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 11.0.0.1

VERITAS
now part of Cohesity

NetBackup™ トラブルシューティングガイド

最終更新日: 2025-10-24

法的通知と登録商標

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

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

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

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

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Cohesity, Inc. およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

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

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

http://www.veritas.com

テクニカルサポート

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

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

https://www.veritas.com/support

次の URL で Cohesity Account の情報を管理できます。

https://my.veritas.com

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

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

マニュアル

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

https://sort.veritas.com/documents

マニュアルに対するご意見

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

NB.docs@veritas.com

次の Cohesity 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/

Cohesity Services and Operations Readiness Tools (SORT)

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

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

目次

第 1 章 概要 10

NetBackup のログと状態コードへの追加リソースの情報 10
問題のトラブルシューティング 10
テクニカルサポートへの問題レポート 13
NetBackup-Java アプリケーションの情報収集について 15

第 2 章 トラブルシューティングの手順 17

トラブルシューティング手順について 19
NetBackup の問題のトラブルシューティング 21
すべてのプロセスが UNIX または Linux サーバーで実行されていることの確認 24
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 27
インストールの問題のトラブルシューティング 30
構成の問題のトラブルシューティング 31
デバイス構成の問題の解決 33
プライマリサーバーおよびクライアントの検証 36
メディアサーバーおよびクライアントの検証 40
UNIX クライアントとのネットワーク通信の問題の解決 44
Windows クライアントとのネットワーク通信の問題の解決 48
vnetd プロキシ接続のトラブルシューティング 51
vnetd プロキシ接続の必要条件 52
vnetd プロキシ接続のトラブルシューティングの開始点 53
vnetd プロセスとプロキシがアクティブであることの確認 53
ホスト接続がプロキシされることの確認 54
vnetd プロキシ接続のテスト 55
接続と受け入れのプロセスのログファイルの確認 57
vnetd プロキシログファイルの表示 57
セキュリティ証明書失効のトラブルシューティング 58
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 59
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 60
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 60

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 61
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 62
利用不能なリソースが原因で NetBackup ジョブが失敗する 63
プライマリサーバーのセキュリティ証明書が失効している 64
NetBackup ホストの証明書の状態の確認 65
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 68
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 70
NetBackup のホスト名およびサービスエントリの検証 74
UNIX プライマリ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 78
UNIX プライマリ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 80
UNIX PC クライアントのホスト名とサービスエントリの例 82
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 83
bpclntcmd ユーティリティについて 85
[ホストプロパティ (Host Properties)]を使用した構成設定へのアクセス 88
空きがなくなったディスクの問題の解決 89
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 91
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 91
メディアが凍結される状況について 92
NetBackup Web サービスの問題のトラブルシューティング 95
NetBackup Web サービスのログの表示 96
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 96
NetBackup Web サーバー証明書の問題のトラブルシューティング 99
PBX の問題の解決 100
PBX インストールの確認 101
PBX が実行中であるかどうかの確認 101
PBX が正しく設定されているかどうかの確認 102
PBX のログへのアクセス 103
PBX のセキュリティのトラブルシューティング 104
PBX デーモンかサービスが利用可能かどうかの判断 106
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 107
ホストの検証に関連するログの表示 108
NetBackup 8.0 以前のホストとの安全でない通信の有効化 109
保留中のホスト ID からホスト名へのマッピングの承認 109
ホストキャッシュの消去 111
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 111

A.I.R. (自動イメージレプリケーション) と SLP で使用されるプライマリサーバーのルール 120
外部証明書の構成で、ターゲット型 A.I.R. の信頼できるプライマリサーバーの操作に失敗する 120
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 123
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 127
bp.conf ファイルの SERVER エントリについて 129
使用できないストレージユニットの問題について 129
Windows での NetBackup 管理操作のエラーの解決 130
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 130
NetBackup Web UI と 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 130
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 131
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 132
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 137
外部証明書の構成に関する問題のトラブルシューティング 143
Windows 証明書ストアの問題のトラブルシューティング 146
バックアップエラーのトラブルシューティング 150
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 151
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 155
Windows システムの電子メール通知に関する問題のトラブルシューティング 163
KMS 構成の問題のトラブルシューティング 164
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のトラブルシューティング 168
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のトラブルシューティング 169
auth.conf ファイルのグループ名の形式に関する問題のトラブルシューティング 175
VxUpdate パッケージ追加処理のトラブルシューティング 177
FIPS モードの問題のトラブルシューティング 179
マルウェアスキャンの問題のトラブルシューティング 181
移動中のデータの暗号化が有効になっている NetBackup ジョブの問題のトラブルシューティング 191
非構造化データのインスタントアクセスの問題のトラブルシューティング 194
多要素認証の問題のトラブルシューティング 195

マルチパーソン認証の問題のトラブルシューティング 199
NetBackup Scale-Out Relational Database への接続に関するトラブルシューティング 204
秘密鍵の暗号化に関する問題のトラブルシューティング 205
セキュリティ構成リスク機能に関する問題のトラブルシューティング 210
リスクエンジンベースの異常検出オプションに関する問題のトラブルシューティング 214

第 3 章 NetBackup ユーティリティの使用 217

NetBackup のトラブルシューティングユーティリティについて 217
NetBackup デバッグログの分析ユーティリティについて 219
ログ収集ユーティリティについて 223
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 223
NetBackup サポートユーティリティ (nbsu) について 224
NetBackup サポートユーティリティ (nbsu) の出力 226
NetBackup サポートユーティリティ (nbsu) の進捗状況の表示の例 228
NetBackup の一貫性チェックユーティリティ (NBCC) について 229
NetBackup の一貫性チェックユーティリティ (NBCC) の出力 230
NBCC の進捗状況の表示の例 231
NetBackup の一貫性チェックの修復 (NBCCR) ユーティリティについて 238
nbcplogs ユーティリティについて 240
ロボットテストユーティリティについて 241
UNIX でのロボットテスト 241
Windows でのロボットテスト 242
NetBackup Smart Diagnosis (nbsmartdiag) ユーティリティについて 243
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 245
ジョブ ID ごとのログ収集について 247

第 4 章 ディザスタリカバリ 253

ディザスタリカバリについて 253
バックアップに関する推奨事項 255
ディザスタリカバリの要件と注意事項 258
ディザスタリカバリパッケージ 259
ディザスタリカバリ設定について 260
UNIX および Linux のディスクリカバリ手順について 261
Linux のプライマリサーバーのディスクリカバリについて 261
UNIX の NetBackup メディアサーバーのディスクリカバリについて 267
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 268

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 268
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 269
UNIX クラスタまたは Linux クラスタ全体のリカバリ 270
Windows のディスクリカバリ手順について 272
Windows のプライマリサーバーのディスクリカバリについて 272
Windows の NetBackup メディアサーバーのディスクリカバリについて 279
Windows クライアントのディスクリカバリ 279
Windows のクラスタ化された NetBackup サーバーのリカバリについて 281
Windows VCS クラスタでの障害が発生したノードの置き換え 282
Windows VCS クラスタでの共有ディスクのリカバリ 283
Windows VCS クラスタ全体のリカバリ 284
ディザスタリカバリインストール後のクラスタ化されたプライマリサーバーでの証明書の生成 285
DR_PKG_MARKER_FILE 環境変数について 286
Windows でのディザスタリカバリパッケージのリストア 287
Linux でのディザスタリカバリパッケージのリストア 291
NetBackup カタログをリカバリするためのオプション 295
NetBackup カタログまたは NetBackup カタログイメージファイルのリカバリの前提条件 296
Windows コンピュータでの NetBackup カタログリカバリについて 298
ディスクデバイスからの NetBackup カタログリカバリについて 298
NetBackup のカタログリカバリとシンボリックリンクについて 299
NetBackup ディザスタリカバリ電子メールの例 299
NetBackup カタログ全体のリカバリについて 303
NetBackup カタログイメージファイルのリカバリについて 315
NetBackup データベースのリカバリについて 330
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 342
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 NetBackup 344
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 344
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 345
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 351
NetBackup オンラインカタログリカバリメディアの凍結の解除 351

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 …… 352

1

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への追加リソースの情報
- 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への追加リソースの情報

『NetBackup ログリファレンスガイド』には次の資料が含まれます。

- 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」

NetBackup の状態コードに関する説明と推奨処置について詳しくは、『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	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。NetBackup 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。 ログには、適切に行われた処理とともに問題の発生時に NetBackup 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であることなどが表示されます。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。 『NetBackup ログリファレンスガイド』を参照してください。
手順 2	問題発生時に実行していた操作の確認	次について質問します。 ■ 試行された操作。 ■ 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利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。 ■ 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。 ■ サイトでプライマリサーバーとメディアサーバーの両方を使用している場合、プライマリサーバーとメディアサーバーのどちらであるか。 ■ クライアントの種類 (クライアントが関連する場合)。 ■ 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。 ■ Service Pack のバージョン。 ■ 最新の、特に NetBackup 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。 ■ 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。

手順	処理	説明
手順 3	すべての情報の記録	重要になる可能性がある情報を入手します。 ■ NetBackup の進捗ログ ■ NetBackup のレポート ■ NetBackup ユーティリティのレポート ■ NetBackup のデバッグログ ■ メディアおよびデバイスの管理のデバッグログ ■ 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)。 ■ 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 ■ 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)。 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、Cohesity Technical Support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。 『NetBackup ログリファレンスガイド』を参照してください。
手順 4	問題の修正	問題を定義した後、次の情報を使って問題を修正します。 ■ 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。 『状態コードリファレンスガイド』を参照してください。 ■ 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.21 の「NetBackup の問題のトラブルシューティング」を参照してください。
手順 5	Cohesity Technical Supportの問題レポートへの入力	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Cohesity Technical Supportに連絡する準備をします。 p.13 の「テクニカルサポートへの問題レポート」を参照してください。 p.15 の「NetBackup-Java アプリケーションの情報収集について」を参照してください。 UNIX システムの場合、`/usr/openv/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Cohesity Technical Support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。
手順 6	Cohesity Technical Supportへのお問い合わせ	Cohesity Technical Support 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。 次の URL のCohesity Technical Supportにアクセスします。 https://www.veritas.com/support/en_US.html

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。プライマリサーバーとメディアサーバーは同一です。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:

_____ My.com - ケース管理ポータル

_____ mft.veritas.com - https アップロードのファイル転送ポータル

_____ 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。

`jnbSA` (NetBackup-Java 管理アプリケーションの起動スクリプト)	`/usr/openv/netbackup/logs/user_ops/nbjlogs` 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なりません (通常は 2 KB 未満)。`/usr/openv/java/Debug.properties` 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。
Windows の NetBackup-Java 管理アプリケーション	アプリケーションが起動されているコンピュータ上に NetBackup がインストールされている場合、スクリプトは *`install_path`*`¥NetBackup¥logs¥user_ops¥nbjlogs` でログファイルにデータを書き込みます。 NetBackup 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、`install_path¥java¥nbjava.bat` 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。 NetBackup 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 *`install_path`*`¥Veritas¥Java¥logs` でログファイルにデータを書き込みます。 **メモ:** アプリケーションが起動されているコンピュータ上に NetBackup がインストールされていて、install_path が `setconf.bat` ファイルで設定されていない場合、スクリプトは *`install_path`*`¥Veritas¥Java¥logs` のログファイルにデータを書き込みます。
`/usr/openv/java/get_trace`	UNIX/Linux のみ。 テクニカルサポートが分析するための Java Virtual Machine 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。
UNIX または Linux の場合: `/usr/openv/netbackup/bin/support/nbsu` Windows の場合: *`install_path`*`¥NetBackup¥bin¥support¥nbsu.exe`	ホストに問い合わせて、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.224 の「NetBackup サポートユーティリティ (nbsu) について」を参照してください。

次の例では、Cohesity 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。	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/openv/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/openv/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と、NetBackup の構成を変更するたびに、このコマンドを実行します。
Cohesity 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。

2

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
- プライマリ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)]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 Web UI と 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
- 外部証明書の構成に関する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のトラブルシューティング
- KMS 構成の問題のトラブルシューティング
- 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のトラブルシューティング

- 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のトラブルシューティング
- auth.conf ファイルのグループ名の形式に関する問題のトラブルシューティング
- VxUpdate パッケージ追加処理のトラブルシューティング
- FIPS モードの問題のトラブルシューティング
- マルウェアスキャンの問題のトラブルシューティング
- 移動中のデータの暗号化が有効になっている NetBackup ジョブの問題のトラブルシューティング
- 非構造化データのインスタントアクセスの問題のトラブルシューティング
- 多要素認証の問題のトラブルシューティング
- マルチパーソン認証の問題のトラブルシューティング
- NetBackup Scale-Out Relational Database への接続に関するトラブルシューティング
- 秘密鍵の暗号化に関する問題のトラブルシューティング
- セキュリティ構成リスク機能に関する問題のトラブルシューティング
- リスクエンジンベースの異常検出オプションに関する問題のトラブルシューティング

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。

Cohesity 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

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.21 の「NetBackup 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.24 の「すべてのプロセスが UNIX または Linux 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.27 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。
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.30 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.31 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.36 の「プライマリ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.40 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.44 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.48 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.74 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.85 の「bpclntcmd ユーティリティについて」を参照してください。 p.74 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.89 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.91 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.92 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.127 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.78 の「UNIX プライマリ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.80 の「UNIX プライマリ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.82 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.83 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、最初に調査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。	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。 NetBackup のすべてのバージョンの互換性リストを参照してください。 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。 http://www.veritas.com/docs/DOC5332
手順 2	レポートを使用してエラーを検索します。	[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。 『NetBackup Web UI 管理者ガイド』の「レポート」の章を参照してください。 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。(このレポートは、NetBackup 管理コンソールで利用可能です。) 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。 『 状態コードリファレンスガイド』を参照してください。
手順 3	オペレーティングシステムのログを確認します。	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/Linux 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。 ■ NetBackup によって状態コードが表示されない。 ■ 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。 ■ 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。 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。
手順 4	デバッグログを確認します。	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。 『NetBackup ログリファレンスガイド』を参照してください。
手順 5	操作を再試行します。	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。

手順	処理	説明
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。	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に問題が起きた場合は、次の手順を参照してください。 p.30 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。 p.31 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。
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。	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、NetBackup 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.261 の「UNIX および Linux のディスクリカバリ手順について」を参照してください。 p.272 の「Windows のディスクリカバリ手順について」を参照してください。
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。	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。 UNIX/Linux 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。 次のディスクパーティションを確認します。 ■ 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。 ■ NetBackup プライマリ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。 ■ 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。 ■ NetBackup ログが格納されているパーティション。 ■ 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。
手順 9	ログレベルを上げます。	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。ログレベルの変更に関する詳細情報が利用可能です。 『NetBackup ログリファレンスガイド』を参照してください。
手順 10	実行中のデーモンまたはプロセスを特定します。	UNIX/Linux 版または Windows 版の NetBackup サーバーの手順に従います。 p.24 の「すべてのプロセスが UNIX または Linux 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.27 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。

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

1 プライマリ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/openv/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。

プライマリサーバー

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

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 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/openv/netbackup/bin/initbprd
```

4 NetBackup Web 管理コンソール (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/openv/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/openv/volmgr/bin/stopltid
```

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/openv/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 acssel 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/openv/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/openv/netbackup/bin/bp.kill_all
/usr/openv/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	プライマリサーバー上ですべてのサービスを起動します。	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、NetBackup アクティビティモニターまたは Windows の[コントロールパネル]の[サービス]を使用して、これらのサービスを起動します。 すべてのサービスを起動するには、*install_path*¥NetBackup¥bin¥bpup.exe を実行します。 プライマリサーバー上のサービス: ■ NetBackup Authentication ■ NetBackup Client Service ■ NetBackup Compatibility Service ■ NetBackup Database Manager ■ NetBackup Discovery Framework ■ NetBackup Enterprise Media Manager ■ NetBackup Event Manager ■ NetBackup Indexing Manager ■ NetBackup Job Manager ■ NetBackup Policy Execution Manager ■ NetBackup Scale-Out Relational Database 接続プールサービス ■ NetBackup Scale-Out Relational Database Manager ■ NetBackup Remote Manager and Monitor Service ■ NetBackup Request デーモン ■ NetBackup Resource Broker ■ NetBackup Service Layer ■ NetBackup Service Monitor ■ NetBackup Storage Lifecycle Manager ■ NetBackup Vault Manager ■ NetBackup Volume Manager ■ NetBackup Web 管理コンソール ■ Veritas Private Branch Exchange **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 を参照してください。

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。	メディアサーバー上のサービス: ■ NetBackup Client Service ■ 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) ■ NetBackup 重複排除マネージャ (システムにデータ重複排除が構成されている場合) ■ 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) ■ 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) ■ 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) ■ NetBackup Volume Manager サービス
手順 3	クライアントのすべてのサービスを起動します。	クライアントのサービス: ■ NetBackup Client Service ■ NetBackup Legacy Client Service ■ Veritas Private Branch Exchange
手順 4	avrd およびロボットのプロセスを起動します。	NetBackup 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。 ■ 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) ■ すべての構成済みロボットに対するプロセス。 『NetBackup Web UI 管理者ガイド』を参照してください。 これらのプロセスが実行中でない場合、NetBackup Device Manager サービスを停止してから再起動します。NetBackup アクティビティモニターまたは Windows の[コントロールパネル]の[サービス]を使用します。

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。	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。 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.36 の「プライマリ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.40 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。 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 NetBackup の問題が示されていないかどうかを確認します。 『NetBackup ログリファレンスガイド』を参照してください。 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。

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、プライマリ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。	失敗の原因として、次のことが考えられます。 ■ Windows システムの場合、管理者 (Administrator) 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) ■ 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) ■ 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) ■ 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) ■ 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)

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。	**メモ:** 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、`bpcd -standalone` サービスと `vnetd -standalone` 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 プライマリサーバーと Linux クライアントの間で適切な通信が行われます。 **メモ:** 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。 **メモ:**『NetBackup Appliance 管理者ガイド』を参照してください。 次の手順を実行します。 ■ 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。 ■ 正しいクライアント名がポリシー構成にある。 ■ 正しいサーバー名がクライアントの `/.rhosts` ファイルにある。 インストールがハングアップした場合、クライアントで root 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、`.login` によって、端末の種類が定義される前に `stty`(`stty ^erase` など) 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、`.login` ファイルを変更して、`stty` 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 `.login` ファイルを他のファイル名に変更しておきます。 ■ 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、`ftp` 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。
手順 3	ネットワークの問題を解決します。	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.44 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.48 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。

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。 ■ 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。 ■ ドライブが不正な形式または密度で構成されている。 ■ ロボットドライブ番号が不適切である。 ■ 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。 ■ 複数のロボットに同じロボット番号が使用されている。 ■ 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。 ■ 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。 ■ ロボットデバイスで LUN 1 (一部のロボットハードウェアで必要) を使用するように構成されていない。 ■ 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。 ■ 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。 ■ 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。 ■ 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。 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。 ■ 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)。 ■ 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)。 ■ デーモンまたはサービスの実行中に構成が変更された。 ■ 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 Web UI 管理者ガイド』を参照してください。 ■ 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。

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。	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、NetBackup の状態コードまたはメッセージを確認します。 ■ [すべてのログエントリ (All log entries)]レポートに、該当する期間の NetBackup 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 (Activity monitor)]でジョブの[状態の詳細 (Detailed Status)]を確認します。[バックアップの状態 (Status of Backups)]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。 『 状態コードリファレンスガイド』を参照してください。 ■ 問題がメディアまたはデバイスの管理に関するものであり、NetBackup が状態コードを示さない場合は、システムログ (UNIX 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 (Windows 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。 ■ 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。 『NetBackup ログリファレンスガイド』を参照してください。
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。	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.89 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.91 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.92 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.127 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。

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.)	NetBackup Server 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。NetBackup Server 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、NetBackup Server 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。NetBackup 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)	NetBackup 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。 ■ 新しいデバイスマッピングファイルを Cohesity のサポート Web サイトからダウンロードし、再試行します。 ■ ロボットライブラリを手動で構成します。 ■ NetBackup 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。
(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 (またはパ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。 ■ 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。 ■ このドライブにパススルーパスが定義されていない。	ドライブのアダプタを変更するか、またはドライブにパススルーパスを定義します。SCSI アダプタのパ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詳しくは、『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。 ■ 新しいデバイスマッピングファイルを Cohesity のサポート Web サイトからダウンロードし、再試行します。 ■ ドライブを手動で構成します。 ■ NetBackup でサポートされているドライブだけを使用します。

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詳しくは、『NetBackup デバイス構成ガイド』を参照してください。

プライマリ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 Web UI 管理者ガイド Vol. 1』を参照してください。

