼を確立するときに外部証明書が存在しない場合

### 推奨処置

- ECA\_TRUST\_STORE\_PATH 構成オプションで指定されたパスが空でないかどうかを確認します。
- ECA\_TRUST\_STORE\_PATH で指定されたパスがアクセス可能で、CA 証明書ファイルに必要なアクセス許可があるかどうかを確認します。
- 有効な外部証明書を指定し、ログインを試行します。

Windows 証明書ストアの場合は、次の操作を行います。

- Windows 証明書ストアの[信頼できるルート認証局 (Trusted Root Certification Authorities)]にルート CA 証明書が追加されているかどうかを確認します。
- certlm.msc コマンドを実行します。[証明書管理 (Certificate Management)]ウィンドウで、[信頼できるルート認証局 (Trusted Root Certification Authorities)]という名前のストアを開きます。[信頼できるルート認証局 (Trusted Root Certification Authorities)]ストアには、そのマシンで信頼されるすべての自己署名証明書が含まれています。  
 certlm.msc が動作しない場合は、mmc.exe を実行して Windows 証明書ストアにアクセスできます。[ファイル (File)]、[スナップインの追加と削除 (Add Remove Snap in)]の順に移動します。
  - 左側から証明書を選択します。
  - [追加 (Add)]をクリックします。
  - コンピュータアカウントを選択します。[次へ (Next)]をクリックします。
  - [完了 (Finish)]をクリックして、[OK]をクリックします。
  - [信頼できるルート認証局 (Trusted Root Certification Authorities)]、[証明書 (Certificates)]の順にクリックします。
  - 証明書チェーンのルート CA 証明書が[信頼できるルート認証局 (Trusted Root Certification Authorities)]ストアに存在するかどうかを確認します。
- ルート CA 証明書が存在しない場合は、次の操作を行います。
  - [すべてのアクション (All Actions)]、[インポート (Import)]の順にクリックします。
  - 証明書の .PEM、.CRT、または .CER ファイルを選択し、[インポート (Import)]をクリックします。

---

**メモ:** 証明書はすべて、現在のユーザーストアではなくローカルマシンストアにインポートする必要があります。[証明書管理 (Certificate Management)] ウィンドウで現在のストアを確認できます。

---

- 有効な外部 CA 証明書を追加し、ログインを試行します。

## シナリオ

外部 CA が署名した証明書が存在しない、またはアクセスできず、次のエラーが表示される場合

The host does not have external CA-signed certificate. The certificate is mandatory to establish a secure connection.

## 推奨処置

- NetBackup 構成ファイルの ECA\_CERT\_PATH で指定されたパスが空でないかどうかを確認します。
- ECA\_CERT\_PATH で指定されたパスが証明書チェーン全体を指しているかどうかを確認します。
- ECA\_CERT\_PATH で指定されたパスがアクセス可能で、必要なアクセス許可があるかどうかを確認します。
- 有効な外部 CA が署名した証明書を指定し、ログインを試行します。

Windows 証明書ストアの場合は、次の操作を行います。

- ECA\_CERT\_PATH に、適切な値 (Windows Certificate Store Name¥Issuer Name¥Subject Name) が含まれているかどうかを確認します。Windows 証明書ストアに証明書が存在するかどうかを確認します。
  - certlm.msc コマンドを実行します。  
certlm.msc が動作しない場合は、mmc.exe を実行して Windows 証明書ストアにアクセスできます。  
[ファイル (File)]、[スナップインの追加と削除 (Add Remove Snap in)] の順に移動します。
  - 入力した Windows 証明書ストア名¥発行者名¥サブジェクト名に従って、証明書に移動します。
  - 証明書をダブルクリックして開きます。
  - 証明書が有効で、秘密鍵があり、発行者名とサブジェクト名が正しいことを確認します。  
サブジェクト名で \$hostname を使用している場合は、証明書のサブジェクトにホストの完全修飾ドメイン名が設定されていることを確認します。

そうでない場合は、ECA\_CERT\_PATH を変更するか、適切な証明書を Windows 証明書ストアに配置してログインを再試行します。

## シナリオ

証明書失効リスト (CRL) が信頼できる認証局によって署名されていない。

### 推奨処置

これは、NetBackup 証明書を使用するようにマスターサーバーが構成され、後で外部証明書の使用を有効化した場合、またはその逆の場合にログイン時に発生します。アクティビティモニターをクリックすると NetBackup 管理コンソールが新しい CRL の使用を開始し、画面をロックして、ログインを再試行するか、1 時間ごとの定期チェックで証明書の失効状態の検証に失敗します。

この問題を修正するには、ピアホストの証明書と CRL を同期させるため、コンソールを閉じて再度ログインする必要があります。

再度ログインしても問題が修正されない場合、新しい CRL がダウンロードされていないことが原因である可能性があります。

CRL の形式を修正した後に、次のコマンドを実行します。

UNIX の場合: /usr/opensv/netbackup/bin/nbcertcmd -updateCRLCache

Windows の場合: install\_path¥Veritas¥Netbackup¥bin¥nbcertcmd  
-updateCRLCache

## シナリオ

CRL の形式が無効であるため、CRL を使用してホスト証明書の失効状態を検証できない。

### 推奨処置

このエラーは、差分 CRL が使用されているときに発生する場合があります。

NetBackup は差分 CRL をサポートしていないため、差分ではない CRL を使用する必要があります。

CRL の形式を修正した後に、次のコマンドを実行します。

UNIX の場合: /usr/opensv/netbackup/bin/nbcertcmd -updateCRLCache

Windows の場合: install\_path¥Veritas¥Netbackup¥bin¥nbcertcmd  
-updateCRLCache

## シナリオ

ホスト名の証明書が無効化されている。

## 推奨処置

エラーが発生して証明書が無効化された場合は該当ホストの証明書を再発行します。

意図的に証明書が無効化した場合はセキュリティ違反が発生した可能性があります。セキュリティ管理者にお問い合わせください。

## シナリオ

証明書失効リストをダウンロードできない。このため、証明書失効状態を検証できない。

## 推奨処置

考えられる原因は、次のとおりです。

- ECA\_CRL\_PATH が見つからない、またはパスが正しくない
- CRL ファイルが見つからない CRL ファイルをロック解除できない
- CRL ファイルをロックできない
- CRL ファイルをロック解除できない

詳しくは、bpjava ログを参照してください。

## シナリオ

証明書失効リストが更新されていない。このため、証明書失効状態を検証できない。

## 推奨処置

考えられる原因は、次のとおりです。

- CRL の次の更新日時が現在のシステム日時より前である
- ログイン時には CRL が有効だったが、コンソールが開かれ、CRL が無効になったシステム時刻が正しいことを確認します。

新しい CRL がダウンロードされていない場合は、次のコマンドを実行します。

UNIX の場合: /usr/openv/netbackup/bin/nbcertcmd -updateCRLCache

Windows の場合: install\_path\Veritas\Netbackup\bin\nbcertcmd  
-updateCRLCache

## シナリオ

NetBackup Web 管理コンソールサービスに接続できない。

## 推奨処置

考えられる原因は、次のとおりです。

- NetBackup Web 管理コンソールサービスが停止している

- ECA\_CERT\_PATH が証明書チェーン全体を指していない
- Web サービス証明書の発行者とホスト証明書の発行者が一致していない  
両方の証明書が同じ外部 CA によって発行されていない場合は、証明書の信頼の検証は失敗します。

次の項目を確認してください。

- 証明書チェーン全体を含む、証明書ファイルへのパスを指定する必要があります (ルート証明書を除く)。
- チェーンが指定されていない場合は、証明書の信頼の検証が失敗し、コンソールは Web サービスに接続できません。
- Web サーバーの証明書とホスト証明書が同じ外部 CA によって発行されていることを確認してください。

## ファイルベースの外部証明書の問題のトラブルシューティング

この問題の発生は、次のいずれかが理由と考えられます。

- 通信に使用される Web サービス証明書が正しく構成されていない。
- 一部の NetBackup Core Services が開始されていない。
- 外部証明書の必要な前提条件が満たされていない。
- 外部証明書の構成パス (ECA\_CERT\_PATH) が正しく構成されていない。
- 証明書の失効の確認に失敗した。

この問題を解決するには、次の原因を確認し、次のコマンドを実行して問題の現在の状態を判断します。

```
Install_Path/bin/nbcertcmd -enrollCertificate -preCheck -server  
server_name
```

*Install\_Path* は、次を指します。

Windows の場合: VERITAS\NetBackup\bin

UNIX の場合: /usr/opensv/netbackup/bin

### 原因 1: 通信に使用される Web サーバー証明書が正しく構成されていない。

- NetBackup Web サーバーが外部証明書を使用するように構成されていません。  
次のエラーが表示されます。  
終了状態 26: クライアント/サーバーのハンドシェイクが失敗しました。

- マスターサーバーで次のコマンドを実行し、外部 CA が構成されているかどうか (オンかオフか) を確認します。

```
Install_Path/nbcertcmd -getSecConfig -caUsage
```

**Windows** の場合: C:¥Program Files¥ VERITAS¥NetBackup¥bin¥nbcertcmd  
 -getSecConfig -caUsage

**Unix** の場合: /usr/opensv/netbackup/bin/netbackup/bin/nbcertcmd  
 -getSecConfig -caUsage

例: C:¥Program Files¥Veritas¥NetBackup¥bin>nbcertcmd -getSecConfig  
 -caUsage

出力:

```
NBCA:OFF ECA:ON
```

外部 CA が構成されていない場合は、Web サーバーで  
 configureWebServerCerts コマンドを実行します。

場合によっては、Web サーバーで外部 CA が構成されていないときに次のエラー  
 も発生する可能性があります。

終了状態 5982: 証明書失効リストを使用できません。

この場合は、まず ECA パラメータの値を確認します。この値がオフの場合は、  
 configureWebServerCerts コマンドを実行します。

- 通信に使用される Web サービス証明書が認証局に信頼されていません。
  - 証明書のパス (configureWebServerCert -certPath オプション) で、リーフ  
 証明書と、トラストアンカー (ルート CA) を除く CA 証明書のチェーン全体が指定  
 されている必要があります。

- 次のコマンドを実行し、Web サーバー用に構成されている証明書を一覧表示し  
 ます。

```
nbcertcmd -listallcertificates -jks
```

**Windows** の場合: C:¥Program Files¥ VERITAS¥NetBackup¥bin¥nbcertcmd  
 -listallcertificates -jks

**UNIX** の場合: /usr/opensv/netbackup/bin/netbackup/bin/nbcertcmd  
 -listallcertificates -jks

- 次のコマンドを実行して、NetBackup マスターサーバーのホスト証明書の詳細を  
 一覧表示します。

```
Install_Path/goodies/nbsslcmd x509 -in certificate_path -noout  

-text -purpose
```

**Windows** の場合: C:¥Program Files¥

```
VERITAS¥NetBackup¥bin¥goodies¥nbsslcmd x509 -in certificate_path  

-noout -text -purpose
```

UNIX の場合:

```
/usr/openssl/netbackup/bin/netbackup/bin/goodies/nbsslcmd x509  
-in certificate_path -noout -text -purpose
```

マスターサーバーのホスト証明書が、Web サーバー証明書と同じルート CA によって発行されているかどうかを検証します。

ホスト証明書が、Web サーバー証明書と同じルート CA によって発行されていない場合、NetBackup マスターサーバーの CA で新しい証明書を発行し、再度証明書を登録します。

- 指定したサーバー名が Web サービス証明書内に見つかりませんでした。サーバー名がサーバーの証明書に表示されているどのホスト名とも一致しません。サーバーの証明書に表示されている名前は、次のとおりです:  
DNS: nb-master\_ext  
DNS: nb-master.some.domain.com  
DNS: nb-master\_web\_svr EXIT STATUS 8509:  
Web サーバー証明書に存在するいずれかの名前を使用してマスターサーバーを参照するように NetBackup ホストの構成を更新するか、証明書の NetBackup ドメインに認識されているマスターサーバーのすべての名前を含めます。

詳しくは、次の記事を参照してください。

[https://www.veritas.com/support/en\\_US/article.000126751](https://www.veritas.com/support/en_US/article.000126751)

## 原因 2

一部の NetBackup Core Services が開始されていない。

この問題を解決するには、次の手順を実行します。

- NetBackup/bin ディレクトリから bpps コマンドを実行し、次のサービスの状態を確認します。
  - nbsl
  - vnetd -standalone
  - NB\_dbsrv (UNIX の場合) または dbsrv16 (Windows の場合)  
NetBackup 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。
- nbsl サービスと vnetd サービスを起動します (起動していない場合)。
- NB\_dbsrv (UNIX の場合) サービスまたは dbsrv16 (Windows の場合) サービスを起動します (起動していない場合)。

次の手順を実行し、nbsl、vnetd、NB\_dbsrv (または dbsrv16) サービスを再起動します。

Windows の場合:

```
Install_Path¥bin¥bpdown -e "NetBackup Service Layer" -f -v
Install_Path¥bin¥bpup -e "NetBackup Service Layer" -f -v
Install_Path¥bin¥bpdown -e "NetBackup Legacy Network Service" -f -v
Install_Path¥bin¥bpup -e "NetBackup Legacy Network Service" -f -v
Install_Path¥bin¥bpdown -e "SQLANYs_VERITAS_NB" -f -v
Install_Path¥bin¥bpup -e "SQLANYs_VERITAS_NB" -f -v
```

または、**Service Control Manager** を使用して、**NetBackup Service Layer (NBSL)**、**NetBackup Legacy Network Service (vnetd)**、**SQLANYs\_VERITAS\_NB** サービスを再起動できます。

次に例を示します。

```
C:¥Program Files¥Veritas¥NetBackup¥bin¥bpdown -e "NetBackup Service
Layer" -f -v
C:¥Program Files¥Veritas¥NetBackup¥bin¥bpup -e "NetBackup Service
Layer" -f -v
C:¥Program Files¥Veritas¥NetBackup¥bin¥bpdown -e "NetBackup Legacy
Network Service" -f -v
C:¥Program Files¥Veritas¥NetBackup¥bin¥bpup -e "NetBackup Legacy
Network Service" -f -v
C:¥Program Files¥Veritas¥NetBackup¥bin¥bpdown -e "SQLANYs_VERITAS_NB"
-f -v
C:¥Program Files¥Veritas¥NetBackup¥bin¥bpup -e "SQLANYs_VERITAS_NB"
-f -v
```

**UNIX** の場合:

```
Install_Path/netbackup/bin/nbsl -terminate
Install_Path/netbackup/bin/nbsl
```

vnetd と NB\_dbsrv を停止するには、次の例を参照してください。

vnetd と NB\_dbsrv を起動するには、次のコマンドを実行します。

```
install_path/netbackup/bin/vnetd -standalone
install_path/db/bin/NB_dbsrv
```

次に例を示します。

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

```
# ps -fed | grep vnetd | grep standalone
root 16018 1 4 08:47:35 ? 0:01 ./vnetd -standalone

# kill 16018

# ps -fed |grep NB_dbdrv
root 11959 1 4 08:47:35 ? 0:01 ./NB_dbdrv
root 16174 16011 0 08:47:39 pts/2 0:00 grep ./NB_dbdrv

# kill 11959

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

/usr/opensv/db/bin/NB_dbdrv
```

問題が解決しない場合は、テクニカルサポートチームにお問い合わせください。

### 原因 3

外部証明書の必要な前提条件が満たされていない。

次の前提条件を確認してください。

- サブジェクト DN は一意で、各ホストで安定している必要があります。255 文字未満にする必要があり、空にはできません。
- 証明書のサブジェクト DN と X509v3 サブジェクトの別名では、ASCII 7 文字のみがサポートされています。
- サーバーとクライアントの認証属性 (SSL サーバーと SSL クライアント) を証明書に設定する (または true にする) 必要があります。
- 証明書は PEM 形式です。
- CRL 配布ポイント (CDP) は、HTTP/HTTPS のみでサポートされます。

次のコマンドを実行して、前提条件が満たされているかどうかを確認します。

```
Install_Path/goodies/nbsslcmd x509 -in certificate_path -noout -text -purpose
```

---

**メモ:** `configureWebServerCert -certPath` オプションと `ECA_CERT_PATH` オプションに指定されている証明書のパスで、リーフ証明書と、トラストアンカー (ルート CA) を除く CA 証明書のチェーン全体が指定されている必要があります。

---

望ましい条件:

- 証明書の登録に使用されるホスト名 (`CLIENT_NAME`) は、DNS タイプの X509v3 サブジェクトの別名の一部にする必要があります。
- サブジェクト名の一般名 (CN) を空にはできません。

---

**メモ:** `nbsslcmd` コマンドを実行すると次の警告が生成されますが、無視してかまいません。

```
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
```

---

## 原因 4

外部証明書の構成パスが正しく構成されていない。

次の外部証明書の構成オプションが正しく構成されていることを確認します。

- `ECA_CERT_PATH`
- `ECA_TRUST_STORE_PATH`
- `ECA_PRIVATE_KEY_PATH`
- `ECA_CRL_PATH`
- `ECA_CRL_CHECK`

次の項目について確認します。

- ピアホスト証明書に **CRL 配布ポイント (CDP)** が指定されている。  
`ECA_CRL_PATH` を指定しない場合、**NetBackup** はピアホスト証明書の **CDP** で指定されている **URL** の **CRL** を使用します。
- `ECA_CRL_PATH` は、**Windows** の **volumeID** パスではありません。

次のコマンドを実行し、外部証明書の構成パラメータを検証します。

**UNIX** の場合: `Install_Path/bin/nbgetconfig | grep ECA`

**Windows** の場合: `Install_Path/bin/nbgetconfig | findstr ECA`

.

構成オプションについて詳しくは、『**NetBackup セキュリティおよび暗号化ガイド**』を参照してください。

## 原因 5

原因 3 に記載されている必要条件が満たされていない。

- 証明書の登録に使用されるホスト名 (`CLIENT_NAME`) が、**DNS** タイプの **X509v3** サブジェクトの別名の一部ではありません。  
このエラーによって登録に失敗した場合は、次のいずれかの操作を行います。
  - 証明書のサブジェクトの別名にホスト名が存在する新しい証明書を生成します。
  - マスターサーバーの外部証明書データベースで、証明書 (**RFC 2253 準拠**) のサブジェクト名を追加または更新 (削除してから追加) します。  
次のコマンドを実行して、ホストと関連サブジェクト名のエントリを **NetBackup** 証明書データベースに追加します (管理者のみがこの操作を実行できます)。

```
Install_Path/bin/nbcertcmd -createECACertEntry -host host_name  
| -hostId host_id -subject subject name of external cert  
[-server master_server_name]
```

または、次のコマンドを実行して、**NetBackup** 証明書データベースからホストと関連サブジェクト名のエントリを削除してから、`-createECACertEntry` コマンドを使用してエントリを追加します (管理者のみがこの操作を実行できます)。

```
Install_Path/bin/nbcertcmd -deleteECACertEntry -subject subject  
name of external cert [-server master_server_name]
```

- サブジェクト名の一般名 (CN) が証明書内に存在しない。  
このエラーによって証明書の登録に失敗した場合は、次のいずれかの操作を行います。
  - 証明書に一般名が存在する新しい証明書を生成します。
  - 証明書のサブジェクトの別名にホスト名が存在する新しい証明書を生成します。
  - **NetBackup** ホストデータベースにホストを追加し、ホストとその関連サブジェクト名のエントリを **NetBackup** 証明書データベースに追加します。  
次のコマンドを実行して、ホストを **NetBackup** ホストデータベースに追加します (管理者のみがこの操作を実行できます)。

```
Install_Path/bin/admincmd/nbhostmgmt -addhost -host host_name  
| -hostId host_id [-server master_server_name]
```

次のコマンドを実行して、ホストと関連サブジェクト名のエントリを **NetBackup** 証明書データベースに追加します。

```
Install_Path/bin/nbcertcmd -createECACertEntry -host host_name  
| -hostId host_id -subject subject name of external cert  
[-server master_server_name]
```

外部証明書のサブジェクト名は、RFC 2253 準拠である必要があります。

## 原因 6

証明書の失効の確認に失敗した。

外部証明書の登録は、次の理由により証明書無効化エラーで失敗する場合があります。

- 外部証明書が無効化されている
- Web サーバー証明書が無効化されている
- ホストまたはマスターサーバーで CRL が使用できない

p.66 の「外部 CA が署名した証明書の無効化に関する問題のトラブルシューティング」を参照してください。

**NetBackup** での外部証明書の登録について詳しくは、『**NetBackup** セキュリティおよび暗号化ガイド』を参照してください。

# Windows 証明書ストアの問題のトラブルシューティング

Windows 証明書ストアの使用時に、Web サービス証明書が不明な認証局によって発行された

## 問題

ホスト証明書の登録中に Web サービス証明書が信頼されません。

原因

この問題は次のいずれかの原因で発生する可能性があります。

- 通信に使用される Web サービス証明書が正しく構成されていない。
- Windows 証明書ストアの信頼できるルート認証局に、Web サービス証明書の証明書チェーンのルート証明書が存在しない。

## 解決方法

この問題を解決するには、次の原因を確認し、次のコマンドを実行して問題の現在の状態を判断します。

```
Install_Path/bin/ nbcertcmd -enrollCertificate -preCheck -server  
server_name
```

*Install\_Path* は、次を指します。

Windows の場合: VERITAS¥NetBackup¥bin

UNIX の場合: /usr/opensv/netbackup/bin

## 次が原因である場合の解決方法: 通信に使用される Web サービス証明書が正しく構成されていない

有効な証明書とその CA 証明書を使用して Web サーバーが構成されていることを確認します。

- 次のコマンドを実行し、Web サーバー用に構成されている証明書を一覧表示します。

```
Install_Path/nbcertcmd -listallcertificates -jks
```

Windows の場合: C:¥Program Files¥ VERITAS¥NetBackup¥bin¥nbcertcmd  
-listallcertificates -jks

UNIX の場合: /usr/opensv/netbackup/bin/netbackup/bin/nbcertcmd  
-listallcertificates -jks

- チェーン内のすべての証明書 (ルート CA 証明書を除く) が jks に存在することを確認します。

nbcertcmd -listallcertificates -jks の出力で、次のパラメータを確認します。

- エイリアス名: eca

- エントリ形式: PrivateKeyEntry

これらが存在しない場合は、Web サービス証明書ファイルであるエンティティ証明書ファイルの最後に CA チェーンを追加します。最上位に Web サービス証明書、その下にその発行者の CA 証明書、その下にその CA 証明書の発行者、のようにします。証明書チェーンに 2 つの証明書 (ルート証明書と Web サービス証明書) しかない場合、証明書ファイルには 1 つの証明書 (Web サービス証明書) のみが存在します。configureWebServerCerts コマンドを実行します。

## 次が原因である場合の解決方法: Web サービス証明書の証明書チェーンのルート証明書が Windows 証明書ストアに存在しない

- certlm.msc コマンドを実行します。

[証明書管理 (Certificate Management)] ウィンドウで、[信頼できるルート認証局 (Trusted Root Certification Authorities)] という名前のストアを開きます。  
[信頼できるルート認証局 (Trusted Root Certification Authorities)] ストアには、そのマシンで信頼されるすべての自己署名証明書が含まれています。

  - certlm.msc が動作しない場合は、mmc.exe コマンドを実行して Windows 証明書ストアにアクセスできます。
  - [ファイル (File)]、[スナップインの追加と削除 (Add Remove Snap in)] の順に移動します。
  - 左側から証明書を選択します。
  - [追加 (Add)] をクリックします。
  - コンピュータアカウントを選択します。
  - [次へ (Next)]、[完了 (Finish)]、[OK] の順にクリックします。
  - [信頼できるルート認証局 (Trusted Root Certification Authorities)]、[証明書 (Certificates)] の順にクリックします。
  - [信頼できるルート認証局 (Trusted Root Certification Authorities)]、[証明書 (Certificates)] の順にクリックします。
- ルート CA 証明書が存在しない場合は、[すべてのアクション (All Actions)]、[インポート (Import)] の順にクリックし、証明書の .PEM、.CRT、または .CER ファイルを選択して [インポート (Import)] をクリックします。

証明書はすべて、現在のユーザーストアではなくローカルマシンストアにインポートする必要があります。

[証明書管理 (Certificate Management)] ウィンドウで現在のストアを確認できます。

## 問題

証明書の公開鍵アルゴリズムがサポートされていません。

公開鍵アルゴリズムは **NetBackup** でサポートされていません。現在、**RSA** アルゴリズムのみがサポートされています。

## 原因

指定されたパスの証明書が **Windows** 証明書ストアに存在しますが、その署名アルゴリズムがサポートされていません。

## 解決方法

**NetBackup** でサポートされている公開鍵アルゴリズムが使用された証明書を使用する必要があります。

**NetBackup** での外部証明書の登録について詳しくは、『**NetBackup** セキュリティおよび暗号化ガイド』を参照してください。

## 問題

指定した証明書の秘密鍵を利用できません。

パスで指定した証明書に対応する秘密鍵が、**Windows** 証明書ストアにインポートされていません。

## 原因

これは通常、**.pfx** ではなく、**.crt**、**.cer**、または **.pem** 証明書を **Windows** 証明書ストアに手動でインポートしたことが原因です。

## 解決方法

証明書の秘密鍵がインポート済みであることを確認します。

- **certlm.msc** コマンドを実行します。  
**certlm.msc** が動作しない場合は、**mmc.exe** コマンドを実行して **Windows** 証明書ストアにアクセスできます。  
[ファイル (File)]、[スナップインの追加と削除 (Add Remove Snap in)]の順に移動します。
- 証明書に移動します。
- 証明書をダブルクリックして開きます。  
秘密鍵付きの証明書では、この証明書に対応する秘密鍵があることを示すメッセージが表示されます。
- 証明書を手動で登録する場合は、**.cer** または **.crt** ファイルだけでなく、**.pfx** ファイルもインポートします。

**NetBackup** での外部証明書の登録について詳しくは、『**NetBackup** セキュリティおよび暗号化ガイド』を参照してください。

## 問題

指定したサブジェクト名の証明書が見つかりません。

ECA\_CERT\_PATH に特殊なキーワード **\$hostname** が使用されていると、証明書が見つかりません。

## 原因

指定された ECA\_CERT\_PATH のローカルマシンストアに証明書が存在しません。

ストア名、発行者名、サブジェクト名のいずれかの属性が、ローカルマシンストアの属性と一致していません。

## 解決方法

- 証明書がローカルマシンストアに存在するかどうかを確認します。次を実行します。
  - certlm.msc コマンドを実行します。  
certlm.msc が動作しない場合は、mmc.exe コマンドを実行して Windows 証明書ストアにアクセスできます。  
[ファイル (File)]、[スナップインの追加と削除 (Add Remove Snap in)]の順に移動します。
  - 証明書が存在するかどうかを確認します
- 次の条件を満たしていることを確認します。
  - 証明書の場所は、パスまたはカンマ区切りのパスで、各パスはスラッシュ (¥) で区切られたストア名、発行者名、サブジェクト名を使用して指定されている。
  - ストア名は、証明書が存在するストアと完全に一致する必要がある。
  - 発行者名とサブジェクト名は必ず ECA\_CERT\_PATH に含まれている必要がある。発行者名に何も指定されていない場合は、任意の発行者を考慮することを意味する。
  - \$hostname は特殊なキーワードで、サブジェクト名で使用できる。証明書を検索するとき、\$hostname はホストの実際の FQDN に置き換えられる。
  - \$hostname を使用する場合、証明書は CN の一部として FQDN を指定する必要がある。
  - 実際のストア名、発行者名、サブジェクト名にバックスラッシュ (¥) が存在する場合は、二重引用符を使用する。
  - サブジェクト名は必ず ECA\_CERT\_PATH の一部にする必要がある。ただし、CN =example CN は許可されない。  
ECA\_CERT\_PATH のサブジェクトは、実際の CN、OU、O、L、S、C などの任意の部分文字列にする必要がある。

NetBackup での外部証明書の登録について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

## バックアップエラーのトラブルシューティング

### 問題

当該ドメインでホストとの通信に NetBackup CA の証明書を使用できないため証明書操作が失敗するピアホストの検証エラーで、バックアップが失敗します。

### 原因

失敗の原因として、次のことが考えられます。

- 外部 CA が署名した証明書のみを使用するようにマスターサーバー (Web サーバー) が構成されているが、メディアサーバーまたはクライアントが外部証明書を使用するように構成されていない。これらの外部証明書が、マスターサーバードメインに登録されていない。
- 外部 CA が署名した証明書のみを使用するようにマスターサーバー (Web サーバー) が構成されているが、メディアサーバーまたはクライアントがまだ 8.1.2.1 にアップグレードされていない。

### 解決方法

- `nbcertcmd -getseconfig -caUsage` コマンド、NetBackup 管理コンソール、または NetBackup Web UI で、マスターサーバー認証局 (CA) の構成を確認します。外部証明書のみを使用するように Web サーバーが構成されている場合は、次の操作を行います。
- 通信が失敗する 2 つのホストを特定します。
- 2 つのホストのいずれかが 8.1.2.1 で、外部証明書を使用するように構成されていないかどうかを確認します。  
これに該当する場合は、ホストの外部証明書をマスターサーバーのドメインに登録します。
- 2 つのホストのいずれかが 8.1.x かどうかを確認します。  
これに該当する場合は、ホストを 8.2 以降にアップグレードしてホストの外部証明書をマスターサーバーのドメインに登録するか、外部証明書と NetBackup 証明書の両方を使用するように Web サーバーを構成します。
- 次のコマンドを使用して、ホストのキャッシュメモリをクリアします。  
`bpcplntcmd -clear_host_cache`
- `install_path/logs/nbpxyhelper` にある `vnet proxy` ログを確認します。
- `install_path/logs/nbwebsevice` にある Web サービスのログを確認します。

# NAT クライアントまたは NAT サーバーのバックアップエラーの問題のトラブルシューティング

バックアップが、エラー「**bpbrm (pid = 31553) ホスト上の BPCD が状態 21 で終了したため、メールを送信できません: ソケットを開けませんでした (bpbrm (pid=31553) cannot send mail because BPCD on host exited with status 21: socket open failed)**」で失敗する

この問題の発生は、次のいずれかが理由と考えられます。

- メディアサーバーが NetBackup Messaging Broker (または nbmqbroker) サービスに接続できない。
- マスターサーバーで nbmqbroker サービスを実行できない。
- NAT クライアントがリバース接続を受け入れるように構成されていない。
- クライアントが NAT クライアントではない。
- 8.1.2 以前のクライアントである。
- nbmqbroker サービスのポート構成が更新された。
- マスターサーバーのサービスが再起動された。

## 原因 1

メディアサーバーが nbmqbroker サービスに接続できない。

## 原因 2

マスターサーバーで nbmqbroker サービスを実行できない。

原因 1 と原因 2 には、次の同じ解決策があります。

- メディアサーバーの *Install\_Path/logs/bpbrm* で、bpbrm ログを確認します。
- 次の場所にある nbmqbroker ログファイルを確認します。  
UNIX の場合: */usr/opensv/mqbroker/logs*  
Windows の場合: *Install\_Path/mqbroker/logs*
- マスターサーバーで nbmqbroker サービスが実行中であることを確認します。次のコマンドを使用します。
  - bpps コマンドを実行します。
  - マスターまたはメディアサーバーから `bptestbpcd -host hostname` コマンドを実行し、*Install\_Path/logs/admin* で管理ログを確認します。

### 原因 3: NAT クライアントまたは NAT サーバーがリバーズ接続を受け入れるように構成されていない

次を実行します。

- 次の場所にあるサブスクリバのログを確認します。  
UNIX の場合: `usr/opensv/logs/nbsubscriber`  
Windows の場合: `Install_Path/logs/nbsubscriber`
- `Install_Path/logs/vnetd` で `vnetd` ログを確認します。
- マスターまたはメディアサーバーで `bptestbpcd -host hostname` コマンドを実行し、`Install_Path/logs/admin` で管理ログを確認します。
- `nbmqutil -publish -master hostname -message message_text -remoteHost hostname` コマンドを実行します。
- `nbgetconfig` コマンドを使用して、`ACCEPT_REVERSE_CONNECTION` 構成オプションが `TRUE` に設定されていることを確認します。
- `bpps` コマンドを実行し、NAT クライアントでサブスクリバサービスが実行中であることを確認します。

### 原因 4: クライアントが NAT クライアントではない

次を実行します。

`nbgetconfig` コマンドを使用して、マスターサーバーまたはメディアサーバーで `ENABLE_DIRECT_CONNECTION` 構成オプションが `TRUE` に設定されていることを確認します。

### 原因 5: 8.1.2 以前のクライアントです。

次を実行します。

`nbgetconfig` コマンドを使用して、マスターサーバーまたはメディアサーバーで `ENABLE_DIRECT_CONNECTION` 構成オプションが `TRUE` に設定されていることを確認します。

### 原因 6: nbmqbroker サービスのポート構成が更新された

次を実行します。

- キャッシュが消去されるまで待機します。
- メディアサーバーで、`bpcIntcmd -clear_host_cache` コマンドを使用し、ホストキャッシュを消去します。

### 原因 7: マスターサーバーのサービスが再起動された

次を実行します。

## NAT クライアントまたは NAT サーバーのバックアップエラーの問題のトラブルシューティング

- 次の場所にあるサブスクリバサービスのログを確認します。  
UNIX の場合: `usr/openv/logs/nbsubscriber`  
Windows の場合: `Install_Path/logs/nbsubscriber`
- クライアントでサブスクリバサービスが起動するまで待機します。
- サブスクリバサービスを再起動します。

### バックアップが、エラー「**bpbrm (pid = 9880) ホスト上の BPCD が状態 48 で終了しました: クライアントのホスト名が見つかりませんでした (bpbrm (pid=9880) bpcd on host exited with status 48: client hostname could not be found)**」で失敗する

この問題の発生は、次のいずれかが理由と考えられます。

- NAT クライアントのホスト名がホスト ID にマップされていない。
- クライアントに関連付けられているホスト ID が null または無効である。

次を実行します。

- `Install_Path/logs/bpbrm` で bpbrm ログを確認します。
- マスターまたはメディアサーバーで `Install_Path/bin/admincmd/nbhostmgmt -li -json` コマンドを実行し、クライアントの既存のホスト ID からホスト名へのマッピングを確認します。
- クライアント名がホスト ID にマッピングされていない場合、  
`Install_Path/bin/admincmd/nbhostmgmt -add -hostid hostid -mappingname hostname` コマンドを使用し、クライアントの新しい名前を追加して既存のホスト ID にマッピングします。
- `Install_Path/bin/bpclntcmd -clear_host_cache` を使用して、クライアント上のホストキャッシュを消去します。

### バックアップが完了するまでの時間が長すぎる

この問題の発生は、次のいずれかが理由と考えられます。

- クライアントの構成ファイル (UNIX または Windows のレジストリの `bp.conf` ファイル) に、誤ったメディアサーバーのエントリが含まれている。
- この `ENABLE_DATA_CHANNEL_ENCRYPTION` オプションは、NAT ホストで `FALSE` に設定されていません。

### 原因 1: クライアントの構成ファイルに誤ったメディアサーバーのエントリが含まれている

次を実行します。

- マスターまたはメディアサーバーから `Install_Path/bin/admincmd/bptestbpcd -host hostname` を実行し、`Install_Path/logs/admin` で管理ログを確認します。

- クライアントの `/etc/hosts` ファイルにメディアサーバー名を追加します。
- `nbsetconfig` コマンドを使用して、クライアントの構成ファイルにメディアサーバー名を追加します。

## 原因 2: `ENABLE_DATA_CHANNEL_ENCRYPTION` オプションが有効になっている

次を実行します。

- `nbsetconfig` コマンドを使用して、`ENABLE_DATA_CHANNEL_ENCRYPTION` を `FALSE` に設定します。

## ジョブがハングアップしてポリシーの新しいジョブがトリガされないため、バックアップが失敗する

この問題の発生には、次の理由が考えられます。

- NAT ホストが受信メッセージを待機しているが、`nbmqbroker` サービスがクライアントの接続を閉じ、閉じられた接続をクライアントが検出できない。

次を実行します。

- クライアントのログに次のメッセージが含まれているかどうかを確認します。

```
Trying to get Message from MQ Broker:[master server name]
```

- サーバーの `SUBSCRIBER_HEARTBEAT_TIMEOUT` 構成オプションに設定されている現在のハートビート値を確認します。`nbgetconfig` コマンドを使用します。
- `SUBSCRIBER_HEARTBEAT_TIMEOUT` オプションの値を最小に設定し、閉じられた接続をクライアントが検出できるようにします。
- クライアントでサブスクライバサービスを再起動します。

## `CLIENT_CONNECT_TIMEOUT` の後にバックアップまたはリストアジョブが失敗する

この問題の発生には、次の理由が考えられます。

- サブスクライバがメディアサーバーとのリバース接続を確立できなかった。
- パブリッシャでメッセージが配信されたが、サブスクライバがメッセージを受信しなかった。

次を実行します。

- サブスクライバサービスのログをチェックし、サブスクライバサービスが `PBX` 一時 ID に接続できることを確認します。
- サブスクライバサービスのログをチェックし、パブリッシャメッセージがサブスクライバに配信されていることを確認します。

ログメッセージ:

```
Got Message from MQ Broker:[<message>] with return:<status code>
total timeout,reset:<timeout reset>
```

**サービスの再起動後に NAT メディアサーバーの状態が停止する**  
次の手順を実行します。

- 1 マスターサーバー上で次のコマンドを実行します。  
`Install_Path/bin/admincmd/bptestbpcd -host host_name`
- 2 `Install_Path/logs/admin` のログを確認します。
- 3 NetBackup 管理コンソールを使用して、メディアサーバーがオフラインになっているかどうかを確認します。[メディアおよびデバイスの管理 (Media and Device Management)]、[デバイス (Devices)]、[メディアサーバー (Media Servers)]の順に選択します。
- 4 マスターサーバーサービスを再起動した場合は、メディアサーバーを再起動し、メディアサーバーがオンラインになるまで待機します。
- 5 ログレベルが 1 より大きい値に設定されている場合は、メディアサーバーのサブスクライバログが接続メッセージを受信する準備ができていないかどうかを確認します。次はその例です。

接続が切断されている状態の場合のログメッセージ: `Retrying connection stopped for n seconds with attempt:m`

接続が確立されている状態の場合のログメッセージ: `Successfully connected to MQ Broker: master server host with Host UUID NAT host ID`

## NetBackup Messaging Broker (または nbmqbroker) サービスに関する問題のトラブルシューティング

**NetBackup Messaging Broker サービスが実行されていない**  
次を実行します。

- マスターサーバーでサービスが構成され、開始されていることを確認します。サービスを構成するには、`configureMQ` コマンドを実行します。  
『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

**NetBackup Messaging Broker サービスを開始できない**

原因:

- サービス用に構成されたポートがその他のプロセスによって使用されている。

**NetBackup Messaging Broker (または nbmqbroker) サービスに関する問題のトラブルシューティング**

- 構成ファイルが破損している。

次を実行します。

1. `configureMQ` コマンドログでエラーを確認します。
2. `nbmqbroker` サービスログでエラーを確認します。
3. `configureMQ` コマンドを実行します。

『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

**NetBackup Messaging Broker サービスが NAT クライアントに接続されていない**

原因:

- サービス用に構成されたポートを使用できない。
- 何らかの SSL 例外で接続に失敗した。
- マスターサーバーで `configureWebServerCerts` コマンドを実行した後、`nbmqbroker` サービスが再起動されていない。

次を実行します。

1. `nbmqbroker` サービス用に構成されたポートが利用可能で、**NetBackup** ホストからアクセス可能であることを確認します。
2. `nbcertcmd -ping` コマンドを使用し、マスターサーバーと NAT クライアント間の接続を確認します。
  - コマンドが正常に実行されない場合は、**NetBackup Web** サービスのトラブルシューティングのセクションを参照してください。
  - コマンドが正常に実行されたら、`configureMQ` コマンドを実行し、`nbmqbroker` サービスを構成します。
3. `nbmqbroker` サービスを再起動します。

**サブスクリバまたはパブリッシャが NetBackup Messaging Broker サービスに接続できない**

原因:

- NAT クライアントの JSON Web トークン (JWT) を更新できない。
- NAT クライアントのセキュリティ証明書が失効している。
- **NetBackup Web** 管理コンソール (または `nbwmc`) サービスが実行されていない。

次を実行します。

1. サブスクリバのトラブルシューティング手順を参照してください。
2. クライアントのセキュリティ証明書が失効した場合、証明書を再発行します。

3. nbwmc サービスを起動します。

## ディザスタリカバリ後に NetBackup Messaging Broker サービスを起動できない

原因:

- ディザスタリカバリパッケージが失われた。
- ディザスタリカバリ (DR) のインストール後に、configureMQ コマンドが実行されていない。

次を実行します。

- configureMQ または configureMQ -defaultPorts コマンドを実行します。  
『NetBackup コマンドリファレンスガイド』を参照してください。

## NetBackup がインストールされているボリュームで、8dot3 ショートファイル名の設定が無効になっている場合、Windows で NetBackup メッセージングブローカーサービスの起動が失敗する

インストールルートフォルダで 8dot3 ファイル名の設定が有効になっているかどうかを確認するには、フォルダから次のコマンドを実行します。

```
>dir /x
```

例: Program Files ディレクトリで 8dot3 ファイル名の設定が有効になっているため、短い名前「PROGRA ~ 1」が生成されます。

ただし、これは「not8 Dot3」ディレクトリとは異なります。

```
C:¥>dir /x
```

ドライブ C のボリュームにはラベルがありません。

ボリュームのシリアル番号は FE21-2F8E です。

C:¥ のディレクトリ

```
-5.6.3
```

```
12/06/2019 02:24 PM <DIR> not8 Dot3
12/02/2019 06:35 AM <DIR> PROGRA~1 Program Files
12/02/2019 10:44 AM <DIR> PROGRA~2 Program Files (x86)
```

この問題を解決するには、次を実行します。

- 1 `fsutil` コマンドを使って NetBackup インストールルートフォルダの `8dot3` 名ファイル設定を有効にします。  
  
`Fsutil 8dot3name` を参照してください。
- 2 問題が解決しない場合は、ベリタスのテクニカルサポートにお問い合わせください。

### 外部 CA が設定されている場合にディザスタリカバリパッケージをリストアした後に、NetBackup Messaging Broker サービスが正しく動作しない

次のシナリオを検討します。

NetBackup は、カタログバックアップ時に外部 CA が署名した証明書のみを使用するように構成されています。したがって、カタログバックアップ中に作成されたディザスタリカバリパッケージには、必要な外部証明書が含まれています。NetBackup のインストール後に、そのようなディザスタリカバリパッケージを使用してホスト ID がリカバリされた場合、インストール中に発行された NetBackup CA 署名証明書が原因で、nbmqbroker サービスが正しく動作しないことがあります。

この問題を解決するには

- 1 NetBackup 環境で、外部 CA が署名した証明書のみを使用しているかどうかを確認します。次のコマンドを実行します。

```
nbcertcmd -getSecConfig -caUsage
```