表 2-6　　プライマリ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。	プライマリ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、『NetBackup ログリファレンスガイド』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。	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。 または、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テストポリシーを設定します。プライマリサーバーをクライアントとして指定し、プライマリ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)。また、NetBackup ボリュームプールにボリュームを構成し、ドライブにボリュームを挿入します。bplabel 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。
手順 3	デーモンとサービスを検証します。	プライマリサーバー上で 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。 ■ 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。 /usr/openv/netbackup/bin/bpps -x ■ 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。
手順 4	ポリシーをバックアップおよびリストアします。	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。 これらの操作によって、次のことが検証されます。 ■ 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。 ■ 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。
手順 5	エラーを確認します。	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。 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。 問題をさらに特定するには、デバッグログを使用します。 一連のプロセスの概要について詳しくは、『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。
手順 6	デバッグログ以外の情報を確認します。	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。 ■ システムログ (UNIX システムの場合) ■ 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) ■ 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 ■ 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 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。

手順	処理	説明
手順 7	ロボットドライブを検証します。	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。 特に、次を検証します。 ■ 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。 ■ 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。 UNIX 版 NetBackup 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、tpreq 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 tpunmount コマンドを実行します。
手順 8	テストポリシーにロボットを含めます。	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 EMM データベースホスト上の NetBackup ボリュームプールに存在する必要があります。 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、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。
手順 9	ロボットテストユーティリティを使います。	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.241 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。 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。
手順 10	テストポリシーを拡張します。	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。

手順	処理	説明
手順 11	ファイルをバックアップおよびリストアします。	プライマリ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、プライマリ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。 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。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。 UNIX システムでは、デバッグログは /usr/openv/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 *install_path*¥NetBackup¥logs¥ ディレクトリに存在します。 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。 ■ bparchive (UNIX の場合のみ) ■ bpbackup (UNIX の場合のみ) ■ bpbkar ■ bpcd ■ bplist ■ bprd ■ bprestore ■ nbwin (Windows の場合のみ) ■ bpinetd (Windows の場合のみ) 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。 ログについて詳しくは、『NetBackup ログリファレンスガイド』を参照してください。
手順 12	テストポリシーを再構成します。	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、NetBackup クライアントソフトウェアをインストールします。
手順 13	デバッグログディレクトリを作成します。	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。 ■ サーバー上の bprd ■ クライアント上の bpcd ■ クライアント上の bpbkar ■ クライアント上の nbwin (Windows の場合のみ) ■ クライアント上の bpbackup (Windows クライアント以外の場合) ■ bpinetd (Windows の場合のみ) ■ tar ■ メディアサーバー: bpbrm、bpdm、bptm 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。 ログについて詳しくは、『NetBackup ログリファレンスガイド』を参照してください。

手順	処理	説明
手順 14	クライアントとプライマリサーバーの間の通信を検証します。	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プライマリサーバー間の通信、クライアントの NetBackup ソフトウェアを検証します。 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。 [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。
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、プライマリ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、プライマリサーバー上のすべての問題を解決します。

p.36 の「プライマリ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。	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。 UNIX および Linux の場合: `/usr/openv/netbackup/logs/mklogdir` Windows の場合: *install_path*¥NetBackup¥logs¥mklogdir.bat 『NetBackup ログリファレンスガイド』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、レガシー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。	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。 ■ 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)。 ■ 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。 ■ ドライブにボリュームを挿入します。bplabel 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。
手順 3	デーモンとサービスを検証します。	すべての NetBackup デーモンまたはサービスがプライマリ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。 この検証を実行するには、次のいずれかを行います。 ■ UNIX システムの場合は、次のコマンドを実行します。 /usr/openv/netbackup/bin/bpps -x ■ 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。
手順 4	ファイルをバックアップおよびリストアします。	プライマリ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、ファイルの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。 このテストによって、次のことが検証されます。 ■ NetBackup メディアサーバーソフトウェア。 ■ 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。 ■ プライマリサーバープロセス (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。 ■ 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。 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。
手順 5	プライマリサーバーとメディアサーバーの間の通信を確認します。	プライマリ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。 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。 ■ システムログ (UNIX サーバーの場合) ■ 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 サーバーの場合) ■ vmd のデバッグログ

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。	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。 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。 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。 特に、次を検証します。 ■ 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。 ■ 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。 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、tpreq 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、tpunmount コマンドを実行して、メディアのマウントを解除します。

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。	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。 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。 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。 『NetBackup 管理者ガイド Vol. 1』を参照してください。 [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。 ■ メディアサーバー上のシステムログ (UNIX サーバーの場合) ■ ロボットの EMM サーバー上に存在する vmd のデバッグログ ■ 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) 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。 テストユーティリティを試行します。 p.241 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。 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。
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。	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 9	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、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。

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/openv/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。	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す。 次のディレクトリを作成します。 ■ `bpcd` (プライマリサーバーおよびクライアント上) ■ `vnetd` (プライマリサーバーおよびクライアント上) ■ `bprd` (プライマリサーバー上) 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プライマリサーバーの通信の問題をデバッグするには、`bprd` のログディレクトリを使用します。
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。	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。 ■ 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。 ■ 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。 ■ 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。 p.74 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。 クライアント上で `hostname` コマンドを実行して、クライアントがプライマリ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。プライマリサーバー上の `bprd` 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。

手順	処理	説明

手順 3	名前解決を検証します。	名前解決を検証するには、プライマリ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。
		
		`# bpclntcmd -hn client name`
		
		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。
		
		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プライマリ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。
		
		`# bpclntcmd -hn server name`
		
		`# bpclntcmd -ip IP address of server`

手順 4	ネットワークの接続を検証します。	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。
		
		`# ping clientname`
		
		ここで、*clientname* 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。
		
		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。
		
		`# 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`
		
		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。
		
		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。
		
		`# ping ant 1556`
		
		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。

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。
		
		`netstat -a | grep bpcd`
		`netstat -a | grep 13782`
		`rpcinfo -p | grep 13782`
		
		1556 (PBX) と 13724 (vnetd) 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。
		
		`# 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`
		
		LISTEN 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。
		
		NetBackup 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。
		
		`# ps -ef | egrep 'pbx_exchange|vnetd|bpcd' | grep -v grep`
		`root 306 1 0 Jul 18 ? 13:52 /opt/VRTSpbx/bin/pbx_exchange`
		`root 10274 1 0 Sep 13 ? 0:11 /usr/openv/netbackup/bin/vnetd -standalone`
		`root 10277 1 0 Sep 13 ? 0:45 /usr/openv/netbackup/bin/bpcd -standalone`
		
		プライマリ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。

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 1556 (PBX) と 13724 (vnetd) 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、Ctrl+C を押して接続を切断します。
		
		`telnet` *`clientname`* `1556`
		`telnet` *`clientname`* `13724`
		
		ここで、*clientname* 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。
		
		次に例を示します。
		
		`# 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。
		
		プライマリ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。

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。	プライマリ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。
		
		`# netstat -na | grep '<client_IP_address>' | egrep '1556|13724'`
		`10.82.105.11.45856 10.82.104.99.1556 49152 0 49152 0 ESTABLISHED`
		
		`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。
		
		`$ netstat -na | grep '<client_IP_address>'`
		`10.82.105.11.45856 10.82.104.99.1234 49152 0 49152 0 ESTABLISHED`
		
		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。	プライマリ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。
		
		`$ netstat -na | grep '<source_port>'`
		`10.82.104.99.1556  10.82.105.11.45856  49152 0 49152 0 ESTABLISHED`
		
		次のいずれかの状況が発生します。
		■ 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。
		■ 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。

手順 9	クライアントとプライマリ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、クライアントからプライマリ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 プライマリサーバーへの問い合わせが開始されます。その後、プライマリ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.85 の「bpclntcmd ユーティリティについて」を参照してください。 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 プライマリサーバー上に `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.74 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する方法については、『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.88 の「[ホストプロパティ (Host Properties)]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.88 の「[ホストプロパティ (Host Properties)]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.88 の「[ホストプロパティ (Host Properties)]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 bpclntcmd ユーティリティを使用して、クライアントからプライマリ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) プライマリサーバーへの問い合わせが開始されます。その後、プライマリ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.85 の「bpclntcmd 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

Cohesity 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.52 の「vnetd プロキシ接続の必要条件」を参照してください。

p.53 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.53 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.54 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.55 の「vnetd プロキシ接続のテスト」を参照してください。

p.57 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.57 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、Cohesity 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

メモ: NetBackup ホスト ID のマッピングと 8.0 以前のホストとの通信の設定を確認するには、NetBackup Web UI を開きます。右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。[安全な通信 (Secure communication)]タブをクリックします。

同じ NetBackup ドメイン内での通信の場合は、次の要件に注意してください:

- 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 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、bpclntcmd -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。
  Web UI の代わりに、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¥NetBackup¥bin¥admincmd¥nbseccmd -getsecurityconfig -autoaddhostmapping
  UNIX の場合:
  /usr/openv/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。
  Web UI の代わりに、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¥NetBackup¥bin¥admincmd¥nbseccmd -getsecurityconfig -insecurecommunication
  UNIX の場合:
  /usr/openv/netbackup/bin/admincmd/nbseccmd -getsecurityconfig -insecurecommunication
- プライマリサーバー上の 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*¥NetBackup¥bin¥nbcertcmd -ping

UNIX の場合: /usr/openv/netbackup/bin/nbcertcmd -ping

- 外部 CA が署名した証明書を使用するようにプライマリ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プライマリ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。

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プライマリサーバーすべてで、ソースプライマリ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プライマリ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プライマリ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、『NetBackup Deduplication ガイド』を参照してください。

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 76*xx* 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。

次のリソースは状態コードを記述します。

- NetBackup 状態コードリファレンスガイド。
- ジョブの詳細で、状態コードをクリックします。

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/openv/netbackup/bin/vnetd -standalone
root  13606  1  0 Jun27 ?  00:01:55 /usr/openv/netbackup/bin/vnetd -proxy inbound_proxy

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

  -number 0
root  13610  1  0 Jun27 ?  00:00:06 /usr/openv/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。nbpxytnl 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 NetBackupbptestbpcd 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/openv/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@primary.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = a753da9b-b1ff-4a5f-b57d-69a4e2b47e29
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@primary.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 = primary.example.com
EMM_SERVER = primary.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。

vnet 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 bpclntcmd コマンドを使用してプライマリ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¥bpclntcmd -pn -verbose

UNIX の場合:

/usr/openv/netbackup/bin/bpclntcmd -pn -verbose

次に、bpclntcmd コマンドに対する正常な応答の例を示します。

```
# bpclntcmd -pn -verbose
expecting response from server primary.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@primary.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = 7157d866-8eb2-45bb-bde8-486790c0b40c
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@primary.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 bpclntcmd クライアントでの NetBackup コマンドに対する応答を示します。

```
# bpclntcmd -pn -verbose
Unable to perform peer host name validation. Curl error has occurred for peer name:
primary.example.com, self name: connect-host: 0
       [PROXY] Encountered error (VALIDATE_PEER_HOST_PROTOCOL_RUNNING) while processing
```

```
        (ValidatePeerHostProtocol).: 1
Can't connect to host primary.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

プロキシ	コンポーネント名	オリジネータ ID
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

ジョブの場合、NetBackup は、ジョブの詳細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.57 の「vnetd プロキシログファイルの表示」を参照してください。

次のリソースは状態コードを記述します。

- NetBackup 状態コードリファレンスガイド。
- ジョブの詳細で、状態コードをクリックします。

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.60 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.61 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.62 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.63 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.64 の「プライマリ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、Cohesity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。
- `bptm` 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

プライマリサーバーの 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 ホストがプライマリ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 NetBackup

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。

グローバルセキュリティ設定を確認してください。これらの設定を確認するには、NetBackup Web UI を開きます。右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。

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。
- プライマリ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、またはプライマリサーバーの 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.65 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.68 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.65 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.57 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.65 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.68 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.65 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.68 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。

プライマリサーバーのセキュリティ証明書が失効している

NetBackup プライマリ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、プライマリ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、プライマリ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.57 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 primary_server` コマンド出力は、プライマリ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.65 の「NetBackup ホストの証明書の状態の確認」を参照してください。

プライマリ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、プライマリサーバーのセキュリティ証明書を再発行してから、プライマリサーバーを稼働状態に戻します。
3. 問題を解決してプライマリ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、プライマリサーバーの証明書の無効化を元に戻すか、プライマリサーバーの新しい証明書を登録できます。

p.68 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。

ホスト自体からホスト証明書を確認する	この方法では、NetBackup `nbcertcmd` コマンドを使用します。 p.66 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。
NetBackup サーバーからホスト証明書を確認する	この方法では、NetBackup `bptestbpcd` コマンドを使用します。 p.66 の「別のホストの証明書が失効している場合に NetBackup サーバーから確認する方法」を参照してください。
ホスト自体からホスト証明書を確認する	p.67 の「ホストの証明書を確認するには」を参照してください。

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/openv/netbackup/bin/nbcertcmd -getCRL [-server primary_server_name]`

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -getCRL [-server primary_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、`-server`*`primary_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/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster] [-server primary_server_name]`

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -hostSelfCheck [-cluster] [-server primary_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 プライマリサーバークラスタのアクティブノードでこのオプションを使用します。
`-server`	デフォルト以外のプライマリサーバーから証明書を確認するには、*primary_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 プライマリサーバーまたは 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/openv/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。

ホストの証明書を確認するには

1. NetBackup Web UI を開きます。
2. 左側で、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
3. 証明書名をクリックして、証明書の状態を確認します。

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。

ホスト自体からホスト証明書を確認する	p.67 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。
NetBackup サーバーからホスト証明書を確認する	p.68 の「別のホストの証明書が失効している場合に NetBackup サーバーから確認する方法」を参照してください。

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.68 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/openv/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、クラスタプライマリ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 プライマリサーバーまたは 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/openv/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/openv/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/openv/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/openv/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プライマリ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、プライマリサーバーは `/usr/openv/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、プライマリサーバーは、[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、ターゲットホストによって接続しているホストのピアホスト名が判断されます。ターゲットホストがプライマリサーバーの場合は、ピアホスト名からクライアントの構成名も判断されます。

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)。

プライマリサーバーでは、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、総あたり的な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。プライマリ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 bpclntcmd 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/openv/netbackup/bin/bpclntcmd -pn (UNIX)
```

```
# install_path¥NetBackup¥bin¥bpclntcmd -pn (Windows)

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。
- プライマリサーバーの 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/openv/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。

traceroute (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プライマリサーバーの DNS で認識されないと、プライマリ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、プライマリサーバーの 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、プライマリ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/openv/netbackup/db/altnames/host.xlate (UNIX)

install_path¥NetBackup¥db¥altnames¥host.xlate (Windows)

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、プライマリサーバーの `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、プライマリサーバーの NetBackup 構成で構成された名前である必要があり、通常はポリシー内のクライアントです。プライマリ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、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)) をプライマリ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.70 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 Windows クライアントの場合

次の手順を実行します。

- [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)] ドロップダウンリストで、プライマリ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 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)]ドロップダウンリストをクリックします。
  Windows コンピュータでは、現在のプライマリ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。プライマリサーバー上で 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、プライマリ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 (NetBackup 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。
- プライマリ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。
- プライマリサーバーの `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.88 の「[ホストプロパティ (Host Properties)]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。

- 構成内のプライマリ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。プライマリサーバーはリストの最初の名前である必要があります。
  プライマリサーバー上で SERVER エントリを追加または変更する場合は、bprd と bpdbm を停止してから再起動して変更を有効にします。
- プライマリサーバーの bp.conf では、CLIENT_NAME = *primary server name* としてのプライマリサーバー以外に、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/openv/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/openv/netbackup/bp.conf の同じオプションより優先されます。

プライマリサーバー上

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/openv/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.78 の「UNIX プライマリ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.80 の「UNIX プライマリ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.82 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.83 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 か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 bprd 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 (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)]ドロップ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)]ドロップ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.85 の「bpclntcmd ユーティリティについて」を参照してください。

UNIX プライマリ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 プライマリサーバーが示されています。

図 2-1 UNIX プライマリサーバーおよびクライアント

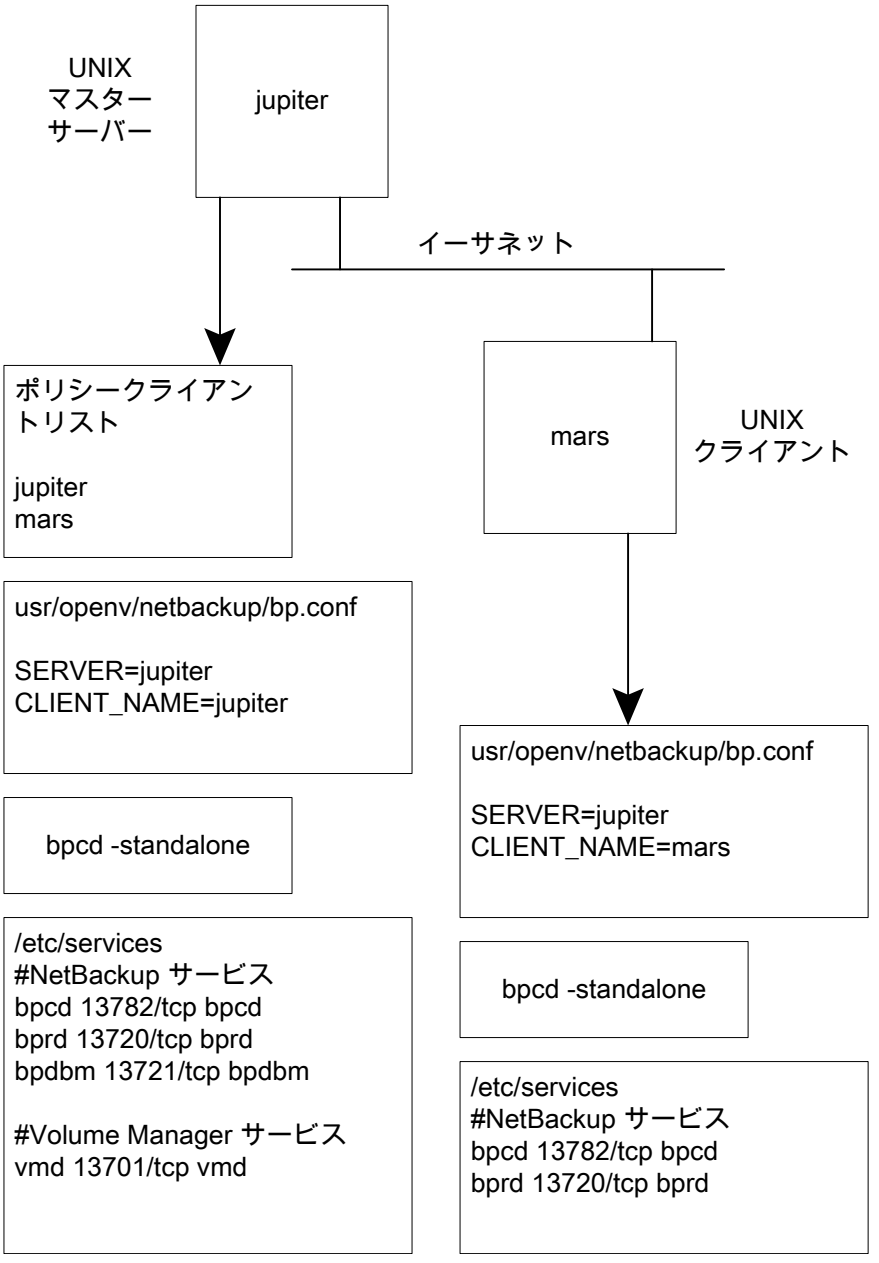

図 2-1について、次の点を考慮してください。

- 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 プライマリ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、プライマリサーバー *jupiter* の SERVER エントリの下に存在します。