- 2 nbmqbroker サービスが使う証明書を確認します。次のコマンドを実行します。

Unix の場合: `cat /usr/opensv/var/global/mqbroker/mqbroker.config | grep ssl_options`

Windows の場合: `type`

```
"NetBackup_Install_path%var%global%mqbroker%mqbroker.config" | findstr "ssl_options"
```

お使いの環境で外部 CA が署名した証明書のみが使用されている場合、このコマンドは、`externalcacreds` エントリを含むパスを表示します。

コマンドで `nbcacreds` エントリを含むパスが表示される場合、NetBackup CA が署名した証明書が使用されます。

例:

```
{ssl_options, [{cacertfile,
"/usr/opensv/var/global/mqbroker/certstore/nbcacreds/ca.pem"}],
{ssl_options, [{cacertfile,
"/usr/opensv/var/global/mqbroker/certstore/nbcacreds/ca.pem"}],
```

nbmqbroker サービスが適切に機能するように、NetBackup 証明書を削除する必要があります。

- 3 次のコマンドを実行して、NetBackup 証明書を削除します。

```
configureWebServerCerts -removeNBCert
```

## NetBackup Messaging Broker (または nbmqbroker) サービスに関する問題のトラブルシューティング

4 NetBackup Web 管理コンソール (nbwmc) サービスと nbmqbroker サービスを再起動して変更を反映します。

5 nbmqbroker サービスが使う証明書を確認します。次のコマンドを実行します。

Unix の場合: `cat /usr/opensv/var/global/mqbroker/mqbroker.config | grep ssl_options`

Windows の場合: `type`

`"NetBackup_Install_path%var%global%mqbroker%mqbroker.config" | findstr "ssl_options"`

外部証明書専用モードの予想出力:

```
{ssl_options, [{cacertfile,
"/usr/opensv/var/global/mqbroker/certstore/externalcacreds/ca.pem"},
{ssl_options, [{cacertfile,
"/usr/opensv/var/global/mqbroker/certstore/externalcacreds/ca.pem"},
```

p.250 の「[UNIX でのディザスタリカバリパッケージのリストア](#)」を参照してください。

p.248 の「[Windows でのディザスタリカバリパッケージのリストア](#)」を参照してください。

## Linux の NetBackup Web UI に新しい nbmqbroker サービス固有の通知が表示されない

nbmqbroker サービスログには次のエラーが示されます。

```
escript: exception error: undefined function
rabbitmqctl_escript:main/1

in function escript:run/2 (escript.erl, line 758)

in call from escript:start/1 (escript.erl, line 277)

in call from init:start_em/1

in call from init:do_boot/3
```

根本原因:

マスターサーバーの特定の構成変更により、nbmqbroker サービスの構成に不整合が生じる場合があります。この問題を解決するには、nbmqbroker サービスを再構成する必要があります。

nbmqbroker サービスを再構成するには

- 1 次のコマンドを実行して nbmqbroker サービスを停止します。

```
/usr/opensv/mqbroker/bin/nbmqbroker stop
```

- 2 次のコマンドを実行して nbmqbroker 環境を構成します。

```
/usr/opensv/mqbroker/bin/install/configureMQEnv
```

- 3 次のコマンドを実行して nbmqbroker サービスを構成します。

```
/usr/opensv/mqbroker/bin/install/configureMQ
```

- 4 次のコマンドを実行して nbmqbroker サービスを起動します。

- /usr/opensv/mqbroker/bin/nbmqbroker start
- bp.start\_all command

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。

## NetBackup Messaging Broker サービスが Linux IPv6 のみのプライマリサーバーで起動しない

原因:

使用されるのが IPv6 アドレスのみであっても、プライマリサーバー名は IPv4 と IPv6 の両方のアドレスに解決される可能性があります。

次のコマンドを実行して、出力に IPv4 アドレスが含まれているかどうかを確認します:

```
nslookup primary_server_name
```

次に出力例を示します。

```
# nslookup primary-server.com

Server: 2600:100:f0a1:9000::a
Address: 2600:100:f0a1:9000::a#53

Non-authoritative answer:

Name: primary-server.com
Address: 10.200.100.60

Name: primary-server.com
Address: 2600:100:f0a1:9014::335
```

想定される出力:

## NetBackup Messaging Broker (または nbmqbroker) サービスに関する問題のトラブルシューティング

```
# nslookup primary-server.com

Server: 2600:100:f0a1:9000::a
Address: 2600:100:f0a1:9000::a#53

Non-authoritative answer:

Name: primary-server.com
Address: 2600:100:f0a1:9014::335
```

次を実行します。

- すべての構成を修正して、適切な IPv6 のみのセットアップを作成します。
- 問題が解決しない場合は、次の構成変更を行って nbmqbroker サービスを開始します。  
この構成では、nbmqbroker サービスは常に IPv6 アドレスを最初に使用して名前解決を試みます。

#### 構成を変更するには

- 1 次のコマンドを実行して必要なファイルを作成します。

```
cat > /usr/openv/var/global/mqbroker/erl_inetrc
```

- 2 コマンドプロンプトで、次の内容を入力します。末尾のドット(.)は省略可能ではないことに注意してください。

```
{inet6,true}.
```

- 3 次のコマンドを実行して、/usr/openv/mqbroker/bin/setmqenv ファイルの権限を確認します。

```
ls -l /usr/openv/mqbroker/bin/setmqenv
```

出力は次のとおりです。

```
-rwxr-x---. 1 nbwebsvc nbwebgrp 3869 date
/usr/openv/mqbroker/bin/setmqenv
```

- 4 /usr/openv/mqbroker/bin/setmqenv ファイルに次のエントリを追加します。

```
RABBITMQ_SERVER_ADDITIONAL_ERL_ARGS="-kernel inetrc
'/usr/openv/var/global/mqbroker/erl_inetrc' -proto_dist inet6_tcp"

RABBITMQ_CTL_ERL_ARGS="-proto_dist inet6_tcp"

export RABBITMQ_SERVER_ADDITIONAL_ERL_ARGS
export RABBITMQ_CTL_ERL_ARGS
```

- 5 更新後にファイル権限が変更されていないことを確認します。
- 6 nbmqbroker サービスを起動します。

## Windows システムの電子メール通知に関する問題

バックアップ管理者またはホスト管理者への電子メール通知が届かない場合は、次の項目を確認します。

- 電子メールアドレスが正しく設定されています。
- **BLAT** のバイナリが有効で、電子メールシステムと互換性があります。最新バージョンをダウンロードします。
- スクリプトで正しい **BLAT** 構文が使用されています。
- nbmail.cmd スクリプトで、**BLAT** コマンドがコメントアウトされていないことを確認します。
- blat.exe コマンドが %system32 ディレクトリにない場合、nbmail.cmd スクリプトで blat.exe へのパスが指定されていることを確認します。
- システムで遅延が発生した場合、-ti n タイムアウトパラメータを使用できます。
- 電子メールアカウントがメールサーバーで有効です。
- メールサーバーで **SMTP** の認証が必要な場合は、**NetBackup** クライアントプロセスに使用するアカウントが認可されていることを確認します。デフォルトは、ローカルシステムのアカウントです。

## KMS 構成に関する問題

### KMS の構成後、KMS 対応ストレージでバックアップが失敗する

NetBackup は、NetBackup Key Management Service (NetBackup KMS) と外部キー管理サービス (外部 KMS) をサポートします。

この項では、次のシナリオで発生したバックアップエラーの問題を解決する手順について説明します。

- NetBackup KMS が設定されている場合
- 外部 KMS が設定されている場合

KMS の構成について詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

**NetBackup KMS が構成されている設定でバックアップエラーの問題を解決するには**

- 1 テープ、AdvanceDisk、またはクラウドストレージを使用するように NetBackup ポリシーが構成されている場合は、ジョブの詳細を確認します。エラーが発生した場合は、『[NetBackup 状態コードリファレンスガイド](#)』を参照してください。

たとえば、テープストレージタイプの場合、[ジョブの詳細 (Job Details)] タブに次のエラーが表示されることがあります。

```
Mar 27, 2020 5:20:40 PM - Error bptm (pid=11143) KMS failed with error status: Error details :
Error Code : 1298, Error Message : Cannot communicate with one or more key management servers.,
Server - example.master.com:0, Error code - 25, .
Mar 27, 2020 5:20:40 PM - Info bptm (pid=11143) EXITING with status 83 <-----
Mar 27, 2020 5:20:43 PM - Info bpbkar (pid=11132) done. status: 83: media open error
```

- 2 NetBackup KMS が構成されているかどうかを確認するため、マスターサーバーで次のコマンドを実行します。

```
Install_Path/bin/nbkmscmd -listKMSConfig -name nbkms
```

NetBackup KMS 構成がリストされない場合は、nbkms サービスが実行されているかどうかを確認します。

- nbkms サービスが実行されている場合は、次のコマンドを実行して nbkms サービスの構成を追加します。

```
Install_Path/bin/nbkmscmd -discoverNBkms
```

- nbkms サービスが実行されていない場合は、次の場所にある nbkms ログを確認します。

UNIX の場合: /usr/opensv/logs/nbkms

Windows の場合: Install\_Path¥NetBackup¥logs¥nbkms

必要なキーグループを使用して、KMS サーバーでキーが作成されているかどうかを確認します。

- 3 次のコマンドを使用して、NetBackup KMS 構成を検証します。

```
Install_Path/bin/nbkmscmd -validateKMSConfig -name
KMS_configuration_name
```

- 4 次のコマンドを使用して、少なくとも 1 つのアクティブなキーが表示されていることを確認します。

```
Install_Path/bin/nbkmscmd -listKeys -name KMS_configuration_name
-keyGroupName key_group_name
```

- 5 キーがリストされない場合は、必要なキーグループでキーを作成し、メディアサーバーのキャッシュをクリアします。次のコマンドを実行します。

```
Install_Path/bin/bpctlntcmd -clear_host_cache
```

- 6 詳しくは、次のログを確認してください。

テープ、AdvanceDisk、クラウドストレージの場合:

```
Install_Path/netbackup/logs/bptm
```

MSDP ストレージの場合: `MSDP_config_path/log/spoold/spoold.log`

マスターサーバー上の Web サービスログの場合:

```
Install_path/logs/nbwebsevice/<51216-495-***-***-***.log>
```

NetBackup KMS の nbkmiutil ログの場合: `Install_Path/logs/nbkms`

外部 KMS が構成されている設定でバックアップエラーの問題を解決するには

- 1 テープ、AdvanceDisk、またはクラウドストレージを使用するように NetBackup ポリシーが構成されている場合は、ジョブの詳細を確認します。エラーが発生した場合は、『[NetBackup 状態コードリファレンスガイド](#)』を参照してください。
- 2 外部 KMS が構成されているかどうかを確認するため、マスターサーバーで次のコマンドを実行します。

```
Install_Path/bin/nbkmscmd -listKMSConfig -name  
KMS_configuration_name
```

構成がリストされない場合は、外部 KMS サーバーを構成します。

- 3 次のコマンドを使用して、外部 KMS 構成を検証します。

```
Install_Path/bin/nbkmscmd -validateKMSConfig -name  
KMS_configuration_name
```

- 4 次のコマンドを実行して、マスターサーバーに証明書ファイルがあるかどうかを確認します。

```
Install_Path/netbackup/bin/goodies/nbkmiutil -validate -kmsServer  
kms_server_name -port 5696 -certPath certificate_file_path  
-privateKeyPath private_key_file_path -trustStorePath  
ca_file_path
```

出力は JSON 形式です。

- 5 必要なキーグループを使用して、外部 KMS サーバーでキーが作成されているかどうかを確認します。

- 6 次のコマンドを使用して、少なくとも 1 つのアクティブなキーが表示されていることを確認します。

```
Install_Path/bin/nbkmscmd -listKeys -name KMS_configuration_name  
-keyGroupName key_group_name
```

キーがリストされない場合は、必要なキーグループでキーを作成し、メディアサーバーのキャッシュをクリアします。次のコマンドを実行します。

```
Install_Path/bin/bpcIntcmd -clear_host_cache
```

- 7 詳しくは、次のログを確認してください。

テープ、AdvanceDisk、クラウドストレージの場合:

```
Install_Path/netbackup/logs/bptm
```

MSDP ストレージの場合: *PDDE\_Install\_Path/log/spoold/spoold.log*

マスターサーバー上の Web サービスログの場合:

```
Install_Path/logs/nbwebsservice/<51216-495-***-***-***.log>
```

外部 KMS の nbkmiputil ログの場合:

```
Install_Path/netbackup/logs/nbkmiputil
```

## KMS 対応ストレージのバックアップデータのリストアに失敗する

KMS 対応ストレージの場合に、リストアエラーの問題を解決するには、次の手順を実行します。

リストアエラーの問題を解決するには

- 1 テープ、AdvanceDisk、クラウドストレージの場合は、ジョブの詳細を確認します。
- 2 次のコマンドを使用して、KMS 構成を検証します。

```
Install_Path/bin/nbkmscmd -validateKMSConfig -name  
KMS_configuration_name
```

- 3 次のコマンドを実行して、マスターサーバーに証明書ファイルがあるかどうかを確認します。*Install\_Path/netbackup/bin/goodies/nbkmiputil -validate -kmsServer KMS\_server\_name -port 5696 -certPath certificate\_file\_path -privateKeyPath private\_key\_file\_path -trustStorePath ca\_file\_path*

出力は JSON 形式で表示されます。

- 4 バックアップの暗号化に使用したキーが KMS サーバーでまだアクティブであることを確認します。

リストアに必要なキータグを取得するため、nbwebservice ログで次のエラーを確認します。

マスターサーバー上の **Web** サービスログで、次のログ文を確認します:

```
Install_Path/logs/nbwebservice/<51216-495-***-***-***.log>
```

ログのスニペットは次のとおりです。

```
[Debug] NB 51216 nbwebapi 495 PID:10984 TID:149 File ID:495 [No context] 5
[com.netbackup.config.PeerInfoPopulatorFilter]
Request URL : https://<Master-Server>:1556/netbackup/security/key-management-services/keys

Connection Info :ConnectionInfo

[Debug] NB 51216 nbwebapi 495 PID:10984 TID:149 File ID:495 [No context] 5
[com.netbackup.security.kms.resource.KMSConfigResource]
HTTP GET filter query string is : KeyId eq
'bd3492b015d4a9ab25426465b12adac6a834dfc6b4449c490922d6155719958'
and kadlen eq 32

[Debug] NB 51216 nbwebapi 495 PID:10984 TID:149 File ID:495 [No context] 5
[com.netbackup.security.kms.resource.KMSConfigResource]
com.netbackup.security.kms.resource.KMSConfigResource getKeys() -
NBKMSRecordNotFoundException
occured due to missing KMS
record.com.netbackup.nbkms.exception.NBKMSRecordNotFoundException:
security.error.kms.KeyRecordNotFound
```

- 5 詳しくは、次のログを確認してください。

テープ、AdvanceDisk、クラウドストレージの場合:

```
Install_Path/netbackup/logs/bptm
```

MSDP ストレージの場合: *PDDE\_Install\_Path/log/spoold/spoold.log*

マスターサーバー上の **Web** サービスログの場合:

```
Install_Path/logs/nbwebservice/<51216-495-***-***-***.log>
```

nbkmiutil ログの場合:

- NetBackup KMS の場合: *Install\_Path/logs/nbkms*
- 外部 KMS の場合: *Install\_Path/netbackup/logs/nbkmiutil*

## キーサイズが大きいことによる NetBackup CA の移行を開始するときの問題

キーサイズが大きいため、インストール中またはアップグレード中に NetBackup CA 移行の開始がタイムアウトになることがあります。

次に、インストールログに記録されるエラーの例を示します。

```
06-19-2020,20:40:39 : Initiating the NetBackup CA migration with
16384
bits key size.

06-19-2020,20:40:39 : NetBackup security service is still generating
key
pairs with key size of 16384 bits.

06-19-2020,20:40:39 : NetBackup will recheck the status of the
NetBackup
CA migration initiation phase after every 30 seconds

06-19-2020,20:40:40 : The NetBackup CA migration initiation process
is
taking more time than expected

06-19-2020,20:40:40 : Failed to set up the new NetBackup CA

06-19-2020,20:40:40 : network connection timed out(Error code: 41)

06-19-2020,20:40:40 : Command returned status 41

06-19-2020,20:40:40 : "C:\Program Files\Veritas\NetBackup\bin\admincmd
\nbseccmd.exe" -nbcamigrate -initiatemigration -quiet -keysize 16384
-reason
"Upgrade" -installtime, ERROR: nbseccmd.exe failed with error status:
41
```

このようなエラーが発生した場合、CA の移行は正常に開始されましたが、キーのサイズが大きいため要求がタイムアウトしている可能性があります。ただし、バックグラウンドで CA 移行の開始が完了し、証明書が新しい CA で更新される可能性があります。

**NetBackup CA の移行の開始が正常だったかどうかを確認するには**

1 次のコマンドを実行します。

```
nbseccmd -nbcaMigrate -summary
```

2 NetBackup CA の移行状態が INITIATED かどうかを確認します。

- 移行の状態が `NO_MIGRATION` の場合は、インストール中に **CA** の移行が失敗したことを意味します。  
次のコマンドを使用して、新しい移行を開始します。  

```
nbseccmd -nbcaMigrate -initiateMigration | -i -keysize  
<key-value> [-reason <comment>] [-json] [-quiet]
```
- 3 移行の状態が `INITIATED` であることを確認したら、次のコマンドを実行して、新しい **CA** がリストに表示されているかどうかを確認します。  

```
nbseccmd -nbcalist
```

  - リストに新しい **CA** が存在する場合は、移行が正常に開始されたことを意味します。
  - 新しい **CA** がリストに存在しない場合は、次のコマンドを実行します。  

```
nbseccmd -nbcaMigrate -syncMigrationDB
```
- 4 証明書がまだ更新されていない場合は、ベリタステクニカルサポートにお問い合わせください。

## 特権のないユーザー (サービスユーザー) アカウントに関する問題

このトピックでは、特権のないユーザー、ルート以外のユーザー、またはサービスユーザーに固有の問題に関するトラブルシューティングの情報を提供します。

**NetBackup 9.1** 以降、マスターサーバーのほとんどのサービスを特権のないユーザーが実行できます。特権のないユーザーとして実行することを強くお勧めします。この新しいユーザーはサービスユーザーと呼ばれます。

サービスユーザーについて詳しくは『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

### nbcertcmd コマンドオプションのログ

nbcertcmd コマンドオプションは、サービスユーザーのコンテキストで内部的に実行されます。nbcertcmd コマンドオプションのログは、`SERVICE_USER.xxxxxx_xxxxx.log` ファイル内で確認できます。

表 2-11 サービスユーザーの問題のトラブルシューティング

通し 番号	問題	考えられる理由	解決方法
1	UNIX プラットフォームでの NetBackup のインストールまたはアップグレード中に、3 回のプロンプトが表示された後でもサービスユーザーを指定できない。	考えられる理由は、次のとおりです。 <ul style="list-style-type: none"> <li>■ 理由 1 - サービスユーザーがローカル、LDAP、または NIS に存在しない。</li> <li>■ 理由 2 - nbwebsvc がサービスユーザーとして使用されている。</li> <li>■ 理由 3 - nbwebgrp がサービスユーザーのセカンダリグループではない。</li> </ul>	解決方法は次のとおりです。 <ul style="list-style-type: none"> <li>■ 解決方法 1 - 次のコマンドを実行します。 <b>id service_user</b> ID コマンドが正常に実行される必要があります。</li> <li>■ 解決方法 2 - nbgetconfig コマンドを実行し、NetBackup 構成ファイル (bp.conf) の WEBSVC_USER エントリを確認します。 サービスユーザーは、WEBSVC_USER 構成オプションに設定されている値と同じにはできません。</li> <li>■ 解決方法 3 - nbgetconfig コマンドを実行し、NetBackup 構成ファイル (bp.conf) の WEBSVC_USER エントリを確認します。 次のコマンドを実行します。 <b>id service_user</b> コマンド出力で、gid が WEBSVC_GROUP オプション値の gid と同じではないこと、グループに WEBSVC_GROUP 値が指定されていることを確認します。</li> </ul>

通し 番号	問題	考えられる理由	解決方法
2	<p>UNIX プラットフォームで、非アクティブなクラスタノードに <b>NetBackup</b> をインストール中、次のいずれかのエラーが発生する。</p> <ul style="list-style-type: none"> <li>■ Service user name on active node does not match with service user name entered on inactive node.</li> <li>■ SERVICE_USER_ID '10021' retrieved from active node does not match with the user ID '1002' of local user 'nonroot'.</li> </ul>	<p>サービスユーザー名とユーザー ID が一致しません。</p>	<p>すべてのクラスタノードでサービスユーザー名とユーザー ID が一致していることを確認し、アクティブノードと非アクティブノードへの <b>NetBackup</b> のインストール時に同じユーザー名とユーザー ID を指定します。</p>
3	<p>UNIX プラットフォームで、非アクティブなクラスタノードの <b>NetBackup</b> のアップグレード中、次のエラーが発生する。</p> <pre>Failed to retrieve the 'SERVICE_USER' or 'SERVICE_USER_ID' entries from the configuration file on the server 'cluster_virtual_name'. You must provide the same 'SERVICE_USER' (daemon user name) that is configured on the active node.</pre>	<p>bpgetconfig コマンドで、アクティブノードからサービスユーザーと ID を取得できませんでした。</p>	<p>アクティブノードのサービスユーザーを指定し、すべてのクラスタノードでサービスユーザーのユーザー ID が同じであることを確認します。</p>
4	<p>UNIX プラットフォームで、<b>NetBackup</b> のインストールまたはアップグレード中、次のエラーが発生する。</p> <pre>/usr/openv 内のファイルの所有者として ユーザー serviceuser を設定できません。</pre>	<p>これは、インストールディレクトリの所有権を変更するときの問題が原因である可能性があります。</p>	<p>次の見出しの下にあるインストールトレースで指定されたエラーを修正します。</p> <pre>Fix below errors and then retry</pre>

通し 番号	問題	考えられる理由	解決方法
5	Windows 証明書ストアで外部 CA が構成され、サービスがローカルサービスアカウントのコンテキストで実行されている場合、NetBackup ホストの通信が機能しない。	<p>NetBackup サービスに、秘密鍵へのアクセス権がありません。通常、この場合のエラーは nbpxyhelper ログで確認できます。</p> <p>Windows API CryptAcquireCertificatePrivateKey がエラー「0x80090016: キーセットが存在しません」で失敗します。</p>	<p>次のように、秘密鍵の権限を確認します。</p> <p>証明書を右クリックします。[すべてのタスク]、[秘密キーの管理]の順にクリックします。</p> <p>すべての NetBackup サービスに、秘密鍵を読み取る権限が必要です。</p> <p>次のコマンドを実行して権限を設定します。</p> <pre>nbcertcmd -setWinCertPrivKeyPermissions</pre> <p>以下のコマンドを実行して構成を検証します。</p> <pre>nbcertcmd -ecaHealthCheck</pre>
6	<p>setconfig コマンドが次のエラーで失敗する。</p> <pre>Failed to open /usr/opensv/netbackup/bp.conf.d53: Permission denied (13)</pre>	<p>/usr/opensv/netbackup の所有権がルートユーザーに変更されています。</p> <p>その他の原因として、rpm を使用して言語パックがインストールされている可能性があります。</p>	<p>次のコマンドを実行して、所有権の問題を解決します。</p> <pre>/usr/opensv/netbackup/bin/goodies/ update_install_folder_perms</pre>
7	<ul style="list-style-type: none"> <li>■ カタログバックアップポリシーの作成または更新操作が失敗する。</li> <li>■ カタログバックアップが失敗する。</li> <li>■ カタログリカバリが失敗する。</li> </ul>	<p>サービスユーザーアカウントに、ポリシーで指定されたディザスタリカバリ (DR) パスへのアクセス権がない可能性があります。</p>	<p>状態コード 9201 と 9202 を確認します。</p> <p>『NetBackup 状態コードガイド』を参照してください。</p> <p>サービスユーザーアカウントにアクセス権を付与する方法については『NetBackup セキュリティおよび暗号化ガイド』を参照してください。</p>
8	ディザスタリカバリに失敗する。	NBHostIdentity -import コマンドが失敗します。	<p>次の項目について確認します。</p> <ul style="list-style-type: none"> <li>■ ディザスタリカバリ (DR) の前にシステムにサービスユーザーが存在している。</li> <li>■ サービスユーザーに DR パッケージへのアクセス権がある。</li> </ul>

通し 番号	問題	考えられる理由	解決方法
9	次のコマンドのいずれかがエラー「サービスユーザーアカウント [service_user_name] に指定されたパスとその内容へのアクセス権があることを確認してください。」で失敗する。 <ul style="list-style-type: none"> <li>■ nbdb_admin</li> <li>■ nbdb_move</li> <li>■ nbdb_backup</li> <li>■ nbdb_restore</li> <li>■ nbdb_unload</li> <li>■ create_nbdb</li> <li>■ cat_export</li> <li>■ cat_import</li> </ul> パス: UNIX の場合: <i>Install_Path/db/bin</i> Windows の場合: <i>Install_Path¥netbackup¥bin</i>	サービスユーザーアカウントに、指定したパスとその内容に対するアクセス権が付与されていない場合があります。	サービスユーザーアカウントにアクセス権を付与する方法については『 <a href="#">NetBackup セキュリティおよび暗号化ガイド</a> 』を参照してください。
10	VMware サーバーの追加操作が失敗する。	500 システムエラー	サービスユーザーアカウントが temp ディレクトリ (/tmp) にアクセスできることを確認します。
11	bpjava-test-login ワークフローの問題	ファイル所有権が「ルート」と表示されます。	ファイルの所有権をサービスユーザーアカウントに変更します。
12	nbcertcmd 操作が失敗する。	権限の不足	certmapinfo.json ファイルが作成され、サービスユーザーによって所有されているかどうかを確認します。
13	nbcertcmd または bpnbaz がエラーコード 123 で失敗する。	秘密鍵ファイル (PrivKeyFile-2048.pem)、公開鍵ファイル (PubKeyFile-2048.pem)、または ACL (アクセス制御リスト) の更新に失敗しました。	NetBackup の SID が構成され、公開鍵と秘密鍵の両方が AT_DATA_DIR に存在することを確認します。

通し番号	問題	考えられる理由	解決方法
14	NBAC の構成時に、 nbserveusercmd -changeUser 操作が認証エラーで失敗した。	新しいサービスユーザーが NBAC セキュリティ管理者グループに属し ていません。	新しいサービスユーザーを NBAC セ キュリティ管理者グループに追加しま す。次のコマンドを実行します。  vssaz addazgrpmember --azgrpname ¥"Security Administrators¥" --prplinfo prplinfo
15	NetBackup 9.1 のインストールおよびア ップグレード後、NBAC (NetBackup アク セス制御) または EA (拡張監査) が有効 な場合、ルートユーザーの NetBackup 管理コンソールへのログインが失敗する。	ユーザー証明書ディレクトリが変更 されました。	環境内で NBAC または EA が有効 になっている場合は、NetBackup の アップグレード後に bpnbat -login コマンドを実行する必要が あります。
16	ECA (外部 CA) の健全性チェックが失敗 するため、nbcertcmd -enrollCertificate コマンドが失 敗する。  次のパスにあるファイルへのアクセス中に エラーが発生しました。  certificates/private key/passphrase file/crl	コマンド nbcertcmd -enrollCertificate はサー ビスユーザーのコンテキストで実行 されますが、サービスユーザーに関 連ファイルへのアクセス権がありま せん。	サービスユーザーに必要なアクセス 権を付与します。  enrollCertificate コマンドを 再度実行する前に、次のコマンドを 実行してアクセス権を確認すること をお勧めします。  nbcertcmd -ecaHealthCheck -serviceUser user_name

## auth.conf ファイルのグループ名の形式に関する問題

auth.conf ファイルで定義されているユーザーグループのメンバーが、認可済みの  
**NetBackup** 管理コンソールの操作 (ノード) またはバックアップ、アーカイブ、リストア機  
 能に対して期待どおりにアクセスできない場合、グループ名の形式を確認します。

### グループ名の形式を検証して修正するには

- 1 次のコマンドを実行して、auth.conf ファイルで定義されたグループ名の形式を検証します。

UNIX の場合:

```
install_path/netbackup/sec/at/bin/vssat validateprpl -p user name  
-d unixpwd -b broker host:1556:nbatd
```

Windows の場合:

```
install_path¥NetBackup¥sec¥at¥bin¥vssat validateprpl -p user name  
-d nt:domain name -b broker-host:1556:nbatd
```

このコマンドの出力で、**NetBackup** 管理コンソールの特定のノードまたは操作にアクセスできないユーザーに関連付けられたグループの名前が表示されます。

- 2 期待どおりにノードにアクセスするには、コマンド出力に表示されたグループ名をコピーして、auth.conf ファイルに貼り付けます。

次の例を考えてみましょう。

```
vssat validateprpl -p user@addomain.com -d unixpwd -b  
localhost:1556:nbatd
```

使用するデータディレクトリ: /usr/opensv/var/vxss/at

出力:

```
ValidatePrincipal :
```

```
ID : <UID>
```

```
Name : user@addomain.com
```

```
Display Name : user@addomain.com
```

```
Domain :
```

```
Description : User
```

```
Group(s) Details :
```

```
Count : 2
```

```
Name(s) and ID(s) : group1@addomain.com
```

```
GID of group1 :
```

```
group2@addomain.com
```

```
GID of group2
```

auth.conf ファイルに、次の形式でグループ名を追加します。

```
<GRP> group1@addomain.com ADMIN=SUM+AM JBP=ALL
```

## VxUpdate パッケージ追加処理のトラブルシューティング

NetBackup Web UI または API を介して NetBackup VxUpdate パッケージを追加すると、パッケージは非同期的に処理されます。パッケージ追加処理の状態は、GET API または nbrepo コマンドを使用して調べることができます。これらのオプションはどちらも利用可能なパッケージの一覧を表示します。追加される 1 つ以上のパッケージが数分経っても利用できない場合は、下記の手順を使用して、エラーの原因を特定します。

**VxUpdate パッケージ追加操作をトラブルシューティングするには:**

- 1 API を使用して、目的のパッケージが利用できないことを確認します。

```
GET URL https://server/netbackup/deployment/packages
```

または、nbrepo コマンドを使用して、利用可能なパッケージの一覧を表示します。

- Windows の場合: `install_path¥NetBackup¥bin¥admincmd¥nbrepo.exe -l`
- Linux の場合: `/usr/opensv/netbackup/bin/admincmd/nbrepo -l`

- 2 トラブルシューティングログが存在することを確認します。

- Windows の場合:

```
install_path¥NetBackup¥logs¥bprd
```

```
install_path¥NetBackup¥logs¥nbwebsservice
```

- Linux の場合:

```
/usr/opensv/netbackup/logs/bprd
```

```
/usr/opensv/logs/vxul/nbwebsservice
```

- 3 パッケージの追加を試行するおおよその時間の前後にログファイルを確認します。

nbwebsservice と bprd ログファイルの両方で、要求された VxUpdate SJA ファイル名を検索します。

- 4 ログファイルで、追加の試行で受け取った 1 つ以上の状態コードを確認します。

- 5 『NetBackup 状態コードガイド』で状態コードの推奨処置を確認します。

**例**

以下のログセクションは nbwebsservice ログのもので、VxUpdate パッケージの追加時に発生する可能性があるエラーの例を示しています(わかりやすいように強調されています)。

```
0,51216,495,495,10738,1633618954821,12920,229,16:5F6DBAD64588994B,393:PackagesServiceImpl.  
validateCreatePackagesBulkInputs - The Package file for file path [¥¥nbserver_store¥  
vxupdate¥NetBackup_9.1.2_VU_2of4¥vxupdate_nb_9.1.2_windows_x64.sja] was not found, or  
is  
not accessible to NetBackup processes on the primary server. If the file exists, it must  
  
be in a location that is accessible to NetBackup, such as a local directory on the  
primary  
server.,61:com.netbackup.deployment.packages.service.PackagesServiceImpl,50,51216,495,495,  
10739,1633618954822,12920,229,16:5F6DBAD64588994B,11659:Raised exception The Package  
file  
for file path [¥¥nbserver_store¥vxupdate¥NetBackup_9.1.2_VU_2of4¥
```

```
vxupdate_nb_9.1.2_windows_x64.sja] was not found, or is not accessible to NetBackup processes on the primary server. If the file exists, it must be in a location that is accessible to NetBackup, such as a local directory on the primary server. - errorCode: 7284
```

この追加の試行は **NetBackup** 状態コード **7284** で失敗しました。この例のファイルは存在しますが、プライマリサーバーからアクセスできないネットワーク共有にあります。**UNC** パスまたはネットワーク共有のファイルを読み取るための適切な権限を持つアカウントで、**bprd** などの **NetBackup** サービスが有効でない可能性があります。

ユーザーのデスクトップなどの **Windows** プロファイルディレクトリに **.sja** ファイルを配置すると、**NetBackup** は同様のエラーを生成します。このエラーは、**NetBackup** サービスおよびプロセスがその場所に対する十分な権限を持っていないために発生します。

『[NetBackup 状態コードガイド](#)』で推奨処置を確認してください。

## FIPS モードの問題

### FIPS に準拠していないキーを使用した ECA の構成が失敗する

ECA の構成で指定された秘密鍵が FIPS に準拠していない PKCS1 形式であることが原因で、ECA の構成が失敗します。

理由:

秘密鍵の暗号化に使用される PKCS1 形式では、FIPS 準拠アルゴリズムではない MD5 アルゴリズムが使用されます。したがって、FIPS モードでは ECA の構成が失敗します。

サンプルログメッセージ:

```
PEM_read_PrivateKey failed to read private key from file[C:\%eca%private%key-pkcs1_ENCRYPTED.pem]. Provided private key is not FIPS supported.
```

解決策:

PKCS8 形式の秘密鍵を使用します。

### FIPS モードが有効な場合、UNIX での NetBackup 管理コンソールの起動に通常より長い時間がかかる

この問題は、**NetBackup** 管理コンソールが実行されているホストでエントロピーが不十分な場合に発生することがあります。

エントロピーとは、オペレーティングシステムによって収集されるランダム性です。

理由:

Java プロセスは、暗号化による安全なランダム出力を NetBackup 環境内で提供するため、`/dev/random` をデフォルトの文字型デバイスとして使用します。これをブロック呼び出しと呼びます。

NetBackup 管理コンソールを実行しているホストのエントロピーの状態を確認するには、次のコマンドを実行します。コマンドが 200 未満の値を返した場合、そのホストのエントロピーに問題があります。

```
cat /proc/sys/kernel/random/entropy_avail
```

解決策:

`nbj.conf` 構成ファイルで `USE_URANDOM` オプションを 1 に設定します。Java プロセスは、`/dev/urandom` デバイスの使用を開始します。

## NetBackup Web 管理コンソールサービス (nbwmc) の起動に異常に長い時間がかかる

この問題は、nbwmc サービスが実行されているホストでエントロピーが不十分な場合に発生することがあります。

エントロピーとは、オペレーティングシステムによって収集されるランダム性です。

理由:

Java プロセスは、暗号化による安全なランダム出力を NetBackup 環境内で提供するため、`/dev/random` をデフォルトの文字型デバイスとして使用します。これをブロック呼び出しと呼びます。

マスターサーバーのエントロピーの状態を確認するには、次のコマンドを実行します。コマンドが 200 未満の値を返した場合、そのサーバーのエントロピーに問題があります。

```
cat /proc/sys/kernel/random/entropy_avail
```

解決策:

構成ファイルで `USE_URANDOM` オプションを 1 に設定します。nbwmc サービスが `/dev/urandom` デバイスの使用を開始します。

## NetBackup Web 管理コンソールサービス (nbwmc) の起動に失敗する

理由:

NetBackup CA または ECA 階層のキーサイズが 2048 を下回っているか、3072 を超えている場合に、FIPS モードを有効にしようとしています。

サンプルログメッセージ:

```
Attempt to use RSA key with non-approved size: 1024: RSA
```

解決策:

NetBackup CA 階層を再構成し、FIPS モードでサポートされているキーサイズ (2048 ビットまたは 3072 ビット) を使用します。

## マルウェアスキャンの問題

表 2-12

エラー	説明	回避方法
スキャンホストへの接続に失敗しました。	メディアサーバーからホストをスキャンするための SSH 接続に失敗しました。	次のスキャンホストのクレデンシアルを確認します。 <ul style="list-style-type: none"> <li>■ RSA (SHA256) キー</li> <li>■ ユーザー名</li> <li>■ パスワード</li> </ul> スキャンホストの構成については、『NetBackup™ Web UI 管理者ガイド』を参照してください。
スキャンホスト OS の決定に失敗しました。	サポート対象外のスキャンホストがエラーの原因である可能性があります。	スキャンホストのサポート対象プラットフォームの一覧については、『ソフトウェア互換性リスト』を参照してください。
NetBackup マルウェアユーティリティをスキャンホストにコピーできませんでした。	<ul style="list-style-type: none"> <li>■ スキャンホストで利用可能な領域が不足しています。</li> <li>■ SSH ユーザーに、スキャンホスト上の必要なディレクトリへのアクセス権がありません。</li> </ul>	<ul style="list-style-type: none"> <li>■ Windows スキャンホストの場合、C:¥の空き領域を確認します。</li> <li>■ Linux スキャンホストの場合、/tmp の空き領域を確認します。</li> </ul>
スキャンホストクレデンシアルの取得に失敗しました。	メディアサーバーがプライマリからスキャンホストにアクセスするためのクレデンシアルをフェッチできません。	スキャンホストのクレデンシアルが指定されていることを確認します。
スキャン中にタイムアウトが発生しました。	デフォルトでは、スキャン操作は 2 日後にタイムアウトします。スキャン時間は、作業負荷の種類、ネットワーク帯域幅、バックアップサイズなどの要因によって変わる場合があります。	スキャンのタイムアウトは構成可能で、構成キーを設定して変更できます。 MALWARE_SCAN_OPERATION_TIMEOUT <ul style="list-style-type: none"> <li>■ 最小値: 1 時間</li> <li>■ 最大値: 30 日</li> </ul>

エラー	説明	回避方法
NetBackup マルウェアユーティリティから応答を取得できませんでした。	nbmalwareutil バイナリと ScanManager が一致していません。	NetBackup サポートにお問い合わせください。
スキャナの起動に失敗しました。	マルウェアスキャナ固有のエラーメッセージ。	メディアサーバーの nbmalwarescanner ログを参照してください。
バックアップイメージのマウントに失敗しました。	スキャンホストから IA 共有にアクセスできません。	ストレージサーバーの IA 構成を確認します。アクティビティモニターで、IA ジョブが成功したことを確認します。
バックアップイメージのマウント解除に失敗しました。	IA 共有がビジー状態であるか、IA 共有にアクセスできません。	メディアサーバーの nbmalwarescanner ログを参照してください。
スキャンの実行に失敗しました。	バックアップイメージのスキャン中の一般的なエラーです。	メディアサーバーの nbmalwarescanner ログを参照してください。
<ul style="list-style-type: none"> <li>■ ファイルを開けませんでした。</li> <li>■ ディレクトリを作成できません。</li> <li>■ 結果ファイルの生成に失敗しました。</li> <li>■ 出力ファイルを開けませんでした。</li> <li>■ 結果ファイル用のディレクトリを作成できません。</li> <li>■ 結果ファイルを開けませんでした。</li> <li>■ マウント先のディレクトリを作成できません。</li> <li>■ ログファイル用のディレクトリを作成できません。</li> </ul>	<ul style="list-style-type: none"> <li>■ スキャンホストで利用可能な領域が不足しています。</li> <li>■ SSH ユーザーに、スキャンホスト上の必要なディレクトリへのアクセス権がありません。</li> </ul>	<ul style="list-style-type: none"> <li>■ Windows スキャンホストの場合、C:¥の空き領域を確認します。</li> <li>■ Linux スキャンホストの場合、/tmp の空き領域を確認します。</li> </ul>

エラー	説明	回避方法
すべてのマウントドライブが使用済みです。	Windows スキャンホストでは、5つのバックアップイメージのみを同時にマウントできます。	<ul style="list-style-type: none"> <li>■ スキャンホストが複数の NetBackup ドメインの一部でないことを確認します。</li> <li>■ net use コマンドを実行して、スキャンホストに無効なマウントがあるかどうかを確認します。</li> <li>■ Windows スキャンホストでの IA 共有のマウントには、次のドライブ文字が使用されます。これらが使用中でないことを確認します。 L:¥ M:¥ N:¥ O:¥ P:¥</li> </ul>
Windows Defender がインストールされていないか、環境変数が設定されていません。	Windows Defender がスキャンホストにインストールされていないか、正しく構成されていません。	Microsoft Windows Defender がスキャンホストにインストールされていることを確認します。  スキャンホストの構成については、『NetBackup™ Web UI 管理者ガイド』を参照してください。
Symantec Protection Engine がインストールされていないか、環境変数が設定されていません。	Symantec Protection Engine がスキャンホストにインストールされていないか、正しく構成されていません。	スキャンホストに Symantec Protection Engine がインストールされていることを確認します。  スキャンホストの構成については、『NetBackup™ Web UI 管理者ガイド』を参照してください。
バックアップイメージのマルウェアスキャンの実行に失敗しました。	スキャンの失敗の一般的なエラーです。	NetBackup サポートにお問い合わせください。
NetBIOS 名に指定できるのは最大 15 文字です。	SMB 共有の場合、ストレージサーバーのホスト名に指定できるのは最大 15 文字です。  Windows Server 2016 を使用して AD ドメインを設定した場合、ホスト名の長さが 15 文字を超えるストレージサーバーは参加できません。	文字数制限を確認してください。

# 移動中のデータの暗号化が有効になっている NetBackup ジョブの問題

対象の NetBackup ジョブは、バックアップ、リストア、複製、レプリケーション、インポート、検証などの場合があります。ジョブに対しては、グローバル DTE 設定またはクライアント DTE モードによって、移動中のデータの暗号化 (DTE) が有効になっています。

DTE について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

## 問題: 操作が「EXIT STATUS 23: ソケットの読み込みに失敗しました」で失敗する

対象の操作は、バックアップ、リストア、インポート、検証、複製、合成バックアップなどの場合があります。このエラーは、対象の操作の DTE モードを決定する際に発生します。これは、グローバル DTE モードが bpcd プロセスで更新されないため、このモードをフェッチするときにエラーが発生したことが原因です。

bpcd では次のエラーが表示されます。

```
The global data-in-transit encryption setting cannot be fetched (8304).
```

表 2-13 確認するログ

操作	ログ
バックアップまたはアーカイブ	プライマリサーバー - nbjm, bpcd, nbwebservice
リストア	プライマリサーバー - admin (カタログリカバリ)、bprd, bpcd, nbwebservice
複製、検証、合成バックアップ、レプリケーション	プライマリサーバー - admin, bpcd, nbwebservice
インポート	プライマリサーバー - admin, bpcd, nbwebservice メディアサーバー - bpdm または bptm

UNIX のログ:

レガシーログ: /usr/opensv/netbackup/logs

VxUL ログ: /usr/opensv/logs

Windows のログ: `install_path\NetBackup\logs`

## 原因

bpcd のグローバル DTE キャッシュが更新されないため、NetBackup Web サービスの再起動に時間がかかりました。その結果、DTE モードを決定する際に、対象の操作が失敗しました。

## 解決方法

サービスを再起動してから 2 分後に操作を再実行し、次の反復処理でグローバル DTE モードが Web サービスによって正常に更新されるようにします。

### 問題: DTE (移動中のデータの暗号化) モードを判断できない。状態 3000004

このエラーは、対象の操作の DTE モードを決定する際に発生します。これは、メディアサーバー DTE モードを取得できないためです。

表 2-14 確認するログ

操作	ログ
バックアップまたはアーカイブ	プライマリサーバー - nbjm, nbemm
リストア	プライマリサーバー - bprd, nbemm
複製、検証、合成バックアップ、レプリケーション	プライマリサーバー - admin, nbemm
インポート	プライマリサーバー - admin, nbemm メディアサーバー - bpdm または bptm

UNIX のログ:

レガシーログ: /usr/opensv/netbackup/logs

VxUL ログ: /usr/opensv/logs

Windows のログ: `install_path¥NetBackup¥logs`

## 原因

EMM からメディアサーバー DTE 設定を取得できなかったため、操作が失敗します。

## 解決方法

操作を再実行して、メディアサーバー DTE モードを正常に取得します。

**問題: エラー「TLS 通信に必要な事前共有キーを取得できませんでした (8316)」で操作が失敗する**

**表 2-15**                      確認するログ

操作	ログ
バックアップまたはアーカイブ	クライアント - bpbkar または dbclient、vnetd、 bpcIntcmd メディアサーバー - bptm、bpcIntcmd、vnetd
リストア	クライアント - tar または dbclient、vnetd、bpcIntcmd メディアサーバー - bpbrm、bptm、bpcIntcmd、vnetd
複製	両方のメディアサーバー - bptm または bpdm、vnetd、 bpcIntcmd

UNIX のログ: /usr/openv/netbackup/logs

Windows のログ: install\_path¥NetBackup¥logs

**原因**

ホスト間の TLS ハンドシェイクに必要な事前共有キーを取得するときにエラーが発生しました。これは、bpcIntcmd での次のような問題のいずれかが原因です。

- bpcIntcmd への事前共有キーの格納に失敗した
- bpcIntcmd が事前共有キーの提供に失敗した

この問題により、複数の NetBackup 操作 (バックアップ、リストア、複製など) が失敗します。

**解決方法**

既存の bpcIntcmd -store プロセスを停止し、操作を再試行します。

**問題: エラー「ソケットに接続できないか (25)、要求された操作は部分的に成功しました (1)」で複製が失敗する**

**表 2-16**                      確認するログ

操作	ログ
複製	ターゲットメディアサーバー - bptm または bpdm、vnetd

UNIX のログ: /usr/openv/netbackup/logs

Windows のログ: install\_path¥NetBackup¥logs

ジョブの詳細のエラー:

```
Jan 19, 2022 8:49:36 PM - Error bpdm (pid=18607) cannot connect to
the
writing side process for duplication, Success Jan 19, 2022 9:37:02
PM - Error bptm
(pid=1028) listen protocol error - couldn't accept from data socket,

The operation completed successfully. Jan 19, 2022 9:37:03 PM - Info
bptm
(pid=1028) EXITING with status 25 <-----
```

## 原因

移動中のデータの暗号化 (DTE) が有効な場合、vnetd プロセスは DTE TLS ハンドシェイクに必要な前提条件を設定します。ビジー状態のマシンでは、vnetd がこの処理により多くの時間を費やすと、bptm は vnetd が接続を転送する前にタイムアウトになります。その結果、複製は失敗します。

## 解決方法

ターゲットホストで、vnetd からの接続を受け入れるタイムアウトを増やします。nbgetconfig コマンドと nbsetconfig コマンドを使用して、VNET\_OPTIONS 構成オプションのタイムアウトを増やします。

たとえば、タイムアウトを 120 秒から 300 秒に変更するには、次のコマンドを実行します。

```
nbgetconfig VNET_OPTIONS VNET_OPTIONS = 120 3600 200 40 3 1 30 10
1793 32 0 0

nbsetconfig nbsetconfig> VNET_OPTIONS = 300 3600 200 40 3 1 30 10
1793 32 0 0
```

最初の値のみが「300」に変更されます。

# NetBackup 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。

- [NetBackup のトラブルシューティングユーティリティについて](#)
- [NetBackup デバッグログの分析ユーティリティについて](#)
- [ログアシスタントについて](#)
- [ネットワークトラブルシューティングユーティリティについて](#)
- [NetBackup サポートユーティリティ \(nbsu\) について](#)
- [NetBackup の一貫性チェックユーティリティ \(NBCC\) について](#)
- [NetBackup の一貫性チェックの修復 \(NBCCR\) ユーティリティについて](#)
- [nbcplogs ユーティリティについて](#)
- [ロボットテストユーティリティについて](#)
- [NetBackup Smart Diagnosis \(nbsmartdiag\) ユーティリティについて](#)

## NetBackup のトラブルシューティングユーティリティについて

NetBackup の問題を診断するために、いくつかのユーティリティを使用できます。  
NetBackup デバッグログの分析ユーティリティと NetBackup サポートユーティリティ (nbsu) は、トラブルシューティングを行う場合に特に有効です。

表 3-1 トラブルシューティングユーティリティ

ユーティリティ	説明
NetBackup デバッグログの分析ユーティリティ	<p>NetBackup の既存のデバッグ機能が拡張され、ジョブのデバッグログが 1 つに統合された形式で提供されます。</p> <p>p.184 の「<a href="#">NetBackup デバッグログの分析ユーティリティについて</a>」を参照してください。</p>
ログアシスタント	<p>サポートで使用するための証拠の収集を簡略化します。</p> <p>詳しくは、次を参照してください。</p> <ul style="list-style-type: none"> <li>■ 『NetBackup 管理者ガイド Vol. 1』とNetBackup 管理コンソールのオンラインヘルプ</li> <li>■ NetBackup ログアシスタント FAQ:  <a href="http://www.veritas.com/docs/000088104">http://www.veritas.com/docs/000088104</a></li> </ul>
ネットワークトラブルシューティングユーティリティ	<p>構成に誤りがないことを確認するために NetBackup の内部と外部のネットワーク構成のさまざまな側面を検証します。</p> <p>p.188 の「<a href="#">ネットワークトラブルシューティングユーティリティについて</a>」を参照してください。</p>
NetBackup サポートユーティリティ (nbsu)	<p>ホストに問い合わせ、NetBackup とオペレーティングシステムに関する適切な診断情報を収集します。</p> <p>p.189 の「<a href="#">NetBackup サポートユーティリティ (nbsu) について</a>」を参照してください。</p>
NetBackup の一貫性チェックユーティリティ (NBCC)	<p>テープメディアに関連する NetBackup の構成とカタログおよびデータベース情報の一部の整合性を分析します。</p> <p>p.193 の「<a href="#">NetBackup の一貫性チェックユーティリティ (NBCC) について</a>」を参照してください。</p>
NetBackup の一貫性チェックの修復 (NBCCR) ユーティリティ	<p>データベースカタログの修復操作を処理し、承認済みの推奨される修復操作を自動的に適用します。</p> <p>p.203 の「<a href="#">NetBackup の一貫性チェックの修復 (NBCCR) ユーティリティについて</a>」を参照してください。</p>
nbcplogs ユーティリティ	<p>ベリタスのテクニカルサポートに提供するログを集める処理を簡略化します。Veritas</p> <p>p.205 の「<a href="#">nbcplogs ユーティリティについて</a>」を参照してください。</p>
ロボットテストユーティリティ	<p>ロボット周辺機器を使用して直接通信します。</p> <p>p.206 の「<a href="#">ロボットテストユーティリティについて</a>」を参照してください。</p>

## NetBackup デバッグログの分析ユーティリティについて

デバッグログの分析ユーティリティを使用すると、NetBackup の既存のデバッグ機能が拡張され、ジョブのデバッグログが 1 つに統合された形式で提供されます。

NetBackup ジョブは、複数のサーバーに分散された複数のプロセスにまたがって実行されます。

NetBackup ジョブをトレースするには、複数のホスト上の複数のログファイルのメッセージを参照し、それらを関連付ける必要があります。ログの分析ユーティリティを使用すると、ジョブのデバッグログが 1 つに統合された形式で提供されます。このユーティリティによって、ジョブの実行時にサーバー間にわたって実行されたすべてのプロセスのログがスキャンされます。ユーティリティでは、クライアント、ジョブ ID、ジョブの開始時刻およびジョブに関連付けられているポリシーごとにジョブの情報を統合できます。

表 3-2 では、ログの分析ユーティリティについて説明します。各ユーティリティのパラメータ、制限事項および使用例を表示するは、`-help` オプションを使用してコマンドを実行します。すべてのコマンドは管理者権限を必要とします。ログの分析ユーティリティは、NetBackup サーバーがサポートされているすべてのプラットフォームで利用できます。

---

**メモ:** ユーティリティはサポート対象のプラットフォームで起動する必要があります。ただし、このユーティリティは UNIX と Windows のほとんどの NetBackup クライアントプラットフォームとサーバープラットフォームのデバッグログファイルを分析できます。

---

表 3-2 NetBackup デバッグログの分析ユーティリティ

ユーティリティ	説明
backupdbtrace	<p>指定した NetBackup データベースバックアップジョブのデバッグログメッセージが統合され、標準出力に書き込まれます。メッセージは時間順にソートされます。backupdbtrace では、リモートサーバーとクライアント間のタイムゾーンの相違およびクロックのずれに対する補正が試行されます。</p> <p>少なくとも、マスターサーバー上の <code>admin</code> およびメディアサーバー上の <code>bptm</code> と <code>bpbkar</code> のデバッグログを有効にする必要があります。最良の結果を得るには、ログの詳細度を 5 に設定し、前述のプロセスに加えて、マスターサーバー上の <code>bpdbm</code> およびすべてのサーバー上の <code>bpcd</code> のデバッグログを有効にします。</p> <p>backupdbtrace の詳しい説明については、『NetBackup コマンドリファレンスガイド』を参照してください。</p>

ユーティリティ	説明
backuptrace	<p>指定したバックアップジョブ (オンラインホットカタログバックアップを含む) に関連するデバッグログの行が標準出力にコピーされます。</p> <p>backuptrace ユーティリティは、通常のファイルシステム、データベース拡張機能および代替バックアップ方式のバックアップジョブに対して使用できます。このユーティリティを使用すると、指定した <b>NetBackup</b> ジョブのデバッグログが統合されます。ユーティリティによって、関連するデバッグログのメッセージが標準出力に書き込まれ、時間順にソートされます。backuptrace では、リモートサーバーとクライアント間のタイムゾーンの相違およびクロックのずれに対する補正が試行されます。出力は、タイムスタンプ、プログラム名、サーバー名またはクライアント名による <b>sort</b> や <b>grep</b> の実行が比較的容易な形式で生成されます。</p> <p>backuptrace ユーティリティを使用するには、マスターサーバー上の nbpem、nbjm および nbrb のログが必要です。また、メディアサーバー上の bpbrm と bptm または bpdm、およびクライアント上の bpbkar のデバッグログを有効にする必要があります。最良の結果を得るには、ログの詳細度を <b>5</b> に設定し、前述のプロセスに加えて、マスターサーバー上の bpdbm と bprd およびすべてのサーバーとクライアント上の bpcd のデバッグログを有効にします。</p> <p>backuptrace の詳しい説明については、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>
bpgetdebuglog	<p>backuptrace と restoretrace。このプログラムは単独で使うこともでき、すべての <b>NetBackup</b> サーバークラウドプラットフォームで利用できます。</p> <p>bpgetdebuglog を実行すると、指定したデバッグログファイルの内容が標準出力に表示されます。リモートマシンのパラメータだけを指定した場合、bpgetdebuglog ではローカルコンピュータとリモートコンピュータ間のクロックのずれの秒数が標準出力に表示されます。</p> <p>bpgetdebuglog の詳しい説明については、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>
duplicatetrace	<p>指定した <b>NetBackup</b> 複製ジョブのデバッグログが統合され、標準出力に書き込まれます。メッセージは時間順にソートされます。duplicatetrace では、リモートサーバーとクライアント間のタイムゾーンの相違およびクロックのずれに対する補正が試行されます。</p> <p>少なくとも、マスターサーバー上の admin およびメディアサーバー上の bptm または bpdm のデバッグログを有効にする必要があります。最良の結果を得るには、ログの詳細度を <b>5</b> に設定し、前述のプロセスに加えて、マスターサーバー上の bpdbm およびすべてのサーバーとクライアント上の bpcd のデバッグログを有効にします。</p> <p>duplicatetrace の詳しい説明については、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>

ユーティリティ	説明
importtrace	<p>指定した <b>NetBackup</b> インポートジョブのデバッグログメッセージが統合され、標準出力に書き込まれます。メッセージは時間順にソートされます。importtrace では、リモートサーバーとクライアント間のタイムゾーンの相違およびクロックのずれに対する補正が試行されます。</p> <p>少なくとも、マスターサーバー上の admin のデバッグログを有効にする必要があります。bpbrm については、メディアサーバー上の you must enable debug logging for bptm と tar のデバッグログを有効にする必要があります。最良の結果を得るには、ログの詳細度を <b>5</b> に設定し、前述のプロセスに加えて、マスターサーバー上の bpdgm およびすべてのサーバーとクライアント上の bpcd のデバッグログを有効にします。</p> <p>importtrace の詳しい説明については、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>
restoretrace	<p>指定したリストアジョブに関連するデバッグログの行が標準出力にコピーされます。</p> <p>restoretrace ユーティリティを実行すると、指定した <b>NetBackup</b> リストアジョブのデバッグログが統合されます。ユーティリティによって、指定したジョブに関連するデバッグログのメッセージが標準出力に書き込まれ、時間順にソートされます。restoretrace では、リモートサーバーとクライアント間のタイムゾーンの相違およびクロックのずれに対する補正が試行されます。出力は、タイムスタンプ、プログラム名、サーバー名またはクライアント名による <b>sort</b> や <b>grep</b> の実行が比較的容易な形式で生成されます。</p> <p>少なくとも、マスターサーバー上の bprd のデバッグログを有効にする必要があります。また、メディアサーバー上の bpbrm と bptm または bpdm、およびクライアント上の tar のデバッグログを有効にします。最良の結果を得るには、ログの詳細度を <b>5</b> に設定し、マスターサーバー上の bpdgm およびすべてのサーバーとクライアント上の bpcd のデバッグログを有効にします。</p> <p>restoretrace の詳しい説明については、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>
verifytrace	<p>指定した検証ジョブのデバッグログメッセージが統合され、標準出力に書き込まれます。時間順にメッセージをソートします。verifytrace コマンドは、リモートサーバーとクライアント間のタイムゾーンの違いとクロックのずれに対する補正を試行します。</p> <p>少なくとも、マスターサーバー上の admin およびメディアサーバー上の bpbrm、bptm (または bpdm) と tar のデバッグログを有効にする必要があります。最良の結果を得るには、ログの詳細度を <b>5</b> に設定し、前述のプロセスに加えて、マスターサーバー上の bpdgm およびすべてのサーバーとクライアント上の bpcd のデバッグログを有効にします。</p> <p>verifytrace の詳しい説明については、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>

分析ユーティリティに次の制限事項があります。

- メディアおよびデバイスの管理ログは分析されません。
- レガシーデバッグログファイルは、サーバーおよびクライアント上の標準の場所に存在する必要があります。

UNIX の場合 `/usr/opensv/netbackup/logs/<PROGRAM_NAME>/log.mmddyy`

Windows の `install_path¥NetBackup¥Logs¥<PROGRAM_NAME>¥mmddyy.log`  
場合

今後、分析されたログファイルを代替パスに配置できるオプションが追加される可能性があります。

---

**メモ:** 統合ログ機能を使用するプロセスの場合、ログディレクトリは自動的に作成されます。

---

- 統合されたデバッグログには、関連のないプロセスからのメッセージが表示される場合があります。ジョブの実行時間外のタイムスタンプを持つ `bprd`、`nbpem`、`nbjm`、`nbrb`、`bpdbm`、`bpbrm`、`bptm`、`bpdm` および `bpcd` からのメッセージは無視できます。

ログの分析ユーティリティからの出力行は次の形式を使います。

```
daystamp.millisecs.program.sequence machine log_line
```

<code>daystamp</code>	<code>yyyymmdd</code> 形式のログの日付。
<code>millisecs</code>	ローカルコンピュータで午前 0 時から経過したミリ秒数。
<code>program</code>	ログが記録されるプログラム名 ( <code>BPCD</code> 、 <code>BPRD</code> など)。
<code>sequence</code>	デバッグログファイル内の行番号。
<code>machine</code>	NetBackup サーバーまたはクライアントの名前。
<code>log_line</code>	デバッグログファイルに表示される行。

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。

## ログアシスタントについて

NetBackup の問題のヘルプでは、ログアシスタントを使ってベリタステクニカルサポートで使用する証拠を収集できます。ヒントや原因を求めて NetBackup デバッグログを独自に調査する必要はありません。デバックログは、テクニカルサポートが分析するためのものです。

ログアシスタントに関する広範な情報は、次の Veritas マニュアルから入手できます。

- NetBackup 管理者ガイド、ボリューム I、NetBackup 管理者コンソールのオンラインヘルプ。
- ログアシスタントについて:  
<http://www.veritas.com/docs/000088104>

## ネットワークトラブルシューティングユーティリティについて

一連のユーティリティプログラム (コマンド) は、構成に誤りがないことを確認するために NetBackup の内部と外部のネットワーク構成の様々な側面を検証します。また、ユーティリティは検出したエラーに関するユーザーフレンドリなメッセージも提供します。

ネットワーク構成は大きく次のカテゴリに分類されます。

- ハードウェア、オペレーティングシステム、NetBackup レベルの設定。  
 例には、正しい DNS 参照、ファイアウォールポートの開放、ネットワークのルートと接続が含まれています。NetBackup Domain Network Analyzer (nbdna) はこの構成を検証します。
- NetBackup レベルの設定を検証する一連のユーティリティ。  
 これらのユーティリティは bptestbpcd と bptestnetconn を含み、検証する設定は接続方法と CORBA エンドポイントの選択を含んでいます。

表 3-3 ネットワークトラブルシューティングユーティリティ

ユーティリティ	説明
bptestbpcd	<p>NetBackup サーバーから別の NetBackup システムの bpcd デーモンへの接続の確立が試行されます。成功すると、確立されているソケットに関する情報がレポートされます。</p> <p>bptestbpcd の詳しい説明については、『NetBackup コマンドリファレンスガイド』を参照してください。</p>
bptestnetconn	<p>ホストの任意の指定のリストでの 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。このリストには、NetBackup 構成のサーバーリストが含まれます。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。</p> <p>bptestnetconn の詳しい説明については、『NetBackup コマンドリファレンスガイド』を参照してください。</p>

ユーティリティ	説明
nbdna (NetBackup Domain Network Analyzer)	<p>NetBackup ドメインのホスト名を評価します。nbdna ユーティリティは、NetBackup ドメインを自己検出してホスト名情報を評価し、次にそれらのホスト名への接続をテストしてネットワーク関係の状態を検証します。</p> <p>NetBackup ドメインのネットワーク接続の評価は困難です。NetBackup ドメインは複雑なネットワークポロジリーによって何百ものサーバーや何千ものクライアントに拡大する可能性があるためです。</p> <p>nbdna の詳しい説明については、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>

## NetBackup サポートユーティリティ (nbsu) について

NetBackup サポートユーティリティ (nbsu) はコマンドラインツールです。このユーティリティは、ホストに問い合わせを行い、NetBackup およびオペレーティングシステムに関する適切な診断情報を収集します。nbsu を使用すると、収集されたさまざまな形式の診断情報を広範囲にわたって制御できます。たとえば、NetBackup 構成設定、特定のトラブルシューティング領域、NetBackup またはメディアの管理ジョブの状態コードに関する情報を取得できます。

NetBackup サポートユーティリティ (nbsu) は次の場所に存在します。

UNIX の場合 `/usr/opensv/netbackup/bin/support/nbsu`

Windows の `install_path¥NetBackup¥bin¥support¥nbsu.exe`  
場合

---

**メモ:** NetBackup サポートユーティリティ (nbsu) が NetBackup 8.1.1 で更新されました。nbsu の以前のバージョン (名前が変更された old\_nbsu) は非推奨で、今後の NetBackup リリースで削除される予定です。Veritas は新しいバージョン (nbsu) を使用することをお勧めします。

---

次の状況で Veritas NetBackup サポートユーティリティ (nbsu) を実行することを推奨します。

- NetBackup のインストール時にベースラインデータを取得する場合。このデータは、後で問題が発生した場合に役立つ場合があります。
- NetBackup またはオペレーティングシステムの環境の変更を記録する場合。nbsu を定期的に行い、ベースラインデータを最新の状態で保持します。
- NetBackup またはオペレーティングシステムの問題の特定に役立つ場合。
- 問題を Veritas のテクニカルサポートに報告する場合。

次の推奨事項は nbsu ユーティリティをより効果的に実行するのに役立ちます。

- nbsu の使用例や、Veritas テクニカルサポートに送信する診断情報を収集する方法など、nbsu 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。

テクニカルサポートから ##### の形式でケース ID が提供されている場合は、ログファイルの名前をケース ID 番号に変更します。それらのファイルを手動で Veritas の証拠サーバーにアップロードします。詳しくは、次を参照してください。

<http://www.veritas.com/docs/000097935>

- トラブルシューティングを行うには、システムが問題の発生時と同じ状態のときに nbsu を実行します。たとえば、エラーの発生後に **NetBackup** プロセスを停止して再起動したり、サーバーまたはネットワークを変更したりしないでください。これを行った場合、nbsu は問題に関する重要な情報を収集できない場合があります。
- **NetBackup** コンポーネントが動作していない (たとえば、bpgetconfig から情報が戻されない) 場合、nbsu がシステムについて適切に報告できない場合があります。このような場合は、-g コマンドラインオプションを使用して、OS および **NET** コマンドのみを収集します。

nbsu が予想どおりに動作しない場合、次の処置を実行します。

- デフォルトでは、nbsu によってエラーメッセージが標準エラー出力 (STDERR) に送信されるほか、出力ファイルにもメッセージが示されます。nbsu のエラーメッセージは、次の方法でも確認できます。

nbsu エラーメッ      次のように入力します。

ッセージを標準出力  
(STDOUT) に出力す  
る方法

- **Windows** の場合  
`install_path¥NetBackup¥bin¥support¥nbsu.exe 2>&1`
- **UNIX** の場合  
`/usr/opensv/netbackup/bin/support/nbsu 2>&1`

エラーメッセージを  
含む nbsu のすべ  
ての画面出力をファ  
イルに送信する方法

- 次のように入力します。  
`nbsu 2>&1 > file_name`  
 2>&1 によって標準エラーが標準出力に出力され、file\_name によつて標準出力が指定したファイルに送信されます。

- nbsu に関連するデバッグメッセージを生成するには、次を入力します。

```
# nbsu -debug
```

メッセージは **STDOUT** に書き込まれます。

nbsu\_info.txt ファイルは nbsu が動作する環境の概要を提供します。次を含んでいます。

- nbsu プログラムの一般的なフロー
- 実行された診断のリスト
- 0 (ゼロ) 以外の状態が戻された診断のリスト

nbsu\_info.txt の情報によって、nbsu が特定の値を戻した理由や、nbsu が特定のコマンドを実行しなかった理由が示される場合があります。

nbsu が適切な情報を生成しない場合や、動作が正常でない場合は、`-debug` オプションを指定して nbsu を実行します。このオプションは nbsu\_info.txt ファイルに追加のデバッグメッセージを含めます。

nbsu 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。

## NetBackup サポートユーティリティ (nbsu) の出力

デフォルトでは、nbsu コマンドは、nbsu 実行可能ファイルと同じディレクトリに、出力を圧縮ファイルとして作成します。コマンド出力の形式は次のとおりです。

`NBSU_hostname_role_mmdyyyymmdd_timestamp.extension`

次に例を示します。

- UNIX および Linux の場合: `NBSU_mylinuxvm_master_11072017_152100.tgz`
- Windows の場合: `NBSU_mywindowsvm_master_11072017_152100.cab`

nbsu を実行する NetBackup 環境によって、nbsu で作成される特定のファイルが決定されます。nbsu は、オペレーティングシステムおよび NetBackup のバージョンと構成に適切な診断コマンドだけを実行します。nbsu は、実行する診断コマンドごとに個別のファイルにコマンド出力を書き込みます。通常、各出力ファイルの名前には、nbsu が出力を取得するために実行したコマンドの情報が反映されます。たとえば、nbsu が NetBackup の `bpplclients` コマンドを実行した場合は `NBU_bpplclients.txt` ファイル、オペレーティングシステムの `set` コマンドを実行した場合は `OS_set.txt` ファイルが作成されます。

各出力ファイルの先頭には、nbsu が実行したコマンドを識別するヘッダーがあります。ファイルに複数のコマンドからの出力が含まれている場合、出力のヘッダーに `[internal procedure]` と示されます。

次に、`bpgetconfig` コマンドの nbsu 出力ファイルの一部の例を示します。STDERR はコマンドの出力として表示され、出力ファイルにキャプチャされます。終了状態は、次のように出力ファイルに出力されます: `Exit status: <exit status code>`

```
#####Command used:
```

```
/usr/opensv/netbackup/bin/admincmd/bpgetconfig -g sivbl17.domain.com -L#####
```

```
Client/Master = Master
NetBackup Client Platform = Linux, RedHat2.6.18
NetBackup Client Protocol Level = 8.1.0
Product = NetBackup
Version Name = 8.1
Version Number = 810000
NetBackup Installation Path = /usr/opensv/netbackup/bin
Client OS/Release = Linux 3.10.0-229.el7.x86_64
```

```
Exit status: 0
```

```
#####Command used: /usr/opensv/netbackup/bin/admincmd/bpgetconfig#####
```

```
SERVER = sivb117.domain.com
WEB_SERVER_CONNECTION_TIMEOUT = 30
WEB_SERVER_TUNNEL_USE = AUTO
WEB_SERVER_TUNNEL_ENABLED = YES
WEB_SERVER_TUNNEL
TRUSTED_MASTER
KNOWN_MASTER
MASTER_OF_MASTERS
USEMAIL =
BPBACKUP_POLICY = any
BPBACKUP_SCHED = any
```

```
Exit status: 0
```

nbsu が実行されているホストで、サポートされているアーカイブプログラムが使用できる場合、nbsu によって複数の出力ファイルが 1 つのアーカイブファイルにまとめられます。サポートされている圧縮ユーティリティが使用できる場合、nbsu によってアーカイブファイルが圧縮されます。いずれも使用できない場合、個々の出力ファイルはアーカイブも圧縮もされません。

nbsu によって作成された圧縮アーカイブファイルの例を次に示します。

```
/usr/opensv/netbackup/bin/support/NBSU_host1_master_01172018_220505.tgz
```

ここで、**host1** は **nbsu** が実行されたホストの名前です。**master** は、このホストが **NetBackup** マスターサーバーであることを示しています。日付は `mmddyyyy` の形式のファイル名で埋め込まれます。

nbsu は、アーカイブには **tar**、圧縮には **gzip** をサポートしています。

nbsu 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。

## NetBackup サポートユーティリティ (nbsu) の進捗状況の表示の例

デフォルトでは、NetBackup サポートユーティリティ (nbsu) は標準出力に進捗状況を表示します。次の例に示すように、最初に、環境に関する問い合わせが表示され、次に、実行している診断コマンドが表示されます。

```
NBU Install path: C:\Program Files\Veritas\
mywindowsvm is a master server
Collecting NBU_adv_disk info
Collecting NBU_all_log_entries info
Collecting NBU_altnames info
Collecting NBU_auth_methods_names info
Collecting NBU_available_media info
Collecting NBU_backup_status info
Collecting NBU_bpclient info
.
.
.
Collecting OS_filesystem info
Collecting OS_process_list info
Collecting OS_set info
CAB file created successfully.

Final NBSU output located at
NBSU_mywindowsvm_master_01172018_085005.cab

The execution time : 662.53431
```

nbsu 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。

## NetBackup の一貫性チェックユーティリティ (NBCC) について

NetBackup の一貫性チェックユーティリティ (NBCC) はコマンドラインユーティリティです。NetBackup の構成、カタログ、データベース情報の一部の整合性を分析する場合に使用します。この分析には NetBackup ストレージユニット、EMM サーバー、ボリュームプール、テープメディア、テープメディアに関連付けられたバックアップイメージの確認が含まれます。

NBCC には、次の機能があります。

- EMM データベースに問い合わせを実行してプライマリホスト名、関連付けられたホスト名、ホスト名の正規化のためのサーバー属性を入手します

- **NetBackup** の構成の診断を通して、クラスタ、アプリケーションクラスタ、サーバーを識別します
- データベースやカタログの情報を集めます
- 集められた構成とデータベースおよびカタログ情報の一貫性を分析します
- ベリタス社テクニカルサポートによる調査用のパッケージバンドルを作成します**Veritas**

NBCC は次の場所に存在します。

UNIX の場合 /usr/opensv/netbackup/bin/support/NBCC

Windows の `install_path\NetBackup\bin\support\NBCC.exe`  
 場合

次の状況で **Veritas NBCC** を実行することを推奨します。

- テープメディアの観点から **NetBackup** の構成とカタログおよびデータベース情報の一貫性を確認する場合
- ベリタス社テクニカルサポートの指示によりパッケージバンドルを収集し作成する場合 **Veritas**

次の項目は、NBCC ユーティリティを実行するのに役立ちます。

- NBCC をオプションなしで使用すると、すべてのデータやレポートが収集されます。ほとんどの場合これは推奨されます。追加情報、NBCC の説明、例、テクニカルサポートに送信する **NetBackup** のカタログ情報とデータベース情報の収集方法については、NBCC `-help` コマンドを参照してください。
- NBCC は **NetBackup** マスターサーバーで動作するように設計されています。
- 場合によっては、オペレーティングシステムか **NetBackup** の処理またはサービスが機能していないために NBCC が正しく実行されないか、または完了できないことがあります。NBCC は、各種のオペレーティングシステムまたは **NetBackup** コンポーネントの確認を実行するときに、処理対象を標準出力 (STDOUT) に出力します。NBCC はカタログおよびデータベースのコンポーネントの処理時に、処理したレコードの数を表示します。処理されるレコードの数は処理されるカタログおよびデータベースのサイズに直接関係します。NBCC が失敗を検出する場合は、関連情報は標準エラー出力 (STDERR) に出力されます。STDOUT または STDERR への情報は nbcc-info.txt ファイルにも出力されます (利用可能な場合)。

NBCC が予想どおりに動作しない場合、次の処置を実行します。

- テキストエディタを使用して nbcc-info.txt ファイルでエラー通知を見つけます。
- デフォルトでは、NBCC によってエラーメッセージが標準エラー出力 (STDERR) に送信されるほか、NBCC の出力ファイルのヘッダー「STDERR」の下にもそのメッセージが示されます。

- NBCC が適切な情報を生成しない場合や、NBCC の動作が不適切な場合は、`-debug` オプションを指定して NBCC を実行し、追加のデバッグメッセージが `nbcc-info.txt` ファイルに含まれるようにします。
- トラブルシューティングを行うには、システムが問題の発生時と同じ状態のときに NBCC を実行します。たとえば、エラーの発生後に **NetBackup** プロセスを停止して再起動したり、サーバーまたはネットワークを変更したりしないでください。NBCC は問題に関する重要な情報が収集できない場合があります。

`nbcc-info.txt` ファイルは NBCC が動作する環境の概要を提供し、次の情報を含んでいます。

- NBCC が検出する環境のオペレーティングシステムそして **NetBackup** の構成の一般情報。
- `STDOUT` または `STDERR` に送信された NBCC の処理情報のコピー。

この情報は NBCC が実行した処理を示します。

`nbcc-info.txt` レポートは **NetBackup** の構成で検出される各システムの NBCC 処理を概略化する情報のセクションを含みます。このセクションは NBCC が検出する EMM のサーバー形式を示します。「**Summary of NBCC <type> processing**」で始まります。

p.196 の「[NBCC の進捗状況の表示の例](#)」を参照してください。

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

## NetBackup の一貫性チェックユーティリティ (NBCC) の出力

NBCC は、次のディレクトリの一連のファイルに集めた情報を書き込みます。

**UNIX および Linux**    `/usr/opensv/netbackup/bin/support/output`  
                           `/nbcc/hostname_NBCC_timestamp`

**Windows の場合**     `install_path\NetBackup\bin\support\output`  
                           `\nbcc\hostname_NBCC_timestamp`

NBCC が実行されているホストで、サポートされているアーカイブプログラムが使用できる場合、NBCC によって複数の出力ファイルが 1 つのアーカイブファイルにまとめられます。サポートされている圧縮ユーティリティが使用できる場合、NBCC によってアーカイブファイルが圧縮されます。いずれも使用できない場合、個々の出力ファイルはアーカイブも圧縮もされません。

NBCC によって作成された圧縮アーカイブファイル (UNIX) の例を次に示します。

```
/usr/opensv/netbackup/bin/support/output/NBCC/host1_NBCC_20060814_164443/host1_NBCC_20060814_164443.tar.gz
```

ここで **host1** は NBCC が実行されていたホストの名前です。

UNIX プラットフォームでは、NBCC は UNIX ファイルのアーカイブと圧縮のための **tar**、**compress**、**gzip** ユーティリティをサポートします。Windows プラットフォームでは、NBCC は Windows ファイルのアーカイブと圧縮のための **tar**、**Makecab**、**gzip** ユーティリティをサポートします。

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

## NBCC の進捗状況の表示の例

デフォルトでは、NetBackup の一貫性チェックユーティリティ (NBCC) は標準出力に進捗状況を数値で表示します。出力ファイルの名前は `nbcc-info.txt` です。

次に、NBCC の出力例を簡略化して示します。

```
1.0 Gathering initial NBCC information
1.1 Obtaining initial NetBackup configuration information

NBCC is being run on NetBackup master server
server1
NBCC version 8.1 Gather mode = full
NBCC command line = C:\Veritas\NetBackup\bin\support\NBCC.exe -nozip
OS name = MSWin32
OS version = Microsoft Windows [Version 6.1.7601]
NetBackup Install path = C:\Program Files\Veritas\
> dir output\nbcc\server1_NBCC_20130227_091747 2>&|
Parsed output for "bytes free"

5 Dir(s) 862,367,666,176 bytes free

2.0 Gathering required NetBackup configuration information
2.1 Determining the date format to use with NetBackup commands...
Using the date format /mm/dd/yyyy
2.2 Building EMM host configuration information...
Detected the EMM Server hostname
lidabl11
Detected the EMM master server hostname
lidabl11
Detected the EMM Virtual Machine entry
pambl11vm3
```

```

Detected the EMM NDMP Host entry
  fas3240a
...
2.3 Obtaining EMM server aliases...
EMM aliases for detected EMM Server
  server1
    lidabl11.acme.com
EMM aliases for detected master server
  server1
    lidabl11.acme.com
EMM aliases for detected media server
  server4
...
2.4 Obtaining Storage Server information...
  Detected FalconStor OST direct copy to tape Storage Server
    falconstorvt15
2.5 Building NetBackup storage unit list...
  Detected Storage Unit for NetBackup for NDMP media server
    reabl3
  and NDMP Host
    falconstorvt15
  Detected disk media storage unit host
    lidabl11
  Detected Disk Pool
    lidabl11_pdde_pool
...
2.6 Obtaining Disk Pool information...
  Detected Disk Pool
    lidabl11_pdde_pool
    host
      lidabl11
    Detected Disk Pool lidabl11_pdde_pool member
      lidabl11
...
2.7 Obtaining tpconfig Storage credential information...
  Detected the master server hostname
    lidabl11
  and associated Storage server hostname
    lidabl11
...
2.8 Obtaining tpconfig NDMP configuration information...
  Detected the EMM NDMP Host hostname
    fas3240a

```

```

Detected the EMM NDMP Host hostname
fas3240b
...
2.9 Analyzing EMM master and/or media servers and configured
Storage Units...
The following EMM server entries do not have configured
Storage Units or Disk Pools:

Media server - lidabl14

2.10 Obtaining NetBackup unrestricted media sharing status...
Configuration state = NO
2.11 Obtaining NetBackup Media Server Groups...
No Server Groups configured
2.12 Building NetBackup retention level list...
3.0 Obtaining NetBackup version from media servers
lidabl11...
lidabl14...
reabl3...
virtualization5400a...
...
3.1 Gathering required NetBackup catalog information
Start time = 2013-02-27 09:41:07
3.2 Gathering NetBackup EMM conflict table list
Found 0 EMM conflict records
3.3 Gathering list of all tapes associated with any Active Jobs
Building NetBackup bpdjobs list
3.4 Gathering all TryLog file names from the
C:\Program Files\netbackup\%db%\jobs\trylogs
directory
Found 10 TryLogs for 10 active jobs.
TryLogs found for all Active Jobs
3.5 Building NetBackup Image database contents list
Reading Image number 1000
Reading Image number 2000
Reading Image number 3000
Reading Image number 4000
Found 4014 images in the Image database
3.6 Building EMM database Media and Device configuration
attribute lists
Obtaining the EMM database Media attribute list for disk
virtual server
lidabl11 ...