図 2-2 UNIX プライマリサーバーおよびメディアサーバー

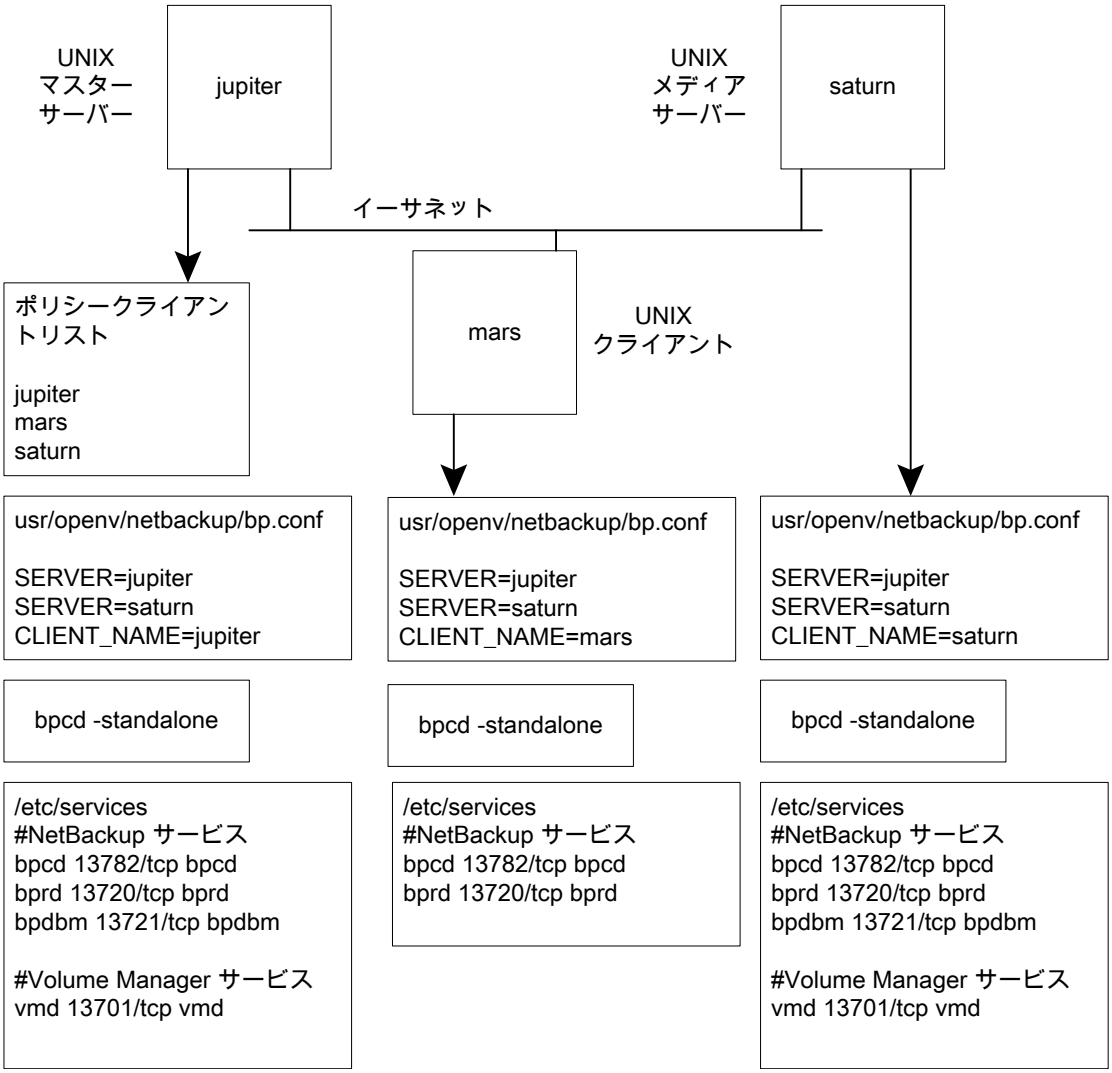

図 2-2について、次の点を考慮してください。

- 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 プライマリ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

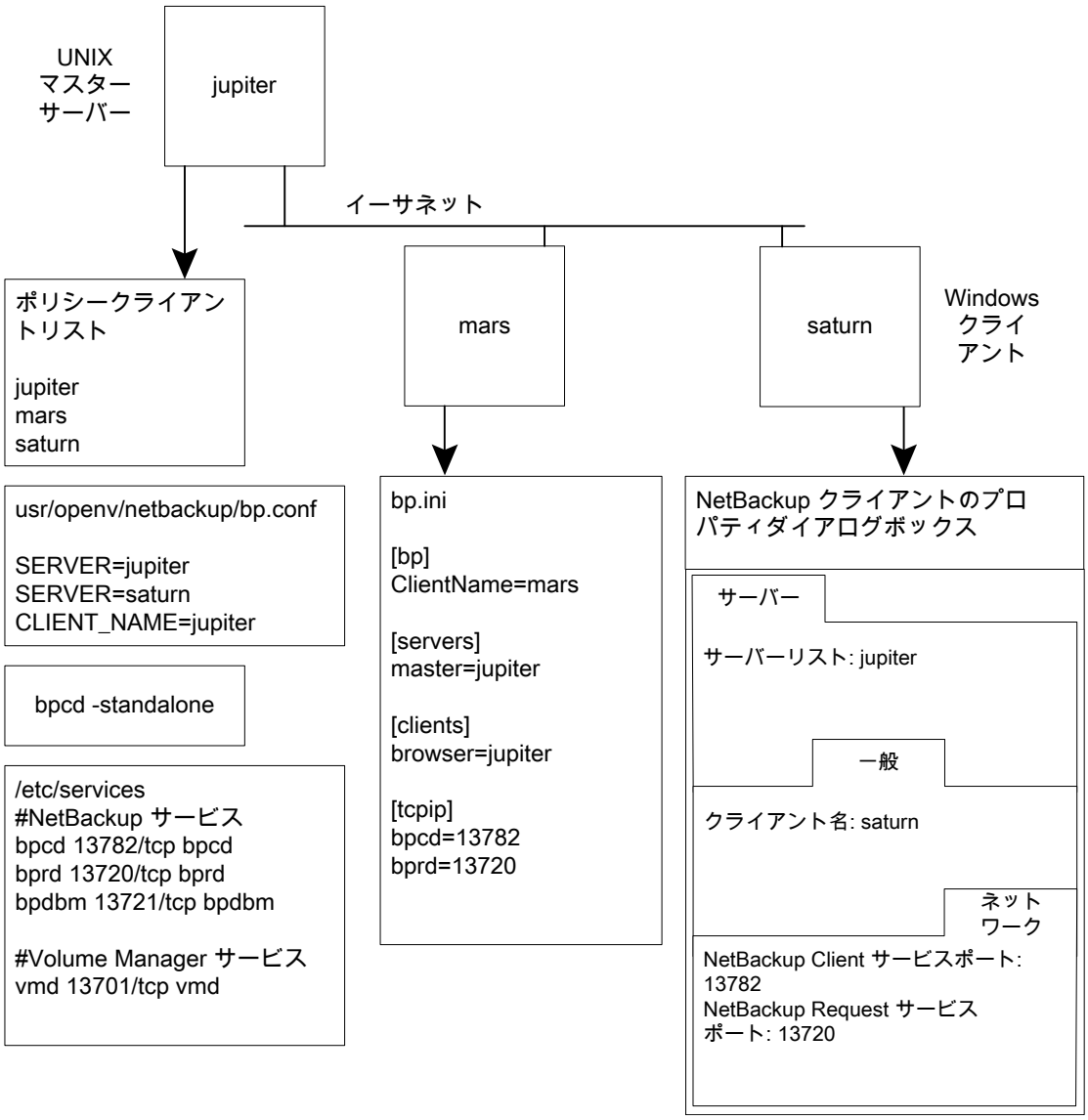

図 2-3については、次の点を考慮してください。

- 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

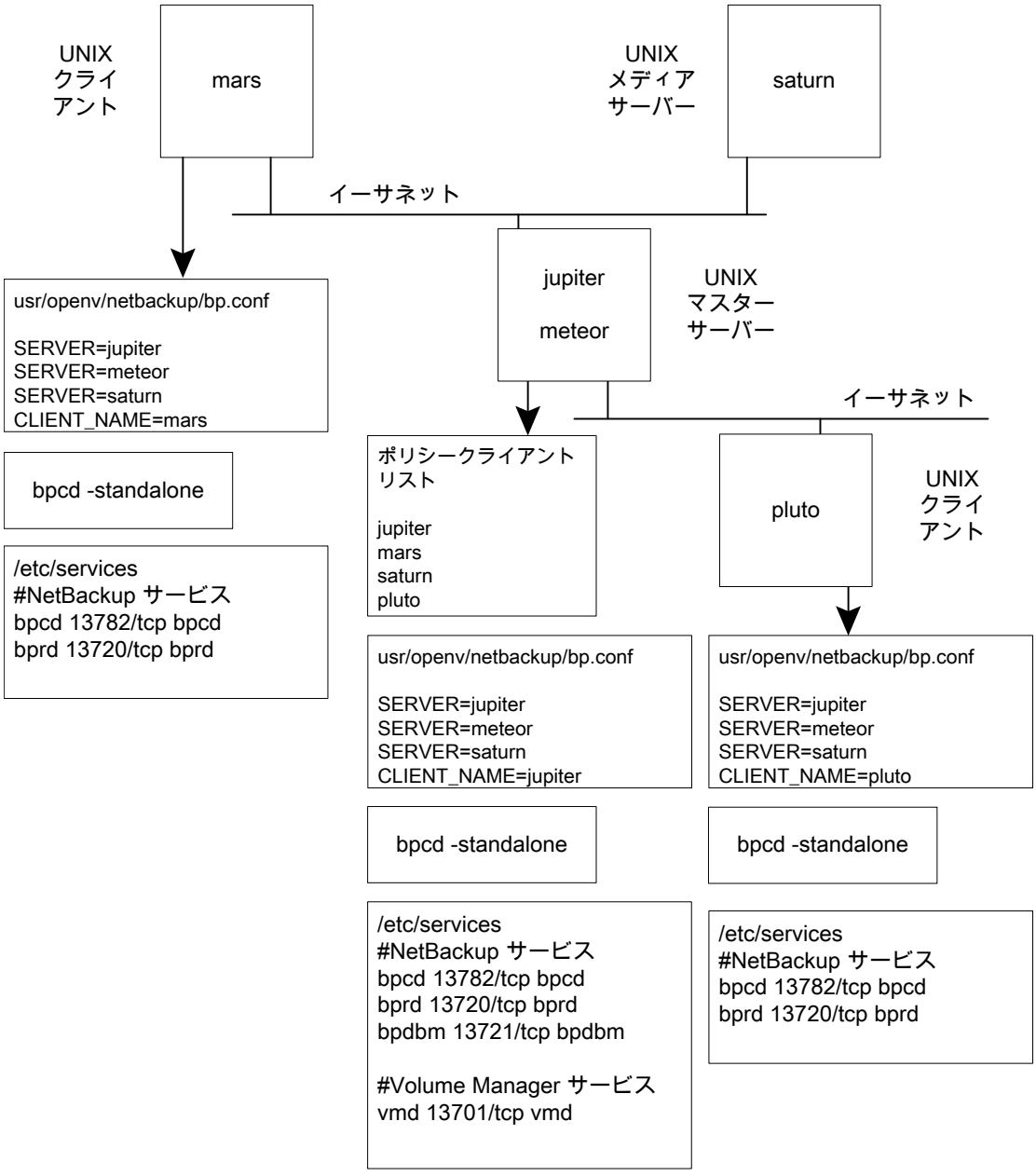

図 2-4については、次の点を考慮してください。

- 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、プライマリ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。

プライマリサーバー上の 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 (プライマリサーバーの名前) は *jupiter* です。これは、プライマリ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、プライマリ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。

bpclntcmd ユーティリティについて

bpclntcmd 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 bpclntcmd でプライマリサーバーに接続し、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、プライマリ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/openv/netbackup/bin

Windows の場合、MS-DOS コマンドウィンドウでこの bpclntcmd 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 bpclntcmd のオプションは、-ip、-hn、-sv および -pn です。

-ip　　bpclntcmd -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。bpclntcmd 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　　bpclntcmd -hn *Hostname*

-hn オプションはホスト名を指定します。bpclntcmd 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　　bpclntcmd -sv

-sv オプションを使うと、プライマリサーバー上に 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 プライマリ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、プライマリサーバーの観点からの情報で、プライマリ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プライマリサーバーエントリです。
- dove.friendlyanimals.com は、プライマリサーバーによって戻された接続名 (ピアネーム) です。プライマリサーバーは、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、プライマリ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、bpclntcmd -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、bpclntcmd -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: bpclntcmd コマンドは usr/openv/netbackup/logs/bpclntcmd ディレクトリ (UNIX) または *install_path*¥NetBackup¥logs¥bpclntcmd (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、bpclntcmd ログは bpclntcmd 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)]を使用した構成設定へのアクセス

[ホストプロパティ (Host properties)]を使用すると、NetBackup クライアントとサーバーに対する多くの構成設定にアクセスできます。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。これらの設定にアクセス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 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 (NetBackup client properties)]ダイアログボックスの設定の多くは、NetBackup Web UI の[ホストプロパティ (Host properties)]でも利用可能です。

ホストプロパティを使用して構成設定にアクセスする方法

1. NetBackup Web UI にサインインします。
2. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。
3. 更新するホストを選択し、[接続 (Connect)]をクリックします。

4 ホストの種類に応じて、次のいずれかをクリックします。

- プライマリサーバーの編集 (Edit primary server)
- メディアサーバーの編集 (Edit media server)
- クライアントの編集 (Edit client)

5 編集するプロパティを選択し、変更します。

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 Scale-Out Relational Database Manager 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 `vrtsdbsvc_psql` デーモンです。

3 NetBackup Scale-Out Relational Database Manager 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。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ときに `nbrb` サービスを停止すると、エラーが起きることがあります。

- NetBackup Scale-Out Relational Database Manager サービスを再起動します。

4 NetBackup Scale-Out Relational Database Manager 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/openv/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/openv/db/bin/nbdb_admin -validate -verbose`

Windows の場合: *install_path*¥VERITAS¥NetBackup¥bin¥ nbdb_admin -validate -verbose

検証が失敗した場合は、Cohesity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/openv/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、Cohesity Technical Support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、Cohesity Technical Support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、Cohesity Technical Support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。
- メディアを解凍するには、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 つずつ解凍します。
- 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
- メディアを凍結したメディアサーバーの bptm ログ。

  /usr/openv/netbackup/logs/bptm
- オペレーティングシステムの管理メッセージか syslog。

Windows
- メディアを凍結したメディアサーバーの bptm ログ。

  install_dir¥VERITAS¥NetBackup¥logs¥bptm
- Windows のイベントビューアのシステムログ。
- Windows のイベントビューアのアプリケーションログ。

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とき、bptm ログはアクティビティモニターより詳しい情報を含むことがあります。各メディアサーバーのホストプロパティ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.91 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.92 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 Cohesity の次のサポート Web サイトにあります。 netbackup.com/compatibility
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/openv/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 Web UI を開きます。左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順に選択します。

メディアサーバーのプロパティを開きます。

[メディア (Media)]をクリックします。

[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/openv/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.96 の「NetBackup Web サービスのログの表示」を参照してください。

プライマリ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

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、統合ログを使いません。これらのログの形式について、およびログがどのように作成されるかについて詳しくは、http://tomcat.apache.org にある Apache Tomcat のマニュアルを参照してください。これらのログは次の場所に書き込まれます。

  ```
  usr/openv/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/openv/logs/nbwebservice
  install_path¥NetBackup¥logs¥nbwebservice
  ```

  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¥nbwebservice.jks]
due to [Illegal character in opaque part at index 2: C:¥Program
Files¥Veritas¥NetBackup¥var¥global¥wsl¥credentials¥tpcredentials¥nbwebservice.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/openv/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/openv/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/openv/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プライマリ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/openv/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。

- プライマリ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 プライマリサーバーを認証して、クライアントがプライマリ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/openv/logs/nbcert
/usr/openv/wmc/webserver/logs/configureCerts.log
/usr/openv/logs/nbatd
```

```
install_path¥NetBackup¥logs¥nbcert
C:¥ProgramData¥Veritas¥NetBackup¥InstallLogs¥WMC_configureCerts_yyyymmdd_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/openv/logs/nbwebservice
/usr/openv/wmc/webserver/logs/configureCerts.log
/usr/openv/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.101 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.101 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.102 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.103 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.104 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.106 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 プライマリサーバーで次のディレクトリを検索します。

- Windows の場合: *install_path*¥VxPBX
- UNIX の場合: /opt/VRTSpbx

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/VRTSpbx/bin/pbxcfg -v

PBX が実行中であるかどうかの確認

PBX が NetBackup プライマリ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/VRTSpbx/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/VRTSpbx/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/VRTSpbx/bin/pbxcfg -a -u root
```

- Secure Modeを false に設定する場合:

```
/opt/VRTSpbx/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、次の場所に書き込まれます。

- /opt/VRTSpbx/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/VRTSpbx/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 vmoprcmd 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ます。/opt/VRTSpbx/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/VRTSpbx/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/VRTSpbx/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/openv/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/VRTSpbx/bin/vxpbx_exchanged stop

5 PBX を起動します。

- UNIX の場合:

  /opt/VRTSpbx/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/openv/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と、次に類似したメッセージが /opt/VRTSpbx/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。このサービスを起動するには、次の手順を実行します。

   (UNIX または Linux) nbemm コマンドを入力します。

   (Windows) NetBackup Enterprise Media Manager サービスを起動します ([スタート]、[ファイル名を指定して実行]の順に選択し、「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/openv/netbackup/bin/bp.kill_all
/usr/openv/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、プライマリ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.108 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 サービスがプライマリサーバーで実行されていることを検証します。
  p.95 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.99 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。
- ホストがプライマリサーバー上の 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プライマリ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.109 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。
- プライマリサーバー上で承認が保留されているリモートホストのホスト 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.109 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、プライマリ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.111 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プライマリ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/openv/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/openv/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: exampleprimary 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

プライマリサーバーで 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/openv/netbackup/bin/admincmd/nbseccmd -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/openv/netbackup/bin/admincmd/nbseccmd -setsecurityconfig -insecurecommunication on

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/openv/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 myprimary
  出力例: `example1.com is successfully updated.`
- UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbhostmgmt -add -hostid xxxxx-52e8-xxxx-ba92-7be20c6dceb9 -mappingname myprimary`
  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¥bpclntcmd -clear_host_cache
- UNIX の場合: /usr/openv/netbackup/bin/bpclntcmd -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 (A.I.R.) 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: 複数のプライマリサーバードメインにわたるレプリケーションは、A.I.R. 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。

A.I.R. 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。

A.I.R. 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。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イメージがあることを確認するには、NetBackup Web UI で［ストレージ (Storage)］、［ディスクストレージ (Disk storage)］の順に開き、［ディスクプール (Disk pools)］タブをクリックします。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場合は、［ディスクボリュームの更新 (Update disk volume)］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
A.I.R. 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。 ■ SLP がアクティブか ■ nbstserv デーモンが実行中か ■ 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
A.I.R. 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。
A.I.R. レプリケーションジョブが状態 191 などで失敗した	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:ss1.acme.com
LSU Name: PureDiskVolume
Allocation : STS_LSU_AT_STATIC
Storage: STS_LSU_ST_NONE
Description: PureDisk storage unit (/ss1.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 -stype 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 -stype 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。

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 -stype 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 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 を使用する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:                   ss1.acme.com
Storage Server:                 ss1.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 `ss1.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
```

A.I.R. ジョブのフローをトラブルシューティングするには、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他のジョブに使用するのと同じコマンドラインを使用してください。たとえば、リモートプライマリ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
```