```

```

        There were 0 bpmedialist records detected for media server
        lidabl11
        Getting device configuration data from server
        lidabl11 ...
    ...
3.7 Building EMM database Unrestricted Sharing Media attribute lists

        Found 0 Unrestricted Sharing media records in the EMM
        database
3.8 Building the EMM database Volume attribute list...
        Getting the EMM database Volume attributes from EMM server
        mlbmbu ...
        Found 43 Volume attribute records in the EMM database
3.9 Building NetBackup volume pool configuration list
        EMM Server lidabl11
3.10 Building NetBackup scratch pool configuration list
        EMM Server lidabl11
3.11 Gathering NetBackup EMM merge table list
        Found 0 EMM merge table records

Summary of gathered NetBackup catalog information
End time = 2013-02-27 09:44:16
Number of Images gathered = 4014
Number of database corrupt images gathered = 0
Number of EMM database Media attribute records gathered = 38
Number of EMM database Volume attribute records gathered = 43

Catalog data gathering took 189 seconds to complete

dir results for created NBCC files:
02/27/2013 09:42 AM          8 nbcc-active-tapes

02/27/2013 09:42 AM      752,698 nbcc-bpbdjobs-most_columns

07/07/2011 09:43 AM    2,211,811 nbcc-bpimagelist-1
...

4.0 Verifying required catalog components were gathered

5.0 Beginning NetBackup catalog consistency check
Start time = 2013-02-27 09:44:18
5.1 There were no tape media involved in active NetBackup jobs
    
```

```
5.3 Processing EMM database Volume attribute records, pass 1 (of
2),
    4 records to be processed
    Processed 4 EMM database Volume attribute records.
5.4 Checking for duplicate EMM server host names in Volume
attribute data
5.5 Processing Image DB, pass 1 (of 2),
    3751 images to be processed
    3751 images processed on pass 1
    There were 0 images with at least one copy on hold detected.
5.6 Processing EMM database Media attribute records, pass 1 (of 3),

    2 records to be processed
    Processed 2 EMM database Media attribute records.
    There were 0 tape media detected that are on hold.
5.8 Check for duplicate media server names in the EMM database
Media attribute data
5.9 Processing EMM database Media attribute records, pass 2 (of 3),

    2 records to be processed
5.10 Processing Image DB, pass 2 (of 2),
    3751 images to be processed
CONSISTENCY_ERROR Oper_7_1

5.11 NetBackup catalog consistency check completed
    End time = 2013-02-27 09:19:25

5.12 Checking for the latest NBCCR repair output directory
    C:\Program Files\Veritas\netbackup\bin\support\output\nbccr
    No repair file output directory detected.
```

```
Summary of NBCC EMM Server processing
+++++
+ Primary hostname:
+
+ lidabl11
+
+ Alias hostnames:
+
+ lidabl11
+
+ Sources:
```



```

Summary of NBCC Media server processing
+++++
+ Primary hostname:
+
+ lidabl14
+
+ Alias hostnames:
+
+ lidabl14.acme.com
+ Sources:
+
+ nbemmcmd bpgetconfig
+
+ Media server = yes
+
+ EMM NetBackup version = 8.1.0.0
+
+ NBCC NetBackup version = 8.1
+
+ Tape STU detected = no - Disk STU detected = no
+
+ EMM tape media record extract attempted = yes
+
+++++
...

***NBCC DETECTED A NetBackup CATALOG INCONSISTENCY!***

Report complete, closing the
.%output¥nbcc¥lidabl11_NBCC_20130227_094057¥nbcc-info.txt
output file.
    
```

NBCC オプションの詳細な説明については、『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

## NetBackup の一貫性チェックの修復 (NBCCR) ユーティリティについて

NetBackup の一貫性チェックの修復 (NBCCR) ユーティリティは、データベースカタログの修復操作を処理するコマンドラインツールです。承認済みの推奨される修復操作を自動的に適用します。Veritas のテクニカルサポートは NBCCR ユーティリティによって収集されるデータとサイト固有の構成情報を分析します。この分析によって、推奨される修復操作 (SRA) ファイルが生成されます。NBCCR が稼働する前に、Veritas テクニカルサポートは必要な修復を判断するためにお客様と対話します。望ましくない修復操作は SRA ファイルから削除されるか、またはコメントアウトされます。SRA ファイルの各行は、関連付けられたパラメータと組み合わせられる 1 つの修復操作を含んでいます。

NBCCR ユーティリティは、各修復操作を複数の段階で実行します。

表 3-4 修復の段階

段階	名前	説明
段階 1	データ収集	NBCCR は、修復の実行に必要な情報を最初に集めます。
段階 2	修復の認定	推奨される修復が適用される直前に、テープの現在の状態が要求された修復の実施に引き続き適合するかどうかを NBCCR は確認します。データが集められてから時間が経過し、環境が変わったかもしれないことが認識されます。その場合、修復が認定されないことを履歴ファイルで報告します。
段階 3	修復	最後に、NBCCR は SRA ファイルのすべての修復エントリに対して最大 3 つの修復手順を実行します。修復を有効にするために修正される要素があることがあり、修復後の手順が必要になることがあります。修復が修復操作の間に失敗する場合は、NBCCR は修正処置が新しいエラーをもたらさないように修復をロールバックすることを試みます。

NBCCR は次の場所に存在します。

UNIX の場合 /usr/opensv/netbackup/bin/support/NBCCR

Windows の `install_path¥NetBackup¥bin¥support¥NBCCR.exe`  
 場合

NBCCR は 1 つの入力ファイルを受け入れ、2 つの出力ファイルを作成し、1 つの一時ファイルを使います。

**入力ファイル** NBCCR は `mastername_NBCCA_timestamp.txt` という名前の推奨される修復操作 (SRA) ファイルを入力として受け入れます。テクニカルサポートは NBCC サポートパッケージを分析し、エンドユーザーに送信されるこのファイルを生成します。このファイルは NBCCR の処理用に次のディレクトリに配置されます。

UNIX の場合:

```
/usr/opensv/netbackup/bin/support/input/nbccr/SRA
```

Windows の場合:

```
install_path¥NetBackup¥bin¥support¥input¥nbccr¥SRA
```

**出力ファイル** NBCCR は処理される SRA ファイルごとに別のディレクトリを自動的に作成します。ファイル名は SRA ファイルの内容に基づいています。ディレクトリの名前は次のとおりです。

UNIX の場合:

```
/usr/opensv/netbackup/bin/support/output/nbccr/mastername_nbccr_timestamp
```

Windows の場合:

```
install_path¥NetBackup¥bin¥support¥output¥nbccr¥mastername_nbccr_timestamp
```

修復処理の完了後、NBCCR は同じディレクトリに SRA ファイルを再配置します。

また、NBCCR は次の出力ファイルを作成し、同じディレクトリに配置します。

- NBCCR は `NBCCR.History.txt` を作成します。これは、試みられたすべての修復処理の履歴ファイルです。
- NBCCR は `NBCCR.output.txt` を作成します。

**一時ファイル** 実行中、NBCCR ユーティリティは、この表の出力ファイルと同じ場所に表示される `KeepOnTruckin.txt` を使います。

修復処理中に NBCCR を終了するには、このファイルを削除します。この操作により NBCCR は現在の修復を完了し、それから終了します。他の方法による中断は未定の結果を引き起こします。

次の `NBCCR.output.txt` ファイルの例は 2 つの MContents 修復の結果を示します。1 つの例では、テープですべてのイメージが見つけれられ、もう 1 つの例では、テープでイメージが 1 つも見つけれませんでした。

- 例 1: NBCCR はテープですべてのイメージを見つけました。MContents の修復操作は成功です。

```
MContents for ULT001 MediaServerExpireImagesNotOnTapeFlag
ExpireImagesNotOnTape flag not set
ULT001 MContents - All images in images catalog found on tape
MContents ULT001 status: Success
```

- 例 2: NBCCR はテープで 1 つもイメージを見つけませんでした。MContents の修復処理は実行されませんでした。

```
MContents for ULT000 MediaServerExpireImagesNotOnTapeFlag
ExpireImagesNotOnTape flag not set
  Did NOT find Backup ID winmaster_123436 Copy 1 AssignTime
    2011-02-11 01:19:13 (123436) on ULT000
  Leaving winmaster_123436 Copy 1 on ULT000 in ImageDB
  ULT000 MContents - One or more images from images catalog NOT

  found on tape
MContents ULT000 status: ActionFailed
```

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

## nbcplogs ユーティリティについて

問題を解決するとき、問題をデバッグするために正しいログを集め、コピーしてください。ログの形式 (レガシー、vxul、vm、pbx など) は、さまざまな場所に分散していることがあります。Veritas のテクニカルサポートに提供するログを取得する処理が複雑になり時間がかかることがあります。

デフォルトで、nbcplogs が nbsu ユーティリティを実行し、ホストシステムの nbsu の情報を収集するようになりました。この機能により、情報収集にかかる時間とキー操作を節約できます。ユーティリティはまた、クラスタとバック履歴情報の追加のログ情報も集めます。

テクニカルサポートから ##### の形式でケース ID が提供されている場合は、ログファイルの名前をケース ID 番号に置き換えます。それらのファイルを手動で Veritas の証拠サーバーにアップロードします。詳しくは、次を参照してください。

<http://www.veritas.com/docs/000097935>

このユーティリティは、nbcplogs コマンドのオプションとして次の種類の検索アルゴリズムをサポートします。

- --filecopy. ファイルコピーはデフォルト条件です。ログファイル全体をコピーします。圧縮を使用したファイルコピーは、通常、ジョブを完了するのに十分です。
- --fast. 高速検索はバイナリ検索を使用してファイルの時間枠の外にある行を除外します。この機能は bpdbm のような大きいログファイルをコピーするときに有用です。このオプションが必要とされることはまれで、慎重に使う必要があります。

デフォルト条件は、ログファイル全体をコピーするファイルコピーです。高速検索アルゴリズムはバイナリ検索を使用してファイルの時間枠の外にある行を除外します。この機能は bpdbm のような大きいログファイルをコピーするときに有用です。

nbcplogs ユーティリティは、次のオプションの指定によってログをコピーする処理を単純化するように意図されています。

- ログの時間枠。
- 収集したいログの形式。
- データのバンドルと送信中のデータ圧縮。

さらに、コピーするログデータの量をプレビューできます。

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

## ロボットテストユーティリティについて

各ロボットソフトウェアパッケージには、ロボット周辺機器と直接通信するためのロボットテストユーティリティが含まれています。これらのテストは診断に使用され、マニュアルはオンラインヘルプだけです。このオンラインヘルプは、ユーティリティの起動後に疑問符(?)を入力することによって表示できます。-h を指定すると、使用方法についてのメッセージが表示されます。

---

**メモ:** バックアップまたはリストアの実行中は、ロボットテストユーティリティを使用しないでください。テストを実行すると、ロボット制御パスがロックされ、対応するロボットソフトウェアによる操作 (メディアのロードやロードの解除など) が実行されません。マウントが要求されると、対応するロボットプロセスでタイムアウトが発生し、停止状態になります。その結果、通常、メディアのマウントでタイムアウトが発生します。また、テストの完了後はユーティリティを終了してください。

---

## UNIX でのロボットテスト

ロボットが構成済み (NBDB に追加されている) である場合、robtest コマンドを実行してロボットテストユーティリティを起動します。これによって、ロボットおよびドライブのデバイスパスが自動的にテストユーティリティに渡されるため、時間がかかりません。手順を次に示します。

robtest コマンドを使用するには、示されている順に次の操作を行います。

- 次のコマンドを実行します。

```
/usr/opensv/volmgr/bin/robtest
```

テストユーティリティのメニューが表示されます。

- ロボットを選択し、**Enter** キーを押します。  
テストが開始されます。

ロボットが構成されていない場合、robtest は実行できません。次に示すとおり、テスト対象のロボットに対応するコマンドを実行する必要があります。

ACS `/usr/opensv/volmgr/bin/acstest -r ACSLS_hostpath`  
UNIX および Linux の場合、acstest を実行するには acssei と csessi が実行されている必要があります。

TLD `/usr/opensv/volmgr/bin/tldtest -r roboticpath`

ACS ロボット制御に関する詳細情報が利用可能です。

『[NetBackup デバイス構成ガイド](#)』を参照してください。

前述のコマンドリストにおいて、`roboticpath` はロボット制御 (SCSI) のデバイスファイルへのフルパスです。`roboticpath` の適切な値については、ご使用のプラットフォームの項を参照してください。

オプションのパラメータを使用してドライブのデバイスファイルパスを指定すると、このユーティリティで SCSI インターフェースを使用してドライブをアンロードできます。

## Windows でのロボットテスト

ロボットが構成済み (NBDB に追加されている) である場合、robtest コマンドを実行してロボットテストユーティリティを起動します。これによって、ロボットおよびドライブのデバイスパスが自動的にテストユーティリティに渡されるため、時間がかかりません。

robtest コマンドを使用するには、示されている順に次の操作を行います。

- 次のコマンドを実行します。

```
install_path%Volmgr%bin%robtest.exe
```

テストユーティリティのメニューが表示されます。

- ロボットを選択し、Enter キーを押します。  
テストが開始されます。

---

**メモ:** ロボットが設定されていない場合、robtest を使うことはできません。テストするロボットに適用されるコマンドを実行する必要があります (次のリストを参照)。

---

ACS `install_path%Volmgr%bin%acstest -r ACSLS_HOST`

TLD `install_path%Volmgr%bin%tldtest -r roboticpath`

ACS ロボット制御に関する詳細情報が利用可能です。

『[NetBackup デバイス構成ガイド](#)』を参照してください。

前述のコマンドリストにおいて、*roboticpath* はロボット制御 (SCSI) のデバイスファイルへのフルパスです。*roboticpath* の適切な値については、ご使用のプラットフォームの項を参照してください。

オプションのパラメータを使用してドライブのデバイスファイルパスを指定すると、このユーティリティで SCSI インターフェースを使用してドライブをアンロードできます。

次に使用方法を示します。

```
install_path <-p port -b bus -t target -l lan | -r  
roboticpath>
```

ここで、*roboticpath* は、チェンジャ名 (Changer0 など) です。

## NetBackup Smart Diagnosis (nbsmartdiag) ユーティリティについて

NetBackup Smart Diagnosis (nbsmartdiag) ユーティリティを使用すると、高い CPU 使用率、高いメモリ使用率、登録された NetBackup プロセスのデッドロックなど、パフォーマンスの問題を検出できます。nbsmartdiag が問題を検出すると、ユーザーによる操作なしで、トラブルシューティングをさらに進めるために必要な証拠の収集を開始します。nbsmartdiag は、NetBackup マスターサーバー、メディアサーバー、クライアントに配備できるサービスまたはデーモンです。

---

**メモ:** nbsmartdiag サービスは、Windows と Linux (RHEL および SUSE) プラットフォームでのみサポートされます。

---

### 証拠

証拠は、NetBackup のパフォーマンスのトラブルシューティングに役立てるために収集する情報セットです。

収集される 1 セットの証拠の内容は次のとおりです。

#### Windows の場合

- パフォーマンスの問題が発生しているプロセスのプロセスダンプ
- CSV ファイル形式のメモリパフォーマンスカウンタ
- CSV ファイル形式のネットワークパフォーマンスカウンタ
- CSV ファイル形式のディスクパフォーマンスカウンタ
- ネットワークの問題に対する netstat コマンド出力

#### Linux の場合

- パフォーマンスの問題が発生しているプロセスのプロセスダンプ

- メモリの詳細を示す `vmstat`、`free`、`top` などのコマンド出力
- プロセスの `gstack`、`pmap`
- ディスク I/O の詳細を示す `mpstat`、`iostat` コマンド出力
- ネットワークの問題に対する `netstat` コマンド出力

### 証拠の例:

- Windows で収集される証拠のサンプル。

```
Directory of NBSD_EVIDENCE_PATH\nbsmartdiag\bpdbm\5004\Evidence1
04/08/2021 02:07 AM <DIR> .
04/08/2021 02:07 AM <DIR> ..
04/08/2021 02:08 AM 197,979,709 5004_08-04_02.07.38_Deadlock.dmp
04/08/2021 02:07 AM 4,363 5004_08-04_02.07.38_DiskPerf_Deadlock.csv
04/08/2021 02:07 AM 1,530 5004_08-04_02.07.38_MemoryPerf_Deadlock.csv
04/08/2021 02:07 AM 5,572 5004_08-04_02.07.38_Netstat_Deadlock.log
04/08/2021 02:07 AM 23,249 5004_08-04_02.07.38_NetworkPerf_Deadlock.csv
5 File(s) 198,014,423 bytes
2 Dir(s) 188,446,031,872 bytes free
```

- Linux で収集される証拠のサンプル。

```
Cmd$ ls -l /root/NBTestData/nbsd.evd/nbsmartdiag/vnetd/29696/Evidence1 total
1154144
-rw-r--r-- 1 root root 1180858264 Apr 8 15:25 29696_08-04_15.24.43_CPU.29696
-rw-r--r-- 1 root root 197 Apr 8 15:24 29696_08-04_15.24.43_CPU.DiskPerf_iostat
-rw-r--r-- 1 root root 193 Apr 8 15:24 29696_08-04_15.24.43_CPU.DiskPerf_mpstat
-rw-r--r-- 1 root root 560374 Apr 8 15:24 29696_08-04_15.24.43_CPU.MemoryPerf
-rw-r--r-- 1 root root 185787 Apr 8 15:24 29696_08-04_15.24.43_CPU.Netstat
-rw-r--r-- 1 root root 214191 Apr 8 15:24 29696_08-04_15.24.43_CPU.ProcessData
```

### nbsmartdiag に関する重要な注意事項

- NetBackup の設計では、`bpup` コマンドによる `nbsmartdiag` サービスの起動は許可されていません。
- 証拠のパスではキリル文字はサポートされません。
- `nbsmartdiag` サービスは、Windows のローカルシステムアカウントと Linux のルート権限で実行できます。

- Java プロセスには共通ランタイム名があります。NetBackup 管理コンソールを監視するにはプロセス名に `adminconsole` を使用し、NetBackup Web 管理サービスには `nbwmc` を使用します。

## NetBackup ホストの通信に nbsmartdiag ユーティリティを使用するワークフロー

トラブルシューティング中に問題を検出するように nbsmartdiag を構成するには、次の手順を指定された順序で実行します。

**表 3-5** nbsmartdiag を使用して問題をトラブルシューティングするワークフロー:

手順	説明
手順 1	<p>次の項目について確認します。</p> <ul style="list-style-type: none"> <li>■ ご使用のプラットフォームで nbsmartdiag サービスがサポートされている必要があります。</li> </ul> <p>次のオペレーティングシステムで nbsmartdiag がサポートされています。</p> <ul style="list-style-type: none"> <li>■ Windows</li> <li>■ RHEL</li> <li>■ SUSE</li> </ul> <p><b>メモ:</b> Windows の場合、Windows Server 2012 R2 以降のバージョンに nbsmartdiag サービスをインストールする必要があります。古いバージョンの Windows Server に nbsmartdiag サービスをインストールすると、エラーメッセージが表示されインストールが失敗します。</p> <ul style="list-style-type: none"> <li>■ Linux の場合、サポート対象の証拠をすべて収集するには、次のコマンドがシステムに存在する必要があります。</li> </ul> <ul style="list-style-type: none"> <li>■ gcore</li> <li>■ gstack</li> <li>■ iostat</li> <li>■ mpstat</li> <li>■ netstat</li> <li>■ pmap</li> <li>■ top</li> <li>■ vmstat</li> </ul> <p>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。</p> <p><a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></p>

手順	説明
手順 2	<p>マスターサーバー、メディアサーバー、またはクライアントに <b>nbsmartdiag</b> をインストールします。</p> <pre>nbsmartdiag demo \$ /usr/opensv/netbackup/bin/nbsmartdiag -install.</pre> <p>Performing the install operation.  Performed the install operation successfully.</p>
手順 3	<p><b>nbsmartdiag</b> サービスを開始します。 <b>nbsmartdiag -start</b></p> <p><b>Windows</b> では、<b>nbsmartdiag</b> サービスはサービスコントロールマネージャーから起動します。</p> <pre>Nbsmartdiag demo \$ /usr/opensv/netbackup/bin/nbsmartdiag -start</pre> <p>Performing the start operation.  Info:Daemon is running.  Performed the start operation successfully.</p>
手順 4	<p><b>bp.conf</b> の <b>NBSD_EVIDENCE_PATH</b> 値で指定された場所にある <b>nbsmartdiag</b> フォルダから証拠を収集します。</p> <ul style="list-style-type: none"> <li>■ プロセスのフォルダ内には、プロセスのインスタンスごとにサブフォルダが作成されます。</li> <li>■ そのプロセス ID フォルダには、イベントが発生するたびに証拠が集められます。</li> </ul> <p><b>bp.configuration</b> オプションについて詳しくは、『<b>NetBackup 管理者ガイド Vol. 1</b>』を参照してください。  <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></p>
手順 5	<p>証拠の収集が完了したら、<b>nbsmartdiag</b> サービスを停止します。次のコマンドを実行します。 <b>nbsmartdiag -terminate</b></p>

## nbsmartdiag ユーティリティのアンインストール

次のコマンドを使用して NetBackup Smart Diagnosis サービスをアンインストールできます。

**nbsmartdiag -uninstall** を実行し、**Windows** のサービスと **Linux** のデーモンをアンインストールします。

# ディザスタリカバリ

この章では以下の項目について説明しています。

- [ディザスタリカバリについて](#)
- [ディザスタリカバリの要件について](#)
- [ディザスタリカバリパッケージ](#)
- [ディザスタリカバリ設定について](#)
- [バックアップに関する推奨事項](#)
- [UNIX および Linux のディスクリカバリ手順について](#)
- [UNIX および Linux のクラスタ化された NetBackup サーバーのリカバリについて](#)
- [Windows のディスクリカバリ手順について](#)
- [Windows のクラスタ化された NetBackup サーバーのリカバリについて](#)
- [ディザスタリカバリインストール後にクラスタマスターサーバーで証明書を生成する](#)
- [ディザスタリカバリパッケージのリストアについて](#)
- [DR\\_PKG\\_MARKER\\_FILE 環境変数について](#)
- [Windows でのディザスタリカバリパッケージのリストア](#)
- [UNIX でのディザスタリカバリパッケージのリストア](#)
- [NetBackup カタログのリカバリについて](#)

## ディザスタリカバリについて

データのバックアップは、すべてのデータ保護方針(特に、ディザスタリカバリを支援するための方針)に必須です。定期的にデータのバックアップをとることで、特定の時間範囲

内でそのデータをリストアできることは、リカバリする際の重要事項です。どのようなリカバリを実施するかにかかわらず、バックアップによって、致命的なシステム障害が発生した場合のデータの損失を回避できます。また、バックアップイメージをオフサイト(遠隔地にある保管場所の)ストレージに保管することによって、オンサイトメディアが破損した場合や、障害が発生して施設やサイトが被害を受けた場合のデータの損失を回避できます。

リカバリを正常に実行するには、データを追跡する必要があります。データがバックアップされた時点を認識しておく、リカバリできない情報を組織内で判断できます。データのバックアップは、組織のリカバリポイント目標 (RPO: Recovery Point Objective) を達成できるようにスケジュールを設定します。RPO とは、それ以前のデータの損失を許容できない時点を示します。組織で許容できるデータの損失が 1 日分である場合、1 日 1 回以上バックアップを行うようにスケジュールを設定する必要があります。そうすることで、障害が発生する前日の RPO を達成できます。

組織で、リカバリ時間目標 (RTO: Recovery Time Objective) が設定されている場合があります。RTO とは、リカバリにかかると想定される時間を示します。リカバリ時間は、障害の種類とリカバリに使用される方法の相関関係で決定されます。組織でリカバリが必要なサービスの種類およびその期限に応じて、複数の RTO を設定することもできます。

高可用性技術を使用すると、障害発生ポイントに非常に近い、または障害発生ポイントと同じリカバリポイントを設定できます。また、リカバリ時間の大幅な短縮が可能になります。ただし、RTO および RPO を障害発生ポイントに近づけるほど、リカバリするために必要なシステム構築および維持にかかるコストが増大します。組織のリカバリ計画を作成する際には、さまざまなリカバリ方針のコストおよび利点を分析する必要があります。

効果的なディザスタリカバリ手順を実現するには、環境に固有の手順が必要です。これらの手順では、障害に対する準備および障害からのリカバリについての詳細情報が提供されます。この章のディザスタリカバリ情報は基準として使用するだけとし、この情報を評価して、ディザスタリカバリの独自の計画および手順を作成してください。

---

**警告:** この章のディザスタリカバリ手順を試す前に、Veritas では、テクニカルサポートに連絡することをお勧めします。

このトピックでは、システムディスクに障害が発生した場合に、NetBackup のインストールを行い、必要に応じてカタログのリカバリする手順について説明します。Veritas では、元のシステムディスクか、または元のシステムディスクと厳密に同じ構成のディスクにリカバリすることを前提としています。

---

**警告:** 再インストールおよびリカバリを、異なるパーティションまたは異なる状態にパーティション化されたパーティションに対して行うと、内部構成情報が原因で NetBackup が適切に機能しない場合があります。代わりに、交換したディスクは、障害が発生したディスクと同じパーティションで構成します。それから NetBackup を以前と同じパーティションに再インストールします。

---

障害が発生したディスクの交換、パーティションや論理ボリュームの構築およびオペレーティングシステムの再インストールに関する特定の手順は、複雑で時間がかかる可能性があります。このマニュアルでは、このような手順については説明しません。ベンダーごとに該当する情報を参照してください。

## ディザスタリカバリの要件について

Veritas では、災害後にディザスタリカバリモードで **NetBackup** をインストールするときに、ディザスタリカバリメールに記載されている利用可能なマスターサーバー名を使用することを強くお勧めします。

---

**メモ:** カタログリカバリ時に、アクティブノードと非アクティブノードの証明書はリカバリされません。そのため、ディザスタリカバリモードで **NetBackup** をインストールした後、再発行トークンを使用してすべてのクラスタノードに証明書を手動で配備する必要があります。

p.245 の「[ディザスタリカバリインストール後にクラスタマスターサーバーで証明書を生成する](#)」を参照してください。

---

すべての環境でディザスタリカバリを成功させるためには、次のことを把握している必要があります。

- ディザスタリカバリパッケージ (.drpkg) ファイルの場所。  
p.215 の「[ディザスタリカバリパッケージ](#)」を参照してください。
- その特定のディザスタリカバリパッケージのパスフレーズ。

パスフレーズを忘れた場合は、次の記事を参照してホスト ID を再取得してください。

<http://www.veritas.com/docs/000125933>

---

**メモ:** 権限のないユーザー (またはサービスユーザー) アカウントを構成している場合は、ディザスタリカバリパッケージが存在するディレクトリに対する書き込みアクセス権がサービスアカウントに割り当て済みであることを確認します。

サービスユーザーアカウントについて詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

---

### 外部 CA が署名した証明書を使用している NetBackup ドメイン

NetBackup ドメインで、ホストとの通信に外部 CA が署名した証明書を使用している場合は、ディザスタリカバリインストールを開始する前に、次を確認してください。

- 必要な証明書失効リスト (CRL) を構成した。
- カタログのバックアップ中にバックアップされていない場合は、Windows 証明書ストア内の有効な外部証明書をコピーした。

---

**メモ:** NetBackup では、マスターサーバーのディザスタリカバリのプッシュ、リモート、またはサイレントインストールはサポートされません。例外: NetBackup マスターサーバークラスタ内のホストでは、これらのインストール方法が NetBackup でサポートされます。

---

## ディザスタリカバリパッケージ

セキュリティ向上のため、各カタログがバックアップされる際にディザスタリカバリパッケージが作成されます。ディザスタリカバリパッケージファイルの拡張子は .drpkg です。

ディザスタリカバリ (DR) パッケージには、マスターサーバーホストの識別情報が保存されます。このパッケージは、災害発生後にマスターサーバーの識別情報を NetBackup に再取得させるために必要です。ホストの識別情報をリカバリすると、カタログリカバリを実行できます。

ディザスタリカバリパッケージには、次の情報が含まれます。

- マスターサーバー証明書と NetBackup 認証局 (CA) 証明書の、NetBackup CA が署名した証明書と秘密鍵
- ドメイン内のホストについての情報
- セキュリティ設定
- 外部 CA が署名した証明書  
外部 CA が署名した Windows 証明書ストアからの証明書 (該当する場合)
- 外部 CA が署名した証明書に固有の NetBackup 構成オプション
- キーマネージメントサービス (KMS) 構成

---

**メモ:** デフォルトでは、KMS 構成はカタログバックアップ時にバックアップされません。カタログバックアップ時に、KMS 構成をディザスタリカバリパッケージの一部として含めるには、KMS\_CONFIG\_IN\_CATALOG\_BKUP 構成オプションを 1 に設定します。

---

---

**メモ:** カatalogバックアップが成功するようにディザスタリカバリパッケージのパスフレーズを設定する必要があります。

---

p.216 の「[ディザスタリカバリ設定について](#)」を参照してください。

## ディザスタリカバリ設定について

セキュリティ向上のため、各カタログがバックアップされる際にディザスタリカバリパッケージが作成されます。

p.215 の「[ディザスタリカバリパッケージ](#)」を参照してください。

ディザスタリカバリパッケージは、各カタログのバックアップの際に作成され、ユーザーが設定するパスワードで暗号化されます。災害発生後に **NetBackup** をマスターサーバーにディザスタリカバリモードでインストールする際は、この暗号化パスワードを入力する必要があります。

[ディザスタリカバリ (Disaster Recovery)] タブには以下のオプションが表示されます。

表 4-1 ディザスタリカバリの設定

設定	説明
パスワード	ディザスタリカバリパッケージを暗号化するパスワードを入力します。 <ul style="list-style-type: none"><li>デフォルトでは、パスワードを 8 ～ 1024 文字で指定する必要があります。</li></ul> <code>nbseccmd -setpassphraseconstraints</code> コマンドオプションを使用して、パスワードの制約を設定できます。 <ul style="list-style-type: none"><li>既存のパスワードと新しいパスワードは異なるものにする必要があります。</li><li>パスワードでサポートされる文字は、空白、大文字 (A-Z)、小文字 (a-z)、数字 (0-9)、および特殊文字のみです。特殊文字には、<code>~!@#\$%^&amp;*()_+-='{}[] :;'. /? &lt;&gt;"</code> が含まれます。</li></ul>
パスワードの確認	確認のため、パスワードを再入力します。

**注意:** パスワードにサポート対象の文字のみが含まれていることを確認します。サポートされていない文字を入力した場合、ディザスタリカバリパッケージのリストア中に問題が発生する可能性があります。パスワードは検証されないことがあり、ディザスタリカバリパッケージをリストアできなくなる可能性があります。

### ディザスタリカバリパッケージの暗号化パスワードを変更する際の注意

- パスワード変更以降のディザスタリカバリパッケージは、ユーザーが設定した新しいパスワードで暗号化されます。

- パスフレーズを変更しても、以前のディザスタリカバリのパッケージでは変更されません。新しいディザスタリカバリパッケージのみが新しいパスフレーズに関連付けられます。
- 災害発生後に **NetBackup** をマスターサーバーにディザスタリカバリモードでインストールする際に入力するパスフレーズは、マスターサーバーのホスト ID のリカバリ元であるディザスタリカバリパッケージのパスフレーズに対応する必要があります。

## バックアップに関する推奨事項

次のバックアップ方法が推奨されます。

バックアップを行うファイルの選択  
ファイルを定期的にバックアップすることに加えて、バックアップ対象のファイルを正しく選択することが重要です。ユーザーおよび組織にとって重要な記録情報が含まれるすべてのファイルをバックアップ対象にします。システムファイルおよびアプリケーションファイルをバックアップします。これによって、障害が発生した場合、迅速かつ正確にシステムのリストアを行い、通常の操作に戻すことができます。

バックアップの対象には、**Windows** のすべてのシステムファイルを含めます。他のシステムソフトウェアに加えて、**Windows** システムディレクトリにはリストア時にクライアントを元の構成に戻すために必要なレジストリが含まれています。クライアントに **NetBackup** のエクスクルードリストを使用する場合、リストには **Windows** のどのシステムファイルも指定しないでください。

実行可能ファイルと他のアプリケーションファイルは省略しないでください。簡単に再インストールできるこれらのファイルを除くことによってテープを節約することもできます。ただし、アプリケーション全体のバックアップを行うことによって、アプリケーションは完全に同じ構成にリストアされます。たとえば、ソフトウェアの更新版またはパッチを適用した場合、バックアップからリストアを行うことによって、それらを再適用する必要がなくなります。

### Bare Metal Restore

**NetBackup Bare Metal Restore (BMR)** は、クライアントシステムを **BMR** 保護用に構成されたポリシーを使用してバックアップすることによって保護します。**BMR** バックアップおよびリカバリ手順の詳細な説明が利用可能です。

『**NetBackup Bare Metal Restore 管理者ガイド**』を参照してください。

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

### クリティカルポリシー

オンラインカタログバックアップ用のポリシーを構成する場合、特定の **NetBackup** ポリシーをクリティカルポリシーとして指定します。クリティカルポリシーでは、エンドユーザー操作に対してクリティカルと見なされるシステムおよびデータをバックアップします。カタログのリカバリ中に、**NetBackup** によって、クリティカルポリシーのリストアに必要なすべてのメディアが利用可能であることが確認されます。

- カタログリカバリ後の完全バックアップ
- 増分バックアップの構成に[アーカイブビットに基づいて、増分バックアップを実行する (Perform Incrementals based on archive bit)]が設定されている Windows クライアントが含まれている場合、カタログリカバリ後にできるだけ早くこれらのクライアントの完全バックアップを実行します。カタログリカバリに使われたカタログバックアップの実行後に増分バックアップされたファイルで、アーカイブビットがリセットされます。カタログリカバリ後にこれらのクライアントの完全バックアップが実行されていない場合、これらのファイルがスキップされ、後続の増分バックアップによってバックアップが行われない場合があります。
- オンラインカタログバックアップ
- オンラインホットカタログバックアップは、ポリシーに基づいたバックアップであり、複数テープにまたがったバックアップおよび増分バックアップをサポートします。このバックアップにより、バックアップ、アーカイブおよびリストインターフェースからカタログファイルをリストアできます。オンラインカタログバックアップは、NetBackup での他の処理中に実行できるため、バックアップ処理が継続的に行われている環境のサポートが強化されます。
- オンラインカタログバックアップのディザスタリカバリファイル
- オンラインカタログバックアップで作成されたディザスタリカバリファイルは、ネットワーク共有またはリムーバブルデバイスに保存することをお勧めします。ディザスタリカバリファイルは、ローカルコンピュータに保存しないでください。オンラインカタログバックアップからのカタログリカバリでは、ディザスタリカバリイメージファイルがないと、手順がより複雑になり、時間がかかります。
- 自動リカバリ
- カタログのディザスタリカバリファイルは、オンラインカタログバックアップ時に作成され、NetBackup リカバリの処理を自動化するために使用されます。最初にバックアップを作成したシステム以外のシステムでリカバリを実行する場合、元のシステムと同じ構成のシステムを使用する必要があります。たとえば、リカバリを実行するシステムに、バックアップを作成した NetBackup サーバーと同じ名前の NetBackup サーバーが含まれている必要があります。そうでなければ、自動リカバリは成功しないことがあります。

オンラインカタログのディザスタ  
リカバリ情報電子メール

組織内の **NetBackup** 管理者にディザスタリカバリ情報のコピーを電子メールで送信するようにオンラインカタログバックアップポリシーを構成します。各カタログバックアップの一部としてこのポリシーを構成します。ディザスタリカバリ情報の電子メールをローカルコンピュータに保存しないでください。ディザスタリカバリイメージファイルやディザスタリカバリ情報電子メールを利用できない場合、カタログリカバリは非常に複雑になり、時間がかかるうえ、支援が必要となります。

**NetBackup** は、次のイベント発生時にディザスタリカバリファイルを電子メールで送信します。

- カatalogがバックアップされた場合。
- カatalogバックアップが重複している、または複製された場合。
- プライマリカatalogバックアップまたはカatalogバックアップのコピーの期限が自動的に切れた、または手動で期限切れにした場合。
- カatalogバックアップのプライマリコピーは次のように変更されます。
  - `bpchangeprimary` コマンドを使用します。
  - カatalogバックアップが手動で複製される場合はプライマリコピーを変更するオプションを使用します。

`mail_dr_info` 通知スクリプトを使ってディザスタリカバリ電子メール処理をカスタマイズできます。詳細が利用可能です。

『**NetBackup** 管理者ガイド Vol. 2』を参照してください。

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

電子メールを設定した後も電子メール経由でディザスタリカバリパッケージを受信できない場合は、次のことを確認してください。

- 電子メール交換サーバーで添付ファイルのサイズがディザスタリカバリパッケージサイズ以上に設定されている。パッケージのサイズ (`.drpkg` ファイルのサイズ) は、カatalogバックアップポリシーで指定したディザスタリカバリファイルの場所で確認できます。
- 環境内のファイアウォールとウイルス対策ソフトウェアで、`.drpkg` の拡張子 (ディザスタリカバリパッケージファイルの拡張子) のファイルが許可されている。
- 電子メール通知アプリケーションとして **BLAT** を使用する場合は、**v2.4** 以降のバージョンである。

正しいカatalogバックアップの識別

リカバリに適切なカatalogバックアップを識別し、使うことを確認します。たとえば、最新のバックアップからリカバリする場合は、最新のバックアップからのカatalogを使います。同様に、特定の時点からリカバリする場合は、その特定の時点のカatalogバックアップを使います。

カatalogリカバリ時間

カatalogのリカバリに必要な時間は、システム環境、カatalogサイズ、場所、バックアップ構成 (完全および増分ポリシースケジュール) などによって決定されます。目標とするカatalogリカバリ時間に適したカatalogバックアップ方式を決定するには、慎重な計画に基づいてテストを行います。

マスターサーバーおよびメディアサーバーのバックアップ

**NetBackup** カatalogバックアップは構成データとカatalogデータを保護します。**NetBackup** インストールのマスターサーバーとメディアサーバーのバックアップスケジュールを設定します。これらのスケジュールは、オペレーティングシステム、デバイス構成およびサーバー上の他のアプリケーションを保護します。

システムディスクが失われた場合のマスターサーバーまたはメディアサーバーのリカバリ手順では、サーバーがカatalogバックアップとは別にバックアップされていることを想定しています。マスターサーバーとメディアサーバーのバックアップには、**NetBackup** バイナリ、構成ファイル、カatalogファイルまたはリレーショナルデータベースのデータを含めないでください。

## UNIX および Linux のディスクリカバリ手順について

UNIX と Linux の 3 種類の異なるディスクリカバリは次のとおりです。

- マスターサーバーのディスクリカバリ手順  
p.220 の「**UNIX および Linux のマスターサーバーのディスクリカバリ**」を参照してください。
- メディアサーバーのディスクリカバリ手順  
p.227 の「**UNIX の NetBackup メディアサーバーのディスクリカバリについて**」を参照してください。
- クライアントのディスクリカバリ手順  
p.227 の「**UNIX クライアントワークステーションのシステムディスクのリカバリ**」を参照してください。

**AdvancedDisk** または **OpenStorage** ディスク上に存在するディスクベースのイメージは、**NetBackup** カatalogを使用してリカバリすることはできません。これらのディスクイメージは、**NetBackup** のインポート機能を使用してリカバリする必要があります。インポートについては、次を参照してください。

『**NetBackup 管理者ガイド Vol. 1**』の **NetBackup** イメージのインポートに関するトピックを参照してください。

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

**NetBackup** では、ディスクイメージのインポート時に、そのイメージの元のカatalogエントリはリカバリされません。代わりに、新しいカatalogエントリが作成されます。

## UNIX および Linux のマスターサーバーのディスクリカバリ

UNIX 版または Linux 版 **NetBackup** マスターサーバーのシステムディスクに障害が発生した場合に、データのリカバリする方法について、以下の 2 つの手順で説明します。

- ルートファイルシステムが消失していない場合。オペレーティングシステム、**NetBackup** ソフトウェアおよび他のいくつか(すべてではなく)のファイルが消失したと想定される場合。

p.221の「ルートが消失していない場合のマスターサーバーのリカバリ」を参照してください。

- ルートファイルシステム、およびディスク上の他のすべてのファイルが消失している場合。この場合、完全なリカバリが必要です。このリカバリでは、代替ブートディスクにオペレーティングシステムを再ロードし、リカバリ時にこのディスクから起動します。リストア中にオペレーティングシステムで使用するファイルを上書きするので、システムがクラッシュすることなく、ルートのパーティションをリカバリできます。

p.224の「ルートパーティションが消失した場合のマスターサーバーのリカバリ」を参照してください。

**NetBackup** マスターサーバーおよびメディアサーバーでは、**NetBackup** カタログのディレクトリ場所が、**NetBackup** カタログバックアップにおいて非常に重要です。**NetBackup** カタログのリカバリでは、**NetBackup** ソフトウェアの再インストール中に同一のディレクトリパスまたはディレクトリ場所を作成する必要があります。ディスクのパーティション化、シンボリックリンクおよび**NetBackup** カタログの再配置ユーティリティが必要なことがあります。

**NetBackup Bare Metal Restore (BMR)** は、クライアントシステムを **BMR** 保護用に構成されたポリシーを使用してバックアップすることによって保護します。**BMR** バックアップおよびリカバリの手順を説明する情報を参照できます。

『**NetBackup Bare Metal Restore** 管理者ガイド UNIX、Windows および Linux』を参照してください。

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

## ルートが消失していない場合のマスターサーバーのリカバリ

次の手順では、オペレーティングシステムを再ロードし、**NetBackup** のリストアを行って、その後で他のすべてのファイルのリストアを行うことによって、マスターサーバーをリカバリします。

### ルートが消失していない場合にマスターサーバーをリカバリする方法

- 1 オペレーティングシステムが正常に動作していること、必要なパッチがインストールされていること、および固有の構成設定が行われていることを確認します。必要に応じて修正します。
- 2 リカバリするサーバーに、NetBackup ソフトウェアを再インストールします。  
手順については、『NetBackup インストールガイド』を参照してください。

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

---

**メモ:** NetBackup Web サービスでは、NetBackup カタログのバックアップを作成したときに使用したものと同一ユーザーアカウントとクレデンシャルを使う必要があります。詳細情報を参照できます。

<http://www.veritas.com/docs/000081350>

---

**メモ:** NetBackup カタログのバックアップを作成したときに使用したものと同一サービスユーザーアカウントを使う必要があります。

サービスユーザーアカウントについて詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

- 3 以前インストールされていた NetBackup のパッチをインストールします。パッチソフトウェアに添付されているマニュアルを参照してください。

---

**メモ:** Veritas は NetBackup の以前のバージョンを使用してバックアップを作成したカタログイメージのリカバリをサポートしません。

- 4 NetBackup カタログバックアップに反映されるような変更をデフォルトのカタログディレクトリに加えた場合は、カタログリカバリの前にディレクトリを作成し直します。

次に例を示します。

- NetBackup カタログディレクトリ構造の一部にシンボリックリンクを使用した場合。
- NetBackup の `nbdb_move` コマンドを使用して NetBackup リレーショナルデータベースカタログの一部を再配置した場合。

- 5 リカバリの一部として、ポリシーまたはカタログバックアップのリストアを行う場合は、適切なリカバリデバイスを構成する必要があります。これには、次の作業が必要となる場合があります。

- リストアするディスクのバックアップ (NetBackup カタログと通常のバックアップ) を読み込むデバイスのロボットソフトウェアのインストールと設定。これらのバック

アップが非ロボットドライブで読み込み可能な場合、ロボットは必要ありません。ただし、複数のメディアが必要な場合は、手動で操作する必要があります。『NetBackup デバイス構成ガイド UNIX、Windows および Linux』を参照してください。

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

- NetBackup [デバイスの構成 (Device Configuration)] ウィザードを使用した、NetBackup のリカバリデバイスの検出および構成。  
『NetBackup 管理者ガイド Vol. 1』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
  - NetBackup コマンド `tpautoconf` を使用した NetBackup のリカバリデバイスの検出と設定。  
『NetBackup コマンドリファレンスガイド』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
  - デバイスマッピングファイルの更新。  
『NetBackup 管理者ガイド Vol. 1』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- 6 メディアに作成したポリシーバックアップまたはカタログバックアップからリストアする必要がある場合は、NetBackup で適切なメディアの設定が必要な場合があります。『NetBackup 管理者ガイド Vol. 1』を参照してください。

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

メディアを構成するには、次のタスクのいくつかまたはすべてが必要になることがあります。

- スタンドアロンリカバリデバイスへの必要なメディアの手動によるロード。
  - `robtest` やベンダー固有のロボット制御ソフトウェアなどの NetBackup ユーティリティを使用した、必要なリカバリデバイスへのメディアのロード。
  - NetBackup のボリュームの構成ウィザードを使った、ロボットデバイスのメディアの内容に対するインベントリ処理。
  - ベンダー固有のロボット制御ソフトウェアを使用した、必要なリカバリデバイスへのメディアのロード。
- 7 NetBackup カタログをリカバリします。

NetBackup カタログは、バックアップ時と同じディレクトリ構造に対してのみリカバリできます (代替パスへのリカバリはできません)。

p.254 の「NetBackup カタログのリカバリについて」を参照してください。

- すべての NetBackup デーモンを停止して、再起動します。次に示す NetBackup コマンド、または NetBackup 管理コンソールの [アクティビティモニター (Activity Monitor)] を使用します。

```
/usr/opensv/netbackup/bin/bp.kill_all  
/usr/opensv/netbackup/bin/bp.start_all
```

- NetBackup のバックアップ、アーカイブおよびリストアインターフェースを起動 (または bp コマンドを使用) し、必要に応じてサーバーに他のファイルのリストアを行います。ファイルのリストアが終了したら、完了です。

## ルートパーティションが消失した場合のマスターサーバーのリカバリ

次の手順では、ルートファイルシステムおよびディスク上の他のすべてのデータが消失した場合を想定しています。このリカバリでは、代替ブートディスクにオペレーティングシステムを再ロードし、リカバリ時にこのディスクから起動します。リストア中にオペレーティングシステムで使用するファイルを上書きするので、システムがクラッシュすることなく、ルートのパーティションをリカバリできます。

### ルートパーティションが消失した場合にマスターサーバーをリカバリする方法

- その種類のサーバーで通常実行する場合と同じ手順で、代替ブートディスク上にオペレーティングシステムをロードします。
- 元のディスクで NetBackup、NetBackup カタログ (該当する場合)、およびデータベースが格納されていたパーティションおよびディレクトリを代替ディスクに作成します。デフォルトでは、`/usr/opensv` ディレクトリに格納されています。
- オペレーティングシステムが正常に動作していること、必要なパッチがインストールされていること、および固有の構成設定が行われていることを確認します。必要に応じて修正します。
- 代替ディスクに NetBackup をインストールします。リストアを行っているディスクのバックアップ (NetBackup カタログのバックアップおよび通常のバックアップ) を読み込むために必要なデバイスのロボットソフトウェアだけをインストールします。これらのバックアップが非ロボットドライブで読み込み可能な場合、ロボットは必要ありません。

---

**メモ:** NetBackup Web サービスでは、NetBackup カタログのバックアップを作成したときに使用したものと同一ユーザーアカウントとクレデンシャルを使う必要があります。詳しくは以下の URL を参照してください。

<http://www.veritas.com/docs/000081350>

---

- 以前インストールされていた NetBackup のパッチをインストールします。パッチソフトウェアに添付されているマニュアルを参照してください。

- 6 カタログディレクトリが **NetBackup** カタログバックアップのカタログディレクトリと異なる場合は、カタログをリカバリする前にディスク上でそのディレクトリ構造を作成し直します。

次に例を示します。

- **NetBackup** カタログディレクトリ構造の一部にシンボリックリンクを使用した場合。
- **NetBackup** の `nbdb_move` コマンドを使用して **NetBackup** リレーショナルデータベースカタログの一部を再配置した場合。

- 7 リカバリの一部として、ポリシーまたはカタログバックアップのリストアを行う場合は、適切なリカバリデバイスを構成する必要があります。

デバイス構成には、次の作業が含まれることがあります。

- リストアするディスクのバックアップ (**NetBackup** カタログと通常のバックアップ) を読み込むデバイスのロボットソフトウェアのインストールと設定。これらのバックアップが非ロボットドライブで読み込み可能な場合、ロボットは必要ありません。ただし、複数のメディアが必要な場合は、手動で操作する必要があります。『**NetBackup** デバイス構成ガイド UNIX、Windows および Linux』を参照してください。

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

- **NetBackup** [デバイスの構成 (Device Configuration)] ウィザードを使用した、**NetBackup** のリカバリデバイスの検出および構成。