リモートプライマリ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            : ss1.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       : ss1.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: ss1.acme.com
  Backup ID           : woodridge_1287610477
  Copy Number         : 102
  Target Machine      : bayside
  Target Info         : PureDiskVolume
  Remote Master       : (none specified)
```

A.I.R. (自動イメージレプリケーション) と SLP で使用されるプライマリサーバーのルール

A.I.R. (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 プライマリサーバードメインの SLP (ストレージライフサイクルポリシー) を使用します。2 つのプライマリ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 (ターゲット型 A.I.R.)、元のドメインで自動イメージレプリケーションの SLP を作成する前にターゲットドメインにインポート SLP を作成する必要があります。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。

- ソースプライマリ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、ターゲットプライマリ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 SLP 内のリモートプライマリ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 SLP は最初のコピーに対する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 SLP 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 SLP 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、ターゲット型 A.I.R. の信頼できるプライマリサーバーの操作に失敗する

外部証明書の構成で、ターゲット型 A.I.R. の信頼できるプライマリサーバーの操作が失敗する場合があります。この場合は、次の操作をトラブルシューティングできます。

- 信頼の追加または更新のトラブルシューティング
  p.121 の「信頼の追加または更新のトラブルシューティング」を参照してください。
- 信頼の削除のトラブルシューティング
  p.122 の「信頼の削除のトラブルシューティング」を参照してください。

信頼の追加または更新のトラブルシューティング

このトピックでは、ソースとターゲットのプライマリサーバー間で、信頼を追加または更新する操作が失敗した場合に問題をトラブルシューティングする方法について説明します。

問題

ソースプライマリサーバーとターゲットプライマリサーバー間で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: ターゲットプライマリサーバーへのソースプライマリサーバーの登録に失敗した。
- 原因 2: 信頼できるプライマリ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プライマリサーバーを TRUSTED_MASTER として追加することに失敗した。

原因 1 (ターゲットプライマリサーバーへのソースプライマリサーバーの外部証明書の登録に失敗した) の解決方法

p.146 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 (信頼できるプライマリ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プライマリサーバーを TRUSTED_MASTER として追加することに失敗した) の解決方法

信頼の追加または更新のトラブルシューティングを行う方法

1 エラーメッセージ ([**終了状態 5630: リモートプライマリサーバーのバージョンの取得に失敗しました。**(EXIT STATUS 5630: Failed to get version of remote primary server.)]) を確認します。

vnetd プロキシサービスが停止している場合、またはソースプライマリサーバーで vnetd 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。

- リモートプライマリサーバーの vnetd プロキシへの接続を確認します。
  リモートプライマリサーバーの vnetd プロキシへの接続を確認するには、bptestbpcd -host *remote_primary_server_name* コマンドを実行します。
- プロキシログを確認します。

Windows の場合: C:¥Program Files¥Veritas¥NetBackup¥logs¥nbpxyhelper¥*log_file*
Linux の場合: /usr/openv/logs/nbpxyhelper/*log_file*

2 エラーメッセージ ([終了状態 5616: ローカルプライマリサーバーにアクセスできません。(EXIT STATUS 5616: The local primary server is not reachable.) 現在、信頼が単方向になっています。リモートプライマリサーバーはローカルプライマリサーバーを信頼していますが、ローカルプライマリ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。(The trust is unidirectional right now, the remote primary server trusts the local primary server, but the local primary server doesn't trust the remote master.) 信頼を除去してください (Please remove the trust)」) を確認します。

ソースプライマリサーバーで bprd 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/openv/netbackup/logs/bprd/*log_file*
- プロキシログを確認します。
  Windows の場合: C:¥Program Files¥Veritas¥NetBackup¥logs¥nbpxyhelper¥*log_file*
  Linux の場合: /usr/openv/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*
  Linux の場合: /usr/openv/logs/nbemm/*log_file*

信頼の削除のトラブルシューティング

このトピックでは、信頼できるプライマリサーバーデータベースおよび構成ファイルからターゲットプライマリサーバーを TRUSTED_MASTER として削除できない場合の問題をトラブルシューティングする方法について説明します。

問題

信頼を削除する操作が失敗しました。

原因

ターゲットプライマリサーバーを、信頼できるプライマリサーバーデータベースと構成ファイルから TRUSTED_MASTER として削除できませんでした。

解決方法

信頼の削除のトラブルシューティングを行う方法

- エラーメッセージ ([**終了状態** 5616: **ローカルプライマリサーバーにアクセスできません。** (EXIT STATUS 5616: The local primary server is not reachable.) **現在、信頼が単方向になっています。リモートプライマリサーバーはローカルプライマリ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プライマリサーバーを信頼していません。**(The trust is unidirectional right now, the remote primary server trusts the local primary server, but the local master server doesn't trust the remote primary.) **信頼を除去してください。**(Please remove the trust.)]を確認します。
  ソースプライマリサーバーで 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
    Linux の場合: /usr/openv/netbackup/logs/bprd/log_file
  - プロキシログを確認します。
    Windows の場合: C:¥Program Files¥Veritas¥NetBackup¥logs¥nbpxyhelper¥*log_file*
    Linux の場合: /usr/openv/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*
    Linux の場合: /usr/openv/logs/nbemm/***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、このプライマリ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。

処理	条件
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 bperror 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プライマリ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 bperror 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 プライマリ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,TCPCKSUM> 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,TCPCKSUM> mtu 1500
   ether 00:07:e9:3e:ca:b4 (auto-unknown-cfg_down) flowcontrol full
   e9b: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCKSUM> 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 プライマリ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 プライマリサーバーソフトウェアまたはメディアサーバーソフトウェアのいずれか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。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。nbftclnt

```
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、アクティビティモニターの[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 Web UI と 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	NetBackup Web UI または NetBackup 管理コンソールで実行される操作によって、NetBackup の他の部分でエラーが検出される場合があります。これらのエラーは、通常、NetBackup の状態コードおよびメッセージの章に記載されているとおりに表示されます。 **メモ:** エラーメッセージには、状態コードが付かない場合もあります。
NetBackup 管理コンソール: アプリケーションサーバーの状態コードおよびメッセージ	これらのメッセージには、500 番台の状態コードが付きます。 **メモ:** エラーメッセージには、状態コードが付かない場合もあります。
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。 ■ NetBackup 管理コンソールのステータスバー ■ `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

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/openv/netbackup/logs/user_ops` 内
- 管理コンソールが起動されたホスト
- `/usr/openv/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プライマリ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/openv/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/openv/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 の次回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/openv/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ークが失敗しました。

- プライマリ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: *install_path*¥NetBackup¥bin¥nbcertcmd -getSecConfig -caUsage
  UNIX の場合: /usr/openv/netbackup/bin/netbackup/bin/nbcertcmd -getSecConfig -caUsage
  例: *install_path*¥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/openv/netbackup/bin/netbackup/bin/nbcertcmd -listallcertificates -jks
  - 次のコマンドを実行して、NetBackup プライマリ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: *install_path*¥goodies¥nbsslcmd x509 -in *certificate_path* -noout -text -purpose
    UNIX の場合:
    /usr/openv/netbackup/bin/netbackup/bin/goodies/nbsslcmd x509 -in *certificate_path* -noout -text -purpose

プライマリサーバーのホスト証明書が、Web サーバー証明書と同じ root 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 root CA によって発行されていない場合、NetBackup プライマリサーバーの 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-primary _ext
  DNS: nb-primary .some.domain.com
  DNS: nb-primary _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プライマリ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プライマリ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

原因 2

一部の NetBackup Core Services が開始されていない。

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。

問題を解決するには、次の手順を使います。

- 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`
  - `postgres` (UNIX) または NetBackup Scale-Out Relational Database Manager (Windows)
- `nbsl` および `vnetd` サービスが実行されていない場合は再起動します。
- NetBackup Scale-Out Relational Database が実行されていない場合は再起動します。

Windows の場合:

次のように、`nbsl`、`vnetd`、および NetBackup Scale-Out Relational Database Manager サービスを再起動します。

```
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 "NetBackup Scale-Out Relational Database Manager" -f -v
install_path¥bin¥bpup -e "NetBackup Scale-Out Relational Database Manager" -f -v
```

UNIX の場合:

次のように nbsl サービスを再起動します。

```
/usr/openv/netbackup/bin/nbsl -terminate
/usr/openv/netbackup/bin/nbsl
```

次のように vnetd サービスを再起動します。

例:

```
# ps -fed | grep vnetd | grep standalone
root 16018 1 4 08:47:35 ? 0:01 ./vnetd -standalone
# kill 16018
/usr/openv/netbackup/bin/vnetd -standalone
```

次のように NetBackup Scale-Out Relational Database を再起動します。

```
/usr/openv/netbackup/bin/nbdbms_start_server -stop
/usr/openv/netbackup/bin/nbdbms_start_server
```

問題が解決しない場合は、Cohesity Technical Support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。
  - プライマリ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 *primary_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 *primary_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 primary_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 primary_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
- ホストまたはプライマリサーバーで CRL が使用できない。

p.68 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。

外部証明書の構成に関する問題のトラブルシューティング

このトピックでは、外部証明書、構成、削除などに固有の問題のトラブルシューティングについて説明します。

外部証明書の構成について詳しくは、『NetBackup セキュリティと暗号化ガイド』を参照してください。

表 2-11

通し番号	問題	考えられる理由	解決方法
1.	外部証明書が構成されている場合に次のエラーが表示されます: `NetBackup Web Management Console service is down with error. nbcertcmd: The -ping operation failed. EXIT STATUS 26: client/server handshaking failed Ensure that NetBackup Web Management Console service is up and running before trying this operation.`	NetBackup Web 管理コンソール (nbwmc) サービスが停止しています。	NetBackup Web 管理コンソール (nbwmc) サービスを起動します。
2.	外部証明書を追加または削除しても、監査エントリが作成されません。	`-force` オプションを指定して `configureWebServerCerts` コマンドが実行されています。	`-force` オプションを指定しないで `configureWebServerCerts` コマンドを実行します。
3.	外部証明書を構成した後、NetBackup Web 管理コンソール (nbwmc) サービスが起動しません。	外部証明書の構成処理に何らかの問題がある可能性があります。	次を実行します。 ■ 証明書チェーン、秘密鍵、トラストストアなどの外部証明書パラメータが正しい形式であることを確認し、外部証明書を再度構成してください。 ■ 問題が解決しない場合は、`-force` オプションを使用して外部証明書を構成してみてください。 ■ 問題が解決しない場合は、すべてのエラーログ情報を保存してからCohesityテクニカルサポートにお問い合わせください。

通し番号	問題	考えられる理由	解決方法
4.	コマンド `./configureWebServerCerts -removeExternalCert -all` が次のいずれかのエラーで終了しました。 ■ 終了状態 7724: 証明書を削除できません。(The certificate cannot be removed.) ■ 終了状態 7733: NetBackup Web UI の外部証明書を削除できません。(External certificate of the NetBackup web UI cannot be removed.) ■ 終了状態 7734: NetBackup ホストの外部証明書を削除できません。	考えられる理由: ■ 既存の Web サーバー構成をバックアップするための容量がディスクに残っていません。 ■ 次の場所にある、Web サーバーの構成を更新する権限に問題があります。 `NetBackup Install Directory/var/global/wsl/webserver/config`	次を実行します。 ■ ディスク容量を増やします。 ■ 問題が解決しない場合は、すべてのエラーログ情報を保存してからCohesityテクニカルサポートにお問い合わせください。
5.	`./configureWebServerCerts -addExternalCert -all -certPath file_path -privateKeypath file_path -trustStorePath file_path` コマンドが次のいずれかのエラーで終了しました。 ■ `EXIT STATUS 7728: The input file of ECA configuration is not valid.` ■ `EXIT STATUS 7730: The private key cannot be added.` ■ `EXIT STATUS 7731: The trust bundle cannot be added.`	考えられる理由: ■ 証明書を追加するための容量がディスクに残っていません。 ■ 次の場所にある、証明書を追加する権限に問題があります。 `NetBackup Install Directory/var/global/wsl/credentials` ■ プライマリサーバーが FIPS モードで実行され、外部証明書を構成するために指定されたファイルが PEM 形式ではありません。	■ ディスク容量を増やします。 ■ プライマリサーバーが FIPS モードで実行されている場合は、PEM 形式のファイルを使用してコマンドを実行します。 ■ 問題が解決しない場合は、すべてのエラーログ情報を保存してからCohesityテクニカルサポートにお問い合わせください。

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/openv/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/openv/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プライマリサーバー (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、プライマリ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プライマリサーバー (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 8.2 以降にアップグレードされていない。

解決方法

- `nbcertcmd -getsecconfig -caUsage` コマンド、NetBackup Web UI を使用して、プライマリサーバー認証局 (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プライマリ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プライマリ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。
  `bpclntcmd -clear_host_cache`
- *install_path*`/logs/nbpxyhelper` にある `vnet proxy` ログを確認します。
- *install_path*`/logs/nbwebservice` 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。
- nbmqbroker サービスがプライマリサーバーで起動し実行されていない可能性がある。
- 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。
- プライマリサーバー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

nbmqbroker サービスがプライマリサーバーで起動し実行されていない可能性がある。

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 および Linux の場合: /usr/openv/mqbroker/logs
  Windows の場合: *Install_Path*/mqbroker/logs
- プライマリサーバーで 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。
  - プライマリ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 サーバーがリバース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ライバのログを確認します。
  UNIX および Linux の場合: `usr/openv/logs/nbsubscriber`
  Windows の場合: *`Install_Path`*`/logs/nbsubscriber`
- *`Install_Path`*`/logs/vnetd` で `vnetd` ログを確認します。
- プライマリ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ライ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、プライマリ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: クライアントが 8.1.2 以前のバージョンである

次を実行します。

`nbgetconfig` コマンドを使用して、プライマリ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、`bpclntcmd -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: プライマリサーバーのサービスが再起動された

次を実行します。

- 次の場所にあるサブスクライバサービスのログを確認します。
  UNIX および Linux 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ライバサービスが起動するまで待機します。
- サブスクライ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。
- プライマリ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。

- プライマリ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:[primary 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. プライマリサーバーで次のコマンドを実行します。

   `/user/openv/netbackup/bin/admincmd/bptestbpcd -host` *`host_name`*

2. `/user/openv/netbackup/logs/admin` のログを確認します。
3. メディアサーバーがオフラインかどうかを確認します。NetBackup Web UI を開きます。左側で［ストレージ (Storage)］、［メディアサーバー (Media servers)］の順に選択します。次に、［メディアサーバー (Media servers)］タブをクリックします。
4. プライマリ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ーログが接続メッセージを受信する準備ができている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:` *`primary 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。

- プライマリ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。

- 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。
- プライマリサーバーで 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、プライマリサーバーと 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。

サブスクライ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. サブスクライ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/openv/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/openv/var/global/mqbroker/certstore/nbcacreds/ca.pem"},
{ssl_options, [{cacertfile,
"/usr/openv/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
```

4 NetBackup Web 管理コンソール (nbwmc) サービスと nbqmbroker 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/openv/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/openv/var/global/mqbroker/certstore/externalcacreds/ca.pem"},
{ssl_options, [{cacertfile,
"/usr/openv/var/global/mqbroker/certstore/externalcacreds/ca.pem"},
```

p.291 の「Linux 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.287 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:

プライマリ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/openv/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/openv/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/openv/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/openv/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 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:

```
# 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. 次の手順を実行して必要なファイルを作成します。

   適切なテキストエディタ (Linux の場合は vi、Windows の場合はメモ帳) を使用し、指定したディレクトリに erl_inetrc というファイルを作成します。

   Linux の場合、次のディレクトリに erl_inetrc ファイルを作成します。

   ```
   /usr/openv/var/global/mqbroker/erl_inetrc
   ```

   次のコマンドを実行します。

   ```
   cat > /usr/openv/var/global/mqbroker/erl_inetrc
   ```

   Windows の場合、次のディレクトリに erl_inetrc ファイルを作成します。
   NetBackup_Install_path¥var¥global¥mqbroker¥

2. erl_inetrc ファイルに次の行を追加します。

   ```
   {inet6,true}.
   ```

   末尾のドット (.) は必須であることに注意してください。

3. UNIX の場合、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 次を実行します。

Linux の場合:

/usr/openv/var/global/mqbroker/advanced_setmqenv ファイルに次の行を追加します。

```
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"
```

Windows の場合:

NetBackup_Install_path¥var¥global¥mqbroker¥advanced_setmqenv ファイルに次の行を追加します。

```
RABBITMQ_SERVER_ADDITIONAL_ERL_ARGS=-kernel inetrc
'E:/NetBackup/var/global/mqbroker/erl_inetrc' -proto_dist
inet6_tcp

RABBITMQ_CTL_ERL_ARGS=-proto_dist inet6_tcp
```

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のトラブルシューティング

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 構成の問題のトラブルシューティング

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) と外部キーマネージメントサービス (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.primary.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、プライマリ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/openv/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/bpclntcmd -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

プライマリサーバー上の Web サービスログの場合:
Install_path/logs/nbwebservice/<51216-495-***-***-***.log>

NetBackup KMS の nbkmiputil 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、プライマリ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、プライマリ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/bpclntcmd -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`

プライマリサーバー上の Web サービスログの場合:
`Install_Path/logs/nbwebservice/<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、プライマリ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。

プライマリサーバー上の 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://<Primary-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 'bdc3492b015d4a9ab25426465b12adac6a834dfc6b4449c490922d6155719958'
 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

プライマリサーバー上の Web サービスログの場合:
Install_Path/logs/nbwebservice/<51216-495-***-***-***.log>

nbkmiputil ログの場合:

- NetBackup KMS の場合: *Install_Path*/logs/nbkms
- 外部 KMS の場合: *Install_Path*/netbackup/logs/nbkmiputil

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のトラブルシューティング

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に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、Cohesity Technical Support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のトラブルシューティング

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。

プライマリ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 2-12 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。 ■ 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。 ■ 理由 2 - nbwebsvc がサービスユーザーとして使用されている。 ■ 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。	解決方法は次のとおりです。 ■ 解決方法 1 - 次のコマンドを実行します。 id *service_user* ID コマンドが正常に実行される必要があります。 ■ 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。 ■ 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。 id *service_user* 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。

通し番号	問題	考えられる理由	解決方法
2	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 NetBackup をインストール中、次のいずれかのエラーが発生する。 ■ `Service user name on active node does not match with service user name entered on inactive node.` ■ `SERVICE_USER_ID '10021' retrieved from active node does not match with the user ID '1002' of local user 'nonroot'.`	サービスユーザー名とユーザー ID が一致しません。	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 NetBackup 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。
3	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 NetBackup のアップグレード中、次のエラーが発生する。 `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.`	`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。	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。
4	UNIX プラットフォームで、NetBackup 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。 `/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。	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。	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。 `Fix below errors and then retry`

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。	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。
		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。
			次のように、秘密鍵の権限を確認します。
			証明書を右クリックします。[すべてのタスク]、[秘密鍵の管理]の順にクリックします。
			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。
			次のコマンドを実行して権限を設定します。
			`nbcertcmd -setWinCertPrivKeyPermissions`
			以下のコマンドを実行して構成を検証します。
			`nbcertcmd -ecaHealthCheck`

6	`setconfig` コマンドが次のエラーで失敗する。 `Failed to open /usr/openv/netbackup/bp.conf.d53: Permission denied (13)`	`/usr/openv/netbackup` の所有権がルートユーザーに変更されています。 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。	次のコマンドを実行して、所有権の問題を解決します。 `/usr/openv/netbackup/bin/goodies/update_install_folder_perms`
7	■ 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。 ■ カタログバックアップが失敗する。 ■ カタログリカバリが失敗する。	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。	状態コード 9201 と 9202 を確認します。 『NetBackup 状態コードガイド』を参照してください。 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。
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。	次の項目について確認します。 ■ 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。 ■ 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。

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。 ■ nbdb_admin ■ nbdb_move ■ nbdb_backup ■ nbdb_restore ■ nbdb_unload ■ create_nbdb ■ cat_export ■ cat_import パス: UNIX の場合: *Install_Path*/db/bin Windows の場合: *Install_Path*¥netbackup¥bin	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『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。
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、`nbserviceusercmd -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`*
17	ユーザーをアップグレードまたは変更する前に、サービスユーザーは削除されます。	サービスユーザーは、特定のユーザー操作のために削除される場合があります。	次を実行します。 サービスユーザーをリストアするためにユーザーを再構成します。この記事を参照してください。 次のコマンドを実行します。 ■ `useradd -c 'NetBackup Services account' -d /usr/openv/ nbsvcusr -u` *`old uid`* ■ `usermod -a -G nbwebgrp nbsvcusr`
18	バックアップまたはリストア中に操作エラーが発生しました。	メディアサーバーがクライアントより前のバージョンです。	メディアサーバーをアップグレードするか、クライアントのバージョンと同じかそれ以降のバージョンの代替メディアサーバーを使います。

auth.conf ファイルのグループ名の形式に関する問題のトラブルシューティング

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/openv/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/openv/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¥nbwebservice
   - Linux の場合:
     /usr/openv/netbackup/logs/bprd
     /usr/openv/logs/vxul/nbwebservice

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。

   nbwebservice 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 nbwebservice ログのものです。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 モードの問題のトラブルシューティング

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。

プライマリ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のトラブルシューティング

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

(スキャンホスト RHEL 8.x と NFS バージョン 4.x に該当) 大きいサイズのバックアップ (最大 2 億個のファイル) をスキャンすると、失敗したジョブについて Web UI に次のエラーが表示されます。

```
Failed to get response from NetBackup malware utility.
```

スキャンホストでのスキャンの進行中に、NFS マウントポイントにスキャンホストからアクセスできません。スキャンジョブは進行中のままになり、2 日後にタイムアウトします。ストレージサーバーの NFS エクスポートにアクセスできます。

回避方法: スキャンホストの `/etc/nfsmount.conf` ファイルに次を構成して、NFS を介したスキャンホストでの IA マウントに NFS バージョン 3 を使用していることを確認します。