『**NetBackup** 管理者ガイド Vol. 1』を参照してください。

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

- **NetBackup** コマンド `tpautoconf` を使用した **NetBackup** のリカバリデバイスの検出と設定。

『**NetBackup** コマンドリファレンスガイド』を参照してください。

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

- デバイスマッピングファイルの更新。

『**NetBackup** 管理者ガイド Vol. 1』を参照してください。

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

- 8 メディアに対してバックアップを行ったポリシーバックアップまたはカタログバックアップからリストアを行う必要がある場合は、**NetBackup** で適切なメディアが構成されていることが必要な場合があります。

『**NetBackup** 管理者ガイド Vol. 1』を参照してください。

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

メディアを構成するには、次のタスクのいくつかまたはすべてが必要になることがあります。

- スタンドアロンリカバリデバイスへの必要なメディアの手動によるロード。

- `robtest` やベンダー固有のロボット制御ソフトウェアなどの **NetBackup** ユーティリティを使用した、必要なリカバリデバイスへのメディアのロード。
- **NetBackup** のボリュームの構成ウィザードを使った、ロボットデバイスのメディアの内容に対するインベントリ処理。
- ベンダー固有のロボット制御ソフトウェアを使用した、必要なリカバリデバイスへのメディアのロード。

**9** 代替ディスクへ **NetBackup** カタログをリカバリします。

p.254 の「**NetBackup** カタログのリカバリについて」を参照してください。

カタログは、バックアップ時と同じディレクトリ構造に対してだけリカバリできます (代替パスへのリカバリはできません)。

**10** **NetBackup** のバックアップ、アーカイブおよびリストアインターフェース (または `bp コマンド`) を起動します。すべてのファイルの最新バックアップをリストアします。

これらのファイルは、(**NetBackup** カタログバックアップではなく) マスターサーバーのバックアップからリストアします。リカバリするディスクを代替のリカバリ場所として指定してください。

---

**警告:** `/usr/opensv/var` ディレクトリ、`/usr/opensv/db/data` ディレクトリまたは `/usr/opensv/volmgr/database` ディレクトリ (あるいはそれらが再配置された場所) や、**NetBackup** データベースデータを含むディレクトリには、ファイルをリストアしないでください。このデータは手順 **9** で代替ディスクにリカバリされ、手順 **12** でリカバリディスクに再びコピーされます。

---

**11** 代替ディスクの **NetBackup** から起動したすべての **NetBackup** プロセスを停止します。**NetBackup** 管理コンソールの [アクティビティモニター (Activity Monitor)] を使用するか、次のコマンドを実行します。

```
/usr/opensv/netbackup/bin/bp.kill_all
```

**12** 同じディレクトリ構造を保持し、**NetBackup** カタログを代替ディスクからリカバリするディスクにコピーします。これは、手順 **9** でリカバリを行ったカタログです。

**13** リカバリ済みのディスクを、ブートディスクに再設定して、システムを再起動します。

- 14 リカバリを行ったディスク上の NetBackup を起動し、テストします。

```
/usr/opensv/netbackup/bin/bp.start_all
```

NetBackup 管理ユーティリティを使用してみます。また、バックアップおよびリストアも数回実行してみます。

- 15 リカバリが完了したことを確認したら、代替ディスクから NetBackup ファイルを削除します。または、ディスクがスペアの場合、そのディスクを切り離します。

## UNIX の NetBackup メディアサーバーのディスクリカバリについて

NetBackup 6.0 以上のメディアサーバーでは、NetBackup リレーショナルデータベースに情報が格納されます。NetBackup メディアサーバーのシステムディスクをリカバリする必要がある場合は、クライアントのディスクリカバリ手順と同様の手順をお勧めします。

p.227 の「UNIX クライアントワークステーションのシステムディスクのリカバリ」を参照してください。

## UNIX クライアントワークステーションのシステムディスクのリカバリ

次の手順では、オペレーティングシステムを再ロードし、NetBackup クライアントソフトウェアをインストールして、他のすべてのファイルをリストアすることによって、クライアントをリカバリします。この手順ではホスト名が変更されないことを前提にしています。

### クライアントワークステーションのシステムディスクをリカバリする方法

- 1 その種類のオペレーティングシステムのクライアントワークステーションで通常実行する場合と同じ方法で、オペレーティングシステムをインストールします。
- 2 NetBackup クライアントソフトウェアおよびパッチをインストールします。
- 3 NetBackup のバックアップ、アーカイブおよびリストアインターフェースを使用して、ユーザーファイルの選択およびリストアを行います。

## UNIX および Linux のクラスタ化された NetBackup サーバーのリカバリについて

NetBackup サーバークラスタは、カタログの破損、共有ディスクの消失、またはクラスタ全体の消失を防ぎません。定期的なカタログバックアップを実行する必要があります。クラスタ環境でのカタログバックアップとシステムバックアップのポリシーの構成に関する詳細情報が利用可能です。

『NetBackup High Availability ガイド』を参照してください。

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

次の表では、エラーのシナリオおよびリカバリ手順のポイントについて説明します。

警告: このトピックのリカバリ手順を試す前に、テクニカルサポートにご連絡ください。

表 4-2 クラスタエラーおよびリカバリのシナリオ

シナリオ	手順
ノードエラー	p.228 の「UNIX クラスタまたは Linux クラスタでの障害が発生したノードの置き換え」を参照してください。
共有ディスクエラー	p.230 の「UNIX クラスタまたは Linux クラスタ全体のリカバリ」を参照してください。
クラスタエラー	p.230 の「UNIX クラスタまたは Linux クラスタ全体のリカバリ」を参照してください。

## UNIX クラスタまたは Linux クラスタでの障害が発生したノードの置き換え

NetBackup リソースグループをオンラインおよびオフラインにする方法について、クラスタテクノロジー固有の情報が利用可能です。また、NetBackup リソースグループをフリーズおよびアンフリーズする (つまり、監視を無効化および有効化する) 方法についての情報も利用できます。

『NetBackup High Availability ガイド』の NetBackup の設定に関するトピックを参照してください。

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

次の手順は、共有ディスクと少なくとも 1 つの構成されたクラスタノードが利用可能な場合に適用されます。

### UNIX クラスタまたは Linux クラスタで障害が発生したノードを置き換える方法

- 1 置き換え用のノードで、ハードウェア、システムソフトウェアおよびクラスタ環境を構成します。
- 2 デバイス構成が残りのノードの構成と一致することを確認します。
- 3 交換用のノードに NetBackup をインストールする前に、NetBackup リソースグループがすべてのノードでオフラインであることを確認します。
- 4 NetBackup 共有ディスクが NetBackup がインストールされるノードにマウントされていないことを確認します。
- 5 NetBackup サービスをフリーズします。

- 6 新しいノードまたは交換ノードに **NetBackup** を再インストールします。**NetBackup** 仮想名を **NetBackup** サーバーの名前として使用してください。**NetBackup** サーバーソフトウェアのインストールに関する指示に従ってください。

『**NetBackup** インストールガイド』を参照してください。

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

---

**メモ:** **NetBackup Web** サービスでは、クラスタの他のノードで使用したものと同じユーザーアカウントとクレデンシャルを使う必要があります。詳しくは以下の URL を参照してください。

<http://www.veritas.com/docs/000081350>

---

- 7 新しくインストールされたノードを他のクラスタノードと同じパッチレベルにするために必要な **Maintenance Pack** およびパッチをインストールします。
- 8 新たにインストールされたノード以外のノードで、**NetBackup** リソースグループをオンラインにします。
- 9 **NetBackup** リソースグループがオンラインであるノードにログオンし、次のコマンドを実行します。

```
/usr/opensv/netbackup/bin/cluster/cluster_config -s nbu -o  
add_node -n node_name
```

*node\_name* は、新たにインストールされたノードの名前です。

- 10 **NetBackup** リソースグループを交換用のノードに切り替えます。
- 11 **NetBackup** グループをフリーズします。
- 12 オペレーティングシステムに必要な適切な低レベルのテープデバイスとロボット制御デバイスの構成が実行されたことを確認します。オペレーティングシステムの情報が利用可能です。

『**NetBackup** デバイス構成ガイド UNIX、Windows および Linux』を参照してください。

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

- 13 [デバイス構成ウィザード (**Device Configuration Wizard**)]を実行して、デバイスを構成します。既存のノードでデバイス構成を再実行する必要はありません。特定のクラスタの構成情報が利用可能です。

『**NetBackup** 管理者ガイド Vol. 1』を参照してください。

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

- 14 各ロボットのロボット番号とロボットドライブ番号がクラスタのすべてのノードで一致していることを確認します。ロボットに接続されている他のサーバーに対してこの手順を繰り返し、必要に応じて修正します。

『NetBackup 管理者ガイド Vol. 1』を参照してください。

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

- 15 交換用のノードで構成したデバイスを使用して、NetBackup がリストアを実行できるかどうかをテストします。

- 16 NetBackup リソースグループをアンフリーズします。

## UNIX クラスタまたは Linux クラスタ全体のリカバリ

次の手順は、最初から作成し直す必要があるクラスタ化された NetBackup サーバー環境に適用されます。

続行する前に、有効なオンラインカタログバックアップがあることを確認します。

### UNIX クラスタまたは Linux クラスタ全体をリカバリする方法

- 1 交換クラスタのハードウェア、システムソフトウェアおよびクラスタ環境を構成します。
- 2 オペレーティングシステムに必要な適切な低レベルのテープデバイスとロボット制御デバイスの構成が実行されたことを確認します。

『NetBackup デバイス構成ガイド UNIX、Windows および Linux』を参照してください。

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

- 3 クラスタノードのそれぞれに NetBackup を再インストールします。NetBackup 仮想名を NetBackup サーバーの名前として使用してください。NetBackup サーバーソフトウェアのインストールに関する指示に従ってください。

『NetBackup インストールガイド』を参照してください。

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

---

**メモ:** NetBackup Web サービスでは、NetBackup カタログのバックアップを作成したときに使用したものと同一ユーザーアカウントとクレデンシャルを使う必要があります。詳しくは以下の URL を参照してください。

<http://www.veritas.com/docs/000081350>

---

- 4 クラスタ化された NetBackup サーバーを構成します。  
『NetBackup High Availability 管理者ガイド UNIX、Windows および Linux』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- 5 新しくインストールされた NetBackup サーバーを、置き換えるサーバーと同じパッチレベルにするために必要な Maintenance Pack およびパッチをインストールします。
- 6 NetBackup サーバーソフトウェアのインストールに関する指示に従ってください。  
p.221 の「ルートが消失していない場合のマスターサーバーのリカバリ」を参照してください。
- 7 各ノードの NetBackup リソースグループを順番に有効にし、デバイスの構成ウィザードを実行してデバイスを構成します。  
特定のクラスタの構成情報が利用可能です。  
『NetBackup インストールガイド』を参照してください。  
<http://www.veritas.com/docs/DOC5332>

## Windows のディスクリカバリ手順について

Windows の 3 種類の異なるディスクリカバリは次のとおりです。

- マスターサーバーのディスクリカバリ手順  
p.232 の「Windows のマスターサーバーのディスクリカバリについて」を参照してください。
- メディアサーバーのディスクリカバリ手順  
p.238 の「Windows の NetBackup メディアサーバーのディスクリカバリについて」を参照してください。
- クライアントのディスクリカバリ手順  
p.238 の「Windows クライアントのディスクリカバリ」を参照してください。

AdvancedDisk または OpenStorage ディスク上に存在するディスクベースのイメージは、NetBackup カタログを使用してリカバリすることはできません。これらのディスクイメージは、NetBackup のインポート機能を使用してリカバリする必要があります。インポートの情報に関しては、次のマニュアルの NetBackup イメージのインポートに関する項を参照してください。

『NetBackup 管理者ガイド Vol. 1』を参照してください。

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

---

**メモ:** NetBackup では、ディスクイメージのインポート時に、そのイメージの元のカタログエントリはリカバリされません。代わりに、新しいカタログエントリが作成されます。

---

## Windows のマスターサーバーのディスクリカバリについて

この項では、Windows 版 NetBackup マスターサーバーで 1 つ以上のディスクパーティションが消失した場合に、データのリカバリする手順について説明します。

次の 2 つの場合について説明します。

- Windows は完全な状態であり、破損していない場合。システムで Windows は起動されますが、他のすべてまたはいくつかのパーティションが消失しています。NetBackup ソフトウェアは消失しているとします。  
p.232 の「[Windows が完全な状態である場合のマスターサーバーのリカバリ](#)」を参照してください。
- すべてのディスクパーティションが消失している場合。Windows は再インストールする必要があります。これは完全なリカバリです。これらの手順では、NetBackup マスターディスクで、サポートされている Windows が実行されていたこと、および欠陥のあるハードウェアが交換済みであることを前提としています。  
p.235 の「[マスターサーバーおよび Windows のリカバリ](#)」を参照してください。

NetBackup マスターサーバーおよびメディアサーバーでは、NetBackup カタログのディレクトリ場所が、NetBackup カタログバックアップにおいて非常に重要です。NetBackup カタログのリカバリでは、カタログリカバリする前に同一のディレクトリパスまたはディレクトリ場所を作成する必要があります。

## Windows が完全な状態である場合のマスターサーバーのリカバリ

この手順では、Windows オペレーティングシステムが完全な状態である NetBackup マスターサーバーをリカバリする方法を示します。

### Windows が完全な状態であるマスターサーバーをリカバリする方法

- 1 以前 NetBackup がインストールされていた `install_path` を確認してください。デフォルトでは、NetBackup は `C:\Program Files\VERITAS` ディレクトリにインストールされています。
- 2 NetBackup カタログリカバリで、ディレクトリパスまたはディレクトリ場所を作成する必要があるかどうかを確認します。
- 3 リカバリするディスクを、障害が発生する前と同じ状態にパーティション化します (パーティション化が必要な場合)。その後、各パーティションを障害が発生する前と同じ状態にフォーマットします。

- 4 サーバーに NetBackup ソフトウェアを再インストールします。

『NetBackup インストールガイド』を参照してください。

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

---

**メモ:** NetBackup Web サービスでは、NetBackup カタログのバックアップを作成したときに使用したものと同一ユーザーアカウントと資格情報を使う必要があります。詳しくは以下の URL を参照してください。

<http://www.veritas.com/docs/000081350>

---

- 5 以前インストールされていた NetBackup のパッチをインストールします。パッチソフトウェアに添付されているマニュアルを参照してください。
- 6 カタログディレクトリが NetBackup カタログバックアップのカタログディレクトリと異なる場合は、カタログをリカバリする前にディスク上でそのディレクトリ構造を作成し直します。たとえば、NetBackup の `nbdb_move` コマンドを使用して NetBackup リレーショナルデータベースカタログの一部を再配置した場合です。
- 7 リカバリの一部として、ポリシーまたはカタログバックアップのリストアを行う場合は、適切なリカバリデバイスを構成する必要があります。

次の一部またはすべてを実行する必要がある場合があります。

- リストアするディスクのバックアップ (NetBackup カタログと通常のバックアップ) を読み込むデバイスのロボットソフトウェアのインストールと設定。これらのバックアップが非ロボットドライブで読み込み可能な場合、ロボットは必要ありません。ただし、複数のメディアが必要な場合は、手動で操作する必要があります。『NetBackup デバイス構成ガイド UNIX、Windows および Linux』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- [NetBackup デバイスの構成 (Device Configuration)] ウィザードを使用した NetBackup のリカバリデバイスの検出と設定。  
『NetBackup 管理者ガイド Vol. 1』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- NetBackup コマンド `tpautoconf` を使用した NetBackup のリカバリデバイスの検出と設定。  
『NetBackup コマンドリファレンスガイド』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- デバイスマッピングファイルの更新。  
『NetBackup 管理者ガイド Vol. 1』を参照してください。  
<http://www.veritas.com/docs/DOC5332>

- 8 リカバリの一部として、メディアに対して実行されたポリシーバックアップまたはカタログバックアップのリストアを行う場合は、適切なリカバリデバイスを構成する必要があります。

メディアの構成には、次の作業が必要となる場合があります。

- スタンドアロンリカバリデバイスへの必要なメディアの手動によるロード。
- `robtest` やベンダー固有のロボット制御ソフトウェアなどの **NetBackup** ユーティリティを使用した、必要なリカバリデバイスへのメディアのロード。
- **NetBackup** のボリュームの構成ウィザードを使った、ロボットデバイスのメディアの内容に対するインベントリ処理。
- ベンダー固有のロボット制御ソフトウェアを使用した、必要なリカバリデバイスへのメディアのロード。

- 9 **NetBackup** カタログをリカバリします。

p.254 の「**NetBackup** カタログのリカバリについて」を参照してください。

- 10 カタログのリカバリが完了したら、**NetBackup** サービスを停止し、再起動します。次に示す `bpdown` コマンドと `bpup` コマンド、管理コンソールの **NetBackup** [アクティビティモニター (Activity Monitor)] または **Windows** の [管理ツール] の [サービス] を使用します。

```
install_path¥NetBackup¥bin¥bpdown
install_path¥NetBackup¥bin¥bpup
```

---

**警告:** 手順 11 では、`install_path¥NetBackup¥db` ディレクトリ、`install_path¥NetBackupDB` ディレクトリ、`install_path¥NetBackup¥var` ディレクトリまたは `install_path¥Volmgr¥database` ディレクトリに、ファイルのリストアを行わないでください。カタログは手順 9 でリカバリしているため、そのカタログを通常のバックアップで上書きすると、カタログの一貫性が失われる可能性があります。

---

`nbdb_move` を使用して `install_path¥NetBackupDB¥data` から **NetBackup** リレーショナルデータベースファイルが再配置されていた場合は、手順 9 でリカバリされます。手順 11 ではリストアしないでください。

- 11 他のファイルをすべてリストアするには、次の操作を示される順序で実行します。
- マスターサーバー上で **NetBackup** 管理インターフェースを起動します。
  - バックアップ、アーカイブおよびリストアユーティリティを起動します。
  - リストア対象を表示し、消失したパーティションだけを選択します。システムディレクトリ (通常、`C:¥Windows`) を選択します。これによって、すべてのレジストリファイルのリストアが確実に行われます。

- `install_path¥NetBackup¥db` ディレクトリ、`install_path¥NetBackupDB` ディレクトリ、`install_path¥NetBackup¥var` ディレクトリおよび `install_path¥Volmgr¥database` ディレクトリの選択を解除します (手順 10 の「注意」を参照)。
  - Windows を再インストールする場合は、[既存のファイルの上書き (Overwrite existing files)] オプションを選択します。これにより、既存のファイルはバックアップと置き換えられます。
  - リストアを開始します。
- 12 システムを再起動します。これによって、リストアの実行中にビジー状態であったすべてのファイルが置き換えられます。ブートプロセスが完了すると、システムは最新のバックアップ時の状態にリストアされます。

## マスターサーバーおよび Windows のリカバリ

この手順では、Windows のすべてのディスクパーティションが消失したと想定しています。

### マスターサーバーおよび Windows をリカバリする方法

- 1 Windows オペレーティングシステムを、最小構成でインストールします (高速インストールを実行します)。
  - 以前使用していたものと同じ種類およびバージョンの Windows ソフトウェアをインストールします。
  - 障害が発生する前に使用していたパーティションと同じパーティションに Windows をインストールします。
  - 必要なパッチをインストールします。必要に応じて修正します。
  - デフォルトのワークグループを指定します。ドメインのリストアは行わないでください。
  - ハードウェアの操作に必要な、特別なドライバまたは他のソフトウェア (ディスクドライブ固有のドライバなど) をインストールおよび構成します。
  - システムのテープドライブとの通信に必要な SCSI ドライバまたは他のドライバをインストールします。
  - Compaq システムの SSD のロードなど、該当するハードウェア製造元のすべての指示に従います。
  - Windows のインストールが完了したら、システムを再起動します。
- 2 以前 NetBackup がインストールされていた `install_path` を確認してください。デフォルトでは、NetBackup は `C:¥Program Files¥VERITAS` ディレクトリにインストールされています。

- 3 NetBackup カタログリカバリで、ディレクトリパスまたはディレクトリ場所を作成する必要があるかどうかを確認します。
- 4 パーティション化が必要な場合は、リカバリするディスクを、障害が発生する前と同じ状態にパーティション化します。その後、各パーティションを障害が発生する前と同じ状態にフォーマットします。
- 5 リカバリするサーバーに、NetBackup ソフトウェアを再インストールします。この時点では、NetBackup ポリシーまたはデバイスは構成しないでください。

---

**メモ:** NetBackup Web サービスでは、NetBackup カタログのバックアップを作成したときに使用したものと同一ユーザーアカウントと資格情報を使う必要があります。詳しくは以下の URL を参照してください。

<http://www.veritas.com/docs/000081350>

---

- 6 以前インストールされていた NetBackup のパッチをインストールします。パッチソフトウェアに添付されているマニュアルを参照してください。
- 7 カタログディレクトリが NetBackup カタログバックアップのカタログディレクトリと異なる場合は、カタログをリカバリする前にディスク上でそのディレクトリ構造を作成し直します。たとえば、NetBackup の `nbdb_move` コマンドを使用して NetBackup リレーショナルデータベースカタログの一部を再配置した場合です。
- 8 リカバリの一部として、ポリシーまたはカタログバックアップのリストアを行う場合は、適切なリカバリデバイスを構成する必要があります。

次の一部またはすべての作業を実行する必要がある場合があります。

- リストアするディスクのバックアップ (NetBackup カタログと通常のバックアップ) を読み込むデバイスのロボットソフトウェアのインストールと設定。これらのバックアップが非ロボットドライブで読み込み可能な場合、ロボットは必要ありません。ただし、複数のメディアが必要な場合は、手動で操作する必要があります。『NetBackup デバイス構成ガイド UNIX、Windows および Linux』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- NetBackup の [デバイスの構成 (Device Configuration)] ウィザードを使用した、NetBackup のリカバリデバイスの検出および構成。  
『NetBackup 管理者ガイド Vol. 1』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- NetBackup コマンド `tpautoconf` を使用した NetBackup のリカバリデバイスの検出と設定。  
『NetBackup コマンドリファレンスガイド』を参照してください。  
<http://www.veritas.com/docs/DOC5332>

- デバイスマッピングファイルの更新。  
『NetBackup 管理者ガイド Vol. 1』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- 9 メディアに対してバックアップを行ったポリシーバックアップまたはカタログバックアップからリストアを行う必要がある場合は、NetBackup で適切なメディアが構成されていることが必要な場合があります。

『NetBackup 管理者ガイド Vol. 1』を参照してください。

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

メディアを構成するとき、次の一部またはすべてを実行する必要がある場合があります。

- スタンドアロンリカバリデバイスへの必要なメディアの手動によるロード。
  - `robtest` やベンダー固有のロボット制御ソフトウェアなどの NetBackup ユーティリティを使用した、必要なリカバリデバイスへのメディアのロード。
  - NetBackup のボリュームの構成ウィザードを使った、ロボットデバイスのメディアの内容に対するインベントリ処理。
  - ベンダー固有のロボット制御ソフトウェアを使用した、必要なリカバリデバイスへのメディアのロード。
- 10 NetBackup カタログをリカバリします。
- p.254 の「[NetBackup カタログのリカバリについて](#)」を参照してください。
- 11 カタログのリカバリが完了したら、NetBackup サービスを停止し、再起動します。次に示す `bpdown` コマンドと `bpup` コマンド、管理コンソールの NetBackup [アクティビティモニター (Activity Monitor)] または Windows の [管理ツール] の [サービス] を使用します。

```
install_path¥NetBackup¥bin¥bpdown
```

```
install_path¥NetBackup¥bin¥bpup
```

---

**警告:** 手順 12 では、`install_path¥NetBackup¥db` ディレクトリ、`install_path¥NetBackupDB` ディレクトリ、`install_path¥NetBackup¥var` ディレクトリまたは `install_path¥Volmgr¥database` ディレクトリに、ファイルのリストアを行わないでください。これらのディレクトリは手順 10 でリカバリしているため、そのディレクトリを通常のバックアップで上書きすると、カタログの一貫性が失われる可能性があります。 `nldb_move` を使用して `install_path¥NetBackupDB¥data` からリレーショナルデータベースファイルが再配置されていた場合は、手順 10 でリカバリされます。手順 12 ではリストアしないでください。

---

- 12 他のファイルをすべてリストアするには、次の手順を示される順序で実行します。

- マスターサーバー上で **NetBackup** 管理インターフェースを起動します。
  - 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インターフェースを起動します。
  - リストア対象を表示し、消失したパーティションだけを選択します。システムディレクトリ (通常、`C:\Windows`) を選択します。これによって、すべてのレジストリファイルのリストアが確実に行われます。
  - `install_path\NetBackup\db` ディレクトリ、`install_path\NetBackupDB` ディレクトリ (または再配置された **NetBackup** リレーショナルデータベースのパス)、`install_path\NetBackup\var` ディレクトリまたは `install_path\Volmgr\database` ディレクトリの選択を解除します。この手順の注意を参照してください。
  - **Windows** を再インストールする場合は、[既存のファイルの上書き (Overwrite existing files)] オプションを選択します。これにより、既存のファイルはバックアップと置き換えられます。
  - リストアを開始します。
- 13** システムを再起動します。これによって、リストアの実行中にビジー状態であったすべてのファイルが置き換えられます。ブートプロセスが完了すると、システムは最新のバックアップ時の状態にリストアされます。

## Windows の NetBackup メディアサーバーのディスクリカバリについて

NetBackup メディアサーバーでは、NetBackup リレーショナルデータベースに情報が格納されます。NetBackup メディアサーバーのシステムディスクをリカバリする必要がある場合は、クライアントのディスクリカバリ手順と同様の手順をお勧めします。

p.238 の「[Windows クライアントのディスクリカバリ](#)」を参照してください。

## Windows クライアントのディスクリカバリ

この項では、Windows NetBackup クライアントでシステムディスクに障害が発生した場合に、完全なリカバリする手順について説明します。

NetBackup Bare Metal Restore (BMR) は、クライアントシステムを BMR 保護用に構成されたポリシーを使用してバックアップすることによって保護します。BMR バックアップおよびリカバリ手順の詳細な説明が利用可能です。

『Bare Metal Restore 管理者ガイド UNIX、Windows および Linux』を参照してください。

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

この手順では、システムをブートしてリストアを行うために、Windows オペレーティングシステムおよび NetBackup を再インストールする場合を想定しています。

この他に、次の場合も想定しています。

- **NetBackup** クライアントサーバーで、サポートされているバージョンの **Microsoft Windows** が実行されていた。
- **NetBackup** クライアントが、サポートされているバージョンの **NetBackup** クライアントおよびサーバーソフトウェアを使用してバックアップされている。
- クライアントがバックアップを送信する **NetBackup** マスターサーバーが動作中である。このサーバーからリストアを要求します。
- バックアップに、オペレーティングシステムおよびレジストリが存在するディレクトリが含まれている。  
このディレクトリ内のファイルがバックアップからエクスクルードされている場合、以前の構成と一致するようにシステムのリストアを行うことができない可能性があります。
- 欠陥のあるハードウェアが交換されている。

リカバリを開始する前に、次のものが揃っていることを確認します。

- リストア対象の **NetBackup** クライアントに再インストールする **Windows** システムソフトウェア。以前使用していたものと同じ種類およびバージョンのソフトウェアを再インストールします。
- リストア対象のクライアントにインストールする **NetBackup** のクライアントソフトウェア。
- ハードウェアの操作に必要な、特別なドライバまたは他のソフトウェア (ディスクドライブ固有のドライバなど)。
- **NetBackup** クライアントの IP アドレスおよびホスト名。
- **NetBackup** マスターサーバーの IP アドレスおよびホスト名。
- リストアを行うシステムで使用していたパーティションとフォーマットの状態。**Windows** のインストール中に、その状態を再現する必要があります。

## Windows クライアントのディスクをリカバリする方法

- 1 **Windows** オペレーティングシステムを、最小構成でインストールします (高速インストールを実行します)。

インストール時に、次の作業を実行します。

- 障害が発生する前と同じ状態に、ディスクをパーティション化します (パーティション化が必要な場合)。その後、各パーティションを障害が発生する前と同じ状態にフォーマットします。
- 障害が発生する前に使用していたパーティションと同じパーティションにオペレーティングシステムをインストールします。
- デフォルトのワークグループを指定します。ドメインへのリストアは行わないください。

- 該当するハードウェア製造元のすべての指示に従います。
- 2 インストールが完了したら、システムを再ブートします。
  - 3 NetBackup クライアントシステムを構成し、NetBackup マスターサーバーへのネットワーク接続を再度確立します。

たとえば、ネットワークで DNS を使用する場合、障害が発生する前に使用していた IP アドレスをクライアントの構成に使用する必要があります。また、同じ名前サーバー (または、NetBackup クライアントおよびマスターサーバーの両方を認識する他の名前サーバー) を指定する必要があります。クライアント上で、Windows のコントロールパネルから [ネットワーク] ダイアログボックスを開き、DNS を構成します。

- 4 NetBackup クライアントソフトウェアをインストールします。

クライアントサーバーおよびマスターサーバーに正しい名前を指定していることを確認します。

  - クライアント名を指定するには、クライアント上でバックアップ、アーカイブおよびリストアインターフェースを起動し、[ファイル (File)] メニューから [NetBackup クライアントのプロパティ ( Client Properties)] を選択します。[NetBackup クライアントのプロパティ ( Client Properties)] ダイアログボックスの [一般 (General)] タブにクライアント名を入力します。
  - サーバー名を指定するには、[ファイル (File)] メニューから [NetBackup マシンおよびポリシー形式の指定 (Specify Machines and Policy Type)] を選択します。

詳しくは、『NetBackup インストールガイド』を参照してください。

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

- 5 以前インストールされていた NetBackup のパッチをインストールします。
- 6 クライアントに次のデバッグログディレクトリを作成して、デバッグログを有効にします。

```
install_path¥NetBackup¥Logs¥tar
install_path¥NetBackup¥Logs¥bpinetd
```

NetBackup によって、これらのディレクトリにログが作成されます。

- 7 NetBackup Client Service を停止して、再起動します。

これによって、NetBackup では bpinetd のデバッグログへの書き込みが開始されます。

- 8 NetBackup のバックアップ、アーカイブおよびリストアインターフェースを使用して、クライアントシステムに、システムファイルおよびユーザーファイルのリストアを行います。

たとえば、すべてのファイルが c ドライブ上に存在する場合、このドライブのリストアを行うと、システム全体のリストアが行われます。

ファイルのリストアを行う場合、管理者である必要はありませんが、リストア権限を所有している必要があります。手順については、オンラインヘルプまたは次を参照してください。

『NetBackup バックアップ、アーカイブおよびリストアスタートガイド UNIX、Windows および Linux 』を参照してください。

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

NetBackup では、Windows のシステムファイルのリストア時に、レジストリのリストアが行われます。たとえば、システムファイルが C:\¥winnt ディレクトリに存在する場合、NetBackup によって、ディレクトリ、およびその下に存在するサブディレクトリとファイルのリストア時に、レジストリのリストアが行われます。

- 9 手順 6 で作成したディレクトリのログファイルに、ERR メッセージまたは WRN メッセージが表示されていないかどうかを確認します。

ログに、Windows のシステムファイルのリストアに関する問題が表示されている場合、その問題を解決してから次に進みます。

- 10 NetBackup Client Service を停止し、bpinetd プログラムが動作していないことを確認します。

- 11 NetBackup クライアントシステムを再起動します。

ブートプロセスが完了すると、システムは最新のバックアップ時の状態にリストアされます。

## Windows のクラスタ化された NetBackup サーバーのリカバリについて

NetBackup サーバークラスタは、カタログの破損、共有ディスクの消失、またはクラスタ全体の消失を防ぎません。定期的なカタログバックアップを実行する必要があります。クラスタ環境でのカタログバックアップとシステムバックアップのポリシーの構成に関する詳細情報が利用可能です。

『NetBackup High Availability ガイド』の NetBackup の設定に関するトピックを参照してください。

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

---

**警告:** これらのリカバリ手順を試す前に、テクニカルサポートにご連絡ください。

---

## Windows VCS クラスタでの障害が発生したノードの置き換え

NetBackup リソースグループをオンラインおよびオフラインにする方法について、クラスタテクノロジー固有の情報が利用可能です。また、リソースグループをフリーズおよびアンフリーズする (監視を無効化および有効化する) 方法についての情報も参照できます。

『NetBackup High Availability ガイド』の NetBackup の設定に関するトピックを参照してください。

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

この手順を続行する前に、次の条件を確認してください。

- 交換用のノードで、ハードウェア、システムソフトウェアおよびクラスタ環境が構成されている。
- 再構成されたノードまたは交換用のノードはクラスタのメンバーであり、障害が発生したノードと同じ名前である。

次の手順は、共有ディスクと少なくとも 1 つの構成されたクラスタノードが利用可能な場合に適用されます。

### Windows クラスタで VCS を使用して障害が発生したノードを置き換える方法

- 1 NetBackup サービスをフリーズします。
- 2 NetBackup 共有ディスクが NetBackup がインストールされるノードにマウントされていないことを確認します。
- 3 新しいノードまたは交換ノードに NetBackup を再インストールします。NetBackup 仮想名を NetBackup サーバーの名前として使用してください。NetBackup サーバーソフトウェアのインストールに関する指示に従ってください。

『NetBackup インストールガイド』を参照してください。

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

---

**メモ:** NetBackup Web サービスでは、クラスタの他のノードで使用したものと同一ユーザーアカウントと資格情報を使う必要があります。詳しくは以下の URL を参照してください。

<http://www.veritas.com/docs/000081350>

---

- 4 ノードが既存のクラスタのメンバーであること、および必要な構成が自動的に実行されることを確認します。

- 5 新しくインストールされたノードを他のクラスタノードと同じパッチレベルにするために必要な Maintenance Pack およびパッチをインストールします。
- 6 NetBackup サービスをアンフリーズし、交換用のノードで起動できることを確認します。

## Windows VCS クラスタでの共有ディスクのリカバリ

次の手順は、構成されたクラスタノードは利用可能な状態であるが、共有ディスク上の NetBackup カタログ、データベースファイル、またはその両方が、破損または消失している場合に適用できます。

この手順を続行する前に、次の条件を確認してください。

- 共有ストレージのハードウェアが稼働状態にリストアされている。これにより、空の共有ディレクトリがある状態で共有ディスクのリソースをオンラインにできます。
- 有効なオンラインカタログバックアップが存在する。

### VCS を使用する Windows クラスタで共有ディスクをリカバリする方法

- 1 障害が発生した NetBackup リソースグループを消去し、監視を無効にして、正常なノードで共有ディスクおよび仮想名リソースを起動します。
- 2 すべての NetBackup 共有ディスクに、NetBackup の最初のインストールおよび構成時に使用していたドライブ文字が割り当てられていることを確認します。
- 3 NetBackup をクラスタ用に再構成するには、アクティブノードで次のコマンドを順に実行し、データベースを初期化します。

```
bpclusterutil -ci  
tpext  
bpclusterutil -online
```

- 4 適切な NetBackup カタログリカバリの手順を実行して、共有ディスクに NetBackup カタログ情報をリストアします。

p.235 の「マスターサーバーおよび Windows のリカバリ」を参照してください。

- 5 クラスタ化された NetBackup サーバーがメディアサーバーである場合、リストアされた `vm.conf` ファイルにアクティブノードのホスト固有の `MM_SERVER_NAME` 構成エントリが正しく含まれていることを確認します。`MM_SERVER_NAME` がローカルホスト名と異なる場合は、ファイルを編集し、サーバー名をローカルホスト名に変更します。

```
MM_SERVER_NAME=<local host name>
```

- 6 NetBackup を使用して、共有ディスクにデータをリストアします。リストアを実行する方法の詳細を参照できます。  
『NetBackup バックアップ、アーカイブおよびリストアスタートガイド UNIX、Windows および Linux』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- 7 必要なデバイスとメディアを構成し、NetBackup カタログをリカバリします。
- 8 アクティブノードの NetBackup を手動で停止し、再起動します。
- 9 NetBackup リソースグループの監視を再度有効にします。
- 10 構成されたすべてのノードで NetBackup サーバーをオンラインにできるようになったことを確認します。

## Windows VCS クラスタ全体のリカバリ

次の手順は、最初から作成し直す必要があるクラスタ化された NetBackup サーバー環境に適用されます。

続行する前に、有効なオンラインカタログバックアップがあることを確認します。

### Windows VCS クラスタ全体をリカバリする方法

- 1 交換クラスタのハードウェア、システムソフトウェアおよびクラスタ環境を構成します。
- 2 オペレーティングシステムに必要な適切な低レベルのテープデバイスとロボット制御デバイスの構成が実行されたことを確認します。  
『NetBackup デバイス構成ガイド UNIX、Windows および Linux』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- 3 クラスタノードのそれぞれに NetBackup を再インストールします。NetBackup 仮想名を NetBackup サーバーの名前として使用してください。NetBackup サーバーソフトウェアのインストールに関する指示に従ってください。  
『NetBackup インストールガイド』を参照してください。  
<http://www.veritas.com/docs/DOC5332>

---

メモ: NetBackup Web サービスでは、NetBackup カタログのバックアップを作成したときに使用したものと同じユーザーアカウントとクレデンシャルを使う必要があります。詳しくは以下の URL を参照してください。

<http://www.veritas.com/docs/000081350>

---

- 4 クラスタ化された NetBackup サーバーを構成します。  
 『NetBackup High Availability 管理者ガイド UNIX、Windows および Linux』を参照してください。  
<http://www.veritas.com/docs/DOC5332>
- 5 新しくインストールされた NetBackup サーバーを、置き換えるサーバーと同じパッチレベルにするために必要な Maintenance Pack およびパッチをインストールします。
- 6 必要なデバイスとメディアを構成し、NetBackup カタログをリカバリします。  
 p.235 の「マスターサーバーおよび Windows のリカバリ」を参照してください。
- 7 各ノードの NetBackup リソースグループを順番に有効にし、デバイスの構成ウィザードを実行してデバイスを構成します。  
 クラスタ (WSFC または VCS) の構成情報を参照できます。  
 『NetBackup High Availability 管理者ガイド UNIX、Windows および Linux』を参照してください。  
<http://www.veritas.com/docs/DOC5332>

## ディザスタリカバリインストール後にクラスタマスターサーバーで証明書を生成する

クラスタ化されたマスターサーバーのディザスタリカバリが完了した後は、アクティブノードとすべての非アクティブノードで証明書を生成する必要があります。この手順は、クラスタのバックアップとリストアを成功させるために必須です。

### ディザスタリカバリの後に各クラスタノードでローカル証明書を生成するインストール

- 1 すべての非アクティブノードをクラスタに追加します。  
 クラスタのすべてのノードが現在クラスタの一部ではない場合、最初にこれらをクラスタに追加します。このプロセスについて詳しくは、オペレーティングシステムのクラスタの手順を参照してください。  
 サポート対象のクラスタ技術に関する詳細情報を参照できます。『NetBackup マスターサーバーのクラスタ化管理者ガイド』を参照してください。
- 2 nbcertcmd コマンドを実行し、認証局の証明書を格納します。  
 UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -getCACertificate`  
 Windows の場合: `install_path¥Veritas¥NetBackup¥bin¥nbcertcmd -getCACertificate`

- 3 以下に示す `bpnbat` コマンドを使用し、必要な変更を許可します。認証ブローカーを求めるメッセージが表示されたら、ローカルノード名ではなく仮想サーバー名を入力します。

```
bpnbat -login -loginType WEB
```

- 4 `nbcertcmd` コマンドを使用して再発行トークンを作成します。`hostname` は、ローカルノード名です。コマンドを実行すると、トークン文字列値が表示されます。各クラスターノードには一意の再発行トークンが必要です。

```
nbcertcmd -createtoken -name token_name -reissue -host hostname
```

- 5 `nbcertcmd` コマンドとともに再発行トークンを使用して、ホスト証明書を格納します。このコマンドでは、トークン文字列値が求められます。`nbcertcmd -createToken` コマンドから入手したトークン文字列値を入力します。

```
nbcertcmd -getCertificate -token
```

詳細情報を参照できます。『Veritas NetBackup セキュリティおよび暗号化ガイド』で、マスターサーバーノードでの証明書の配備に関するセクションを参照してください。

p.215 の「ディザスタリカバリパッケージ」を参照してください。

p.214 の「ディザスタリカバリの要件について」を参照してください。

## ディザスタリカバリパッケージのリストアについて

ディザスタリカバリパッケージには、**NetBackup** マスターサーバーホスト ID が含まれます。このパッケージはカタログバックアップ時に作成されます。災害発生後に **NetBackup** をマスターサーバーにインストールすると、ホスト ID が必要になります。

p.215 の「ディザスタリカバリパッケージ」を参照してください。

### 重要な注意事項

- カタログリカバリではホスト ID はリカバリされません。ホスト ID やディザスタリカバリパッケージをリストアするには、ディザスタリカバリモードで **NetBackup** をインストールし、必要なパッケージをインポートする必要があります。ディザスタリカバリパッケージをリカバリすると、カタログをリカバリすることができます。
- ディザスタリカバリパッケージまたはマスターサーバーホスト ID をリストアした後は、すぐにカタログリカバリを実行する必要があります。  
p.254 の「**NetBackup** カatalogのリカバリについて」を参照してください。

**NetBackup** マスターサーバーのディザスタリカバリパッケージは、インストール中またはインストール後にリストアできます。

- インストール時にパッケージをリストアするには、インストールのディザスタリカバリモードを選択します。

インストール時にディザスタリカバリパッケージのパスフレーズを指定する必要があります。誤ったパスフレーズを指定した場合や、パスフレーズを忘れた場合は、インストール後にすべてのホストでセキュリティ証明書を配備する必要があります。ディザスタリカバリパッケージをインストール時にリストアすることはできません。インストール後にディザスタリカバリパッケージをリストアするには、次の記事を参照してください。

<http://www.veritas.com/docs/000125933>

- インストール後にパッケージをリストアするには、`nbhostidentity` コマンドを使用します。

p.248 の「[Windows](#) でのディザスタリカバリパッケージのリストア」を参照してください。

p.250 の「[UNIX](#) でのディザスタリカバリパッケージのリストア」を参照してください。

---

**メモ:** NetBackup アプライアンスのディザスタリカバリパッケージをリストアするには、`nbhostidentity` コマンドを使用します。

---

## DR\_PKG\_MARKER\_FILE 環境変数について

災害の発生前にマスターサーバーで外部 CA が構成され、DR インストールが失敗した場合は、このユーティリティを使用して外部 CA の構成設定を再構成できます。このフックを使用すると、DR パッケージのリカバリ後およびサービスの再起動前に DR インストールを待機できます。これにより、必要に応じて、外部 CA の構成設定を修正または再構成する時間が与えられます。

外部 CA が署名した証明書について詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

p.248 の「[Windows](#) でのディザスタリカバリパッケージのリストア」を参照してください。

p.250 の「[UNIX](#) でのディザスタリカバリパッケージのリストア」を参照してください。

外部 CA の構成設定に必要な変更を加えるまで NetBackup インストーラのインストールプロセスを保留するには、タッチファイルで `DR_PKG_MARKER_FILE` という環境変数を設定する必要があります。この環境変数を設定した後で、DR インストールを開始できます。DR インストールでは、ファイルシステム上に存在するタッチファイルが検出されるかぎり、インストールの終盤まで NetBackup サービスの起動を待機します。この間に、外部 CA の構成設定を変更できます。変更が終了したら、インストーラがインストールプロセスを再開できるように、`DR_PKG_MARKER_FILE` 環境変数を含むタッチファイルを削除する必要があります。

---

**メモ:** このマーカーファイルは、DR インストールに失敗した場合にのみ使用してください。

---

# Windows でのディザスタリカバリパッケージのリストア

災害発生後、リストアするカタログバックアップに対応するディザスタリカバリパッケージをリストアする必要があります。ディザスタリカバリパッケージは、マスターサーバーのホスト ID を再取得します。カタログリカバリを実行する前に、ホスト ID をリストアする必要があります。

## 重要な注意事項

- クラスタマスターサーバーのセットアップ:
  - ディザスタリカバリパッケージには、仮想名のみ ID ファイルと構成が含まれています。
  - DR インストール後に、仮想名の証明書がリストアされます。
  - クラスタノード固有の証明書と構成オプションはバックアップされないため、リカバリされません。DR インストール後に **NetBackup** 証明書または外部証明書を再配備または再構成する必要があります。

## 前提条件

NetBackup ドメインで外部 CA が署名した証明書を使用する場合、次のことを確認します。

- 証明書ファイルのパスが構成され、アクセス可能で、バックアップが作成されたパスと同じである。
- ディザスタリカバリインストールを開始する前に、必要な証明書失効リスト (CRL) を構成した (該当する場合)。  
『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。
- Windows 証明書ストアに必要な外部証明書をコピーした (該当する場合)。
- 災害の発生前にマスターサーバーに外部証明書を構成して DR インストールが失敗した場合は、DR\_PKG\_MARKER\_FILE という環境変数を設定して、DR インストールの終盤で外部証明書の構成を修正できます。  
p.247 の「[DR\\_PKG\\_MARKER\\_FILE 環境変数について](#)」を参照してください。

## NetBackup のインストール中にディザスタリカバリパッケージをリストアする方法

- 1 NetBackup ソフトウェアのインストールを開始します。  
『[NetBackup インストールガイド](#)』の「Windows システムでのサーバーソフトウェアのインストール」セクションを参照してください。
- 2 [NetBackup のライセンスキーとサーバー形式 (NetBackup License Key and Server Type)]画面で、[マスターサーバーのディザスタリカバリ (Disaster Recovery Master Server)]オプションを選択します。

- 3 NetBackup の [ディザスタリカバリ (Disaster Recovery)] 画面で、ディザスタリカバリパッケージの場所を指定します。[参照 (Browse)] をクリックし、リストアするパッケージの場所を選択します。
- 4 リストアするディザスタリカバリパッケージと関連付けられているパスフレーズを指定します。

適切なパスフレーズを指定していることを確認します。

- 誤ったパスフレーズを指定した場合や、パスフレーズを忘れた場合は、インストール後にすべてのホストでセキュリティ証明書を配備する必要があります。ディザスタリカバリパッケージをインストール時にリストアすることはできません。インストール後にディザスタリカバリパッケージをリストアするには、次の記事を参照してください。

<http://www.veritas.com/docs/000125933>

- パスフレーズが検証された場合、インストールを続行します。
- 5 災害が発生する前のカタログバックアップ時に、NetBackup ドメインで外部 CA が署名した証明書を使用している場合、DR インストール時に、証明書失効リスト (CRL) の構成を促す警告メッセージがインストーラによって表示されます。構成可能な CRL 設定も表示されます。

- ECA\_CRL\_CHECK 構成オプションの値を確認します。  
カタログバックアップと外部証明書構成オプションについて詳しくは、『[NetBackup 管理者ガイド Vol.1](#)』を参照してください。
- ECA\_CRL\_CHECK 構成オプションが DISABLE に設定されている場合、CRL を構成する必要はありません。
- ECA\_CRL\_CHECK 構成オプションが有効になっている場合は、CRL を構成するように求められます。  
CRL を構成し、DR インストールを続行します。
- ECA\_CRL\_PATH オプションで指定した値に応じて、必要な CRL を利用できるようにします。
- ECA\_CRL\_PATH が指定されていない場合、NetBackup はピアホストの証明書の CRL 配布ポイント (CDP) から取得できる CRL を使用します。CDP で利用可能な URL にアクセスできることを確認します。
- ECA\_CRL\_PATH を指定すると、NetBackup はこのオプションで指定されたディレクトリで利用可能な CRL を使用します。ECA\_CRL\_PATH に指定したディレクトリで、有効な CRL をコピーします。
- Windows 証明書ストアに外部 CA が署名した証明書を格納し、この証明書のバックアップが DR パッケージに作成されていない場合、外部 CA が署名した証明書の構成を促す警告が表示されます。インストーラまたは対応するディザス

タリカバリ電子メールで指定された値に合わせて、マスターサーバーで次の外部証明書構成オプションを構成します。

- ECA\_CERT\_PATH
- ECA\_PRIVATE\_KEY\_PATH
- ECA\_KEY\_PASSPHRASEFILE
- ECA\_TRUST\_STORE\_PATH
- ECA\_CRL\_PATH

カタログバックアップと外部証明書構成オプションについて詳しくは、『[NetBackup 管理者ガイド Vol.1](#)』を参照してください。

- DR インストールの前に DR\_PKG\_MARKER\_FILE 環境変数が設定された場合、touch ファイルが存在することを示すメッセージが表示されます。外部証明書の構成が完了したら、DR\_PKG\_MARKER\_FILE 環境変数に設定されている touch ファイルを削除します。  
NetBackup サービスが起動されます。
- 6 『[NetBackup インストールガイド](#)』の「Windows システムでのサーバーソフトウェアのインストール」セクションを参照してください。

### NetBackup のインストール後にディザスタリカバリパッケージをリストアする方法

- 1 NetBackup のインストール後に `nhostidentity -import -infile file_path` コマンドを実行します。

『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

- 2 ドメイン内のすべてのホストで許可リストのキャッシュをクリーンアップし、NetBackup サービスを再起動します。

- 3 次のシナリオで NetBackup 証明書ファイルを削除するには、この手順を実行します。

災害前に、外部 CA が署名した証明書のみを使用するように NetBackup が構成されており、ディザスタリカバリパッケージを手動でインポートする前に、NetBackup 証明書または NetBackup 証明書と外部証明書の両方を使用するように NetBackup が構成されている。

次のコマンドを実行して、NetBackup 証明書ファイルを削除します。

```
configureWebServerCerts -removeNBCert
```

## UNIXでのディザスタリカバリパッケージのリストア

災害発生後、リストアするカタログバックアップに対応するディザスタリカバリパッケージをリストアする必要があります。ディザスタリカバリパッケージは、マスターサーバーのホスト

ID を再取得します。カタログリカバリを実行する前に、ホスト ID をリストアする必要があります。

## 重要な注意事項

- クラスタマスターサーバーのセットアップ:
  - ディザスタリカバリパッケージには、仮想名のみ ID ファイルと構成が含まれています。
  - DR インストール後に、仮想名の証明書がリストアされます。
  - クラスタノード固有の証明書と構成オプションはバックアップされないため、リカバリされません。DR インストール後に **NetBackup** 証明書または外部証明書を再配備または再構成する必要があります。

## 前提条件

NetBackup ドメインで外部 CA が署名した証明書を使用する場合、次のことを確認します。

- ファイルベースの外部証明書の場合は、証明書ファイルのパスが構成され、アクセス可能で、バックアップされたものと同じであることを確認します。
- 災害前に証明書ストアとして Windows 証明書ストアを使用しており、カタログバックアップ中に証明書ファイルがバックアップされなかった場合、災害後にホストの外部証明書を手動で構成する必要があります。次の記事を参照してください。  
[https://www.veritas.com/support/en\\_US/article.100044249](https://www.veritas.com/support/en_US/article.100044249)
- ディザスタリカバリインストールを開始する前に、必要な証明書失効リスト (CRL) を構成した (該当する場合)。  
CRL について詳しくは、『**NetBackup セキュリティおよび暗号化ガイド**』を参照してください。
- 災害の発生前にマスターサーバーに外部証明書を構成して DR インストールが失敗した場合は、`DR_PKG_MARKER_FILE` という環境変数を設定して、DR インストールの終盤で外部証明書の構成を修正できます。  
p.247 の「**DR\_PKG\_MARKER\_FILE 環境変数について**」を参照してください。

## NetBackup のインストール中にディザスタリカバリパッケージをリストアする方法

- 1 NetBackup ソフトウェアのインストールを開始します。  
『**NetBackup インストールガイド**』の「UNIX システムでのサーバーソフトウェアのインストール」セクションを参照してください。
- 2 次のメッセージが表示されたら、Enter キーを押して続行します。

```
Is this host a master server? [y/n] (y)
```

- 3 次のメッセージが表示されたら、Y を選択します。

```
Are you currently performing a disaster recovery of a master  
server? [y/n] (y)
```

- 4 次のメッセージが表示された場合、リストアするディザスタリカバリパッケージの名前とパスを指定します。

```
Enter the name of your disaster recovery package along with the  
path, or type q to exit the install script:
```

ドメインで外部証明書が使用されている場合は、警告メッセージが表示されます。以降の手順でインストーラが待機状態になる場合は、手順 6 に従って外部証明書構成オプションを構成します。

- 5 次のメッセージが表示された場合、リストアするディザスタリカバリパッケージと関連付けられているパスフレーズを指定します。

---

**注意:** 適切なパスフレーズを指定していることを確認します。

誤ったパスフレーズを指定した場合や、パスフレーズを忘れた場合は、インストール後にすべてのホストでセキュリティ証明書を配備する必要があります。ディザスタリカバリパッケージをインストール時にリストアすることはできません。インストール後にディザスタリカバリパッケージをリストアするには、次の記事を参照してください。

<http://www.veritas.com/docs/000125933>

---

```
Enter your disaster recovery passphrase, or enter q to exit  
installation:
```

次のメッセージが表示されます。

```
Validating disaster recovery passphrase...
```

パスフレーズが検証された場合、インストールを続行します。

- 6 外部 CA が署名した証明書が NetBackup ドメインで使用される場合、以下を実行します。
- ECA\_CRL\_CHECK 構成オプションの値を確認します。  
カタログバックアップと外部証明書構成オプションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。
  - ECA\_CRL\_CHECK 構成オプションが DISABLE に設定されている場合、CRL を構成する必要はありません。
  - ECA\_CRL\_CHECK 構成オプションが有効になっている場合は、CRL を構成するように求められます。

UNIX インストーラは任意の操作を待機せず、インストーラの次の手順に進みます。次の手順の後にインストーラが待機しているときは、CRL を構成して DR インストールを続行できます。

CRL を構成し、DR インストールを続行します。

- ECA\_CRL\_PATH オプションで指定した値に応じて、必要な CRL を利用できるようにします。
    - ECA\_CRL\_PATH が指定されていない場合、NetBackup はピアホストの証明書の CRL 配布ポイント (CDP) から取得できる CRL を使用します。CDP で利用可能な URL にアクセスできることを確認します。
    - ECA\_CRL\_PATH を指定すると、NetBackup はこのオプションで指定されたディレクトリで利用可能な CRL を使用します。ECA\_CRL\_PATH に指定したディレクトリで、有効な CRL をコピーします。
  - DR インストールの前に DR\_PKG\_MARKER\_FILE 環境変数が設定された場合、touch ファイルが存在することを示すメッセージが表示されます。外部証明書の構成が完了したら、DR\_PKG\_MARKER\_FILE 環境変数に設定されている touch ファイルを削除します。  
NetBackup サービスが起動されます。
- 7 『NetBackup インストールガイド』の「UNIX システムでのサーバーソフトウェアのインストール」セクションを参照してください。

### NetBackup のインストール後にディザスタリカバリパッケージをリストアする方法

- 1 NetBackup のインストール後に `nbhostidentity -import -infile file_path` コマンドを実行します。  
『NetBackup コマンドリファレンスガイド』を参照してください。
- 2 ドメイン内のすべてのホストで許可リストのキャッシュをクリーンアップし、NetBackup サービスを再起動します。
- 3 次のシナリオで NetBackup 証明書ファイルを削除するには、この手順を実行します。

NetBackup が、災害前に外部 CA が署名した証明書のみを使用するように構成されており、ディザスタリカバリパッケージを手動でインポートする前に、NetBackup 証明書または NetBackup 証明書と外部証明書の両方を使用するように構成されている。

次のコマンドを実行して、NetBackup 証明書ファイルを削除します。

```
configureWebServerCerts -removeNBCert
```

# NetBackup カタログのリカバリについて

NetBackup カタログをリカバリする前に、次の操作を実行する必要があります。

- NetBackup がリカバリ環境で実行されていることを確認してください。
- リカバリデバイス NetBackup を構成します。
- カタログバックアップがあるメディアが、NetBackup から利用可能であることを確認してください。
- NetBackup マスターサーバーがクラスタに属している場合は、そのクラスタが機能していることを確認してください。
- ディザスタリカバリパッケージをリストアして、NetBackup ホスト ID をリストアします。  
 p.246 の「ディザスタリカバリパッケージのリストアについて」を参照してください。

---

**注意:** カタログリカバリが正常に完了したら、ディザスタリカバリパッケージのパスフレーズを設定する必要があります。これは、パスフレーズがカタログリカバリ中にリカバリされないためです。

---

NetBackup カタログは複数の部分で構成されます。カタログのリカバリ方法は、カタログのどの部分 (1 つまたは複数) をリカバリするかによって異なります。次に詳細を示します。

**表 4-3**                    **カタログリカバリオプション**

リカバリオプション	説明
カタログ全体のリカバリ	Veritas ベリタス社はカタログ全体をリカバリすることを推奨します。そうすれば、カタログの各種の部分間の一貫性を確保できます。この方法はバックアップされた環境と同じ環境にカタログをリカバリする際に最も有用です。  p.262 の「NetBackup カタログ全体のリカバリについて」を参照してください。
カタログイメージファイルと カタログ構成ファイルのリカバリ	バックアップが実行されたデータに関する情報が含まれます。設定ファイル (databases.conf と server.conf) は SQL Anywhere デーモンの指示を含んでいるフラットファイルです。  この種類のリカバリでは、必要に応じて後の処理で利用できるようにするために、ステー징ディレクトリに NetBackup リレーショナルデータベース (NBDB) もリストアします。  p.277 の「NetBackup カatalogイメージファイルのリカバリについて」を参照してください。

リカバリオプション	説明
リレーショナルデータベースファイルのリカバリ	<p><b>NetBackup</b> データベース (NBDB) は Enterprise Media Manager (EMM) データベースとも呼ばれます。それは、<b>NetBackup</b> ストレージユニットにあるボリューム、ロボット、ドライブについての情報を含んでいます。<b>NetBackup</b>リレーショナルデータベースには <b>NetBackup</b> のカタログイメージファイルも含まれます。イメージファイルにはバックアップの詳細を記述するメタデータが含まれています。</p> <p>リレーショナルデータベースが破損または消失し、有効なカタログイメージファイルがある場合は、リレーショナルデータベースをリカバリしてください。</p> <p>p.294 の「<b>NetBackup</b> リレーショナルデータベースのリカバリについて」を参照してください。</p>

カタログ全体またはカタログイメージファイルのリカバリには、ディザスタリカバリ情報が必要です。この情報はカタログバックアップの際にファイルに保存されます。ディザスタリカバリファイルの場所はカタログバックアップポリシーで構成されます。

p.258 の「**NetBackup** ディザスタリカバリ電子メールの例」を参照してください。

ディザスタリカバリファイルがない場合は、引き続きカタログのリカバリを実行できます。ただし、処理はより難しくなり、時間がかかります。

p.309 の「ディザスタリカバリファイルを使用しない **NetBackup** カタログのリカバリ」を参照してください。

---

**メモ:** カタログリカバリの後で、**NetBackup** は、カタログバックアップを含んでいるリムーバブルメディアを凍結します。この操作によって、それ以降に、メディアの最終的なカタログバックアップイメージが誤って上書きされることが回避されます。この最終的なイメージは、実際のカタログバックアップそのものに含まれますが、カタログバックアップのリカバリには含まれていません。メディアを解凍できます。

p.315 の「**NetBackup** オンラインカタログリカバリメディアの凍結の解除」を参照してください。

---

特別な使用例のための他の手順もあります。

p.306 の「**NetBackup** アクセス制御が構成されている場合の **NetBackup** カタログのリカバリ」を参照してください。

別のトピックでカタログリカバリについての詳細情報を提供します。

p.256 の「**Windows** コンピュータでの **NetBackup** カタログリカバリについて」を参照してください。

p.256 の「ディスクデバイスからの **NetBackup** カタログリカバリについて」を参照してください。

p.257 の「**NetBackup** カタログのリカバリと **OpsCenter** について」を参照してください。

## Windows コンピュータでの NetBackup カタログリカバリについて

Windows コンピュータ上では、NetBackup メディアサーバーのホスト名は Windows レジストリに格納されます。(また、NetBackup にも保存されます)。

カタログリカバリのシナリオで NetBackup をインストールした場合は、インストール時にメディアサーバー名を必ず入力してください。そうすることによって、レジストリにメディアサーバーが追加されます。その後で、カタログリカバリと、既存のメディアサーバーおよびデバイスを使う後続のバックアップが正しく機能します。

## ディスクデバイスからの NetBackup カタログリカバリについて

カタログリカバリでは、リカバリ環境のディスクメディア ID がバックアップ環境のディスクメディア ID と異なる場合があります。これらの ID は次の使用例では異なる場合があります。

- ストレージデバイスは同じでも、新しい NetBackup マスターサーバーがインストールされている。マスターサーバーのホストまたはディスクの障害により、NetBackup のインストールが必要な場合があります。NetBackup でのデバイス設定では、元々割り当てられていたディスクボリュームとは違うディスクメディア ID を割り当てる場合があります。
- ディスクストレージデバイスがカタログバックアップが書き込まれたデバイスと違う。ストレージハードウェアの障害または交換の後にこれと同じ環境になる場合があります。カタログバックアップとクライアントバックアップをレプリケートするのは別のサイトである場合があります。いずれにしても、カタログバックアップとクライアントバックアップは異なるハードウェアに存在します。そのため、ディスクメディア ID が異なる場合があります。

これらのシナリオでは、NetBackup はカタログがリカバリできるようにディスクメディア ID を処理します。この処理は、バックアップ環境からのディスクメディア ID をリカバリの環境のディスクメディア ID にマップします。

この処理は、カタログバックアップが次のストレージタイプの 1 つに存在する場合に発生します。

- AdvancedDisk ディスクプール
- メディアサーバーの重複排除プール (MSDP)
- OpenStorage デバイス

## NetBackup のカタログリカバリとシンボリックリンクについて

NetBackup のカタログをリカバリするときは、次のように NetBackup カタログディレクトリ構造内のすべてのシンボリックリンクを考慮する必要があります。

db/images ディレクトリ	シンボリックリンクのターゲットとなっているストレージに <b>NetBackup</b> の db/images ディレクトリがある場合には、リカバリ環境にもシンボリックリンクが存在している必要があります。また、シンボリックリンクには同じターゲットがリカバリ環境に存在している必要があります。
db/images/client ディレクトリ	db/images ディレクトリの下クライアントサブディレクトリのうちのどれかがシンボリックリンクの場合は、それらもリカバリ環境に存在している必要があります。また、シンボリックリンクには同じターゲットがリカバリ環境に存在している必要があります。
クラスタ化されたマスターサーバーのカタログのリカバリ	クラスタ化されたマスターサーバーからディザスタリカバリサイトの単一のマスターサーバーに <b>NetBackup</b> カタログをリカバリするには、カタログをリカバリする前に、次のシンボリックリンクをリカバリホストに作成する必要があります。

```
/usr/opensv/netbackup/db ->  
/opt/VRTSnbu/netbackup/db  
/usr/opensv/db/staging ->  
/opt/VRTSnbu/db/staging
```

**Solaris** システムについては、カタログをリカバリする前に、次のシンボリックリンクも作成する必要があります。

```
/usr/opensv -> /opt/opensv
```

シンボリックリンクとそのターゲットが存在しない場合は、カタログのリカバリは失敗します。

## NetBackup カタログのリカバリと OpsCenter について

**NetBackup** カタログのリカバリ時に、**NetBackup** はジョブ ID を 1 にリセットします。**NetBackup** は 1 から始まるジョブ番号の割り当てを開始します。

**NetBackup** **OpsCenter** を使用して、**NetBackup** のアクティビティを監視すると、カタログのリカバリ後の **OpsCenter** の重複したジョブ ID を確認できます。ジョブ ID の重複を防ぐには、リカバリ後に **NetBackup** でジョブ番号を付ける必要のあるジョブ ID を指定できます。

p.257 の「[カタログリカバリ後の NetBackup ジョブ ID 番号の指定](#)」を参照してください。

### カタログリカバリ後の NetBackup ジョブ ID 番号の指定

カタログリカバリ後に、**NetBackup** ジョブ ID 番号を指定できます。**OpsCenter** を使用して、**NetBackup** アクティビティを監視する場合、ジョブ ID 番号を指定することで、**OpsCenter** でジョブ ID 番号の重複を防ぎます。

p.257 の「[NetBackup カタログのリカバリと OpsCenter について](#)」を参照してください。

### カタログリカバリ後に NetBackup ジョブ ID 番号を指定する方法

- 1 必要に応じて、バックアップから OpsCenter データベースをリストアします。
- 2 OpsCenter で記録された最後のジョブ ID 番号を特定します。
- 3 NetBackup `jobid` ファイルを編集し、手順 2 から取得した数より 1 大きい値を設定します。`jobid` ファイルへのパス名は次のとおりです。
  - UNIX の場合: `/usr/opensv/netbackup/db/jobs/jobid`
  - Windows の場合: `install_path¥Veritas¥NetBackup¥db¥jobs¥jobid`リカバリでジョブ番号が使われるため、カタログリカバリの前に番号を指定する必要があります。
- 4 NetBackup カタログをリカバリします。

## NetBackup ディザスタリカバリ電子メールの例

カタログのバックアップポリシーはカタログバックアップが終了次第ディザスタリカバリの電子メールを送信できます。カタログバックアップポリシーを構成するには、『NetBackup 管理者ガイド Vol. 1』を参照してください。

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

次に、正常なカタログバックアップ後のディザスタリカバリ電子メールの例を示します。

```
From: NetBackup@example.com
Sent: Thursday, January 3, 2019 05:48
To: NetBackup Administrator
Subject: NetBackup Catalog Backup successful on host
master.example.com status 0
Attachments: cat_backup_1438271286_INCR
cat_backup_1438271286_INCR.drpkg
```

```
Server
master.example.com
```

```
NetBackup Version
8.1.X
```

```
Date
4/27/2017 05:46:45 AM
```

```
Policy
cat_backup
```

Catalog Backup Status

the requested operation was successfully completed (status 0).  
 WARNING: External CA-signed certificates could not be backed up.  
 Refer to the following article to configure external CA-signed certificates  
 on the host after disaster recovery installation:  
[https://www.veritas.com/support/en\\_US/article.100044249](https://www.veritas.com/support/en_US/article.100044249)

DR image file: /dr/nbu\_dr\_file/cat\_backup\_1438271286\_INCR

To ensure that the NetBackup catalog data is protected through  
 1/3/2019 10:46:45 AM, retain a copy of each attached file, and the  
 media or files listed below:

Catalog Recovery Media

Media Server	Disk Image Path	Image File Required
* media-server.example.com	@aaaab	cat_backup_1438267080_FULL
* media-server.example.com	@aaaab	cat_backup_1438271206_INCR
* media-server.example.com	@aaaab	cat_backup_1438271286_INCR

DR file written to

/dr/nbu\_dr\_file/cat\_backup\_1438271286\_INCR

DR Package file written to

/dr/nbu\_dr\_file/cat\_backup\_1438271286\_INCR.drpkg

The CA configuration at the time of catalog backup is as follows:

The master server chl2auto28 is configured to use NetBackup and external  
 CA-signed certificates.

```
ECA_CERT_PATH = MY¥¥chl2auto28.pne.ven.veritas.com
ECA_CRL_PATH = C:¥Users¥Administrator¥Downloads¥divgrt1.crl
ECA_CRL_PATH_SYNC_HOURS = 1
ECA_CRL_REFRESH_HOURS = 24
ECA_CRL_CHECK = 1
ECA_DR_BKUP_WIN_CERT_STORE = YES
```

The master server ms1.exampleveritas.com is configured to use the following  
 Key Management Servers.

```
KMS Server Name = kms1.example.veritas.com , KMS Server Type = KMIP
KMS Server Name = kms2.example.veritas.com , KMS Server Type = KMIP
KMS Server Name = kms3.example.veritas.com , KMS Server Type = KMIP
KMS Server Name = kms4.example.veritas.com , KMS Server Type = KMIP
```

KMS Server Name = ms1.exampleveritas.com , KMS Server Type = NBKMS

\* - Primary Media

#### Catalog Recovery Procedure for the Loss of an Entire Catalog

You should create a detailed disaster recovery plan to follow should it become necessary to restore your organization's data in the event of a disaster. A checklist of required tasks can be a tremendous tool in assisting associates in triage. For example, after the facility is safe for data to be restored, the power and data infrastructure need to be verified. When these tasks are completed, the following scenarios will help to quickly restore the NetBackup environment, and in turn, restore applications and data.

#### Disaster Recovery Procedure using the DR Package file and DR Image File

In the event of a catastrophic failure, use the following procedure to rebuild the previous NetBackup environment.

#### Important Notes:

- If new hardware is required, make sure that the devices contain drives capable of reading the media and that the drive controllers are capable of mounting the drives.
- Keep the passphrase associated with the DR Package file handy. This passphrase is set before the catalog backup policy configuration using the NetBackup Administration Console or the nbseccmd command.
- If this catalog backup is encrypted using a key from a Key Management Server, ensure that the Key Management Server is online before doing any of the following steps.

1. Install NetBackup.
  - a. The installation procedure prompts you to confirm if this is a DR scenario.
    - i. On the UNIX installer, you can see a prompt as "Do you want to do a disaster recovery on this master server? [y,n] (y)".  
Select "y"
    - ii. On the Windows installer click the "Disaster Recovery Master Server" button.
  - b. The installation procedure prompts you for the master server's DR Package

(refer to the /dr/mbu\_dr\_file/cat\_backup\_1438271286\_INCR.drpkg mentioned earlier).

Make sure that the Master Server can access the attached DR package file.

- c. Type the passphrase associated with the Master Server's DR Package, when prompted.
  - i. The installer validates the DR package using that passphrase
  - ii. In case of errors in validation, the installer aborts the operation. To work around the issue, refer to the following article: <http://www.veritas.com/docs/000125933>
2. Configure the devices necessary to read the media listed above.
3. Inventory the media.
4. Make sure that the master server can access the attached DR image file.
5. Start the NetBackup Recovery Wizard from the NetBackup Administration Console. Or, start the wizard from a command line by entering `bprecover -wizard`.

WARNING: CRLs are not backed as part of the DR package backup.

Refer to the following article to manually add the CRLs:

[https://www.veritas.com/support/en\\_US/article.100044250](https://www.veritas.com/support/en_US/article.100044250)

#### Disaster Recovery Procedure without the DR Image File

NOTE: ONLY ATTEMPT THIS AS A LAST RESORT If you do not have the attachment included with this email, use the following instructions to recover your catalog. (If using OpenStorage disk pools, refer to the Shared Storage Guide to configure the disk pools instead of step 2 and 3 below ):

1. Install NetBackup.
2. Configure the devices necessary to read the media listed above.
3. Inventory the media.
4. Run
 

```
To recover from copy 1:
bpimport -create_db_info -stype AdvancedDisk -dp dp-advdisk
-dv /storage/advdisk
```
5. Run:
 

```
cat_export -client client1.example.com
```
6. Go to the following directory to find the DR image file
 

```
cat_backup_1438271286_INCR:
/usr/openv/netbackup/db.export/images/master.example.com/1438000000
```
7. Open `cat_backup_1438271286_INCR` file and find the `BACKUP_ID`

- (for example: master.example.com\_1438271286).
8. Run:  
bpimport [-server name] -backupid master.example.com\_1438271286
  9. Run:  
bprestore -T -w [-L progress\_log] -C master.example.com -t 35  
-p cat\_backup -X -s 1438271286 -e 1438271286 /
  10. Run the BAR user interface to restore the remaining image database if the DR image is a result of an incremental backup.
  11. To recover the NetBackup relational database, run:  
bprecover -r -nbdb
  12. Stop and Start NetBackup.
  13. Configure the devices if any device has changed since the last backup.
  14. To make sure the volume information is updated, inventory the media to update the NetBackup database.

p.254 の「[NetBackup カタログのリカバリについて](#)」を参照してください。

## NetBackup カタログ全体のリカバリについて

**Veritas** ベリタス社はカタログ全体をリカバリすることを推奨します。そうすれば、カタログの各種の部分間の一貫性を確保できます。

リカバリでは、次のように、ディザスタリカバリファイルによって識別されるカタログバックアップ内にあるカタログイメージファイルおよび構成ファイルもリストアされます。

**完全バックアップ** DR ファイルによって識別される **NetBackup** リレーショナルデータベースファイルもリストアされます。ディザスタリカバリファイルによって識別されるイメージと構成ファイルがリストアされます。

**増分バックアップ** DR ファイルによって識別される **NetBackup** リレーショナルデータベースファイルもリストアされます。増分カタログバックアップには、最後の完全カタログバックアップ以降のすべてのカタログバックアップイメージファイルが自動的に含まれます。したがって、最後の完全バックアップ以降に変更されたカタログイメージと構成ファイルのみがリストアされます。その後、[バックアップ、アーカイブおよびリストア (**Backup, Archive, and Restore**)]ユーザーインターフェースを使用して、すべてのバックアップイメージをリストアできます。

---

**メモ:** カタログが **NAT** メディアサーバーでバックアップされている場合は、カタログリカバリの前に、特定の手順を実行して **NAT** メディアサーバーとの接続を確立する必要があります。

p.277 の「[カタログリカバリ前の NAT メディアサーバーとの接続の確立](#)」を参照してください。

---

NetBackup の NAT のサポートについて詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

カタログ全体をリカバリするのに次の方式のどちらかを使うことができます。

- カタログリカバリウィザード  
p.263 の「[カタログリカバリウィザードを使用したカタログ全体のリカバリNetBackup](#)」を参照してください。
- `bprecover -wizard` コマンドおよびオプションによって起動されるテキストベースのウィザード。  
p.271 の「[bprecover -wizard を使用した NetBackup カタログ全体のリカバリ](#)」を参照してください。

リレーショナルデータベースのトランザクションログは完全カタログリカバリ中には適用されません。

NetBackup カタログの構成要素は、[管理者ガイド](#)に記載されています。

## カタログリカバリウィザードを使用したカタログ全体のリカバリ NetBackup

この手順では、[[カタログリカバリウィザード \(Catalog Recovery Wizard\)](#)]を使ってカタログ全体のリカバリする方法を示します。リレーショナルデータベースのトランザクションログは完全カタログリカバリ中には適用されません。

p.254 の「[NetBackup カタログのリカバリについて](#)」を参照してください。

---

**メモ:** 完全カタログリカバリはカタログバックアップのデバイスとメディアの構成情報をリストアします。リカバリ中にストレージデバイスを構成する必要がある場合、Veritas は NetBackup イメージファイルのみをリカバリすることをお勧めします。

p.277 の「[NetBackup カタログイメージファイルのリカバリについて](#)」を参照してください。

---

root (管理) 権限が必要です。

カタログをリカバリしたいマスターサーバーにログオンする必要があります。[[カタログリカバリウィザード \(Catalog Recovery Wizard\)](#)]は、サーバーの変更操作の実行後は動作しません。

---

**メモ:** カatalogリカバリ処理の間に、NetBackup はサービスを停止して再起動することがあります。NetBackup が高可用性アプリケーション(クラスタまたはグローバルクラスタ)として構成されている場合は、リカバリ処理を開始する前にクラスタをフリーズします。そうすることでフェールオーバーを防ぎます。リカバリ処理の完了後にクラスタを解凍します。

---

---

**警告:** NetBackup カタログのリカバリが完了するまでは、クライアントバックアップを実行しないでください。

---

### [カタログリカバリウィザード (Catalog Recovery Wizard)]を使用してカタログ全体をリカバリする方法

- 1 NetBackup が実行されていない場合は、次のコマンドを入力して、すべての NetBackup サービスを起動します。
  - UNIX および Linux の場合:  

```
/usr/opensv/netbackup/bin/bp.start_all
```
  - Windows の場合:  

```
install_path¥NetBackup¥bin¥bpup
```
- 2 NetBackup 管理コンソールを起動します。
- 3 カタログバックアップとリカバリデバイスを利用できない場合は、次の手順を実行します。
  - a NetBackup で必要なリカバリデバイスを構成します。

テープストレージや BasicDisk ストレージの場合は、『NetBackup 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。NetBackup マニュアルについては、次の Web サイトを参照してください。

<http://www.veritas.com/docs/DOC5332>
  - b カタログバックアップが変更不可の (MSDP WORM) ストレージサーバーに書き込まれている場合は、CLI nbdevconfig コマンドを使用して、マスターサーバーの構成にストレージサーバーを追加します。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。
  - c カタログバックアップを含むメディアを NetBackup に利用可能にします。これには、ロボットまたはディスクプールのインベントリの実行、スタンドアロンドライブのメディアの追加、ストレージサーバーとディスクプールの構成などを行います。

テープストレージや BasicDisk ストレージの場合は、『NetBackup 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。NetBackup マニュアルについては、次の Web サイトを参照してください。

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

- 4 NetBackup 管理コンソールウィンドウの左ペインで[NetBackup の管理 (NetBackup Management)]をクリックし、右ペインで[カタログのリカバリ (Recover the catalogs)]をクリックします。

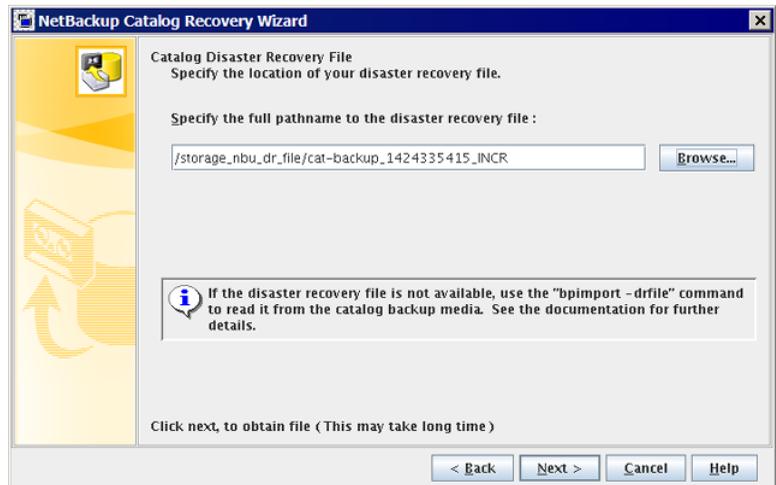
[NetBackup カタログリカバリウィザード (NetBackup Catalog Recovery Wizard)]の[ようこそ (Welcome)]パネルが表示されます。

- 5 [ようこそ (Welcome)]パネルで[次へ (Next)]をクリックして、[カタログのディザスタリカバリファイル (Catalog Disaster Recovery File)]パネルを表示します。

- 6 [カタログのディザスタリカバリファイル (Catalog Disaster Recovery File)]パネルで、ディザスタリカバリファイルの格納場所を指定します。ファイルを参照して選択するか、ディザスタリカバリファイルの絶対パス名を入力できます。

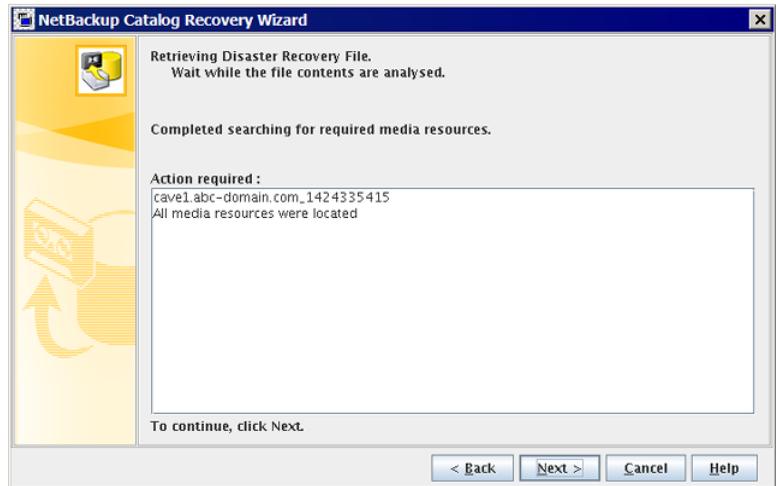
ほとんどの場合、利用可能な最新のディザスタリカバリ情報ファイルを指定します。最新のカタログバックアップが増分バックアップである場合、増分バックアップのディザスタリカバリファイルを使用します。(増分バックアップをリストアする前に完全バックアップをリストアする必要はありません。)

何らかの破損が発生した場合、カタログの以前の状態にリストアすることが必要になる場合もあります。



[次へ (Next)]をクリックして続行します。[ディザスタリカバリファイルを取得していません (Retrieving Disaster Recovery File)]パネルが表示されます。

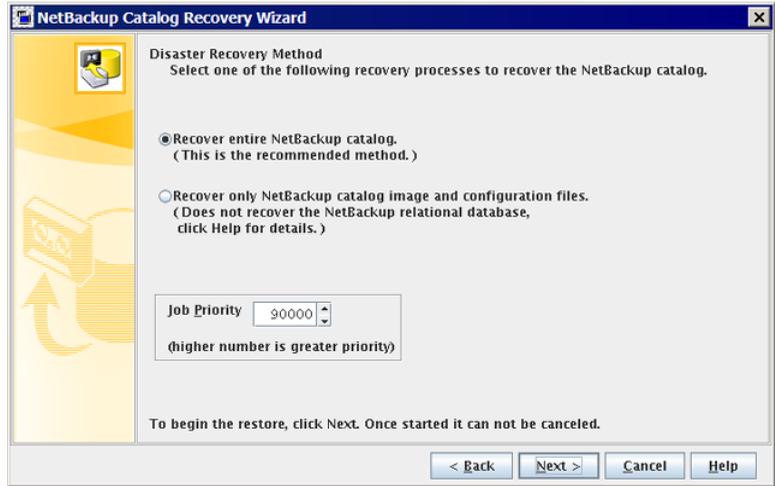
- 7 ウィザードがカタログをリカバリするために必要なメディアを検索し、[ディザスタリカバリファイルを取得しています (Retrieving Disaster Recovery File)]パネルに進捗状況が表示されます。その後、ディザスタリカバリイメージの必要なバックアップ ID が検出されたかどうかが表示されます。メディアが検出されなかった場合は、データベースの更新に必要なメディアが表示されます。



必要に応じて、ウィザードの指示に従って表示されたメディアを挿入し、インベントリを実行して **NetBackup** データベースを更新します。このパネルに表示される情報は、完全バックアップまたは増分バックアップのどちらからリカバリするかによって異なります。

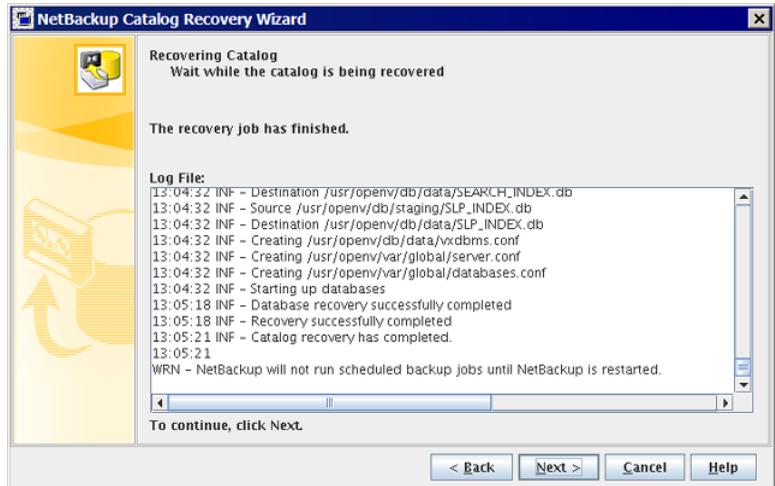
必要なメディアソースがすべて検出されたら、[次へ (Next)]をクリックします。[ディザスタリカバリ方式 (Disaster Recovery Method)]パネルが表示されます。

- 8 デフォルトでは、[NetBackup カタログ全体をリカバリする。(Recover entire catalog)] オプションに[ディザスタリカバリ方式 (Disaster Recovery Method)]パネルでチェックマークが付きまます。



必要に応じて、[ジョブ優先度 (Job Priority)]を選択し、[次へ (Next)]をクリックして NetBackup カタログ全体のリカバリを開始します。[カタログのリカバリ (Recovering Catalog)]パネルが表示されます。

- 9 次のように、[カタログのリカバリ (Recovering Catalog)]パネルにさまざまなカタログコンポーネントのリカバリの進捗状況が表示されます。
- NBDB データベース (EMM データベースを含む)
  - BMR データベース (該当する場合)
  - NetBackup ポリシーファイル
  - 適切なイメージのディレクトリへのバックアップイメージファイル
  - 他の構成ファイル



処理は次のようにリカバリ結果によって決まります。

成功しなかった

ログファイルのメッセージを参照して問題を確認します。[キャンセル (Cancel)]をクリックし、問題を解決してから、ウィザードを再度実行します。

成功する場合

[次へ (Next)]をクリックして最後のウィザードパネルに進みます。

---

**注意:** カタログリカバリが正常に完了したら、ディザスタリカバリパッケージのパスフレーズを設定する必要があります。これは、パスフレーズがカタログリカバリ中にリカバリされないためです。

---

ディザスタリカバリパッケージのパスフレーズが設定されていない場合は、次の警告が表示されます。

```
WRN - Passphrase for the disaster recovery package is not set.
You must set the passphrase for the catalog backups to be
successful.
```

p.215 の「[ディザスタリカバリパッケージ](#)」を参照してください。

パスフレーズを設定するには、次のいずれかの操作を行います。

- NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[グローバルセキュリティ設定 (Global Security Settings)]の順に展開します。詳細ペインで、[ディザスタリカバリ (Disaster Recovery)]タブをクリックし、パスフレーズを指定します。
- `nbseccmd -drpkgpassphrase` コマンドを使用してパスフレーズを指定します。