```
# grep Defaultvers /etc/nfsmount.conf Defaultvers=3
```

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スキャンホストへの SSH 接続に失敗しました。

回避方法: 次のスキャンホストのクレデンシャルを確認します。

- RSA (SHA256) キー
- ユーザー名
- パスワード

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。

回避方法: スキャンホストのサポート対象プラットフォームの完全なリストについては、ソフトウェア互換性リストのマニュアル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

- スキャンホストで利用可能な領域が不足しています。
- 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。

回避方法

- Windows スキャンホストの場合、C:¥ フォルダの空き領域を確認します。
- Linux スキャンホストの場合、/tmp フォルダの空き領域を確認します。

スキャンホストクレデンシャ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ャルをフェッチできません。

回避方法: スキャンホストのクレデンシャ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。

回避方法: スキャンのタイムアウトは構成可能で、構成キー MALWARE_SCAN_OPERATION_TIMEOUT を設定して変更できます。

- 最小値: 1 時間
- 最大値: 30 日

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

nbmalwareutil バイナリと ScanManager が一致していません。

回避方法:

NetBackup の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です。

回避策: nbmalwarescanner ログを、エージェントレスホストタイププールの場合はメディアサーバーで、エージェントベースのスキャンの場合はスキャンホストで参照してください。

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。

回避方法: 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。

回避策: nbmalwarescanner ログを、エージェントレスホストタイププールの場合はメディアサーバーで、エージェントベースのスキャンの場合はスキャンホストで参照してください。

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。

回避策: nbmalwarescanner ログを、エージェントレスホストタイププールの場合はメディアサーバーで、エージェントベースのスキャンの場合はスキャンホストで参照してください。

作成されたインスタントアクセスマウントが、マルウェアスキャンによって削除されません

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。

回避方法:

- スキャンが進行中かどうかを確認します。
- スキャンが進行中でない場合は、GET IA API を使用して作成されたインスタントアクセスマウントの ID を持つ、このようなインスタントアクセスマウントのリストを次のディレクトリから取得します。

  `/netbackup/recovery/workloads/{workload}/instant-access-mounts`
- DELETE API を使用して、インスタントアクセスマウントを削除します。

  `/netbackup/recovery/workloads/{workload}/instant-access-mounts/{mounId}`

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。

回避方法:

- 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。
- `net use` 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。
- 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:¥`

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

Microsoft 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。

回避方法: 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。

回避方法: 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。

回避方法: NetBackup のサポートにお問い合わせください。

NetBIOS 名に設定できる文字は最大 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は最大 15 文字使用できます。

Windows Server 2016 を使用して Active Directory 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への接続は許可されません。

回避方法: 文字数の制限が 15 文字以下であることを確認してください。

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。

回避方法: 次のエラーを確認します。

- `nbmalwarescanner` ログを、エージェントレスホストタイププールの場合はメディアサーバーで、エージェントベースのスキャンの場合はスキャンホストで参照してください。
- メディアサーバーのストレージ領域を確認します。
- メディアサーバーで NFS サービスエラーを確認します。

選択した時間範囲の感染ファイルが多すぎます

選択した日付範囲のバックアップイメージの感染ファイルリストを表示するには、`nbmalwarescanner` を確認します。

回避方法: 感染ファイルの数を減らすため、日付範囲を変更するか、リカバリファイルやリカバリフォルダを選択し直してください。操作を再試行します。次のいずれかを実行することもできます。

- クリーンファイルを選択的にリカバリするために使用できる[マルウェアに感染したファイルのリカバリを許可 (Allow recovery of files impacted by malware)]オプションを選択します。

- リカバリからそのバックアップイメージを除外します。

大量の感染ファイルです

- 選択したスキャン結果に含まれる感染ファイルが多すぎます。スキャン結果に 5,000 を超える感染ファイルがある場合は、次のメッセージが表示されます。

  `Large number of infected files. To view the complete list of infected files, export the list.`

  回避方法: 感染したファイルのリストを `.csv` 形式でエクスポートし、ダウンロードして表示します。

- 選択したスキャン結果に含まれる感染ファイルの数が多いか、感染ファイルのパスが長すぎてデータベースで取得できません。次のエラーメッセージが表示されます。

  `Large number of infected files.`

  回避方法: この結果をエクスポートまたは表示することはできません。
  結果をエクスポートまたは表示できないため、スキャンログで、選択したスキャン結果の感染ファイルに関する詳細な一覧を確認します。

スキャン操作が分割されます

バックアップのサイズが大きい場合、スキャン操作は分割されます。たとえば、バックアップのファイルの合計数が 1,000,000 個の場合、スキャン操作はファイルが 500,000 個ずつの 2 回に分割されます。

各回で作成とスキャンが個別に実行されます。回ごとに異なるスキャンホストを割り当てることができます。マルウェア検出 UI には、バックアップの単一のエントリのみが表示されます。

回避方法: 分割された各回の詳細は、REST API を使用して取得できます。

NB_MALWARE_SCANNER_PATH 環境変数が見つかりません

スキャンホストにインストールされている NetBackup マルウェアスキャナを使用してマルウェアスキャン操作を実行すると、次のエラーメッセージが表示されて失敗します。

```
Missing environment variable NB_MALWARE_SCANNER_PATH
```

回避方法: NetBackup マルウェアスキャナがインストールされていることを確認します。インストール場所をメモします。

プライマリサーバーでのスキャンホストの構成中に指定されたのと同じユーザークレデンシャルを使用して、スキャンホストにユーザーとしてログインします。次の行を `~/.bashrc` に追加します。

```
export
NB_MALWARE_SCANNER_PATH=<installLocation>/savapi-sdk-linux64/bin

export PATH=$PATH:$NB_MALWARE_SCANNER_PATH
```

Windows スキャンホストでマルウェアスキャンの実行に失敗しました

cygwin mks ツールキットがインストールされている場合、Windows スキャンホストでマルウェアスキャンが失敗する場合があります。

回避方法: UNIX ユーティリティはインストールされますが、定義済みの scanuser の PATH 変数にこれらの UNIX ユーティリティを含めることはできません。

スキャンホストの領域とディレクトリアクセスに関する問題

エラー/問題	説明	回避方法
■ ファイルを開けませんでした。 ■ ディレクトリを作成できません。 ■ 結果ファイルの生成に失敗しました。 ■ 出力ファイルを開けませんでした。 ■ 結果ファイル用のディレクトリを作成できません。 ■ 結果ファイルを開けませんでした。 ■ マウント先のディレクトリを作成できません。 ■ ログファイル用のディレクトリを作成できません。	■ スキャンホストで利用可能な領域が不足しています。 ■ 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。	■ Windows スキャンホストの場合、C:¥ の空き領域を確認します。 ■ Linux スキャンホストの場合、/tmp の空き領域を確認します。

NAS-Data-Protection に関連する問題

■ 次のオプションを選択して、NetBackup を以前のバージョンから NetBackup バージョン 10.3 以降にアップグレードすると、[**検索条件に一致するイメージはありません** (No images match the search criteria)]のメッセージが表示されます。

オプション	フィールド
検索条件 (Search by): バックアップイメージ (Backup images)	ポリシー形式 (Policy type): NAS-Data-Protection コピー (Copies): Copy2 マルウェアスキャンの状態 (Malware scan status): 未スキャン (Not scanned)(デフォルト)

オプション	フィールド
検索条件 (Search by): ポリシー形式別の資産 (Assets by policy type)	ポリシー形式 (Policy type): NAS-Data-Protection コピー (Copies): Copy2 スキャナホストプール (Scanner host pool): 必要なスキャナホストプールを選択します。 マルウェアスキャンの状態 (Malware scan status): 未スキャン (Not scanned)(デフォルト)

回避方法
バックアップ済みのイメージを表示するには、以前のバージョンの NetBackup メディアサーバーで作成された NAS-Data-Protection バックアップイメージをスキャンするために、[マルウェアのスキャン状態 (Malware scan status)]オプションに[すべて (All)]を選択していることを確認します。

- ファイルの書き込みエラー
  ファイルの書き込みエラー
  NAS-Data Protection ポリシーでマルウェアスキャンを実行しているときに、.tar.gz ファイル (13 GB 未満) がスキップされ、次のエラーメッセージが表示されました。

  ```
  File write error
  ```

  NetBackup Malware Scanner (Avira) は、スキャンする前に、圧縮またはアーカイブされたファイルの内容をステージングボリュームに抽出します。ステージングボリュームに圧縮またはアーカイブされたファイルを抽出するのに十分な領域がない場合、それらのファイルはスキャン処理中にスキップされ、スキャン不可能なファイルとして報告されます。スキャン結果からスキャン不可能なファイルのリストをエクスポートできます。ファイルがスキップされた理由が次のように示されます。

  ```
  File write error
  ```

  回避方法:
  ステージングボリュームのデフォルトサイズは 10 GB です。バックアップに大量の圧縮もしくはアーカイブされたファイルがある場合、または圧縮もしくはアーカイブされたファイルがネストされている場合 (.jar または .war ファイルを含む zip ファイルなど)、ステージングボリュームのサイズを増やす必要があります。

スキャンパフォーマンスの問題

10.3 より前のバージョンの NetBackup でマルウェアスキャン (従来のマルウェアスキャン) にインスタントアクセスマウントポイントを使用すると、パフォーマンスの問題が発生しました。

回避方法: NetBackup メディアサーバーとストレージサーバーを 10.3 以降にアップグレードします。NetBackup 10.3 では、動的スキャン機能が導入されています。これにより、インスタントアクセスにかかる時間とスキャンのパフォーマンスが向上します。

次の表に、従来のマルウェアスキャンと動的スキャンの違いを示します。

主なスキャン手順	インスタントアクセスマウントポイントを使用した従来のマルウェアスキャン	動的スキャン
インスタントアクセスをステージングする。	tar ストリームを分析し、各ファイルのヘッダーおよびエクステントマップファイル (LMDB データベース) をビルドします。これは、バックアップに多数のファイルがあるために時間がかかります。	フラグメントから TIR (カタログデータベース) と IM (イメージメタデータ) 情報をリストアします。
インスタントアクセス共有 (NFS/SMB) がマウントされ、ユーザーがファイルを一覧表示またはアクセスしようとする。	ヘッダーファイルにアクセスし、そこから属性を読み取ります。	カタログデータベースのディレクトリに問い合わせ、このディレクトリにあるすべてのファイルとディレクトリを取得します。また、各ファイルとディレクトリの属性を出力に問い合わせることもできます。
スキャンホストがファイルを開く	LMDB データベースを開き、ロードします。	メモリ内にインデックスをビルドし、データコンテナから直接読み取ります。 ■ ファイルのエクステントを取得するには、tar ヘッダーを見つけて読み取り、内容を分析します。 ■ SO リストを取得するには (PureDisk のみ)、フラグメントの FP マップから SO リストを検索します。 ■ マッピングテーブルをビルドするには、SO リストを挿入します (PureDisk のみ)。

主なスキャン手順	インスタントアクセスマウントポイントを使用した従来のマルウェアスキャン	動的スキャン
スキャンホストがファイルを読み取る	LMDB データベースから検索し、データコンテナから読み取ります。	ストレージサーバーがサードパーティのストレージベンダー製の場合、データは OST インターフェースを介して直接読み取られます。ストレージサーバーが PureDisk の場合、マッピングテーブルから検索され、データはデータコンテナから読み取られます。

エラーのログファイルの場所の詳細

次の表に、表示される各ログファイルの詳細を使用例ごとに示します。

表 2-13 エージェントレススキャンホストのログファイルの場所

使用例	プライマリサーバーのコンポーネント	メディアサーバーのコンポーネント	ログファイルのパス
構成	nbwebservice	ncfnbcs	プライマリサーバー: ■ /usr/openv/logs/nbwebservice ■ /usr/openv/netbackup/logs/bprd/ メディアサーバー: ■ /usr/openv/logs/ncfnbcs ■ /usr/openv/netbackup/logs/nbmalwarescanner/
スキャンプロセス	nbwebservice bprd	ncfnbcs nbmalwarescanner	
リカバリ	nbwebservice bprd		

表 2-14 スキャンホストとしての NetBackup クライアントのログファイルの場所

使用例	プライマリサーバーのコンポーネント	スキャンホストクライアントのコンポーネント	ログファイルのパス
構成	nbwebservice	nbsubscriber	■ /usr/openv/netbackup/logs/nbscanhostconfig/ ■ /usr/openv/logs/nbsubscriber/
スキャンプロセス	nbwebservice bprd	nbsubscriber	
リカバリ	nbwebservice bprd		

SSH ログインはデフォルトでは無効です

VMware VM バックアップスキャンの場合は、`uid=0` を指定してスキャンユーザーを使用します。SSH ログインはデフォルトでは無効になっており、ユーザーはセキュリティ上の理由から有効にできない場合があります。

回避方法

上記のシナリオでは、次の手順を実行します。

root ユーザーに対して SSH ログインが無効になっている場合、root 以外のスキャンユーザーをグループ 0 (root) に追加して、すべてのファイルをスキャンできるようにします。

例: `uid=1001(scanuser) gid=1001(scanuser) groups=1001(scanuser),0(root)`

Hyper-V イメージのマルウェアの状態が[サポート対象外 (Not supported)]と表示される

アップグレード中、11.0.0.1 より前のバージョンの NetBackup で作成された Hyper-V イメージについては、マルウェアの状態は[サポート対象外 (Not supported)]となります。アップグレード後に新しくバックアップされたイメージについては、Hyper-V バックアップイメージのデフォルトのマルウェアの状態は[未スキャン (Not Scanned)]となります。

回避方法

ユーザーは、[サポート対象外 (Not supported)]と表示された Hyper-V イメージに対してマルウェアスキャンを実行できます。

移動中のデータの暗号化が有効になっている NetBackup ジョブの問題のトラブルシューティング

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 2-15　　確認するログ

操作	ログ
バックアップまたはアーカイブ	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/openv/netbackup/logs

VxUL ログ: /usr/openv/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 分後に操作を再試行し、次回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 2-16 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/openv/netbackup/logs

VxUL ログ: /usr/openv/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

操作を再試行して、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 2-17 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、bpclntcmd メディアサーバー - bptm、bpclntcmd、vnetd
リストア	クライアント - tar または dbclient、vnetd、bpclntcmd メディアサーバー - bpbrm、bptm、bpclntcmd、vnetd
複製	両方のメディアサーバー - bptm または bpdm、vnetd、bpclntcmd

UNIX のログ: /usr/openv/netbackup/logs

Windows のログ: *install_path*¥NetBackup¥logs

原因

ホスト間の TLS ハンドシェー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、bpclntcmd での次のような問題のいずれかが原因です。

- bpclntcmd への事前共有キーの格納に失敗した
- bpclntcmd 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 bpclntcmd -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 2-18 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 ハンドシェー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。

非構造化データのインスタントアクセスの問題のトラブルシューティング

問題:

AKS (Azure Kubernetes Service) または EKS (Amazon Elastic Kubernetes Service) 環境で、非構造化データのインスタントアクセスが、エラーコード 4001 でインスタントアクセスを作成できませんでした。

原因:

バックアップデータが格納される MSDP エンジンが健全な状態ではない可能性があります。

応答メッセージの例:

```
{
  "errorCode": 4001,
  "errorMessage": "Failed to create the instant access mount.",
  "attributeErrors": {},
  "fileUploadErrors": [],
  "errorDetails": [
    "Failed to provision the backup. /usr/openv/pdde/vpfs/bin/vpfs_
     actions failed (1): Unable to getCatalog: ('Could not get
     catalog of backup
(test-mssql1_1654780591): /usr/openv/pdde/vpfs/bin/cata2map failed
(255): ', {'statusInfo': {'msgId': 'Failed to
get catalog', 'parameters': [{'type':
'string', 'name': 'backupId', 'value':
'test-mssql1_1654780591'}]}})¥n"
  ]
}
```

解決方法:

AKS または EKS 環境で MSDP エンジンが正常かどうかを確認します。または、API インターフェースを使用して、新しいバックアップを作成し、非構造化データのインスタントアクセスを再度作成することもできます。

多要素認証の問題のトラブルシューティング

このトピックでは、NetBackup の多要素認証に固有の問題のトラブルシューティングについて説明します。

多要素認証について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

表 2-19

通し番号	問題	考えられる理由	解決方法
1.	NetBackup Web UI へのログインを試行しましたが、多要素認証を構成するためのページが表示されます。	NetBackup 管理者がドメインに多要素認証を適用していますが、まだ自分のユーザーアカウントを構成していません。	多要素認証が適用されているため、自分のユーザーアカウントに対して多要素認証を構成する必要があります。

通し番号	問題	考えられる理由	解決方法
2.	多要素認証の構成中に、多要素認証構成 UI を使用して QR コードをスキャンできません。	QR コードまたは QR コードスキャナに問題があるかもしれません。	多要素認証構成 UI から QR コードをスキャンできない場合は、シークレットキーをコピーまたは参照し、認証アプリケーションにシークレットキーを手動で挿入できます。
3.	多要素認証の構成中に、ユーザーが多要素認証構成 UI からシークレットキーを参照またはコピーできません。	UI の非表示/表示オプションまたはコピーオプションに問題がある可能性があります。	認証アプリケーションから QR コードをスキャンできます。
4.	多要素認証の構成中に、正しいワンタイムパスワードを指定して［構成 (Configure)］をクリックすると、次のエラーが表示されます。 `Failed to validate one-time password.`	ハンドヘルドデバイスの時間と NetBackup プライマリサーバーの時間に違いがあるか、指定されたワンタイムパスワードが間違っています。	ハンドヘルドデバイスの時間が、プライマリサーバーの時間と一致していることを確認します。 期限切れになる前に、正しいワンタイムパスワードを入力します。
5.	多要素認証の構成中に QR コードをスキャンし、認証アプリケーションで既存のセキュリティ情報を上書きしようとすると、エラーが表示されます。	認証アプリケーションはセキュリティ情報を上書きできません。	QR コードをスキャンする前に、重複したエントリが存在しないことを確認してください。
6.	多要素認証が構成されていても、認証アプリケーションのセキュリティエントリが存在しません。その結果、ワンタイムパスワードを表示できず、認証できません。	認証アプリケーションではワンタイムパスワードを生成できません。スマートデバイスは失われます。	多要素認証構成をリセットするには、NetBackup 管理者に連絡する必要があります。 正常にリセットされたら、ユーザーアカウントに対する多要素認証を再構成します。
7.	NetBackup 管理者である自分のユーザーアカウントに多要素認証を構成しているが、ワンタイムパスワードを使用できません。	セキュリティ情報が認証アプリケーションから削除されているか、ハンドヘルドデバイスが認識されていません。	多要素認証構成をリセットするように他の管理者に依頼できます。その後、自分のユーザーアカウントの多要素認証を再構成できます。 または、次のコマンドを使用して多要素認証構成をリセットするように、OS 管理者に対して要求できます。 `nbseccmd -resetMFA -userinfo <domain type>:<domain name>:<user name>`

通し番号	問題	考えられる理由	解決方法
8.	bpnbat -login CLI が次のエラーを示します。 AT authentication failed	自分のユーザーアカウントに多要素認証を構成しましたが、ログイン形式「AT」が多要素認証をサポートしません。	ユーザーアカウントに多要素認証が構成されている場合は、bpnbat -login -logintype WEB コマンドを使用します。 多要素認証が構成されている場合は、対話モード (bpnbat -login (-Interactive | -i)) を使用してログインすることをお勧めします。
9.	自分のユーザーアカウントに多要素認証を構成していませんが、bpnbat -login が失敗します。	NetBackup 管理者が、ドメイン内のすべてのユーザーに多要素認証を適用している可能性があります。	多要素認証が適用されている場合は、自分のユーザーアカウントを構成し、bpnbat -login (-Interactive | -i) コマンドを実行してログインする必要があります。
10.	bpnbat -login の操作中に、正しいユーザー名とパスワードを指定して 10.3 より前の NetBackup ホストにログオンしようとしましたが、認証が失敗します。	ユーザーアカウントに多要素認証が構成されています。	bpnbat -login コマンドを実行する場合は、パスワードの後にワンタイムパスワードを指定する必要があります。
11.	bpnbat -login の操作中に、cred ファイル (-cf) が使用されますが、ログインに失敗しました。	ユーザーアカウントに多要素認証が構成されています。	cred ファイルを使用する場合は、bpnbat -login (-Interactive | -i) コマンドを使用してログインする必要があります。
12.	bpnbat -login の実行中に正しいユーザー名、パスワード、ワンタイムパスワードを指定しましたが、認証に失敗しました。	ハンドヘルドデバイスの時間と NetBackup プライマリサーバーの時間に違いがあるか、指定されたワンタイムパスワードが間違っています。	ハンドヘルドデバイスの時間が、プライマリサーバーの時間と一致していることを確認します。 期限切れになる前に、正しいワンタイムパスワードを入力します。
13.	NetBackup 管理コンソールのログイン中に、[ユーザーアカウントで多要素認証が有効になっているかどうかを確認できませんでした。(Failed to check whether multi-factor authentication is enabled for the user account or not.)] というエラーが表示されます。	Web サービスが停止しているか、要求を処理できません。	Web サービスが起動して実行中であることを確認します。次のログを確認します。 bpjava ログ: /usr/openv/netbackup/logs/bpjava-msvc Web サービスログ: /usr/openv/logs/nbwebservice

通し番号	問題	考えられる理由	解決方法
14.	NetBackup 管理コンソールのログイン中に、正しいユーザー名とパスワードが指定されていても、[ユーザー名またはパスワードが無効です。(Invalid username or password.)]というエラーが表示されます。	ユーザーアカウントに多要素認証が構成されています。	パスワードの後にワンタイムパスワードを指定する必要があります。
15.	NetBackup 管理コンソールに、[ワンタイムパスワードの認証に失敗しました。(Failed to validate the one time password.)]というエラーが表示されます。 `Failed to validate the one-time password.`	ハンドヘルドデバイスの時間と NetBackup プライマリサーバーの時間に違いがあるか、指定されたワンタイムパスワードが間違っています。	ハンドヘルドデバイスの時間が、プライマリサーバーの時間と一致していることを確認します。 期限切れになる前に、正しいワンタイムパスワードを入力します。
16.	`nbseccmd` を使用して NetBackup プライマリサーバー間の信頼を設定するときに、認証に失敗しました。	ユーザーアカウントに多要素認証が構成されています。	パスワードの後にワンタイムパスワードを指定する必要があります。
17.	1 台以上のプライマリサーバーで `nbdeployutil --gather` コマンドが失敗しました。	失敗したプライマリサーバーで、自分のユーザーアカウントに多要素認証が構成されています。	次のコマンドを実行します。 `--apikey-file` オプションを指定して `nbdeployutil --gather` CLI を実行します。 apikey キーファイルの形式は「NetBackup プライマリホスト名 : *APIKey*」である必要があります。NetBackup ドメインが複数ある場合は、すべてのプライマリサーバーホストに対して apikey が提供されていることを確認します。
18.	NetBackup Web UI、NetBackup 管理コンソール、`nbseccmd` CLI からのプライマリサーバー間の信頼の設定に失敗した場合	ユーザーアカウントに多要素認証が構成されています。	ユーザーアカウントが、ターゲットホストで多要素認証用に構成されている場合は、パスワードのほかに適切なワンタイムパスワードを追加します。
19.	Validate OTP API を使用すると、次のエラーが表示されます。 `The multifactor authentication request ID does not exist.`	指定された要求 ID が存在しません。	Validate OTP API の使用中に、有効な要求 ID を指定します。

通し番号	問題	考えられる理由	解決方法
20.	Validate OTP API を使用すると、次のエラーが表示されます。 `The multifactor authentication request is not valid.`	後続の API 呼び出しに使用される JWT トークンが、以前のものと異なります。	両方の API 呼び出しに同じ JWT トークンを使用します。
21.	NetBackup 構成を変更すると、次のエラーが表示されます。 `The configuration cannot be changed using this host.`	ユーザーアカウントに多要素認証が構成されていますが、このホストで多要素認証がサポートされていません。	NetBackup Web UI を使用して操作を実行します。
22.	nbcertcmd または nbseccmd コマンドを実行すると、次のエラーが表示されます。 `EXIT STATUS 3676: invalid error number`	ユーザーアカウントに多要素認証が構成されていますが、このホストで多要素認証がサポートされていません。	NetBackup Web UI を使用して操作を実行します。
28.	グローバルセキュリティ設定の変更、API キーの作成、nbcertcmd または nbseccmd コマンドの実行を行っている際に、次のエラーが表示されます。 `The multifactor authentication request has timed out.`	ワンタイムパスワードの入力で遅延がありました。	多要素認証時には、180 秒以内にワンタイムパスワードを入力してください。 API を使用する場合は、180 秒以内に「Validate OTP」API を続けて呼び出してください。

マルチパーソン認証の問題のトラブルシューティング

このトピックでは、NetBackup のマルチパーソン認証プロセスに固有の問題のトラブルシューティング方法について説明します。

マルチパーソン認証について詳しくは、『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。

表 2-20

通し番号	問題	考えられる理由	解決方法
1.	マルチパーソン認証を有効にすると、NetBackup 管理コンソールで、NetBackup Vault の作成または変更操作が次のエラーで失敗します。 `Intermittent connectivity lost with the server.`	マルチパーソン認証は、イメージの有効期限操作に対して有効になります。	マルチパーソン認証プロセスからユーザーを除外するには、NetBackup セキュリティ管理者にお問い合わせください。
2.	マルチパーソン認証を有効にすると、前のメディアサーバーでの `nbholdutil -delete` コマンドが次のエラーで失敗します。 `Permission Denied by Hold Service`	プライマリサーバーでのイメージ保留の削除操作に対してマルチパーソン認証が有効になっています。	次のいずれかを実行します。 ■ メディアサーバーを最新の NetBackup バージョンにアップグレードします。 ■ ユーザーがマルチパーソン認証の除外ユーザーとして追加されていることを確認します。 詳しくは、『NetBackup Web UI 管理者ガイド』にある「除外されるユーザーの追加」のトピックを参照してください。 ■ `bpnbat -login` を使用して (除外ユーザーとして) ログインします。 ■ `nbholdutil` コマンドを実行します。
3.	次のいずれかの操作が、終了状態 9382 で失敗します。 エラー: `The operation has failed because it is configured for multi-person authorization.` ■ NetBackup 10.3 以前のホストでは、`bpexpdate`、`bpimage -deletecopy`、`nbdecommission` のいずれかのコマンドが失敗します。 ■ `nbdecommission -oldserver` *`serverName`* `-machinetype media` が失敗します。	マルチパーソン認証が、イメージの有効期限操作に対して有効になっています。	■ 呼び出し元ホストが 10.0 より前の NetBackup の場合、ユーザーがマルチパーソン認証プロセスから除外された場合でも、そのようなホストに対するイメージの有効期限操作はブロックされます。 ■ 呼び出し元ホストが NetBackup 10.0 以降の場合に、マルチパーソン認証プロセスからユーザーを除外するには、NetBackup セキュリティ管理者にお問い合わせください。 NetBackup Web UI に再度サインインして、操作を再試行します。

通し番号	問題	考えられる理由	解決方法
4.	マルチパーソン認証プロセスから除外されたユーザーが、CLI を使用してマルチパーソン認証が有効な操作を実行できず、エラーコード 5930 のエラーが表示されます。	ユーザーが認証されていません。bpnbat -login -logintype WEB コマンドは、除外リストにユーザーを追加した後は実行されません。	bpnbat -login -logintype WEBコマンドを実行して現在の権限セットを正常にロードし、次のいずれかのインターフェースを使用してマルチパーソン認証が有効な操作を実行します。 ■ CLI の使用 ■ NetBackup 管理コンソールの使用 ■ NetBackup Web UI の使用
5.	除外されるユーザーのリストから削除されたユーザーが、マルチパーソン認証が必須の操作を 2 回目の承認なしで実行できます。	除外されるユーザーのリストからユーザーを削除すると、マルチパーソン認証チケットが作成されます。ただし、関連付けられたチケットはまだ承認されていません。	マルチパーソン認証構成のチケットが作成されたかどうかを確認します。 マルチパーソン認証の承認者にチケットの承認を依頼します。承認後、ユーザーは除外リストから削除されます。
6.	除外されたユーザーがイメージを期限切れにできませんでした (マルチパーソン認証が有効な操作の実行に失敗しました)	■ ユーザーには操作を実行する権限がありません。 ■ 除外されたユーザーの要求に対して、マルチパーソン認証チケットは作成されません。この問題は、マルチパーソン認証プロセスに関連していない可能性があります。	該当するマニュアルを参照してください。
7.	マルチパーソン認証が有効な操作は、NetBackup 管理コンソールまたは CLI を使用して正常に実行されます。	ユーザーは除外されたユーザーのリストに含まれている必要があります。	このユーザーに対してマルチパーソン認証チケットを作成する場合は、除外されるユーザーのリストからユーザーを削除します。
8.	除外リストにユーザーグループを追加できません。	除外リストへのユーザーグループの追加は許可されません。	除外リストに個々のユーザーを追加します。
9.	NetBackup Web UI からマルチパーソン認証を構成しようとすると、次のエラーが表示されます。 `The date is not within the allowed range that is between 01/01/1970 and the current date`	システム日付が正しく設定されていない可能性があります。	システム日付を確認し、1970 年 1 月 1 日から現在の日付までの有効な日付を指定します。 日付を修正して NetBackup サービスを再起動します。

通し番号	問題	考えられる理由	解決方法
10.	マルチパーソン認証チケットが、スケジュールされた有効期限後も期限切れになりません。	■ NetBackup Web 管理コンソール (nbwmc) サービスまたはデーモンが停止しています。 ■ NetBackup PostgreSQL データベースサービスまたはデーモンが停止しています。	NetBackup Web 管理コンソール (nbwmc) と NetBackup PostgreSQL データベースサービスまたはデーモンを起動します。
11.	マルチパーソン認証チケットが、スケジュールされたパージ期間後もパージされません。	■ NetBackup Web 管理コンソール (nbwmc) サービスまたはデーモンが停止しています。 ■ NetBackup PostgreSQL データベースサービスまたはデーモンが停止しています。 ■ パージ期限に達した[期限切れ (Expired)]、[完了 (Done)]、[拒否済み (Rejected)]、[キャンセル (Canceled)]の状態のチケットがありません。	NetBackup Web 管理コンソール (nbwmc) と NetBackup PostgreSQL データベースサービスまたはデーモンを起動します。
12.	マルチパーソン認証を有効にした後、CLI を使用した NetBackup イメージの有効期限操作の実行が失敗しました。	プライマリサーバーでの操作に対してマルチパーソン認証が有効になっている場合、その操作は Web UI と API を使用した場合にのみ許可されます。 ユーザーが NetBackup 管理コンソールまたはコマンドラインインターフェースを使用して操作を実行しようとすると、操作が失敗します。	■ NetBackup Web UI を使用して操作を実行します。 ■ マルチパーソン認証プロセスからユーザーを除外するには、NetBackup セキュリティ管理者にお問い合わせください。
13.	マルチパーソン認証チケットを取得できません。	■ 指定したチケット ID が無効である可能性があります。 ■ NetBackup Postgres データベースサービスまたはデーモンが停止しています。	■ 有効なチケット ID を指定します。 ■ 必要なすべてのサービスが起動して実行中であ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.	マルチパーソン認証チケットの状態を更新できません。	マルチパーソン認証チケットは、チケットの現在の状態を提案された状態に変更できないため、更新できません。	マルチパーソンチケットの現在の状態を確認し、許可されている次の状態遷移に基づいて操作を実行していることを確認します。 現在の状態 - [保留中 (Pending)]、[期限切れ (Expired)] 提案された状態 - [承認済み (Approved)]、[拒否済み (Rejected)]、[キャンセル (Canceled)]、[保留中 (Pending)]
15.	マルチパーソン認証チケットを更新できません。	あなたがチケットの要求者またはマルチパーソン認証の承認者でない場合、チケットの承認、拒否、キャンセル、更新、またはコメントの追加はできません。	必要な権限については、NetBackup 管理者にお問い合わせください。
16.	マルチパーソン認証の構成中、またはチケットで関連する操作を実行しているときに、次のエラーが表示されます。 `Unable to connect to server`	NetBackup Web 管理コンソールサービスが停止している可能性があります。	すべての必要な NetBackup サービスが起動して実行中であることを確認します。
17.	マルチパーソン認証を有効にした後、CLI を使用したイメージの有効期限操作がエラーコード 9387 で失敗しました。	プライマリサーバーでの操作に対してマルチパーソン認証が有効になっている場合、操作の実行時にチケットが生成されます。	NetBackup Web UI にサインインして、マルチパーソン認証チケットの現在の状態を確認します。 操作が成功すると、チケットが承認されるはずです。
18.	ユーザーが、CLI を使用してマルチパーソン認証が有効な操作を実行できず、エラーコード 5930 のエラーが表示されます。	ユーザーが認証されていません。`bpnbat -login -logintype WEB` コマンドが実行されていません。	`bpnbat -login -logintype WEB` コマンドを実行して現在の権限セットを正常にロードし、CLI を使用してマルチパーソン認証が有効な操作を実行します。
19.	マルチパーソン認証を有効にした後、CLI を使用したイメージの有効期限操作でチケットが作成されません。	■ NBAC が有効になっています。 ■ ユーザーはマルチパーソン認証から除外されており、`bpnbat -login -lointypeWEB` を使用してログイン済みです。	■ NBAC が有効になっていないことを確認します。マルチパーソン認証は NBAC ではサポートされません。 ■ ユーザーが除外されていないことを確認します。除外されたユーザーが、マルチパーソン認証が有効な操作を実行しても、チケットは生成されません。

通し番号	問題	考えられる理由	解決方法
20.	マルチパーソン認証を有効にした後、bid ファイルを使用して CLI を介してイメージの有効期限操作を実行すると、エラーコード 20 で失敗します。	bid ファイルが必須形式になっていません。	bid ファイルが必須形式になっており、含まれるエントリが 100 個までであることを確認します。マルチパーソン認証が有効な場合、最大 100 個のイメージを一括で期限切れにできます。
21.	`nbcertcmd -setsecconfig`, `nbseccmd -setsecurityconfig` コマンドがメディアサーバーとクライアントで失敗します。 証明書配備レベルを設定する要求が失敗しました。 終了状態: 5969 エラー: `Response from the NetBackup Web Management Console service could not be parsed.`	メディアサーバーとクライアントホストが NetBackup 10.3 より前のバージョンです。	NetBackup を最新バージョンにアップグレードしてください。 Web UI での操作について、チケットが作成されているかどうかを確認します。
22.	マルチパーソン認証のチケットの詳細に、UNCHANGED または UPDATED の値がありません。	JSON API ペイロードを読み取ることができません。	API ペイロードのすべてのフィールドが、想定どおりに渡されているかどうかを確認します。
23.	グローバルセキュリティ設定が変更された後、除外されたユーザーに対してマルチパーソン認証のチケットが作成されます。	除外されるユーザーは、マルチパーソン認証構成、グローバルセキュリティ設定、またはリスクエンジンベースの異常検出構成を変更する場合、マルチパーソン認証を通過する必要があります。	チケットの承認については、MPA 承認者にお問い合わせください。
24.	競合があっても、イメージの有効期限操作のチケットに、競合していることを示すマークが付きません。	マルチパーソン認証構成およびグローバルセキュリティ設定の操作では、保留状態のチケットに、競合していることを示すマークは付きません。	イメージの有効期限設定、WORM 構成の変更、WORM 保持ロックの削除、およびイメージ保留の削除の操作についてのチケットには、競合していることを示すマークは付きません。

NetBackup Scale-Out Relational Database への接続に関するトラブルシューティング

使用するアカウントや NetBackup データベースに接続の問題がある場合は、pgbouncer の `userlist.txt` ファイルにあるアカウントとパスワードの情報が NetBackup データ

ベースと同期できていない可能性があります。この状況を解決するには、nbdb_admin -update-user-list コマンドを使用して、ファイルとデータベースの情報を同期します。

userlist.txt ファイルを NetBackup データベースと同期するには

1 次のコマンドを実行します。

UNIX の場合:

```
/usr/openv/db/bin/nbdb_admin -update_user_list
```

Windows の場合:

```
install_path¥NetBackup¥bin¥nbdb_admin -update_user_list
```

2 接続の問題が引き続き表示される場合は、NetBackup サービスを再起動します。

秘密鍵の暗号化に関する問題のトラブルシューティング

このトピックでは、秘密鍵の暗号化に固有の問題のトラブルシューティング方法について説明します。

パスフレーズは、NetBackup のホスト ID ベース証明書の秘密鍵を暗号化および復号するために使用されます。パスフレーズキーは、これらのパスフレーズを暗号化および復号するために使用されます。

NetBackup 証明書の秘密鍵は、AES_256_CBC 暗号化を使用した暗号化形式で格納されます。秘密鍵の暗号化に使用されるパスワードは、ファイルストレージに格納され、AES_256_GCM 暗号化を使用して暗号化されます。

秘密鍵の暗号化ファイルのパス

キーストアの場所:

Windows の場合: *Install path*¥NetBackup¥var¥vxss¥credentials¥keystore

Linux の場合: /usr/openv/var/vxss/credentials/keystore

クラスタのキーストアの場所:

/usr/openv/var/global/vxss/credentials/keystore

Nbcert ログ:

Windows の場合: *Install path*¥NetBackup¥logs¥nbcert

Linux の場合: /usr/openv/netbackup/logs/nbcert

パスフレーズファイルのパス: keystorepath + .yekekp

パスフレーズキーファイルのパス: keystorepath + .yekcneekp

certmapinfo.json ファイルのパス:

Windows の場合: `Install path¥NetBackup¥var¥vxss¥certmapinfo.json`

Linux の場合: `/usr/openv/var/vxss/certmapinfo.json`

表 2-21

通し番号	問題	考えられる理由	解決方法

1	コマンド: `nbcertcmd -listcertdetails`
	
	`Output:`
	`Private Key Encryption State:`
	
	`Encrypted with an unknown passphrase`
		秘密鍵ファイルが改ざんされています。	**1** サーバーの秘密鍵ファイルをクリーンアップします。
			2 ホストに関連付けられているすべてのサーバーで次のコマンドを実行します。
			■ `nbcertcmd -getCertificate -token reissue_token -server server host name -force`

2	以下の問題のシナリオについては、理由と解決策は同じです。
	
	コマンド: `nbcertcmd -listcertdetails`
	
	出力:
	
	`Private Key Encryption State: Encrypted with an unknown passphrase`
	
	コマンド: `nbcertcmd -rotatePassphrasekey`
	
	`The passphrase key rotation failed. EXIT STATUS 1200: Internal error`
		パスフレーズファイルまたはパスフレーズキーファイルが改ざんされています。	**1** パスフレーズファイルの最終更新日を確認します。
			2 キーストアフォルダ (隠しファイルを含む) をクリーンアップします。
			3 ホストに関連付けられているすべてのサーバーで次のコマンドを実行します。
			■ `nbcertcmd -getCertificate -token reissue_token -server server host name -force`

通し番号	問題	考えられる理由	解決方法

3	NetBackup の新規インストール後にカタログのリストアを実行するときに、新規インストールで新しく作成された秘密鍵とリストアされた秘密鍵の両方が表示されます。
	コマンド:
	`ls -la`
	`total 20 drwx------ 2 nbsvcusr nbsvcusr 171 Jun 19 19:38`
	`drwx------ 3 nbsvcusr nbsvcusr 133 Jun 19 19:25 ..`
	`-rw------- 1 nbsvcusr nbsvcusr 1858 Jun 19 19:38`
	`015b91f5-74b5-44fb-865f-6d65827cdb30-key.pem`
	`-rw------- 1 nbsvcusr nbsvcusr 1858 Jun 19 19:38`
	`015b91f5-74b5-44fb-865f-6d65827cdb3r-key.pem`
		カタログをリストアすると、既存の秘密鍵とパスフレーズファイルがキーストアに再統合されます。その結果、キーストアには、新規インストールで新たに作成された秘密鍵とリストアされた秘密鍵の両方が含まれます。	■ `certmapinfo.json` ファイルにエントリがない秘密鍵ファイルを消去します。
			UNIX 上の `certmapinfo.json` ファイルの場所:
			`/usr/openv/var/vxss/certmapinfo.json`

4	NetBackup Web UI に次の通知が表示されます。 `Reissuing the host certificates during private key encryption failed for the following hosts: host1`	秘密鍵の暗号化操作中に証明書の再発行が試行されます。	■ 次のコマンドを実行します。 `nbcert -listCertDetails -json` 以降のサービスの再起動ではすべての秘密鍵が暗号化され、このコマンドの出力には [暗号化済み (Encrypted)] 状態のすべてのキーが表示されます。 暗号化されていないキーがある場合は、[暗号化済み (Encrypted)] 以外の状態の秘密鍵に対して、次のいずれかのコマンドを実行します。 ■ `nbcertcmd -reissuecertificates -server server` ■ `nbcertcmd -getCertificate -token reissue_token -server server host name -force`

通し番号	問題	考えられる理由	解決方法
5		バックアップファイルが存在しないか、ファイルの書き換え処理に問題があるため、リストア操作が失敗しました。	■ 同じキーストアフォルダにバックアップファイル (接尾辞「_bkup」が付いているファイル) があるかどうかを確認します。 ■ 次のように実行します。 ■ 次を使用して状態を確認します nbcertcmd -listcertdetails ■ すべてのプライマリサーバーで秘密鍵の暗号化状態が[暗号化 (Encrypted)]と表示されている場合は、バックアップファイルを手動でクリーンアップし、ローテーション操作を再試行します。 ■ 問題が解決しない場合は、次を確認します。 ■ プライマリサーバーの一部が秘密鍵を示し、暗号化の状態が[不明なパスフレーズで暗号化されています (encrypted with unknown passphrase)]である場合、パスフレーズファイルと対応する秘密鍵ファイルをリストアします。 ■ 再度、次のコマンドを使用して状態を確認します。 nbcertcmd -listcertdetails。残りの秘密鍵に対して、正しい暗号化の状態が表示されるかどうかを確認します。表示される場合は、ローテーション操作を再試行します。 ■ 問題が解決しない場合は、次を確認します。 ■ バックアップファイルが存在せず、コマンドが nbcertcmd -listcertdetails 正しくない暗号化状態を示す場合、キーストアをクリーンアップします。 ■ すべてのサーバーに対して nbcertcmd -getCertificate reissueToken オプションを指定して実行します。

通し番号	問題	考えられる理由	解決方法
	パスフレーズのローテーションの試行が失敗し、秘密鍵ファイルとパスフレーズファイルをリストアできませんでした。 コマンド: [root@example keystore] nbcertcmd -rotatepassphrase この操作は、ホスト ID ベース証明書の秘密鍵を暗号化するパスフレーズのローテーションを実行します。 この操作を実行する前に、NetBackup サービスを停止することを強くお勧めします。サービスの再起動は、操作の実行後に行ってください。 この操作を続行しますか? (y/n) (Are you sure you want to proceed with this operation? (y/n)) y The passphrase rotation failed. EXIT STATUS 9141: Keystore is in inconsistent state. Command: ls -la total 20 drwx------ 2 nbsvcusr nbsvcusr 176 Jul 16 11:55 . drwx------ 3 nbsvcusr nbsvcusr 133 Jul 4 22:24 .. -rw------- 1 nbsvcusr nbsvcusr 1858 Jul 16 11:51 5176ec69-d3cb-44d7-a229- 799555b7bd7e-key.pem -rw------- 1 nbsvcusr nbsvcusr 1858 Jul 16 11:54 5176ec69-d3cb-44d7-a229- 799555b7bd7e-key.pem_bkup -rw------- 1 nbsvcusr nbsvcusr 1858 Jul 16 11:51 PrivKeyFile-2048.pem		

通し番号	問題	考えられる理由	解決方法
	-rw-r--r-- 1 nbsvcusr nbsvcusr 1072 Jul 16 11:51 .yekcneekp -rw-r--r-- 1 nbsvcusr nbsvcusr 271 Jul 16 11:52 .yekekp		

セキュリティ構成リスク機能に関する問題のトラブルシューティング

セキュリティ構成リスクは、NetBackupドメインのセキュリティ設定の状態によって異なります。構成リスクのスコアが高いほど、セキュリティ構成が弱いことを示します。リスクを最小限にするには、すべてのセキュリティ設定を有効にします。

セキュリティ構成リスク機能について詳しくは、『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。

表 2-22

通し番号	問題	考えられる理由	解決方法
1.	次の場所での内部サーバーエラー: `GET API /security/status`	NBSL (NetBackup Service Layer) を介して、指定したホストのクラスタ名またはクライアント名を抽出中にエラーが発生しました。 ログを調べて、次を確認します。 「Cannot retrieve hostName from system property」	NBSL サービスが起動して実行されているかどうかを確認します。 指定したプライマリサーバーにクライアント名 (クラスタの場合は仮想名) が正しく設定されていることを確認します。
		データベースでホスト名によって指定されたホストを検索する場合の例外。 ログを調べて、次を確認します。 "Exception occurred: hostname not found."	NetBackup のデータベースサービスが起動して実行されていることを確認します。詳細度を高めて、操作を再試行します。 Cohesityテクニカルサポートにお問い合わせください。
		データベースからの基本状態テンプレートの読み取りエラー。 ログを調べて、次を確認します。 "Caught exception while reading security template json."	正しい JSON ファイルが EMM_MAIN スキーマ内のデータベースに存在することを確認します。 `emm_hostconffileversiondata` NULL 値を持つキーがないようにします。
		サービスユーザーで構成されたホストの数をデータベースから抽出中にエラーが発生しました。 ログを確認してください。	NetBackup のデータベースサービスが起動して実行されていることを確認します。 詳細度を高めて、操作を再試行します。 Cohesityテクニカルサポートにお問い合わせください。
		API は、ホストのマルウェア構成の詳細の抽出に失敗しました。 ログを調べて、次を確認します。 "Exception raised from getting malware settings"	詳細度を高めて、操作を再試行します。 Cohesityテクニカルサポートにお問い合わせください。
			NetBackup のデータベースサービスが起動して実行されていることを確認します。 詳細度を高めて、操作を再試行します。Cohesityテクニカルサポートにお問い合わせください。

通し番号	問題	考えられる理由	解決方法
		API でデータベースからホスト数の抽出に失敗しました。 ログを調べて、次を確認します。 "Cannot retrieve number of hosts from database."	
		API は MPA のサポート対象操作の抽出に失敗しました。 ログを調べて、次を確認します。 "Error in fetching list of MPA supported operations."	NetBackup のデータベースサービスが起動して実行されていることを確認します。 詳細度を高めて、操作を再試行します。Cohesity テクニカルサポートにお問い合わせください。
8.	POST API /security/configuration-baseline の内部サーバーエラー	要求 DTO の検証に失敗しました。 ログを調べて、次を確認します。 "Request DTO validation failed."	API への入力 JSON を検証します。次を参照して、設定の可能な状態を確認してください。 ■ "allowInsecureBackLevelHost": 0/1 ■ "certificateAutoDeployLevel": 0/1/2 ■ "mfaEnforced": false/true ■ "dteGlobalMode": 'PREFERRED_OFF'/'PREFERRED_ON'/'ENFORCED' ■ "backupAnomalyDetection": "0/1" ■ "mpa" : "ENABLED"/"DISABLED" ■ "hostPercentageWithServiceUser": "<Precentage value 0 to 100>" ■ "hostPercentageWithDteEnabled": "<Precentage value 0 to 100>" ■ "malwareDetection": "NOT_CONFIGURED"/"CONFIGURED"
9.	セキュリティ構成リスクについての通知が生成されません。	セキュリティベースラインが、構成設定の変更から 10 秒以内に変更された可能性があります。	セキュリティ設定の状態を変更してから 10 秒以内にセキュリティベースラインを変更しないでください。 操作を再試行します。この問題が引き続き解決しない場合は、ベリタステクニカルサポートにお問い合わせください。Web サービスのログと NetBackup 監査ログを収集します。

通し番号	問題	考えられる理由	解決方法
10.	[ダッシュボードセキュリティ状態の要求または送信されるデータが無効です。(The dashboard security status request or the data that is sent is not valid.)]のメッセージが表示されて例外が発生します。	考えられる理由: ■ GET/セキュリティ/状態の API がレコード EMM_MAIN を参照しています。 VersionID が最も高い値を持つ EMM_HostConfFileVersionData。このレコードに、フィールドファイルの内容の一部として正しくない JSON が含まれている可能性があります。	セキュリティベースラインを再び設定します。
		NetBackup データベースサービスが実行されていません。	NetBackup のデータベースサービスが起動して実行されていることを確認します。
		異常管理サービスが実行されていません。	異常管理サービスが起動し、実行中であることを確認します。
		nbstserv が実行されていません。	nbstserv が起動し、実行中であることを確認します。
		NetBackup Service Layer サービスが実行されていません。ファイルには service_user 権限が必要です。	NBSL (NetBackup Service Layer) が起動し、実行中であることを確認します。
		要求 DTO の検証に失敗しました。提供されたペイロードに、(API バージョン 13.0 からの) サポートされていない属性のいずれかがあったか、無効な値がありました。	要求 API バージョン 12.0 の POST security/configuration-baseline API への入力 JSON を検証します。 次のペイロード JSON がサポートされます。 { "data": { "type": "securityTemplateRequest", "attributes": { "securitySettingsTemplate": { "allowInsecureBackLevelHost": 0, "certificateAutoDeployLevel": 0, "mfaEnforced": false, "dteGlobalMode": "PREFERRED_OFF", "hostPercentageWithDteEnabled": 0, "backupAnomalyDetection": 0, "mpa": "ENABLED", "malwareDetection": "CONFIGURED", "hostPercentageWithServiceUser": 0 } } } }
		要求 DTO の検証に失敗しました。ペイロードに無効な値を持つ属性が含まれていました。	

通し番号	問題	考えられる理由	解決方法
			要求 API バージョン 13.0 の POST セキュリティ/構成ベースライン API への入力 JSON を検証します。 次の JSON がサポートされます。 { "data": { "type": "securityTemplateRequest", "attributes": { "securitySettingsTemplate": { "allowInsecureBackLevelHost": 0, "certificateAutoDeployLevel": 0, "mfaEnforced": false, "dteGlobalMode": "PREFERRED_OFF", "hostPercentageWithDteEnabled": 0, "backupAnomalyDetection": 0, "mpa": "ENABLED", "malwareDetection": "CONFIGURED", "hostPercentageWithServiceUser": 0, "backupStoragePercentageWithEncryptionEnabled": 0, "isImmutableBackupStorageConfigured": true, "serverPercentageWithLatestNbuVersion": 0, "clientPercentageWithLatestNbuVersion": 0, "isCliAccessToOsAdmins": 0, "isWebUiAccessToOsAdmins": 0, "redirectedRestore": true } } } }
11.	アップグレード後に、一部の設定にベースライン値がありません	NetBackup 11.0 で追加された新しいセキュリティ設定の一部では、明示的に設定しないかぎり、ベースラインが設定されません。	すべてのセキュリティ設定のベースライン値を設定します。

リスクエンジンベースの異常検出オプションに関する問題のトラブルシューティング

NetBackupリスクエンジンは、特定のシステム異常を予防的に検出し、適切なアラートを送信します。環境でセキュリティ上の脅威に直面する前に訂正処理を実行するのに役立ちます。

リスクエンジ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。

表 2-23

通し番号	問題	考えられる理由	解決方法
1.	NetBackup 管理コンソールのログインが次のエラーで失敗します。 `Unable to login, status: 501. You are not authorized to use this application.`	リスクエンジンベースの異常検出の[異常なユーザーサインインの検出 (Detect unusual user sign in)]オプションが有効で、異常に対してマルチパーソン認証チケットのオプションが有効になっています。ユーザーサインインに異常があるため、保留になります。	次のいずれかを実行します。 ■ 異常検出チェックをバイパスするために、マルチパーソン認証の除外ユーザーのリストにユーザーを追加する必要があります。 ■ ユーザーは通常の時間帯にサインインする必要があります。 ■ 異常なサインインに対するマルチパーソン認証チケットの生成を無効にします。
2.	`bpnbat -login` は次のエラーで失敗します。 `You do not have permission to perform the requested operation. AT authentication successful, but web authentication failed.`	リスクエンジンベースの異常検出の[異常なユーザーサインインの検出 (Detect unusual user sign in)]オプションが有効になっています。ユーザーサインイン要求が、以前のバージョンのクライアントからの要求です。	次のいずれかを実行します。 ■ 異常検出チェックをバイパスするために、マルチパーソン認証の除外ユーザーのリストにユーザーを追加する必要があります。 ■ 最新の NetBackup バージョン (11.0) のホストで、`bpnbat -login` コマンドを実行します。
3.	`nbseccmd -setuptrustedmaster` は次のエラーで失敗します。 `The trust setup operation using NetBackup certificate failed. Trusted master operation failed EXIT STATUS 160: Authentication failed [root@exampleserver ~]#`	リスクエンジンベースの異常検出の[異常なユーザーサインインの検出 (Detect unusual user sign in)]オプションが有効になっています。ユーザーサインイン要求が、以前のバージョンのクライアントからの要求です。	次のいずれかを実行します。 ■ 異常検出チェックをバイパスするために、マルチパーソン認証の除外ユーザーのリストにユーザーを追加する必要があります。 ■ 最新の NetBackup バージョン (11.0) のホストで、`nbseccmd -setuptrustedmaster` コマンドを実行します。

通し番号	問題	考えられる理由	解決方法
4.	MPA の制限により、どのユーザーもログインできません。	リスクエンジンベースの異常検出の[異常なユーザーサインインの検出 (Detect unusual user sign in)]オプションが有効になっています。	次のコマンドを実行します。 `nbseccmd -disableLoginAnomalyDetection`
5.	ユーザーはコマンドラインインターフェースからポリシーの更新または削除操作を実行できません。	リスクエンジンベースの異常検出の[ポリシーへの異常な更新の検出 (Detect unusual updates to policies)]オプションが有効になっています。	最新の NetBackup バージョン (11.0) のホストから、nbcmdrun ラッパーコマンドを使用してポリシーを更新または削除します。 例: `nbcmdrun bppldelete P1`

3

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
- ログ収集ユーティリティについて
- 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
- ジョブ ID ごとのログ収集について

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	これらのユーティリティにより、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.219 の「NetBackup デバッグログの分析ユーティリティについて」を参照してください。
ログ収集ユーティリティ	このユーティリティは、サポートで使用するための証拠の収集を簡略化します。 詳しくは、次を参照してください。 ■ p.223 の「ログ収集ユーティリティについて」を参照してください。 ■ NetBackup ログリファレンスガイド ■ ログアシスタント FAQ:
ネットワークトラブルシューティングユーティリティ	これらのユーティリティは、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さまざまな側面を検証します。 p.223 の「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」を参照してください。
NetBackup サポートユーティリティ (nbsu)	このユーティリティは、ホストに問い合わせて、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.224 の「NetBackup サポートユーティリティ (nbsu) について」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)	このユーティリティは、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.229 の「NetBackup の一貫性チェックユーティリティ (NBCC) について」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	このユーティリティは、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.238 の「NetBackup の一貫性チェックの修復 (NBCCR) ユーティリティについて」を参照してください。
nbcplogs ユーティリティ	このユーティリティは、Cohesity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。 p.240 の「nbcplogs ユーティリティについて」を参照してください。

ユーティリティ	説明
ロボットテストユーティリティ	これらのユーティリティは、ロボット周辺機器を使用して直接通信します。 p.241 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。

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	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。 少なくとも、プライマリサーバー上の admin およびメディアサーバー上の bptm と 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、ログ記録レベルを 5 に設定し、前述のプロセスに加えて、プライマリサーバー上の bpdbm およびすべてのサーバー上の bpcd のデバッグログを有効にします。 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。
backuptrace	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。 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 NetBackup 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 sort や grep の実行が比較的容易な形式で生成されます。 backuptrace ユーティリティを使用するには、プライマリサーバー上の 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、ログ記録レベルを 5 に設定します。前述のプロセスに加えて、プライマリサーバー上の 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。 backuptrace 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。
bpgetdebuglog	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 NetBackup サーバープラットフォームで利用できます。 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。 bpgetdebuglog 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。

ユーティリティ	説明
duplicatetrace	指定した NetBackup 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。 少なくとも、プライマリサーバー上の 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、ログ記録レベルを 5 に設定し、前述のプロセスに加えて、プライマリサーバー上の 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。 duplicatetrace 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。
importtrace	指定した NetBackup 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。 少なくとも、プライマリサーバー上の 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、ログ記録レベルを 5 に設定し、前述のプロセスに加えて、プライマリサーバー上の 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。 importtrace 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。
restoretrace	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。 restoretrace ユーティリティを実行すると、指定した NetBackup 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 sort や grep の実行が比較的容易な形式で生成されます。 少なくとも、プライマリサーバー上の 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、ログ記録レベルを 5 に設定し、プライマリサーバー上の 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。 restoretrace 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。

ユーティリティ	説明
verifytrace	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。 少なくとも、プライマリサーバー上の 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、ログ記録レベルを 5 に設定し、前述のプロセスに加えて、プライマリサーバー上の 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。 verifytrace 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。

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/openv/netbackup/logs/*<PROGRAM_NAME>*/log.mmddyy

  Windows の場合　*install_path*¥NetBackup¥Logs¥*<PROGRAM_NAME>*¥mmddyy.log

  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

daystamp　*yyyymmdd* 形式のログの日付。

millisecs　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。

program	ログが記録されるプログラム名 (BPCD、BPRD など)。
sequence	デバッグログファイル内の行番号。
machine	NetBackup サーバーまたはクライアントの名前。
log_line	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。

ログ収集ユーティリティについて

NetBackup の問題を解決するために、ログ収集ユーティリティを使用してテクニカルサポートで使用する証拠を収集できます。このユーティリティは、[ヘルプ (Help)]メニューおよびアクティビティモニターから使用できます。デバッグログは、テクニカルサポートが分析するためのものです。

ログ収集ユーティリティについて詳しくは、『NetBackup ログリファレンスガイド』を参照してください。

ログアシスタントについて詳しくは、ログアシスタントの FAQ の記事を参照してください。

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	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。 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。
bptestnetconn	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。 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。
nbdna (NetBackup Domain Network Analyzer)	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。 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トポロジ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。 nbdna 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 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/openv/netbackup/bin/support/nbsu

Windows の場合　*install_path*¥NetBackup¥bin¥support¥nbsu.exe

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。Cohesity 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 Cohesity 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 を定期的に実行し、ベースラインデータを最新の状態に保持します。
- 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てる場合。
- 問題を Cohesity 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、Cohesity 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 Cohesity 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 エラーメッセージを標準出力 (STDOUT) に出力する方法	次のように入力します。 ■ Windows の場合 *install_path*¥NetBackup¥bin¥support¥nbsu.exe 2>&1 ■ UNIX の場合 /usr/openv/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 によっ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_mmddyyyy_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/openv/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/openv/netbackup/bin
Client OS/Release = Linux 3.10.0-229.el7.x86_64

Exit status: 0

#######Command used: /usr/openv/netbackup/bin/admincmd/bpgetconfig#######
SERVER = sivbl17.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/openv/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。primary は、このホストが NetBackup プライマリ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います。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
- Cohesity 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

NBCC は次の場所に存在します。

UNIX の場合　`/usr/openv/netbackup/bin/support/NBCC`

Windows の場合　*install_path*¥NetBackup¥bin¥support¥NBCC.exe

次の状況で Cohesity 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
- Cohesity 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

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 プライマリ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.231 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/openv/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/openv/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>&1
```

```
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
             falconstorvtl5
2.5  Building NetBackup storage unit list...
     Detected Storage Unit for NetBackup for NDMP media server
         reabl3
       and NDMP Host
         falconstorvtl5
       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 bpdbjobs 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
         mlbnbu ...
       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-bpdbjobs-most_columns

07/07/2011  09:43 AM         2,211,811 nbcc-bpimagelist-l
...

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:
 +
+ nbemmcmd vmoprcmd
 +
+ EMM Server = yes
 +
+ EMM NetBackup version = 8.1
 +
+ NBCC NetBackup version = 8.1
 +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++


       Summary of NBCC Master server processing
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname:
 +
+ lidabl11
 +
+ Alias hostnames:
 +
+ lidabl11
 +
+ Sources:
 +
+ nbemmcmd bpstulist nbdevquery bpgetconfig
 +
+ Master server = yes
 +
+ EMM NetBackup version = 8.1.0.0
```

```
 +
+ NBCC NetBackup version = 8.1
 +
+ Tape STU detected = no - Disk STU detected = yes
 +
+ Disk Pool Host = yes
 +
+ Associated Storage servers:
 +
+ lidabl11 lidaclvm1
 +
+ EMM tape media record extract attempted = yes
 +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++


       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。Cohesityのテクニカルサポートは NBCC 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、Cohesity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、関連付けさ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/openv/netbackup/bin/support/NBCCR

Windows の場合　*install_path*¥NetBackup¥bin¥support¥NBCCR.exe

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 *primaryname*_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/openv/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/openv/netbackup/bin/support/output/nbccr/*primaryname*_nbccr_*timestamp*

Windows の場合:
install_path¥NetBackup¥bin¥support¥output¥nbccr¥*primaryname*_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 つも見つけられませんでした。

- 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。Cohesity 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、クラスタとパ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 Cohesity 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/openv/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/openv/volmgr/bin/acstest -r *ACSLS_hostpath* UNIX および Linux の場合、acstest を実行するには acssel と acsssi が実行されている必要があります。
TLD	/usr/openv/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 プライマリサーバー、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_MemeoryPerf_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	次の項目について確認します。 ■ 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。 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。 ■ Windows ■ RHEL ■ SUSE **メモ:** 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。 ■ 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。 ■ gcore ■ gstack ■ iostat ■ mpstat ■ netstat ■ pmap ■ top ■ vmstat 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。 http://www.veritas.com/docs/DOC5332

手順 2	プライマリサーバー、メディアサーバー、またはクライアントに nbsmartdiag `nbsmartdiag -install`をインストールします。
	`nbsmartdiag demo $ /usr/openv/netbackup/bin/nbsmartdiag -install.`
	`Performing the install operation.`
	`Performed the install operation successfully.`

手順	説明
手順 3	nbsmartdiag サービスを開始します。nbsmartdiag -start Windows では、nbsamartdiag 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。 Nbsmartdiag demo $ /usr/openv/netbackup/bin/nbsmartdiag -start Performing the start operation. Info:Daemon is running. Performed the start operation successfully.
手順 4	bp.conf の NBSD_EVIDENCE_PATH 値で指定された場所にある nbsmartdiag フォルダから証拠を収集します。 ■ 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。 ■ 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。 bp.configuration 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。 http://www.veritas.com/docs/DOC5332
手順 5	証拠の収集が完了したら、nbsmartdiag サービスを停止します。次のコマンドを実行します。nbsmartdiag -terminate

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。

ジョブ ID ごとのログ収集について

NetBackup には、ジョブ ID を指定して関連ログを収集し、収集されたログをアップロードするコマンドラインインターフェースと API オプションが含まれます。指定したジョブ ID を使用して、ジョブの実行時間枠内のログが、到達可能な場合はプライマリサーバー、メディアサーバー、クライアントから収集されます。

レガシーログと試行ファイルログは期間フィルタに基づかないため、これらのログには、ジョブの実行時間枠以外のログが含まれる場合があります。階層のジョブ ID を指定すると、ジョブ階層に関係するすべてのホストのログが収集されます。Cohesityでは、ジョブの期間に含まれるすべてのホストでのログ収集に、時間同期を使うことをお勧めします。有

効なジョブ ID がアクティビティモニターに存在する必要があります。デフォルトでは、ジョブ ID はジョブが完了してから 1 週間後に削除されます。指定されたジョブ ID のジョブ詳細を bpdbjobs またはアクティビティモニターが取得できない場合、nblogadm ユーティリティはジョブ ID のログを収集できません。さらに、ログ収集のコマンドラインインターフェースと API オプションでは、[今すぐバックアップ (Backup Now)]ジョブがサポートされません。VxUL ログは、旧バージョンのメディアサーバーまたはクライアントからは収集されません。

収集されるログには、NetBackup 製品と NetBackup のサポートユーティリティ (nbsu) のログが含まれます。ログ収集では、一度に 1 つのレコード ID がサポートされ、複数のレコード ID からの同時ログ収集はサポートされません。

ログの収集中にプライマリサーバー、メディアサーバー、クライアントのファイルシステムがいっぱいにならないようにするために、Cohesityでは KEEP_LOGS_SIZE_GB オプションを使用することをお勧めします。Cohesityでは、保持する NetBackup ログのサイズを、ログ収集の前に指定することをお勧めします。詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

NetBackup 10.2 で、時間ベースのログクリーンアッププロセスが導入されました。ログが収集の 7 日後に削除されない場合、このプロセスによって、それらの収集されたログとログレコードが削除されます。プライマリサーバーまたはメディアサーバーでログの保持期間を短縮して 5 日間に設定するには、LOG_RECORD_EXPIRY_DAYS を、bpsetconfig で 5 に設定します。クライアントでログの保持期間を短縮して 5 日間に設定するには、LOG_RECORD_EXPIRY_DAYS を、nbsetconfig で 5 に設定します。小さい数が優先されます。NetBackup では、ログのクリーンアップ処理中にエラーが発生した場合、旧バージョンのメディアサーバーまたはクライアントからログが削除されないことがあります。Cohesityでは、この状況が発生した場合は、残っているログを手動で削除することをお勧めします。

プライマリサーバーのファイルシステムが収集されたログでいっぱいになるのを避けるために、10 GB の事前定義済み空き領域ウォーターマークが使用されます。NetBackup は、利用可能なディスク容量がウォーターマークと収集ログの推定サイズの合計より少ない場合に、このウォーターマークを使用してログ収集の開始を確認して抑制します。さらに、プライマリサーバーの利用可能な領域がウォーターマークと収集ログの推定サイズの合計より少なくなった場合、ログ収集プロセスが停止されます。このリリースでは、利用可能な領域の確認がメディアサーバーとクライアントに拡張されています。空き領域のウォーターマークを 5 GB に減らすには、bpsetconfig コマンドで HIGH_WATERMARK_TRB_LOG_RECORDS = 5 と設定します。

より詳細なログを収集する方法として、次の 2 つのオプションがあります。ログ記録を手動で有効にし、『NetBackup ログリファレンスガイド』に記載されているとおりに必要なログレベルを構成できます。または、コマンドラインインターフェースと API オプションを使用して、プライマリサーバー、メディアサーバー、またはクライアントの収集するログレベルの値を構成することもできます。次に、ジョブを再起動し、ログ収集タスクを開始します。この

機能には、最初に指定したジョブが再開された後、新しいジョブのジョブ ID を取得する API オプションが含まれています。

より詳細なログを収集するには、2 つのログレコード ID が必要です。最初のログレコード ID (レコード ID 1) は、あるジョブ ID (ジョブ ID 1) のホストに対してログ記録を有効にし、目的のログレベルを構成するために使用されます。ログレベルを構成し、元のジョブ (ジョブ ID 1) が再起動されると、新しいジョブ ID (ジョブ ID 2) が生成されます。2 番目のログレコード ID (レコード ID 2) は、再起動された新しいジョブ (ジョブ ID 2) の実行時間枠内で、到達可能な場合はプライマリサーバー、メディアサーバー、クライアントからログを収集するために使用されます。複数のメディアサーバーとクライアントが含まれるバックアップドメインでは、レコード ID 1 とレコード ID 2 のメディアサーバーまたはクライアントが、ジョブスケジュールアルゴリズムが原因で同一でない場合があります。

NetBackup 10.2 以降では、収集された各ログの SHA256 チェックサムが、次に示すディレクトリの `Progress.txt` ファイルに含まれています。旧バージョンの NetBackup がインストールされているメディアサーバーまたはクライアントでは、チェックサムの計算が失敗します。

`Progress.txt` ファイルの場所:

- Linux および UNIX

  `/usr/openv/netbackup/logs/nblastaging/record ID-timestamp: YYYYMMDD-HHMMSS`

- Windows

  install_path`¥Veritas¥NetBackup¥logs¥nblastaging¥record ID-timestamp: YYYYMMDD-HHMMSS`

NetBackup 10.2 以降には、プライマリサーバーの必要なログストレージ領域に対する領域使用率の拡張が含まれています。プライマリサーバー、メディアサーバー、クライアントから収集されたログファイルは、プライマリサーバーに格納されなくなります。ホストごとに、次のディレクトリにファイルが格納されます。

- Linux および UNIX

  `/usr/openv/netbackup/logs/nblaevidence/nbla-`*hash*

- Windows

  install_path`¥Veritas¥NetBackup¥logs¥nblaevidence¥nbla-`*hash*

サポート対象のジョブの種類:

- バックアップ
- スナップショットからのバックアップ
- スナップショット

サポート対象のワークロードの種類:

- ファイルシステム

- Hadoop (ログはプライマリサーバーとメディアサーバーからのみ収集されます)
- Microsoft Exchange (ログはプライマリサーバーとメディアサーバーからのみ収集されます)
- Windows Server フェールオーバークラスタ (WSFC)
- Microsoft SQL Server 可用性グループ
- NDMP (ログはプライマリサーバーとメディアサーバーからのみ収集されます)
- Oracle
- Snapshot Manager (ログはプライマリサーバーとメディアサーバーからのみ収集されます)
- VMware

プライマリサーバーで `disableIPResolution` オプションを設定するときに、VMware 作業負荷の種類のジョブ ID を指定した場合、保護対象の仮想マシンのログは収集されません。設定について詳しくは、https://www.veritas.com/content/support/en_US/doc/21902280-158271263-0/v38310204-158271263 を参照してください。

このリリースでは、複数のクライアントを使用した分散作業負荷からのログの収集がサポートされています。分散作業負荷の例として、Oracle RAC や MSSQL 可用性グループがあります。

収集されたログは、コマンドラインインターフェースと API オプションのほか、有効なサポートケース ID を使用して Cohesity テクニカルサポートにアップロードできます。詳しくは、https://www.veritas.com/support/ja_JP/article.100038665 を参照してください。

ログをアップロードするために API に指定されるパスワードは、NetBackup の [クレデンシャルの管理 (Credential management)] ペインにクレデンシャルオブジェクトとして格納されます。これは、ログがアップロードされた後に削除されます。

収集されたログで構成される 1 つの tar ファイルが、Cohesity テクニカルサポートチームの SFTP サーバーまたは指定した SFTP サーバーにアップロードされます。Cohesity テクニカルサポートチームが SFTP サーバーを管理していない場合、SFTP サーバーに同じ名前の `tar` ファイルが存在する場合、アップロード操作は失敗します。

`nblogadm` ログを使用して、ジョブ ID ごとのログ収集のデバッグまたはトラブルシューティングを行います。コマンドラインインターフェースと API オプションの両方に `nblogadm` ログを使用します。`nblogadm` プロセスからログを収集するには、次に示すディレクトリが存在することを確認します。

- Linux および UNIX

  `/usr/openv/netbackup/logs/nblogadm`

- Windows

  `install_path``¥Veritas¥NetBackup¥logs¥nblogadm`

表 3-6 nblogadm ユーティリティに導入された新しいコマンドラインインターフェースフラグ

コマンドラインインターフェース	説明
nblogadm --action getactivecollections --json	進行中のレコードの数を取得します。(一度に複数のレコード ID のログは収集されません)
nblogadm --action createrecord --jobid *job ID* --json	ジョブ ID を取得し、空のログレコードを作成し、作成したレコード ID を返します。
nblogadm --action collectlogsforjob --recid *record ID* --runnbsu --json	指定したレコード ID のログを収集するタスクを作成します。
nblogadm --action startupload --recid *record ID* --sftp_host *sftp host* --sftp_port *sftp port* --supportcase *support case ID* --target_folder *sftp host folder* --fingerprint *sftp host fingerprint, use comma as delimiter without spaces* --passcredentials --json	指定したレコード ID のログと SFTP サーバーアクセス情報をアップロードするタスクを作成します。
nblogadm --action deleterecord --recid *record ID* --json	指定したレコード ID の収集されたログとレコードを削除します。この処理によって、進行中のタスクも終了します。
nblogadm --action casedetail --recid *record ID* --json	指定したレコード ID のログ収集とログアップロードタスクの詳細を取得します。
nblogadm --action getlogging --recid *record ID* --json	指定したレコード ID のホスト、そのコンポーネント、対応するログレベル値のリストを取得します。
nblogadm --action getlogging --recid *record ID* [--hostandlog MASTER|MEDIA|CLIENT:*hostname*] --json	--hostandlog パラメータを使用する場合、このコマンドは指定したレコード ID の指定したホストに対するコンポーネントのログレベル値を返します。--hostandlog パラメータを使用しない場合、このコマンドは指定したレコード ID の複数ホストのリストに対するコンポーネントのログレベル値を返します。

コマンドラインインターフェース	説明
nblogadm --action setlogging --recid *record ID* --hostandlog MASTER|MEDIA|CLIENT:*hostname*@*legacy component1=legacy component1 level*,*vxul component1=debug level*%*diagnostic level*,*misc type=misc type value* --json	指定したレコード ID の指定したホストに対するコンポーネントのログレベル設定を更新します。各ホストを更新するには、個別の呼び出しが必要です。 指定するレガシー名と vxul コンポーネント名は小文字にする必要があります。

4

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
- バックアップに関する推奨事項
- ディザスタリカバリの要件と注意事項
- 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
- 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のクラスタ化されたプライマリサーバーでの証明書の生成
- 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
- Linux でのディザスタリカバリパッケージのリストア
- NetBackup カタログをリカバリするためのオプション

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と、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もあります。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、Cohesity 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。Cohesity 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。

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しい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。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	Cohesity 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。

- カタログがバックアップされた場合。
- カタログバックアップが重複している、または複製された場合。
- プライマリカタログバックアップまたはカタログ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。
- カタログ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。
  - カタログ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で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、カタログ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。

正しいカタログバックアップの識別

リカバリに適切なカタログ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タログを使います。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タログバックアップを使います。

カタログリカバリ時間

カタログのリカバリに必要な時間は、システム環境、カタログサイズ、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。目標とするカタログリカバリ時間に適したカタログ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。

プライマリおよびメディアサーバーのバックアップ

NetBackup カタログバックアップは構成データとカタログデータを保護します。NetBackup インストールのプライマリ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プライマリサーバーまたはメディアサーバーのリカバリ手順では、サーバーがカタログ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。プライマリ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、カタログファイルまたは NetBackup データベースのデータを含めないでください。

ディザスタリカバリの要件と注意事項

ディザスタリカバリを実行する前に、次の情報と要件に注意してください。

- Cohesity 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プライマリサーバー名を使用することを強くお勧めします。
- クラスタ環境では、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。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。
  p.285 の「ディザスタリカバリインストール後のクラスタ化されたプライマリサーバーでの証明書の生成」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.259 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
- 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。

- NetBackup では、プライマリ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 プライマリ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、プライマリ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、災害発生後にプライマリ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。

- プライマリサーバー証明書と 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: カタログ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。

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.259 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フレーズで暗号化されます。災害発生後に NetBackup をプライマリ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、この暗号化パスフレーズ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
パスフレーズの入力 (Enter passphrase)	ディザスタリカバリパッケージを暗号化するパスフレーズを入力します。 ■ デフォルトでは、パスフレーズを 8 ～ 1024 文字で指定する必要があります。 `nbseccmd -setpassphraseconstraints` コマンドオプションを使用して、パスフレーズの制約を設定できます。 ■ 既存のパスフレーズと新しいパスフレーズは異なるものにする必要があります。 ■ パスフレーズ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、~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > " が含まれます。
パスフレーズの確認 (Confirm passphrase)	確認のため、パスフレーズを再入力します。

注意: パスフレーズ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。パスフレーズ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フレーズを変更する際の注意

- パスフレーズ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フレーズで暗号化されます。

- 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 をプライマリ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、プライマリサーバーのホスト 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している必要があります。

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。

- プライマリサーバーのディスクリカバリ手順
  p.261 の「Linux のプライマリ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.267 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.268 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。『NetBackup Web UI 管理者ガイド』の NetBackup イメージのインポートに関する情報を参照してください。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。

Linux のプライマリサーバーのディスクリカバリについて

Linux 版 NetBackup プライマリサーバーのシステムディスクに障害が発生した場合に、データをリカバリする方法について、次に手順で説明します。

- 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.262 の「root が消失していない場合のプライマリ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.265 の「root パーティションが消失した場合のプライマリサーバーのリカバリ」を参照してください。

NetBackup プライマリ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 システム管理者ガイド』を参照してください。

root が消失していない場合のプライマリ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、プライマリサーバーをリカバリします。

root が消失していない場合にプライマリ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。

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。詳細情報を参照できます。

http://www.veritas.com/docs/000081350

カスタム `nbsvcuser` または `nbwebgrp` を使用した場合、インストールを開始する前に、NetBackup のインストール応答ファイルにカスタム名を入力する必要があります。詳しくは、『NetBackup インストールガイド』を参照してください。UNIX および Linux の NetBackup の要件に関する表の Web サービスの要件を参照してください。この表は、UNIX と Linux のインストール要件に関するセクションにあります。

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じ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: Cohesity 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 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 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です。

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』を参照してください。

- NetBackup のリカバリデバイスを検出および構成します。
『NetBackup 管理者ガイド Vol. 1』を参照してください。
- 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。
- 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。

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。

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。
- ロボットデバイスのメディアコンテンツのインベントリを実行します。
- 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.295 の「NetBackup カタログをリカバリするためのオプション」を参照してください。

8 すべての NetBackup デーモンを停止して、再起動します。

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

9 必要に応じてサーバーに他のファイルをリストアします。

NetBackup Web UI、NetBackup 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、または bp コマンドを使用できます。ファイルのリストアが終了したら、完了です。

root パーティションが消失した場合のプライマリ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。

root パーティションが消失した場合にプライマリサーバーをリカバリする方法

1. 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。
2. 元のディスクでコンポーネント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。これらのコンポーネントには、NetBackup とそのカタログ (該当する場合)、およびデータベースが含まれます。デフォルトでは、/usr/openv ディレクトリに格納されています。
3. 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。
4. 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

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 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。

   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』を参照してください。
- NetBackup のリカバリデバイスを検出および構成します。
  『NetBackup 管理者ガイド Vol. 1』を参照してください。
- 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。
- 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。

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。

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。
- ロボットデバイスのメディアコンテンツのインベントリを実行します。
- 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.295 の「NetBackup カタログをリカバリするためのオプション」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 必要に応じてサーバーに他のファイルをリストアします。

NetBackup Web UI、NetBackup 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、または bp コマンドを使用できます。ファイルのリストアが終了したら、完了です。

これらのファイルは、(NetBackup カタログバックアップではなく) プライマリ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/openv/var` ディレクトリ、`/usr/openv/db/data` ディレクトリまたは `/usr/openv/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。