- 10** リカバリが完了したことを示すパネルで、[完了 (Finish)]をクリックします。
- 11** 続行する前に、次の点に注意してください。
- リムーバブルメディアからカタログをリカバリした場合は、**NetBackup** はカタログメディアをフリーズします。  
 p.315 の「**NetBackup** オンラインカタログリカバリメディアの凍結の解除」を参照してください。
  - **NetBackup** を再起動する前に、**Veritas** はリカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結することを推奨します。
  - **NetBackup** では、スケジュールバックアップジョブは、**NetBackup** を停止して再起動するまで実行されません。  
**NetBackup** を停止して再起動する前に、バックアップジョブを手動で開始できます。ただし、リカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結しない場合は、**NetBackup** がそのメディアに上書きすることがあります。
- 12** すべてのホストで許可リストのキャッシュをクリーンアップします。
- 13** 次のように、マスターサーバー上および他のホスト上の **NetBackup** サービスを停止して再起動します。

- **UNIX** および **Linux** の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all
/usr/opensv/netbackup/bin/bp.start_all
```

- **Windows** の場合:

```
install_path¥NetBackup¥bin¥bpdown
install_path¥NetBackup¥bin¥bpup
```

いずれかのホストで **NetBackup** 管理コンソールがアクティブになっている場合、**NetBackup** サービスを停止するコマンドによってコンソールが停止されます。

- 14** サービスを再起動したら、次のコマンドを実行します。

- **NetBackup** (またはホスト ID ベース) の証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合:

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate
```

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate -cluster
```

- 外部 CA が署名した証明書が NetBackup ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate  
-cluster
```

- コマンドが正常に実行された場合は、次の手順に進みます。
- このコマンドが終了状態 5988 を表示して失敗した場合は、次のトピックを参照してください。  
**p.315** の「[カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順](#)」を参照してください。  
 次の手順に進みます。

- 15 カタログリカバリがサーバーのリカバリ手順の一環である場合は、適切なリカバリ手順に従って残りの手順を完了します。

リカバリには次の作業が含まれます。

- バックアップメディアからカタログへのバックアップのインポート。
- メディアの書き込み保護。
- メディアの取り出しおよび保管。
- メディアの凍結。

---

**メモ:** カタログリカバリを実行すると、NetBackup の構成がカタログバックアップの時点に戻されます。カタログバックアップの特定時点の後に行われる構成への変更 (ポリシー、クライアント、ストレージユニットへの変更など) は、必要に応じて再度適用する必要があります。これらの変更は、新しいバックアップを作成する前に再度適用する必要があります。変更が適用されない場合、保護対象と保護の管理方法に影響する可能性があります。

たとえば、新しいイメージに対して WORM ロックの使用を必須とするようにストレージユニットが変更されている場合があります。WORM ロックが再適用されないと、必要な WORM 保護が新しいバックアップに適用されません。

---

## bprecover -wizard を使用した NetBackup カタログ全体のリカバリ

bprecover -wizard コマンドは NetBackup 管理コンソールウィザードの代わりに使うことができます。この手順を実行するには、root (管理) 権限が必要です。

リレーショナルデータベースのトランザクションログは完全カタログリカバリ中には適用されません。

これらの手順を実行するには、root (管理) 権限が必要です。

カタログをリカバリしたいマスターサーバーにログオンする必要があります。

---

**メモ:** カタログリカバリ処理の間に、サービスが停止して再起動することがあります。NetBackup が高可用性アプリケーション (クラスタまたはグローバルクラスタ) として構成されている場合は、リカバリ処理を開始する前にクラスタをフリーズして、フェールオーバーを防ぎます。リカバリ処理の完了後にクラスタを解凍します。

---

**メモ:** 完全カタログリカバリはカタログバックアップのデバイスとメディアの構成情報をリストアします。リカバリ中にストレージデバイスを構成する必要がある場合、Veritas は NetBackup イメージファイルのみをリカバリすることをお勧めします。

p.277 の「[NetBackup カatalog イメージファイルのリカバリについて](#)」を参照してください。

---

**警告:** NetBackup カタログのリカバリが完了するまでは、クライアントバックアップを実行しないでください。

---

### bprecover -wizard を使用してカタログ全体をリカバリする方法

- 1 ディザスタリカバリのサイトなどの新しい NetBackup のインストールにカタログをリカバリする場合は、以下を行います。

- NetBackup をインストールします。
  - リカバリに必要なデバイスを構成します。
  - デバイスへのリカバリに必要なメディアを追加します。
- 2 NetBackup を起動します。
- NetBackup を起動するコマンドを次に示します。
- UNIX および Linux の場合:  

```
/usr/opensv/netbackup/bin/bp.start_all
```
  - Windows の場合:  

```
install_path¥NetBackup¥bin¥bpup.exe
```
- 3 カタログバックアップとリカバリデバイスを利用できない場合は、次の手順を実行します。
- a NetBackup で必要なリカバリデバイスを構成します。  
テープストレージや BasicDisk ストレージの場合は、『NetBackup 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。NetBackup マニュアルについては、次の Web サイトを参照してください。  
<http://www.veritas.com/docs/DOC5332>
  - b カタログバックアップが変更不可の (MSDP WORM) ストレージサーバーに書き込まれている場合は、CLI nbdevconfig コマンドを使用して、マスターサーバーの構成にストレージサーバーを追加します。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。
  - c カタログバックアップを含むメディアを NetBackup に利用可能にします。これには、ロボットまたはディスクプールのインベントリの実行、スタンドアロンドライブのメディアの追加、ストレージサーバーとディスクプールの構成などを行います。  
テープストレージや BasicDisk ストレージの場合は、『NetBackup 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。NetBackup マニュアルについては、次の Web サイトを参照してください。  
<http://www.veritas.com/docs/DOC5332>
- 4 次のコマンドを入力して bprecover ウィザードを起動します。
- UNIX および Linux の場合:  

```
/usr/opensv/netBbckup/bin/admincmd/bprecover -wizard
```
  - Windows の場合:

```
install_path¥Veritas¥NetBackup¥bin¥admincmd¥bprecover.exe
-wizard
```

次のメッセージが表示されます。

```
Welcome to the NetBackup Catalog Recovery Wizard!
```

```
Please make sure the devices and media that contain catalog
disaster recovery data are available
Are you ready to continue?(Y/N)
```

- 5 [Y]を入力して続行します。次のプロンプトが表示されます。

```
Please specify the full pathname to the catalog disaster recovery
file:
```

- 6 リストアするバックアップのディザスタリカバリファイルの完全修飾パス名を入力します。次に例を示します。

```
/mnt/hdd2/netbackup/dr-file/Backup-Catalog_1318222845_FULL
```

最新のカatalogバックアップが増分バックアップである場合、増分バックアップのディザスタリカバリファイルを使用します。(増分バックアップをリストアする前に完全バックアップをリストアする必要はありません)。また、以前のバージョンのCatalogからのリカバリも可能です。

有効な DR ファイルのパス名である場合は、次のようなメッセージが表示されます。

```
vm2.example.com_1318222845
All media resources were located
Do you want to recover the entire NetBackup catalog? (Y/N)
```

DR ファイルまたはパス名が無効である場合は、コマンドラインウィザードが終了します。

- 7 [Y]を入力して続行します。次のメッセージが表示されます。

```
Do you want to startup the NetBackup relational database (NBDB)
after the recovery?(Y/N)
```

イメージファイルが適切なイメージディレクトリにリストアされ、**NetBackup** リレーションアルデータベース (**NBDB** と、該当する場合は **BMRDB**) がリストアおよびリカバリされます。

- 8 Y または N を入力して続行します。

リストアの進行中には、以下が表示されます。

```
Catalog recovery is in progress. Please wait...
```

```
Beginning recovery of NBDB. Please wait...
Completed successful recovery of NBDB on vm2.example.com
INF - Catalog recovery has completed.
```

```
WRN - NetBackup will not run scheduled backup jobs until NetBackup
is restarted.
```

```
For more information, please review the log file:
/usr/openv/netbackup/logs/user_ops/root/logs/Recover1318344410.log
```

---

**注意:** カタログリカバリが正常に完了したら、ディザスタリカバリパッケージのパスフレーズを設定する必要があります。これは、パスフレーズがカタログリカバリ中にリカバリされないためです。

---

ディザスタリカバリパッケージのパスフレーズが設定されていない場合は、次の警告が表示されます。

```
WRN - Passphrase for the disaster recovery package is not set.
You must set the passphrase for the catalog backups to be
successful.
```

パスフレーズを設定するには、次のいずれかの操作を行います。

- **NetBackup** 管理コンソールで、[セキュリティ管理 (Security Management)]、[グローバルセキュリティ設定 (Global Security Settings)]の順に展開します。詳細ペインで、[ディザスタリカバリ (Disaster Recovery)]タブをクリックし、パスフレーズを指定します。
- `nbseccmd -drpkgpassphrase` コマンドを使用してパスフレーズを指定します。

リカバリジョブが完了すると、各イメージファイルが適切なイメージディレクトリにリストアされ、**NetBackup** リレーショナルデータベース (NBDB と、該当する場合は **BMRDB**) がリストアおよびリカバリされます。

**9** 続行する前に、次の点に注意してください。

- リムーバブルメディアからカタログをリカバリした場合は、**NetBackup** はカタログメディアをフリーズします。  

p.315 の「**NetBackup** オンラインカタログリカバリメディアの凍結の解除」を参照してください。
- **NetBackup** を再起動する前に、**Veritas** はリカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結することを推奨します。
- **NetBackup** では、スケジュールバックアップジョブは、**NetBackup** を停止して再起動するまで実行されません。

NetBackup を停止して再起動する前に、バックアップジョブを手動で開始できます。ただし、リカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結しない場合は、NetBackup がそのメディアに上書きすることがあります。

- この操作は部分的なリカバリであるため、カタログのリレーショナルデータベース部分をリカバリする必要があります。  
p.294 の「[NetBackup リレーショナルデータベースのリカバリについて](#)」を参照してください。

**10** すべてのホストで許可リストのキャッシュをクリーンアップします。

**11** 次のように、マスターサーバー上および他のホスト上の NetBackup サービスを停止して再起動します。

NetBackup を停止して再起動するコマンドを次に示します。

- UNIX および Linux の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all  
/usr/opensv/netbackup/bin/bp.start_all
```

- Windows の場合:

```
install_path%NetBackup%bin%bpdwn  
install_path%NetBackup%bin%bpup
```

**12** サービスを再起動したら、次のコマンドを実行します。

- NetBackup (またはホスト ID ベース) の証明書が NetBackup ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -renewcertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -renewcertificate -cluster
```

- 外部 CA が署名した証明書が NetBackup ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate  
-cluster
```

- コマンドが正常に実行された場合は、次の手順に進みます。
- このコマンドが終了状態 **5988** を表示して失敗した場合は、次のトピックを参照してください。  
**p.315** の「[カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順](#)」を参照してください。  
 次の手順に進みます。

**13** カタログリカバリがサーバーのリカバリ手順の一環である場合は、適切なリカバリ手順に従って残りの手順を完了します。

この手順には、次の作業が含まれます。

- バックアップメディアからカタログへのバックアップのインポート
- メディアの書き込み保護
- メディアの取り出しおよび保管
- メディアの凍結

---

**メモ:** カタログリカバリを実行すると、NetBackup の構成がカタログバックアップの時点に戻されます。カタログバックアップの特定時点の後に行われる構成への変更(ポリシー、クライアント、ストレージユニットへの変更など)は、必要に応じて再度適用する必要があります。これらの変更は、新しいバックアップを作成する前に再度適用する必要があります。変更が適用されない場合、保護対象と保護の管理方法に影響する可能性があります。

たとえば、新しいイメージに対して WORM ロックの使用を必須とするようにストレージユニットが変更されている場合があります。WORM ロックが再適用されないと、必要な WORM 保護が新しいバックアップに適用されません。

---

## カタログリカバリ前の NAT メディアサーバーとの接続の確立

カタログが NAT メディアサーバーでバックアップされている場合は、カタログリカバリの前にマスターサーバーで次の手順を実行して NAT メディアサーバーとの接続を確立する必要があります。

NetBackup の NAT のサポートについて詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

### NAT メディアサーバーとの接続を確立するには

- 1 マスターサーバー上で `configureMQ` コマンドを実行します。
- 2 `nbsetconfig` コマンドを使用して、マスターサーバーで次の構成オプションを設定します。
  - カatalogバックアップが作成された NAT メディアサーバーの名前を使用して `NAT_SERVER_LIST` を更新します。
  - `INITIATE_REVERSE_CONNECTION` を `TRUE` に設定します。

構成オプションについて詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

- 3 マスターサーバーでサービスを再起動します。
- 4 マスターサーバーと NAT メディアサーバー間のリバース接続が、`bptestbpcd` コマンドを使用して確立されているかどうかを確認します。

p.262 の「[NetBackup カタログ全体のリカバリについて](#)」を参照してください。

## NetBackup カタログイメージファイルのリカバリについて

カタログイメージファイルには、バックアップされているすべてのデータに関する情報が含まれています。NetBackup カタログの大部分は、この情報です。この形式のカタログリカバリでは次の操作をします。

- イメージ .f ファイルをリカバリします。
- 構成ファイルをリカバリします (databases.conf と server.conf)。
- 必要に応じて後の処理で利用できるように、ステージングディレクトリに NetBackup リレーショナルデータベース (NBDB) をリストアします。  
p.305 の「[ステージングでのリレーショナルデータベースの処理について](#)」を参照してください。
- 必要に応じて、ポリシーとライセンスデータをリカバリします。

表 4-4 は部分的なりカバリに含まれているファイルのリストです。

---

**メモ:** イメージファイルは NetBackup リレーショナルデータベースに格納されます。イメージファイルにはバックアップの詳細を記述するメタデータが含まれています。

---

NetBackup は、ディザスタリカバリでクラスタ環境からクラスタ化されていないマスターサーバーにカタログイメージファイルと構成ファイルをリカバリできます。

## リカバリの推奨事項

p.256 の「[NetBackup のカタログリカバリとシンボリックリンクについて](#)」を参照してください。

Veritas では次のシナリオでカタログイメージファイルをリカバリすることをお勧めします。

- NetBackup リレーショナルデータベースは有効でも、NetBackup ポリシーファイル、バックアップイメージファイルまたは構成ファイルが消失または破損している場合。
- NetBackup カタログ全体をリストアする前に、カタログの一部だけをリストアする場合。この手順を実行すると、カタログイメージと構成ファイルだけがリカバリされます。イメージファイルをリカバリ後、リレーショナルデータベースをリカバリできます。  
p.294 の「[NetBackup リレーショナルデータベースのリカバリについて](#)」を参照してください。
- 異なるストレージデバイスを使用してカタログをリカバリする場合。ストレージハードウェアの障害または交換の後にこれと同じ環境になる場合があります。カタログバックアップとクライアントバックアップをレプリケートするのは別のサイトである場合があります。いずれにしても、カタログバックアップとクライアントバックアップは異なるハードウェアに存在します。  
このリカバリでは、カタログバックアップのもう有効ではない古いストレージデバイス情報で新しいストレージデバイス構成が上書きされません。

## カタログリカバリとバックアップの種類

リカバリには、次のようにディザスタリカバリファイルにリストされたカタログバックアップにあるカタログイメージファイルと構成ファイルが含まれます。

- 完全バックアップ     ディザスタリカバリファイルにリストされたイメージファイルと構成ファイルがリカバリされます。
- 増分バックアップ     次の 2 つのリカバリのシナリオが存在します。
- カタログには対応する完全バックアップと他の増分バックアップについての情報は含まれていません。  
**NetBackup** はその増分バックアップでバックアップされたバックアップイメージ .f ファイル、構成ファイルおよび **NetBackup** ポリシーファイルのみをリストアします。  
 ただし、最新の完全なカタログバックアップまでのカタログのバックアップイメージ .f ファイルすべてはリストアされます。そのため、残りのポリシーファイル、イメージ .f ファイル、構成ファイルは、バックアップ、アーカイブ、リストアインターフェースを使用してリストアできます。
  - カタログには対応する完全バックアップと他の増分バックアップについての情報が含まれます。  
**NetBackup** はカタログバックアップの関連セットに含まれていたすべてのバックアップイメージ .f ファイルと構成ファイルをリストアします。

## カタログイメージファイル

表 4-4 は部分的なカタログリカバリを構成するファイルをリストします。

表 4-4                      カタログイメージファイル

UNIX および Linux	Windows の場合
/usr/opensv/netbackup/bp.conf	なし
/usr/opensv/netbackup/db/*	install_path¥NetBackup¥db¥*
/usr/opensv/netbackup/db/class/*(オプション)	install_path¥NetBackup¥db¥class¥*(オプション)
/usr/opensv/netbackup/vault/sessions*	install_path¥NetBackup¥vault¥sessions¥*
/usr/opensv/var/*(オプション)	install_path¥NetBackup¥var¥*(オプション)
/usr/opensv/volmgr/database/*	install_path¥Volmgr¥database¥*
/usr/opensv/volmgr/vm.conf	install_path¥Volmgr¥vm.conf

## リカバリ方式

次のいずれかの方法でカタログイメージファイルをリカバリできます。

- **NetBackup** 管理コンソールの [カタログリカバリウィザード (Catalog Recovery Wizard)]

p.263 の「[カタログリカバリウィザードを使用したカタログ全体のリカバリNetBackup](#)」を参照してください。

- テキストベースのリカバリウィザード。bprecover -wizard コマンドとオプションによってテキストベースのリカバリウィザードが起動します。

p.271 の「[bprecover -wizard を使用した NetBackup カタログ全体のリカバリ](#)」を参照してください。

## カタログリカバリウィザードを使用した NetBackup カタログイメージファイルのリカバリ

この手順では、[カタログリカバリウィザード (Catalog Recovery Wizard)]を使用して NetBackup カタログイメージファイルをリカバリする方法について説明します。リレーショナルデータベースのトランザクションログはイメージファイルのリカバリ中に適用されます。

p.277 の「[NetBackup カタログイメージファイルのリカバリについて](#)」を参照してください。

この手順を実行するには、root (管理) 権限が必要です。

カタログをリカバリしたいマスターサーバーにログオンする必要があります。[カタログリカバリウィザード (Catalog Recovery Wizard)]は、サーバーの変更操作の実行後は動作しません。

---

**メモ:** このウィザードでは、カタログバックアップの実行中に生成されたディザスタリカバリファイルが必要です。ディザスタリカバリファイルのパスはカタログバックアップポリシーで指定されます。

---

---

**メモ:** カatalogリカバリ処理の間に、NetBackup はサービスを停止して再起動することがあります。NetBackup が高可用性アプリケーション (クラスタまたはグローバルクラスタ) として構成されている場合は、リカバリ処理を開始する前にクラスタをフリーズして、フェールオーバーを防ぎます。リカバリ処理の完了後にクラスタを解凍します。

---

---

**警告:** NetBackup カタログのリカバリが完了するまでは、クライアントバックアップを実行しないでください。

---

p.277 の「[NetBackup カタログイメージファイルのリカバリについて](#)」を参照してください。

カタログリカバリウィザードを使用してカタログイメージファイルをリカバリする方法

1 NetBackup が実行されていない場合は、次のコマンドを入力して、すべての NetBackup サービスを起動します。

- UNIX および Linux の場合:  
`/usr/opensv/netbackup/bin/bp.start_all`

- Windows の場合:  
`install_path¥NetBackup¥bin¥bpup`
- 2 カタログバックアップとリカバリデバイスを利用できない場合は、次の手順を実行します。
    - a NetBackup で必要なリカバリデバイスを構成します。

テープストレージや BasicDisk ストレージの場合は、『NetBackup 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。NetBackup マニュアルについては、次の Web サイトを参照してください。
    - b カタログバックアップを含むメディアを NetBackup に利用可能にします。これには、ロボットまたはディスクプールのインベントリの実行、スタンドアロンドライブのメディアの追加、ストレージサーバーとディスクプールの構成などを行います。

テープストレージや BasicDisk ストレージの場合は、『NetBackup 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。NetBackup マニュアルについては、次の Web サイトを参照してください。
    - c 元の環境のシンボリックリンクと一致するようにシンボリックリンクを作成します。

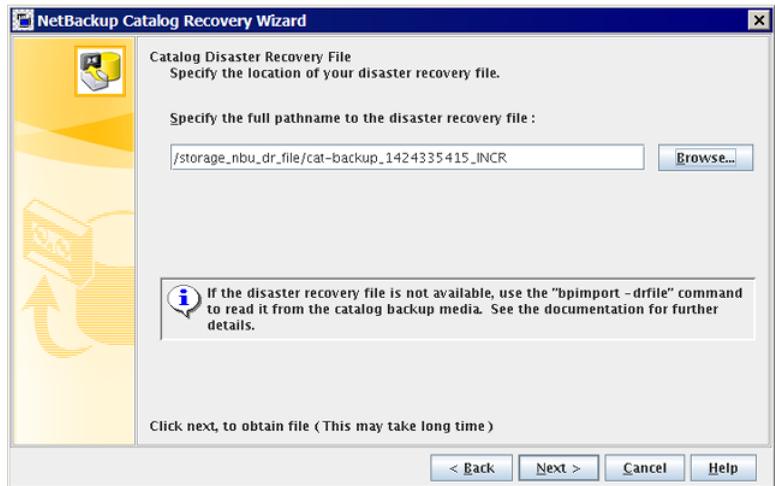
p.256 の「NetBackup のカタログリカバリとシンボリックリンクについて」を参照してください。
  - 3 NetBackup 管理コンソールウィンドウの左ペインで[NetBackup の管理 (NetBackup Management)]をクリックし、右ペインで[カタログのリカバリ (Recover the catalogs)]をクリックします。

[NetBackup カタログリカバリウィザード (NetBackup Catalog Recovery Wizard)]の[ようこそ (Welcome)]パネルが表示されます。
  - 4 [ようこそ (Welcome)]パネルで[次へ (Next)]をクリックして、[カタログのディザスタリカバリファイル (Catalog Disaster Recovery File)]パネルを表示します。

- 5 [カタログのディザスタリカバリファイル (Catalog Disaster Recovery File)] パネルで、ディザスタリカバリファイルの格納場所を指定します。ファイルを参照して選択するか、ディザスタリカバリファイルの絶対パス名を入力できます。

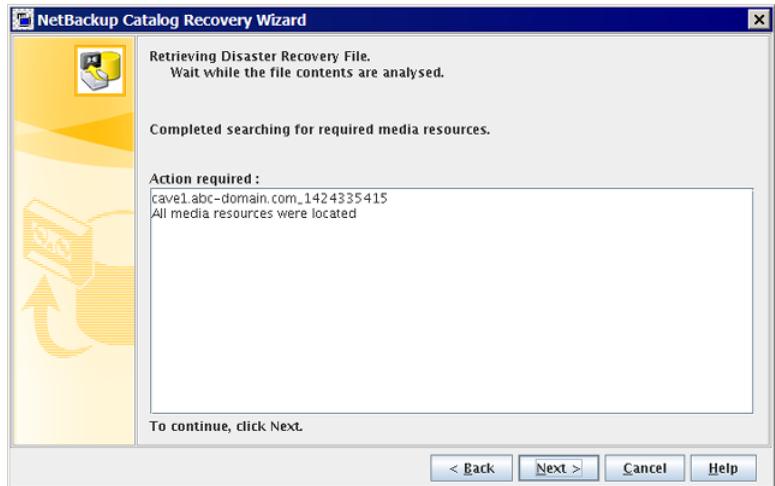
ほとんどの場合、利用可能な最新のディザスタリカバリ情報ファイルを指定します。最新のカタログバックアップが増分バックアップである場合、増分バックアップのディザスタリカバリファイルを使用します。(増分バックアップをリストアする前に完全バックアップをリストアする必要はありません。)

何らかの破損が発生した場合、カタログの以前の状態にリストアすることが必要になる場合もあります。



[次へ (Next)] をクリックして続行します。[ディザスタリカバリファイルを取得しています (Retrieving Disaster Recovery File)] パネルが表示されます。

- 6 ウィザードがカタログをリカバリするために必要なメディアを検索し、[ディザスタリカバリファイルを取得しています (Retrieving Disaster Recovery File)]パネルに進捗状況が表示されます。その後、ディザスタリカバリイメージの必要なバックアップ ID が検出されたかどうかが表示されます。メディアが検出されなかった場合は、データベースの更新に必要なメディアが表示されます。

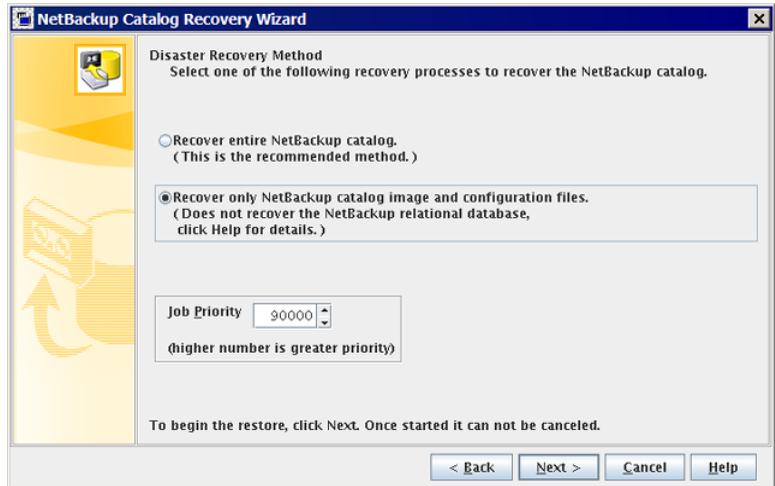


必要に応じて、ウィザードの指示に従って表示されたメディアを挿入し、インベントリを実行して **NetBackup** データベースを更新します。このパネルに表示される情報は、完全バックアップまたは増分バックアップのどちらからリカバリするかによって異なります。

必要なメディアソースがすべて検出されたら、[次へ (Next)]をクリックします。[ディザスタリカバリ方式 (Disaster Recovery Method)]パネルが表示されます。

[ディザスタリカバリ方式 (Disaster Recovery Method)]パネルが表示されます。

- 7 [ディザスタリカバリ方式 (Disaster Recovery Method)]パネルで、次の手順を実行します。
- **NetBackup** のカタログイメージと構成ファイルのみをリカバリします。
  - ジョブ優先度を指定します。



続行するには、[次へ (Next)]をクリックします。

[カタログのリカバリ (Recovering Catalog)]パネルが表示されます。

- 8 [カタログのリカバリ (Recovering Catalog)] パネルにリカバリの進捗状況が表示されます。



処理は次のようにリカバリ結果によって決まります。

- |         |   |
|---------|---|
| 成功しなかった | ログファイルのメッセージを参照して問題を確認します。[キャンセル (Cancel)]をクリックし、問題を解決してから、ウィザードを再度実行します。 |
| 成功する場合  | [次へ (Next)]をクリックして最後のウィザードパネルに進みます。                                       |

- 9 最後のウィザードパネルで、[完了 (Finish)]をクリックします。

リカバリジョブが終了するとき、各イメージファイルは適切なイメージディレクトリにリストアされ、構成ファイルがリストアされます。

- 10 次のとおり、ステー징ディレクトリのリレーショナルデータベースからイメージメタデータをエクスポートします。

```
cat_export -all -staging -source_master source-master-server-name
```

エクスポートはイメージメタデータをリレーショナルデータベースにインポートするために必要です。カタログイメージファイルのリカバリはリレーショナルデータベースを回復しません。

- 11 次のとおり、リレーショナルデータベースにイメージメタデータをインポートします。

```
cat_import -all -replace_destination
```

- 12** ディスクデバイスからカタログをリカバリした場合は、イメージヘッダーのディスクメディア ID 参照の修正が必要になることがあります。イメージヘッダーはカタログバックアップからリカバリされています。

イメージヘッダーのディスクメディア ID を修正するには、次のコマンドを実行します。

```
nbcatsync -backupid image_id -dryrun
```

*image\_id* をカタログバックアップの ID に置き換えます。カタログバックアップのイメージ ID は DR ファイルで調べることができます。

- 13** 続行する前に、次の点に注意してください。
- リムーバブルメディアからカタログをリカバリした場合は、**NetBackup** はカタログメディアをフリーズします。  
[p.315 の「NetBackup オンラインカタログリカバリメディアの凍結の解除」](#)を参照してください。
  - **NetBackup** を再起動する前に、**Veritas** はリカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結することを推奨します。
  - **NetBackup** では、スケジュールバックアップジョブは、**NetBackup** を停止して再起動するまで実行されません。  
**NetBackup** を停止して再起動する前に、バックアップジョブを手動で開始できます。ただし、リカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結しない場合は、**NetBackup** がそのメディアに上書きすることがあります。
  - この操作は部分的なリカバリであるため、カタログのリレーショナルデータベース部分をリカバリする必要があります。  
[p.294 の「NetBackup リレーショナルデータベースのリカバリについて」](#)を参照してください。

- 14** 次のように、マスターサーバー上の **NetBackup** サービスを停止して再起動します。

- **UNIX** および **Linux** の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all  
/usr/opensv/netbackup/bin/bp.start_all
```

- **Windows** の場合:

```
install_path¥NetBackup¥bin¥bpdwn  
install_path¥NetBackup¥bin¥bpup
```

- 15** サービスを再起動したら、次のコマンドを実行します。

非クラスタ設定の場合:

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate
```

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate
```

クラスタ設定の場合:

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate -cluster
```

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

- コマンドが正常に実行された場合は、次の手順に進みます。
- このコマンドが終了状態 5988 を表示して失敗した場合は、次のトピックを参照してください。  
p.315 の「[カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順](#)」を参照してください。  
次の手順に進みます。

- 16** カタログリカバリがサーバーのリカバリ手順の一環である場合は、適切なリカバリ手順に従って残りの手順を完了します。

リカバリには次の作業が含まれます。

- バックアップメディアからカタログへのバックアップのインポート。
- メディアの書き込み保護。
- メディアの取り出しおよび保管。
- メディアの凍結。

## bprecover -wizard を使った NetBackup カタログイメージファイルのリカバリ

この手順を実行するには、root (管理) 権限が必要です。

カタログをリカバリしたいマスターサーバーにログオンする必要があります。[カタログリカバリウィザード (Catalog Recovery Wizard)]は、サーバーの変更操作の実行後は動作しません。

---

**メモ:** このウィザードでは、カタログバックアップの実行中に生成されたディザスタリカバリファイルが必要です。ディザスタリカバリファイルのパスはカタログバックアップポリシーで指定されます。

---

---

**メモ:** カタログリカバリ処理の間に、サービスが停止して再起動することがあります。  
**NetBackup** が高可用性アプリケーション (クラスタまたはグローバルクラスタ) として構成されている場合は、リカバリ処理を開始する前にクラスタをフリーズして、フェールオーバーを防ぎます。リカバリ処理の完了後にクラスタを解凍します。

---

**警告:** NetBackup カタログのリカバリが完了するまでは、クライアントバックアップを実行しないでください。

---

p.277 の「[NetBackup カatalogイメージファイルのリカバリについて](#)」を参照してください。

### bprecover -wizard を使用してカATALOGイメージファイルをリカバリする方法

- 1 ディザスタリカバリのサイトなどの新しい NetBackup のインストールにカATALOGをリカバリする場合は、以下を行います。
  - NetBackup をインストールします。
  - リカバリに必要なデバイスを構成します。
  - デバイスへのリカバリに必要なメディアを追加します。
  - 元の環境の `symlink` と一致するように `symlink` を作成します。  
p.256 の「[NetBackup のカATALOGリカバリとシンボリックリンクについて](#)」を参照してください。
- 2 EMM サーバーがマスターサーバーと異なるホストにある場合は、次のコマンドの入力によってそのホストの NetBackup サービスを開始します。
  - Windows の場合:  

```
install_path¥NetBackup¥bin¥bpup
```
  - UNIX および Linux の場合:  

```
/usr/opensv/netbackup/bin/bp.start_all
```
- 3 次のコマンドの入力によってマスターサーバーの NetBackup サービスを開始します。
  - Windows の場合:  

```
install_path¥NetBackup¥bin¥bpup
```
  - UNIX および Linux の場合:  

```
/usr/opensv/netbackup/bin/bp.start_all
```

- 4 次のコマンドを入力して bprecover ウィザードを起動します。

```
bprecover -wizard
```

次のメッセージが表示されます。

```
Welcome to the NetBackup Catalog Recovery Wizard!  
Please make sure the devices and media that contain catalog  
disaster recovery data are available  
Are you ready to continue?(Y/N)
```

- 5 [Y]を入力して続行します。ディザスタリカバリのフルパス名の入力を促す次のようなプロンプトが表示されます。

```
Please specify the full pathname to the catalog disaster recovery  
file:
```

- 6 リストアするバックアップのディザスタリカバリファイルの完全修飾パス名を入力します。たとえば、

```
/mnt/hdd2/netbackup/dr-file/Backup-Catalog_1318222845_FULL
```

最新のカatalogバックアップが増分バックアップである場合、増分バックアップのディザスタリカバリファイルを使用します。(増分バックアップをリストアする前に完全バックアップをリストアする必要はありません)。また、以前のバージョンのCatalogからのリカバリも可能です。

完全バックアップ用の DR ファイルを指定した場合は、次に示すようなメッセージが表示されます。

```
vm2.example.com_1318222845  
All media resources were located
```

```
Do you want to recover the entire NetBackup catalog? (Y/N)
```

増分バックアップ用の DR ファイルを指定した場合は、次のようなメッセージが表示されます。

```
vm2.example.com_1318309224  
All media resources were located
```

```
The last catalog backup in the catalog disaster recovery file is
```

```
an incremental.
```

```
If no catalog backup images exist in the catalog,  
a PARTIAL catalog recovery will only restore the NetBackup catalog  
files backed up in that incremental backup.
```

```
However, all of the catalog backup images up to the last full  
catalog  
backup are restored. Then you can restore the remaining NetBackup
```

```
catalog files from the Backup, Archive, and Restore user  
interface.
```

```
If catalog backup images already exist, all files that were  
included
```

```
in the related set of catalog backups are restored.
```

```
Do you want to recover the entire NetBackup catalog? (Y/N)
```

- 7** **N** を入力して続行します。次のメッセージが表示されます。

```
A PARTIAL catalog recovery includes the images directory
containing the dotf files and staging of the NetBackup relational
database (NBDB) for further processing.
```

```
Do you also want to include policy data?(Y/N)
```

- 8** **Y** または **N** を入力して続行します。次のメッセージが表示されます。

```
Do you also want to include licensing data?(Y/N)
```

- 9** **Y** または **N** を入力して続行します。次のメッセージが表示されます。

```
Catalog recovery is in progress. Please wait...
```

```
Completed successful recovery of NBDB in staging directory on
vm2.example.com
```

```
This portion of the catalog recovery has completed.
Because this was a PARTIAL recovery of the NetBackup catalog,
any remaining files included in the catalog backup can be restored
using the Backup, Archive, and Restore user interface.
```

```
The image metadata that is stored in NBDB in the staging directory
can be exported using "cat_export -staging", and, imported using
"cat_import".
```

```
The "nbdb_unload -staging" command can be used to unload one or
more
database tables from NBDB in the staging directory.
```

```
The "nbdb_restore -recover -staging" command can be used to
replace
NBDB in the data directory with the contents from the staging
directory.
```

```
WRN - NetBackup will not run scheduled backup jobs until NetBackup
is restarted.
```

```
For more information, please review the log file:
/usr/opensv/netbackup/logs/user_ops/root/logs/Recover1318357550.log
```

- 10** リカバリジョブが終了するとき、各イメージファイルは適切なイメージディレクトリにリストアされ、構成ファイルがリストアされます。ポリシーデータとライセンスデータをリカバリするように選択した場合は、そのデータもリストアされます。

- 11** 次のとおり、ステージングディレクトリのリレーショナルデータベースからイメージメタデータをエクスポートします。

```
cat_export -all -staging -source_master source-master-server-name
```

エクスポートはイメージメタデータをリレーショナルデータベースにインポートするために必要です。カタログイメージファイルのリカバリはリレーショナルデータベースを回復しません。

- 12** 次のとおり、リレーショナルデータベースにイメージメタデータをインポートします。

```
cat_import -all -replace_destination
```

- 13** ディスクデバイスからカタログをリカバリした場合は、イメージヘッダーのディスクメディア ID 参照の修正が必要になることがあります。イメージヘッダーはカタログバックアップからリカバリされています。

p.256 の「[ディスクデバイスからの NetBackup カタログリカバリについて](#)」を参照してください。

イメージヘッダーのディスクメディア ID を修正するには、次のコマンドを実行します。

```
nbcatsync -backupid image_id -prune_catalog
```

*image\_id* をカタログバックアップの ID に置き換えます。bprecover の出力に、リストアするカタログバックアップのイメージ ID が表示されます。カタログバックアップのイメージ ID は DR ファイルで調べることもできます。

- 14** 続行する前に、次の点に注意してください。

- リムーバブルメディアからカタログをリカバリした場合は、**NetBackup** はカタログメディアをフリーズします。

p.315 の「[NetBackup オンラインカタログリカバリメディアの凍結の解除](#)」を参照してください。

- **NetBackup** を再起動する前に、**Veritas** はリカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結することを推奨します。

- **NetBackup** では、スケジュールバックアップジョブは、**NetBackup** を停止して再起動するまで実行されません。

**NetBackup** を停止して再起動する前に、バックアップジョブを手動で開始できます。ただし、リカバリするカタログの日付よりも新しいバックアップを含むメディアを凍結しない場合は、**NetBackup** がそのメディアに上書きすることがあります。

- この操作は部分的なりカバリであるため、カタログのリレーショナルデータベース部分をリカバリする必要があります。

p.294 の「**NetBackup** リレーショナルデータベースのリカバリについて」を参照してください。

- 15 すべてのホストで許可リストのキャッシュをクリーンアップします。
- 16 次のように、マスターサーバー上および他のホスト上の **NetBackup** サービスを停止して再起動します。

- **Windows** の場合:

```
install_path¥NetBackup¥bin¥bpdwn
install_path¥NetBackup¥bin¥bpup
```

- **UNIX** の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all
/usr/opensv/netbackup/bin/bp.start_all
```

- 17 サービスを再起動したら、次のコマンドを実行します。

- **NetBackup** (またはホスト ID ベース) の証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合:

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate
```

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate
```

クラスタ設定の場合:

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate -cluster
```

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

- 外部 CA が署名した証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

外部 CA が署名した証明書が **NetBackup** ドメインで使用される場合、非クラスタ設定で以下を実行します。

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate  
-cluster
```

- コマンドが正常に実行された場合は、次の手順に進みます。
- このコマンドが終了状態 **5988** を表示して失敗した場合は、次のトピックを参照してください。  
p.315 の「[カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順](#)」を参照してください。  
次の手順に進みます。

**18** カタログリカバリがサーバーのリカバリ手順の一環である場合は、適切なリカバリ手順に従って残りの手順を完了します。

この手順には、次の作業が含まれます。

- バックアップメディアからカタログへのバックアップのインポート
- メディアの書き込み保護
- メディアの取り出しおよび保管
- メディアの凍結

## NetBackup リレーショナルデータベースのリカバリについて

NetBackup データベース (NBDB) は Enterprise Media Manager (EMM) データベースとも呼ばれます。それは、NetBackup ストレージユニットにあるボリューム、ロボット、ドライブについての情報を含んでいます。NetBackup リレーショナルデータベースには NetBackup のカタログイメージファイルも含まれます。イメージファイルにはバックアップの詳細を記述するメタデータが含まれています。

NetBackup のリレーショナルデータベースは、カタログ全体のバックアップとは切りはなしてリカバリすることが可能です。

バックアップからのリカバリ

p.295 の「[NetBackup リレーショナルデータベースファイルのバックアップからのリカバリ](#)」を参照してください。

ステージングディレクトリからのリカバリ p.301 の「[NetBackup リレーショナルデータベースのファイルをステージングからリカバリする](#)」を参照してください。

## NetBackup リレーショナルデータベースファイルのバックアップからのリカバリ

バックアップから NBDB (NetBackup) または BMRDB (Bare Metal Restore) のリレーショナルデータベースファイルをリカバリできます。カタログバックアップをリカバリする前に、有効なデータベースがある必要があります。したがって、バックアップからリカバリするための手順は、次のように、場合によって異なります。

データベースが壊れていない場合 NBDB データベースが利用可能であり、SQL Anywhere サーバーが実行中の場合は、データベースを作成する必要はありません。次のステップ 11 およびステップ 13 だけを実行してください。

データベースが壊れている場合 NBDB データベースが破損した場合、または存在しない場合にのみ、この手順のすべてのステップに従ってください。有効な空のデータベースを作成する必要があります。完全な手順には、この作業が含まれています。

カタログバックアップから NetBackup リレーショナルデータベースファイルをリカバリするには

- 1 NetBackup サービスを実行している場合は、次のように停止します。

UNIX の場合 `/usr/opensv/netbackup/bin/bp.kill_all`  
場合:

Windows の `install_path¥NetBackup¥bin¥bpdwn`  
場合:

- 2 データベースファイルのディレクトリから一時ディレクトリに \*.db ファイルと \*.log ファイルを移動します。データベースファイルのデフォルトの場所を次に示します。

UNIX の場合 `/usr/opensv/db/data`  
場合:

Windows の `C:¥Program Files¥Veritas¥NetBackupDB¥data`  
場合:

- 3 ホストの起動時に **SQL Anywhere** が自動的に起動しないように、**SQL Anywhere** を次のように構成します。

UNIX の場     /usr/opensv/db/bin/nbdb\_admin -auto\_start NONE  
合:

Windows の    install\_path¥NetBackup¥bin¥nbdb\_admin -auto\_start  
場合:           NONE

- 4 次のように、**SQL Anywhere** サーバーを起動します。

UNIX の場     /usr/opensv/netbackup/bin/nbdbms\_start\_stop start  
合:

Windows の    install\_path¥NetBackup¥bin¥bpup -e SQLANYs\_VERITAS\_NB  
場合:

- 5 データベースを作成します。実行するコマンドはシナリオによって次のように異なります。

通常のシナリオ

UNIX の場合: `/usr/opensv/db/bin/create_nbdb -drop`

Windows の場合:

`install_path¥NetBackup¥bin¥create_nbdb -drop`

データベースを再配置したか、または環境をクラスタ化している

UNIX の場合: `/usr/opensv/db/bin/create_nbdb -data`

`VXDBMS_NB_DATA -drop -staging`

`VXDBMS_NB_STAGING`

Windows の場合:

`install_path¥NetBackup¥bin¥create_nbdb -data`

`VXDBMS_NB_DATA -drop -staging`

`VXDBMS_NB_STAGING`

ステップ `VXDBMS_NB_DATA` で作成した一時ディレクトリにある `vxdbms.conf` ファイルから `VXDBMS_NB_STAGING` と 2 の値を取得します。

データベースを再配置したか、または環境をクラスタ化している。領域の制約によって最終的な場所にこの一時データベースを作成する

UNIX の場合: `/usr/opensv/db/bin/create_nbdb -drop`

`-data VXDBMS_NB_DATA -index VXDBMS_NB_INDEX`

`-tlog VXDBMS_NB_TLOG -staging`

`VXDBMS_NB_STAGING`

Windows の場合:

`install_path¥NetBackup¥bin¥create_nbdb -drop`

`-data VXDBMS_NB_DATA -index VXDBMS_NB_INDEX`

`-tlog VXDBMS_NB_TLOG -staging`

`VXDBMS_NB_STAGING`

ステップ 2 で作成した一時ディレクトリにある `vxdbms.conf` ファイルからオプションの引数の値を取得します。

- 6 次のように NetBackup サービスを開始します。

UNIX の場合: `/usr/opensv/netbackup/bin/bp.start_all`

Windows の場合: `install_path¥NetBackup¥bin¥bpup`

- 7 次のコマンドを実行して、デフォルトのデバイスプロトコルと設定を NetBackup EMM (Enterprise Media Manager) データベースにロードします。

UNIX の場 合: `/usr/opensv/volmgr/bin/tpext -loadEMM`

Windows の 場 合: `install_path%Volmgr%bin%tpext -loadEMM`

- 8 `nbdb_move` コマンドを使って NetBackup データベースファイルの再配置した場合は、カタログのバックアップ時にデータベースファイルが配置されていたディレクトリを再作成します。次に、`nbdb_move` コマンドでデータベースファイルが移動されるデフォルトの場所を示します。

UNIX の場 合: `/usr/opensv/db/data`

Windows の 場 合: `install_path%NetBackupDB%data`

- 9 次のように、NetBackup マスターサーバー上の NetBackup Device Manager を起動します。

UNIX の場 合: `/usr/opensv/volmgr/bin/ltid -v`

Windows の 場 合: Windows の [コンピュータの管理] を使用して、NetBackup Device Manager サービスを開始します (`ltid.exe`)。

**10** カタログバックアップとリカバリデバイスを利用できない場合は、次の手順を実行します。

**a** **NetBackup** で必要なリカバリデバイスを構成します。

テープストレージや **BasicDisk** ストレージの場合は、『**NetBackup** 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。**NetBackup** マニュアルについては、次の **Web** サイトを参照してください。

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

**b** カタログバックアップを含むメディアを **NetBackup** に利用可能にします。これには、ロボットまたはディスクプールのインベントリの実行、スタンドアロンドライブのメディアの追加、ストレージサーバーとディスクプールの構成などを行います。

テープストレージや **BasicDisk** ストレージの場合は、『**NetBackup** 管理者ガイド Vol. 1』を参照してください。ディスクストレージ形式の場合、そのオプションが記述されたガイドを参照してください。**NetBackup** マニュアルについては、次の **Web** サイトを参照してください。

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

**c** カタログバックアップをこれが存在するメディアからインポートします。

『**NetBackup** 管理者ガイド Vol. 1』を参照してください。

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

**11** マスターサーバーで次のコマンドを実行してカタログをリカバリします。

**UNIX** の場 `/usr/opensv/netbackup/bin/admincmd/bprecover -r -nbdb`  
 合:

**Windows** の `install_path¥NetBackup¥bin¥admincmd¥bprecover -r -nbdb`  
 場合:

**12** すべてのホストで許可リストのキャッシュをクリーンアップします。

- 13** 次のように、マスターサーバー上および他のホスト上の **NetBackup** サービスを停止して再起動します。

UNIX の場     /usr/opensv/netbackup/bin/bp.kill\_all  
 合:            /usr/opensv/netbackup/bin/bp.start\_all

Windows の   install\_path%NetBackup%bin%bpdown  
 場合:         install\_path%NetBackup%bin%bpup

- 14** サービスを再起動したら、次のコマンドを実行します。

- **NetBackup** (またはホスト ID ベース) の証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -renewcertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -renewcertificate -cluster
```

- 外部 CA が署名した証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -enrollCertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate  
-cluster
```

このコマンドが終了状態 5988 を表示して失敗した場合は、次のトピックを参照してください。

p.315 の「[カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順](#)」を参照してください。

## NetBackup リレーショナルデータベースのファイルをステージングからリカバリする

カタログバックアップの間、NetBackup はステージングディレクトリにリレーショナルデータベースのファイルをコピーします。イメージファイルと設定ファイルをリストアするリカバリオプションは、リレーショナルデータベースのファイルもステージングのディレクトリにリストアします。

p.277 の「[NetBackup カatalog イメージファイルのリカバリについて](#)」を参照してください。

NetBackup NBDB リレーショナルデータベースファイルは、ステージングディレクトリからリカバリできます。また、NetBackup のコマンドを使用して、NBDB リレーショナルデータベースのファイルの処理を進められます。

p.305 の「[ステージングでのリレーショナルデータベースの処理について](#)」を参照してください。

リレーショナルデータベースがステージングからリカバリされる時、NetBackup はリカバリ中に最新のオンライントランザクションログも適用します。トランザクションログを適用することで、最新の db/images ディレクトリと可能なかぎり一貫したデータベースにできます。

ステージングディレクトリからのリカバリには次のような 2 つの手順があります。

データベースが壊れていない場合 p.302 の「[データベースが壊れていない場合にリレーショナルデータベースのファイルをステージングからリカバリする](#)」を参照してください。

データベースが壊れている場合 p.302 の「[データベースが壊れている場合にリレーショナルデータベースのファイルをステージングからリカバリする](#)」を参照してください。

データベースが壊れていない場合にリレーショナルデータベースのファイルをステージングからリカバリする

- 1 ステージングから NBDB をリカバリするには、マスターサーバーで次のコマンドを実行してください。

UNIX: `/usr/opensv/db/bin/nbdb_restore -dbn NBDB -recover -staging`

Windows: `install_path¥NetBackup¥bin¥nbdb_restore -dbn NBDB -recover -staging`

- 2 次のように、NetBackup を停止し、再起動します。

UNIX の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all  
/usr/opensv/netbackup/bin/bp.start_all
```

Windows の場合:

```
install_path¥NetBackup¥bin¥bpdown  
install_path¥NetBackup¥bin¥bpup
```

データベースが壊れている場合にリレーショナルデータベースのファイルをステージングからリカバリする

- 1 NetBackup サービスを実行している場合は、次のように停止します。

UNIX の場合: `/usr/opensv/netbackup/bin/bp.kill_all`

Windows の場合: `install_path¥NetBackup¥bin¥bpdown`

- 2 次のデータベースファイルのディレクトリから一時ディレクトリに \*.db と \*.log ファイルを移動します:

UNIX の場合: `/usr/opensv/db/data`

Windows の場合: `C:¥Program Files¥Veritas¥NetBackupDB¥data`

- 3 ホストの起動時に SQL Anywhere が自動的に起動しないように、SQL Anywhere を次のように構成します。

Linux の場合: `/usr/opensv/db/bin/nbdb_admin -auto_start NONE`

Windows の場合: `install_path¥NetBackup¥bin¥nbdb_admin -auto_start NONE`

- 4 次のように、SQL Anywhere サーバーを起動します。

UNIX の場合: `/usr/opensv/netbackup/bin/nbdbms_start_stop start`

Windows の場合: `install_path¥NetBackup¥bin¥bpup -e SQLANYs_VERITAS_NB`

- 5 次のとおり、空のデータベースを作成します:

UNIX の場合: `/usr/opensv/db/bin/create_nbdb -drop`

Windows の場合: `install_path¥NetBackup¥bin¥create_nbdb -drop`

- 6 次のように、**NetBackup** を停止し、再起動します。

UNIX および Linux の場合:

`/usr/opensv/netbackup/bin/bp.kill_all`  
`/usr/opensv/netbackup/bin/bp.start_all`

Windows の場合:

`install_path¥NetBackup¥bin¥bpdown`  
`install_path¥NetBackup¥bin¥bpup`

- 7 次のように、**NetBackup** `tpext` コマンドを実行してデバイスのマップファイルを更新します。

UNIX の場合: `/usr/opensv/volmgr/bin/tpext -loadEMM`

Windows の場合: `install_path¥Volmgr¥bin¥tpext -loadEMM`

- 8 `nbdb_move` コマンドを使用して **NetBackup** データベースファイルの再配置を実行した場合は、カタログのバックアップ時にデータベースファイルが配置されていたディレクトリを再作成します。

- 9 次のように、**NetBackup** デバイスマネージャを起動します。

UNIX の場合: `/usr/opensv/volmgr/bin/ltid -v`

Windows の場合: **Device Manager** サービスを起動します。

- 10 ステージングから **NBDB** をリカバリするには、マスターサーバーで次のコマンドを実行してください。

UNIX: `/usr/opensv/db/bin/nbdb_restore -dbn NBDB -recover -staging`

Windows: `install_path¥NetBackup¥bin¥nbdb_restore -dbn NBDB -recover -staging`

- 11 すべてのホストで許可リストのキャッシュをクリーンアップします。

- 12** 次のように、すべてのホスト上の **NetBackup** サービスを停止して再起動します。

UNIX の場合:

```
/usr/opensv/netbackup/bin/bp.kill_all
/usr/opensv/netbackup/bin/bp.start_all
```

Windows の場合:

```
install_path%NetBackup%bin%bpdown
install_path%NetBackup%bin%bpup
```

- 13** サービスを再起動したら、次のコマンドを実行します。

- **NetBackup** (またはホスト ID ベース) の証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -renewcertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -renewcertificate -cluster
```

- 外部 CA が署名した証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate
```

Windows の場合:

```
install_path%netbackup%bin%nbcertcmd -enrollCertificate
```

クラスタ設定の場合:

UNIX の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
```

Windows の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate  
-cluster
```

このコマンドが終了状態 5988 を表示して失敗した場合は、次のトピックを参照してください。

p.315 の「[カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順](#)」を参照してください。

## ステージングでのリレーショナルデータベースの処理について

NetBackup のイメージファイルと構成ファイルをリカバリすると、NetBackup リレーショナルデータベース (NBDB) もステージングディレクトリにリストアされます。必要に応じ、次の NetBackup コマンドを使用して、NBDB のデータベースの処理を進められます。

cat_import	cat_import を使うと、レガシーフラットファイルにあるイメージメタデータを NBDB リレーショナルデータベースにインポートできます。この NBDB データベースは、実際の本番 DB あるいは別の NetBackup ドメインにある NBDB のいずれかです。
cat_export	cat_export の <code>-staging</code> を使うと、リレーショナルデータベースからイメージのメタデータを抽出できます。これは、 <code>db.export</code> ディレクトリにデータをレガシーフラットファイルフォーマットで書き込みます。すべてのイメージメタデータやそのサブセットは、クライアント別、バックアップ ID 別にエクスポートできます。その後、 <code>cat_import</code> コマンドを使用して、これらのデータを別の NBDB のデータベースに挿入できます。『別の NBDB』とは、実際の本番 DB または別の NetBackup ドメインにある NBDB のいずれかです。
nbdb_restore -staging	ステージングディレクトリからリレーショナルデータベースをリカバリするには、 <code>nbdb_restore -staging</code> を使います。  <a href="#">p.301 の「NetBackup リレーショナルデータベースのファイルをステージングからリカバリする」</a> を参照してください。
nbdb_unload -staging	<code>nbdb_unload</code> の <code>-staging</code> を使うと、メディアテーブルと関連するテーブルを、一連のフラットファイルにアンロードできます。次に、SQL ツールを使用して、サブセットのデータを別の NBDB に挿入できます。『別の NBDB』とは、実際の本番 DB または別の NetBackup ドメインにある NBDB のいずれかです。

**警告:** Veritas では、Veritas サポート担当者の指示による場合のみ、NetBackup のリレーショナルデータベースを操作および処理することを推奨します。NetBackup ドメインの結合や分割について詳しくは、Veritas コンサルティングサービスまでご連絡ください。

[http://www.veritas.com/business/services/consulting\\_services.jsp](http://www.veritas.com/business/services/consulting_services.jsp)

コマンドについての詳しい情報を参照できます。

『NetBackup コマンドリファレンスガイド』を参照してください。

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

## NetBackup アクセス制御が構成されている場合の NetBackup カタログのリカバリ

NetBackup アクセス制御 (NBAC) を構成している場合、認証情報および認可の構成情報は、オンラインホットカタログバックアップによって自動的にバックアップされます。

NBAC の認証および認可データのバックアップおよびリカバリを正常に実行するには、カタログオブジェクトに対して、操作と構成の両方の権限セットが必要です。

以下のように、オペレーティングシステムによって異なるリカバリ手順があります。

- UNIX の場合: [表 4-5](#)
- Windows の場合: [表 4-6](#)

**表 4-5** UNIX 上で NetBackup アクセス制御が構成されている場合に NetBackup カタログをリカバリする方法

手順	作業	手順
手順 1	NBAC が構成されて稼働中であるマスターサーバーにリカバリする場合は、NBAC を無効化します (つまり、[禁止 (Prohibited)] モードに設定します)。	『NetBackup セキュリティおよび暗号化ガイド』を参照してください。 <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a>
手順 2	カタログリカバリウィザードまたは bprecover コマンドを使用して、オンラインカタログバックアップから NetBackup カタログをリカバリします。	p.262 の「NetBackup カタログ全体のリカバリについて」を参照してください。
手順 3	必要なセキュリティレベルに応じて [自動 (Automatic)] か [必須 (Required)] に NetBackup を設定することで、NBAC を使うように NetBackup を構成します。	『NetBackup セキュリティおよび暗号化ガイド』を参照してください。 <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a>
手順 4	NetBackup を再起動します。	/usr/opensv/netbackup/bin/bp.kill_all /usr/opensv/netbackup/bin/bp.start_all

**表 4-6** Windows 上で NetBackup アクセス制御が構成されている場合に NetBackup カタログをリカバリする方法

手順	作業	手順
手順 1	NBAC が構成されて稼働中であるマスターサーバーにリカバリする場合は、NBAC を無効化します (つまり、[禁止 (Prohibited)] モードに設定します)。	『NetBackup セキュリティおよび暗号化ガイド』を参照してください。 <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a>
手順 2	NetBackup サービスを停止します。	<code>install_path\Veritas\NetBackup\bin\bpdwn.exe</code>
手順 3	Windows の場合は、NetBackup Authentication Service と NetBackup Authorization Service の [スタートアップの種類 (Startup type)] を [無効 (Disabled)] に変更してください。	Microsoft Windows の構成手順は、NetBackup のマニュアルの対象外となります。該当する Microsoft 社のマニュアルを参照してください。
手順 4	NetBackup サービスを起動します。	<code>install_path\Veritas\NetBackup\bin\bppup.exe</code>
手順 5	bprecover コマンドを使用して、オンラインカタログバックアップから NetBackup カタログをリカバリします。  NetBackup Authentication Service と NetBackup Authorization Service を [無効 (Disabled)] モードにする必要があります。	p.262 の「NetBackup カタログ全体のリカバリについて」を参照してください。
手順 6	Windows の場合は、NetBackup Authentication Service と NetBackup Authorization Service の [スタートアップの種類 (Startup type)] を [自動 (Automatic)] に変更してください。	Microsoft Windows の構成手順は、NetBackup のマニュアルの対象外となります。該当する Microsoft 社のマニュアルを参照してください。

手順	作業	手順
手順 7	NBAC を使うように NetBackup を構成します。	<p>手順は環境によって次のように異なります。</p> <ul style="list-style-type: none"> <li>■ <b>Windows Server</b> フェールオーバークラスタ環境の <b>NetBackup</b> マスターサーバーの場合は、アクティブノードの <b>NetBackup</b> マスターサーバーで次のコマンドを実行します。  <code>bpnbaz -setupmaster</code>                      このコマンドは、NBAC の必要なエントリを使って、すべてのノードの <b>Windows</b> レジストリをプロビジョニングします。</li> <li>■ 新規インストールにリカバリする場合は、次のコマンドを <b>NetBackup</b> マスターサーバーで実行します。  <code>bpnbaz -setupmaster</code></li> <li>■ 既存の環境でのリカバリの場合、必要なセキュリティレベルに応じて [自動 (Automatic)] か [必須 (Required)] に NBAC を設定します。</li> </ul> <p>『NetBackup セキュリティおよび暗号化ガイド』を参照してください。  <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></p>
手順 8	NetBackup を再起動します。	<pre>install_path\Veritas\NetBackup\bin\bpdown.exe install_path\Veritas\NetBackup\bin\bpup.exe</pre>

p.254 の「NetBackup カタログのリカバリについて」を参照してください。

## カタログバックアップのプライマリコピー以外からのカタログのリカバリ

デフォルトでは、カタログバックアップに複数のコピーを含めることができ、カタログはプライマリバックアップコピーからリカバリされます。プライマリコピーは最初または元のコピーです。ただし、プライマリ以外のコピーからリカバリできます。

---

**メモ:** カタログをリカバリしたいマスターサーバーにログオンする必要があります。  
**NetBackup** 管理コンソールを別のホストで実行しているときにサーバーを変更してウィザードを実行することはできません。

---



---

**メモ:** これらの手順を実行するには、**root** (管理) 権限が必要です。

---

### プライマリコピー以外からカタログをリカバリする方法

- 1 カタログバックアップのコピーがテープ以外のメディアにある場合は、次を実行します。

**BasicDisk** バックアップを含んでいるディスクが、ディザスタリカバリファイルに表示されているとおりに、正しいマウントパスに対してマウントされていることを確認します。

**ディスクプール** ディスクプールのカタログバックアップファイルの場合は、次を実行します。

- [ストレージサーバーの構成ウィザード (Storage Server Configuration Wizard)]を使用してストレージ用のディスクストレージサーバーを作成します。
  - [ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)]を使用してストレージ用のディスクプールを作成します。
  - 新しいディスクプールにディザスタリカバリファイルを同期するには、次のコマンドを実行します。
- ```
nbcatsync -sync_dr_file disaster_recovery_file
```

2 カタログをリカバリするには、次の **NetBackup** コマンドを実行します。

```
bprecover -wizard -copy N
```

*N* はリカバリするコピーの番号です。

## ディザスタリカバリファイルを使用しない NetBackup カタログのリカバリ

ディザスタリカバリファイルが消失した場合は、カタログのバックアップが実行されたときに管理者に送信された電子メールを確認します。ディザスタリカバリファイルは、カタログバックアップポリシーで指定されている場所に書き込まれ、バックアップストリーム自体に追加されます。

### ディザスタリカバリファイルを使用しないでカタログをリカバリする方法

- 1 電子メールには、ディザスタリカバリファイルが含まれているメディア、およびクリティカルポリシーのバックアップに使用されたメディアが示されています。メディアが利用可能であることを確認します。
- 2 通常のカタログリカバリ手順で、[カタログリカバリウィザード (Catalog Recovery Wizard)]または `bprecover` コマンドを実行する前の手順まで実行します。
- 3 次のコマンドを実行して、カタログバックアップメディアからすべてのディザスタリカバリファイルを取得します。

```
bpimport -drfile -id media_id -drfile_dest  
fully_qualified_dir_name
```

このコマンドによって、指定したメディア ID からすべてのディザスタリカバリファイルがリカバリされ、指定したディレクトリに配置されます。ID は、テープメディア ID またはディスクストレージユニットの完全修飾場所のいずれかになります。

- 4 適切なディザスタリカバリファイルが指定したディレクトリ内で利用可能であること、および NetBackup マスターサーバーから使用できることを確認します。
- 5 [カタログリカバリウィザード (Catalog Recovery Wizard)] または `bprecover` コマンドを実行して、通常のカタログのリカバリ手順を続行します。プロンプトが表示されたら、ディザスタリカバリファイルの場所を指定します。

電子メールはカタログをリカバリするための最新の手順であるため、リカバリ手順については電子メールを優先して参照してください。この手順は、カタログバックアップの完了時、またはカタログバックアップイメージの複製時に送信されます。

---

**メモ:** Solaris システムで `bprestore` を使って直接カタログファイルをリストアする場合は、パス `/opt/openssl/netbackup/bin/bprestore` を使います。

---

オンラインカタログバックアップポリシーの名前は **CatalogBackup** です。電子メールは次のファイルに書き込まれます。

```
/storage/DR/CatalogBackup_1123605764_FULLL
```

ファイル名から、バックアップが完全バックアップであるかどうかを判別できます。

p.258 の「**NetBackup ディザスタリカバリ電子メールの例**」を参照してください。

## コマンドラインからの NetBackup のユーザー主導オンラインカタログバックアップのリカバリ

この手順では、ディザスタリカバリ (DR) ファイルが利用可能な場合に、フェーズ 1 のインポートを使用せず、コマンドラインインターフェース (CLI) を使用してカタログを手動でリカバリします。この手順を実行するには、`root` (管理) 権限が必要です。

---

**メモ:** この手順は、重要なデータのリカバリを開始するために必要最小限の NetBackup カタログ情報をリストアする場合だけ使用してください。

---

## コマンドラインインターフェースからユーザー主導のオンラインカタログをリカバリする方法

- 1 完全ホットカタログバックアップまたは増分ホットカタログバックアップから作成されたディザスタリカバリファイルの場所を確認します。これらのファイルは、マスターサーバーのファイルシステムの指定されたパス、および **NetBackup** 管理者宛の電子メールの添付ファイルに格納されます。
- 2 各マスターサーバーおよびメディアサーバーは、最後のカタログバックアップが実行されたときと同じ構成に設定します。マスターサーバーおよびメディアサーバーでは、名前、**NetBackup** のバージョン、オペレーティングシステムのパッチレベルおよびストレージデバイスへのパスが、バックアップされたカタログの構成と同じである必要があります。

必要に応じて、リカバリに使用するデバイスおよびボリュームを構成します。

- 3 リカバリに使用するバックアップに対応する最新の **DR** イメージファイルを特定します。このファイルをエディタで開いて、次の値を確認します。

|                            |                                                                |
|----------------------------|----------------------------------------------------------------|
| <code>master_server</code> | <b>NetBackup</b> 構成で設定されているマスターサーバーの正確な名前。                     |
| <code>media_server</code>  | カタログバックアップで使用されたロボットまたはディスクストレージユニットの場所。                       |
| <code>timestamp</code>     | <b>DR</b> ファイル名の先頭 4 桁の数字の後に <b>0</b> (ゼロ) を 6 つ付けたもの。         |
| <code>media</code>         | ディザスタリカバリファイルの <b>FRAGMENT</b> キーワードに指定されているカタログバックアップメディアの場所。 |
| <code>backup_id</code>     | <b>DR</b> ファイル内の <b>BACKUP_ID</b> に指定されています。                   |

例:

**file:** Hot\_Backup\_1122502016\_INCR

**timestamp:** 1122000000

- 4 マスターサーバー上に **DR** リカバリディレクトリを作成します。

**UNIX** の場合:

```
/usr/opensv/netbackup/db/images/master_server/timestamp/tmp
```

**Windows** の場合:

```
C:\Program Files\VERITAS\NetBackup\db\images\master_server\
timestamp\tmp
```

新しく作成したディレクトリに **DR** ファイルをコピーします。

- 5 netbackup/db/images/master\_server/timestamp/tmp の DR ファイルを次のように編集します。
- IMAGE\_TYPE の値を 1 に変更します。
  - TIR\_INFO の値を 0 に変更します。
  - NUM\_DR\_MEDIAS の値を 0 に変更します。
  - DR\_MEDIA\_REC が含まれているすべての行を削除します。
- 6 カタログリカバリメディアがテープの場合は、vmquery コマンドを実行して、そのメディアをマスターサーバーに割り当てます。

```
vmquery -assigntohost media timestamp master_server
```

例:

```
vmquery -assigntohost DL005L 1122000000 klingon
```

- 7 ホットカタログバックアップからカタログの .f ファイルをリカバリするには、ディザスタリカバリファイルに指定されているメディアでフェーズ 2 のインポートを実行します。

```
bpimport -server master_server -backupid backup_id
```

- 8 使用するカタログバックアップが増分バックアップの場合は、他のすべてのカタログバックアップイメージを最新の完全カタログバックアップの時点までリカバリします。
- NetBackup 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インターフェースを開きます。ポリシー形式として [NBU-Catalog] を選択します。ソースクライアントおよび宛先クライアントには、マスターサーバーを設定します。

- 次のディレクトリに格納されているバックアップを検索し、すべてのファイルをリストアします。

```
install_path/netbackup/db/images/master_server
```

- マスターサーバーですべてのファイルが正常にリストアされたことを確認します。
- 9 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インターフェースまたはコマンドラインを使用して、重要なデータをリストアします。
- データのリカバリが必要な各メディアサーバーに、カタログバックアップイメージをリストアします。
  - バックアップイメージをリストアする場合、ポリシー形式として [NBU-Catalog] を選択します。ソースクライアントおよび宛先クライアントには、マスターサーバーを指定します。BAR GUI の表示を更新します。マスターサーバーのファイルシステムで次の位置に移動します。

```
install_path/netbackup/db/images
```

構成済みの各メディアサーバーにイメージをリストアします。カタログ内を検索して、これらのイメージが存在することを確認します。

- 10 前の手順で使用した各メディアサーバーから、バックアップデータをリカバリします。目的のデータのバックアップが実行されたクライアントに合わせて、ポリシー形式、ソースクライアントおよび宛先クライアントを変更します。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インターフェースから目的のファイルを選択してリストアを行います。
- 11 NetBackup リレーショナルデータベースをリカバリするには、次のコマンドを実行します。

```
bprecover -r -nbdb
```

このコマンドを実行すると、NetBackup のメディア使用情報がリストアされ、バックアップが含まれているメディアが上書きされていないことが確認されてから、ストレージユニットの構成がリストアされます。

NetBackup リレーショナルデータベースを、カタログのバックアップに使用された構成と異なる構成にリカバリすることはできません。代わりに、各バックアップメディアを個別にインポートする必要があります。

- 12 カタログリカバリに使用するメディアがテープの場合は、リカバリに使用するカタログバックアップが含まれているメディアを凍結します。この処理によって、メディアの再利用を防止できます。

```
bpmedia -freeze -m media -h master_server
```

bpmedialist を実行して、メディアが凍結されていることを確認します。

- 13 各マスターサーバーおよびメディアサーバーで、ポリシーおよび構成のデータをリカバリします。

NetBackup ポリシーファイルをリカバリする前に、すべての重要なデータがリカバリされていること、または重要なデータが含まれているメディアが保護されていることを確認します。ポリシー情報がリカバリされると、NetBackup でスケジュールが設定されたジョブの実行が開始され、このジョブによって、最後のカタログバックアップの実行後に書き込まれたメディアが上書きされる場合があります。

NetBackup のバックアップ、アーカイブ、およびリストアクライアントインターフェースを開いて、ポリシー形式として[NBU-Catalog]を選択します。

リストア対象の各サーバーで、ソースクライアントおよび宛先クライアントに、使用しているサーバーを設定します。マスターサーバーから設定を開始します。

ホットカタログバックアップによってバックアップされたすべてのファイルを各サーバーにリストアします。

- 14 すべてのホストで許可リストのキャッシュをクリーンアップします。
- 15 すべてのホスト上の **NetBackup** サービスを停止して再起動します。
- 16 サービスを再起動したら、次のコマンドを実行します。
  - **NetBackup** (またはホスト ID ベース) の証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合:

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate
```

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate
```

クラスタ設定の場合:

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -renewcertificate -cluster
```

- 外部 CA が署名した証明書が **NetBackup** ドメインで使用される場合、以下を実行します。

非クラスタ設定の場合

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate
```

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate
```

クラスタ設定の場合:

**UNIX** の場合:

```
/usr/opensv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
```

**Windows** の場合:

```
install_path¥netbackup¥bin¥nbcertcmd -enrollCertificate  
-cluster
```

このコマンドが終了状態 **5988** を表示して失敗した場合は、次のトピックを参照してください。

p.315 の「[カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順](#)」を参照してください。

## NetBackup オンラインカタログバックアップからのファイルのリストア

オンラインカタログバックアップでは標準バックアップの形式が使用されるため、NetBackup のバックアップ、アーカイブおよびリストアユーザーインターフェースを使用して、特定のファイルをリカバリすることができます。カタログファイルを元の場所に直接リストアすると、NetBackup カタログの一貫性に矛盾が生じたり、NetBackup で障害が発生する可能性があります。代わりに、代替の場所にカタログファイルをリストアする必要があります。

p.254 の「[NetBackup カタログのリカバリについて](#)」を参照してください。

### オンラインカタログバックアップからファイルをリストアする方法

- 1 [NetBackup マシンおよびポリシー形式の指定 (Specify Machines and Policy Type)]メニューから、[NBU-Catalog]ポリシー形式を選択します。
- 2 リストアのソースクライアントには、マスターサーバーを指定します。
- 3 リストアするカタログファイルを選択します。

## NetBackup オンラインカタログリカバリメディアの凍結の解除

この手順では、リムーバブルカタログリカバリメディアを解冻する方法を記述します。

p.254 の「[NetBackup カタログのリカバリについて](#)」を参照してください。

### オンラインカタログリカバリメディアの凍結を解除する方法

- 1 マスターサーバー上で、ディザスタリカバリファイルまたは電子メール内で識別された各リムーバブルメディアに対して、次のコマンドを実行します。

```
bpimport -create_db_info -server server_name -id media_id
```

- 2 マスターサーバーで、次のコマンドを実行します。

```
bpimport
```

- 3 マスターサーバー上で、ディザスタリカバリファイルまたは電子メール内で識別された各メディアに対して、次のコマンドを実行します。

```
bpmedia -unfreeze -m media_id -h server_name
```

## カタログバックアップ中に終了状態 5988 が表示されたときに実行する手順

カタログバックアップ中に終了状態 5988 が表示されたときに、この手順を使用します。

## この問題を解決するには

### 1 次のコマンドを実行します。

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -ping`

UNIX の場合: `/usr/opensv/netbackup/bin/nbcertcmd -ping`

- コマンドが正常に実行された場合は、次の手順に進みます。
- コマンドが状態 **8509** (指定したサーバー名が **Web** サービス証明書内に見つかりませんでした) で失敗した場合は、次の記事の手順に従います。  
[https://www.veritas.com/support/en\\_US/article.000126751](https://www.veritas.com/support/en_US/article.000126751)  
次の手順に進みます。

### 2 マスターサーバー上でユーザーログオンを実行します。次のコマンドを使用します。

```
install_path¥netbackup¥bin¥bpnbat -login -loginType WEB
```

次に例を示します。

```
install_path¥netbackup¥bin¥bpnbat -login -loginType WEB
```

```
Authentication Broker [abc.example.com is default]:  
Authentication port [0 is default]:  
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap)  
[WINDOWS is default]:  
Domain [abc.example.com is default]:  
Login Name [administrator is default]:  
Password:  
Operation completed successfully.
```

### 3 マスターサーバーの **Client\_Name** キーの値に注意してください。クラスタ化されたマスターサーバーの場合は、**Cluster\_Name** キーの値に注意します。

この値は次の場所にあります。

Windows の場合:

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Veritas¥NetBackup¥CurrentVersion¥Config
```

UNIX の場合: `/usr/opensv/netbackup/bp.conf`

この値には **FQDN** または短縮名のいずれも指定できます。

次に例を示します。

```
abc.example.com
```

### 4 マスターサーバーのホスト ID に注意します。この値を取得するには、次のコマンドを実行します。

```
install_path¥netbackup¥bin¥nbcertcmd -listCertDetails
```

クラスタ化されたマスターサーバーの場合は、次のコマンドを実行します。

```
install_path¥netbackup¥bin¥nbcertcmd -listCertDetails -cluster
```

このコマンドは複数のレコードを返すことがあります (1 つのレコードのみが返される場合はそのレコードに指定されているホスト ID を選択)。

- 手順 3 で取得したホスト名が FQDN である場合は、[発行者 (Issued By)] エントリが短縮名と一致しているレコードを選択します。
- 手順 3 で取得したホスト名が短縮名である場合は、[発行者 (Issued By)] エントリが FQDN と一致しているレコードを選択します。

例:

```
install_path¥netbackup¥bin¥nbcertcmd -listCertDetails
```

```
Master Server : abc
Host ID : 78f9eed4-xxxx-4c6a-bb40-xxxxxxxxxx
Issued By : /CN=broker/OU=root@abc/O=vx
Serial Number : 0x62e108c90000000c
Expiry Date : Aug 21 08:42:54 2018 GMT
SHA1 Fingerprint : 50:89:AE:66:12:9A:29:4A:66:E9:DB:71:37:C7:
EA:94:8C:C6:0C:A0
Master Server : xyz
Host ID : 5a8dde7b-xxxx-4252-xxxx-d3bedee63e0a
Issued By : /CN=broker/OU=root@xyz.example.com/O=vx
Serial Number : 0x6ede87a70000000a
Expiry Date : Aug 21 09:52:13 2018 GMT
SHA1 Fingerprint : FE:08:C2:09:AC:5D:82:57:7A:96:5C:C1:4A:E6:
EC:CA:CC:99:09:D2
Operation completed successfully.
```

ここでは、2 つのレコードがフェッチされます。

最初のレコードでは、[発行者 (Issued By)] フィールドの発行者名が手順 3 で取得した `client_name` の短縮名と一致しています。

そのため、このレコードに含まれているホスト ID を選択します。

- 5 マスターサーバーに対し、ホスト ID からホスト名へのマッピングを追加します。手順 4 で取得したホスト ID を手順 3 で取得したホスト名にマッピングします。

次のコマンドを使用します。

```
install_path¥netbackup¥bin¥admincmd¥nbhostmgmt -a -i host ID -hm  
hostname
```

```
install_path¥netbackup¥bin¥admincmd¥nbhostmgmt -a -i  
78f9eed4-xxxx-4c6a-bb40-xxxxxxxxx -hm abc.example.com  
abc.example.com is successfully mapped to  
78f9eed4-xxxx-4c6a-bb40-xxxxxxxxx.
```

また、NetBackup 管理コンソールを使用しても、このホスト ID からホスト名へのマッピングを追加することができます。[セキュリティ管理 (Security Management)] > [ホスト管理 (Host Management)] > [ホスト (Hosts)] タブを使用します。

- 6 証明書を更新するには次の操作を行います。
- マスターサーバーの NetBackup (またはホスト ID ベースの) 証明書を更新するには、次のコマンドを使用します。

```
install_path¥netbackup¥bin¥nbcertcmd -renewCertificate
```

クラスタ化されたマスターサーバーの場合は、次のコマンドを実行します。

```
install_path¥netbackup¥bin¥nbcertcmd -renewCertificate -cluster
```

## 記号

- アーカイブ
  - NBCC 用 195
  - nbsu 192
- インストール
  - Linux の場合 29
- インストールの問題 28
  - NetBackup
    - クライアント 29
- カタログのリカバリ
  - カタログイメージファイル 277
  - クラスタ化されたマスターサーバー 278
- カタログバックアップ
  - ディザスタリカバリパッケージ 215
- キューに投入されたジョブ 87
- クライアント
  - NetBackup
    - ピアネーム 69
    - 構成のテスト 34、38
    - 構成名 69
    - 複数のホスト名 68
- クライアント、NetBackup
  - Windows ディスクのリカバリ 238
- サーバー
  - インストールの問題 28
  - マスターサーバーのテスト手順 34、38
  - メディアサーバーのテスト手順 38
- サービスエントリ
  - 確認 72
- ジョブ
  - 長時間キューへ投入された状態 87
- ストレージユニット 126
- セキュアモード
  - PBX 100
- テストユーティリティ
  - ロボット 206
- ディザスタリカバリパッケージ 215
- ディザスタリカバリパッケージのリストア
  - UNIX 250
  - Windows 248
- ディザスタリカバリパッケージのリストアについて 246
- ディザスタリカバリ
  - 障害に対する準備 213
- ディスクに空きがなくなった状態 87
- ディスクのリカバリ
  - Windows クライアント 238
- ディスク容量
  - ログおよび一時ファイル 128
- デバイスの構成ウィザード 233
- デバイス構成の問題 31
- デバッグ
  - NBCC 194
  - nbsu 190
- デバッグログ
  - 分析ユーティリティ 184
- トラブルシューティング
  - KMS 構成の問題 158
- トラブルシューティング手順
  - インストール 28
  - ホスト名およびサービスエントリ 72
  - 一般
    - マスターサーバーおよびクライアント 34、38
    - メディアサーバーおよびクライアント 38
  - 予備的 20
  - 通信の問題
    - PC クライアント 46
    - UNIX クライアント 42
- ネットワークの問題
  - PC クライアント 46
  - UNIX クライアント 42
- ネットワークインターフェースカード 124
- ネットワーク接続
  - 複数 (Multiple) 68
- パッチ (リカバリ中のインストール) 240
- ピアの検証エラー 55
- ホストプロパティ 86
- ホスト名エントリ
  - 確認 72
- ホスト検証のログ 105
- ボリュームの構成ウィザード 234
- マスターサーバー
  - テスト手順 34、38

- メディアサーバー
    - テスト手順 38
  - ユーティリティ
    - ロボットテスト 206
  - リカバリ手順
    - Windows クライアントのディスク 238
  - リモートホストの検証に関する問題
    - トラブルシューティング 104
  - リレーショナルデータベース 87
  - ログおよび一時ファイルのための追加のディスク容量 128
  - ログの分析ユーティリティ
    - デバッグログ 184
    - 出力形式 187
    - 制限事項 186
  - ロボットテストユーティリティ 206
    - acstest 207
    - tidtest 207
  - 予備的なトラブルシューティング手順 20
  - 二重モードとパフォーマンス 124
  - 代替クライアントへのリストア
    - host.xlate ファイル 71
  - 低いパフォーマンスと NIC カード 124
  - 全二重モード 124
  - 利用不可能 126
  - 半二重モードと低いパフォーマンス 124
  - 圧縮
    - NBCC 用 195
    - nbsu 192
  - 失効した証明書のエラー 53~54
  - 情報の記録 11
  - 情報電子メール 219
  - 手順
    - トラブルシューティング
      - インストールおよび構成 28
      - ホスト名およびサービス 72
      - マスターサーバーおよびクライアント 34
      - メディアサーバーおよびクライアント 38
      - 予備的 20
      - 概要 18
      - 通信の問題 42、46
    - リカバリ
      - Windows クライアントのディスク 238
  - 構成の問題 29
  - 空きがないディスク 87
  - 自動構成の問題 31
  - 証明書失効リスト
    - 証明書が失効しているかどうかの確認 63
  - 認証ユーザー
    - PBX 100
  - 通信の問題
    - PC クライアント 46
    - UNIX クライアント 42
  - 電子メール 219
  - [NetBackup クライアントのプロパティ (NetBackup Client Properties)] ダイアログボックス 86
- ## A
- acstest 207
  - AdvancedDisk 220、231
- ## B
- Bare Metal Restore 217、221、238
  - bp.conf
    - SERVER エントリ 125
  - bp.kill\_all 102、104
  - bp.start\_all 104
  - bpdown コマンド 102~103、234、237
  - bpsps 23
  - bpup コマンド 103
- ## H
- host.xlate ファイル 71
- ## I
- ifconfig
    - NIC の二重モードの確認 125
  - inetd 29
  - ipconfig
    - NIC の二重モードの確認 125
- ## K
- KMS 構成
    - トラブルシューティング 158
- ## L
- Linux 29
- ## N
- NAT クライアントの問題のトラブルシューティング 146
  - NB\_dbssrv デーモン 87
  - NBCC
    - nbcc-info.txt ファイル 195
    - アーカイブおよび圧縮 195
    - トラブルシューティング 194
    - 使用する場合 194

- 出力 195
  - 場所 194
  - 実行に関する注意事項 194
  - 概要 193
  - 機能 193
  - 進捗状況の表示 196
  - nbcc-info.txt ファイル 195
  - nbdb\_move 233
  - nbermm 24
  - nbftclnt
    - bp.conf 126
  - nbjrm 24
  - nbmqbroker サービスに関する問題のトラブルシューティング 150
  - nbpem 24
  - nbrb 24、87
  - NBSD 208
  - nbsmartdiag 208
  - nbsu
    - nbsu\_info.txt ファイル 191
    - まとめる 192
    - アーカイブおよび圧縮 192
    - トラブルシューティング 190
    - 使用する状況 189
    - 出力ファイル 191
    - 場所 189
    - 概要 189
    - 進捗状況の表示 193
  - nbsu\_info.txt ファイル 191
  - NetBackup
    - 応答がない場合 87
  - NetBackup Client Service
    - 起動および停止 26～27
  - NetBackup Compatibility service
    - 起動および停止 26
  - NetBackup Database Manager サービス
    - 起動および停止 26
  - NetBackup Deduplication Engine サービス
    - 起動および停止 27
  - NetBackup Deduplication Manager サービス
    - 起動および停止 27
  - NetBackup Device Manager サービス
    - 起動および停止 27
  - NetBackup Discovery Framework サービス
    - 起動および停止 26
  - NetBackup Enterprise Media Manager サービス
    - 起動および停止 26
  - NetBackup Event Manager サービス
    - 起動および停止 26
  - NetBackup Indexing Manager サービス
    - 起動および停止 26
  - NetBackup Job Manager サービス
    - 起動および停止 26
  - NetBackup Legacy Client Service
    - 起動および停止 27
  - NetBackup Messaging Broker サービスに関する問題のトラブルシューティング 150
  - NetBackup Policy Execution Manager サービス
    - 起動および停止 26
  - NetBackup Relational Database Manager 87
  - NetBackup Relational Database Manager Service
    - 起動および停止 26
  - NetBackup Remote Manager と Monitor Service
    - 起動および停止 26～27
  - NetBackup Request Daemon サービス
    - 起動および停止 26
  - NetBackup Resource Broker サービス
    - 起動および停止 26
  - NetBackup Service Layer サービス
    - 起動および停止 26
  - NetBackup Service Monitor サービス
    - 起動および停止 26
  - NetBackup Smart Diagnosis 208
  - NetBackup Storage Lifecycle Manager サービス
    - 起動および停止 26
  - NetBackup Vault Manager サービス
    - 起動および停止 26
  - NetBackup Volume Manager サービス
    - 起動および停止 26～27
  - NetBackup Web 管理コンソールサービス
    - 起動および停止 26
  - NetBackup の一貫性チェック
    - 「NBCC」を参照 193
  - NetBackup サポートユーティリティ
    - 「nbsu」を参照 189
  - NetBackup プロセスの停止 102、104
  - NetBackup プロセスの起動 104
  - NetBackup 管理コンソール
    - エラー 127
  - NetBackup 認証サービス
    - 起動および停止 26
  - NetBackupDeduplication Multi-Threaded Agent サービス
    - 起動および停止 27
  - NIC カードと全二重 124
- O**
- OpenStorage 220、231

**P****PBX**

セキュアモード 100~101

トラブルシューティング 98

ログ 100

認証ユーザー 100

起動 99

起動および停止 102

pbx\_exchange 99

pbxcfg 100

Private Branch Exchange (PBX) 98

Private Branch Exchange サービス

起動および停止 26~27

**R**

Red Hat 29

robtest 206~207

**S**

SAN クライアント

bp.conf 126

SERVER エントリ

bp.conf 125

SharedDisk 220、231

stderr 127

stdout 127

SuSE 29

**T**

tlptest 207

tpautoconf 225

traceroute 71

tracert 71

**U**

UNIX の NetBackup 管理コンソールのエラーメッセージ

のトラブルシューティング 127

**V**

vnetd プロキシ

トラブルシューティング 51

Vnetd プロキシ接続

トラブルシューティング 49

vnetd プロキシ接続

ピアの検証エラー 55

失効した証明書のエラー 53~54

vxpbx\_exchanged 102

**W**

Web サービスアカウント

リカバリ中 222、224、229~230、233、236、242、  
244

**X**

xinetd 29

**ま**

まとめる

NBCC の出力 195

nbsu の出力 192