```
/usr/openv/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/openv/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 データベースディレクトリを削除します。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 メディアサーバーでは、NetBackup 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.268 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 (Backup, Archive, and Restore)］インターフェースを使用して、ユーザーファイルを選択およびリストアします。

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.269 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.270 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.270 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/openv/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. 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.262 の「root が消失していない場合のプライマリ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。

- プライマリサーバーのディスクリカバリ手順
  p.272 の「Windows のプライマリ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.279 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.279 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 のプライマリ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 プライマリサーバーで 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.273 の「Windows が完全な状態である場合のプライマリ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 プライマリディスクで、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.276 の「プライマリサーバーおよび Windows のリカバリ」を参照してください。

NetBackup プライマリ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プライマリ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 プライマリ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プライマリ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。

   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。
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』を参照してください。

- NetBackup のリカバリデバイスを検出および構成します。
  『NetBackup 管理者ガイド Vol. 1』を参照してください。
- 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。
- 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。

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。
- ロボットデバイスのメディアコンテンツのインベントリを実行します。
- 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.295 の「NetBackup カタログをリカバリするためのオプション」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、または Windows 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。

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

警告: 手順 11 では、次の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。

install_path¥NetBackup¥db *install_path*¥NetBackupDB
install_path¥NetBackup¥var *install_path*¥Volmgr¥database

これらのディレクトリは手順 9 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。nbdb_move を使用して *install_path*¥NetBackupDB¥data からデータベース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。

---

nbdb_move を使用して *install_path*¥NetBackupDB¥data から NetBackup データベース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。

- プライマリサーバーで、NetBackup Web UI を開きます。
- [リカバリ (Recovery)]をクリックします。次に、[標準リカバリ (Regular recovery)]をクリックします。適切なポリシー形式を選択します。
- 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。
- 次のディレクトリの選択を解除します。
  install_path¥NetBackup¥db*install_path*¥NetBackupDB (または再配置された NetBackup データベースパス)
  install_path¥NetBackup¥var
  install_path¥Volmgr¥database
  この手順の前の警告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。

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。再起動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。

プライマリサーバーおよび 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。

プライマリサーバーおよび 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じ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。

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』を参照してください。
- NetBackup のリカバリデバイスを検出および構成します。
『NetBackup 管理者ガイド Vol. 1』を参照してください。
- 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。
- 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。

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。

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。
- ロボットデバイスのメディアコンテンツのインベントリを実行します。
- 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。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。

p.295 の「NetBackup カタログをリカバリするためのオプション」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、アクティビティモニター、または Windows コントロールパネルにある[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、次の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。

install_path¥NetBackup¥db *install_path*¥NetBackupDB
install_path¥NetBackup¥var *install_path*¥Volmgr¥database

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。nbdb_move を使用して *install_path*¥NetBackupDB¥data からデータベース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。

- プライマリサーバーで、NetBackup Web UI を開きます。
- 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。
- 次のディレクトリの選択を解除します。
  install_path¥NetBackup¥db*install_path*¥NetBackupDB (または再配置された NetBackup データベースパス)
  install_path¥NetBackup¥var
  install_path¥Volmgr¥database
  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。再起動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 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.279 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しい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。

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した NetBackup プライマリ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 プライマリサーバーの IP アドレスとホスト名を入力します。
- 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でください。
   - 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 プライマリ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、同じネームサーバー (または、NetBackup クライアントおよびプライマリサーバーの両方を認識する他のネームサーバー) 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プライマリ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。

   『NetBackup インストールガイド』を参照してください。

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 Web UI または NetBackup の[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]インターフェースを使用して、システムファイルとユーザーファイルをクライアントシステムにリストアします。

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。

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。

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じ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.276 の「プライマリサーバーおよび 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。

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.276 の「プライマリサーバーおよび 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のクラスタ化されたプライマリサーバーでの証明書の生成

クラスタ化されたプライマリ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。さらに、セカンダリノードへのフェールオーバーは、クラスタ環境で想定される動作です。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。

プライマリサーバーノードでの証明書の配備について詳しくは、『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。

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 プライマリ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
```

DR_PKG_MARKER_FILE 環境変数について

災害前にプライマリサーバーで外部 CA が構成されていて、DR インストールが正常に行われなかった場合は、DR パッケージのリカバリ後にサービスの再起動を待機するように DR インストールを構成できます。この時間で、外部 CA の構成を修正または再構成できます。

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。

メモ: このマーカーファイルは、DR インストールエラーが発生した場合にのみ使用してください。

インストール処理を保留するように DR_PKG_MARKER_FILE 環境変数を構成する方法

1 touch ファイルで DR_PKG_MARKER_FILE という名前の環境変数を設定します。

2 DR インストールを開始します。

DR インストールの終盤まで、NetBackup はファイルシステム上に存在する touch ファイルを検出し、NetBackup サービスの起動を待機します。

3 外部 CA の構成を変更します。

4 変更を完了したら、DR_PKG_MARKER_FILE 環境変数を含む touch ファイルを削除します。

5 インストーラによってインストール処理が再開されます。

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。このパッケージは、カタログバックアップ時に作成され、NetBackup プライマリサーバーホスト ID が含まれます。

重要な注意事項

ディザスタリカバリパッケージのリストアとカタログリカバリについては、次の点に注意してください。

- 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した後、カタログをリカバリできます。
- ディザスタリカバリパッケージ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。
- クラスタ化されたプライマリサーバーをリカバリする場合は、次の点に注意してください。
  - ディザスタリカバリパッケージには、仮想名のみの 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。
- 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.351 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。

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)。
- 災害前にプライマリサーバーで外部証明書を構成した場合、DR のインストールに失敗する場合があります。外部証明書の構成を修正する環境変数を設定できます。
p.286 の「DR_PKG_MARKER_FILE 環境変数について」を参照してください。

Windows でのディザスタリカバリパッケージのリストアオプション

NetBackup プライマリ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。

p.288 の「Windows への NetBackup のインストール中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.290 の「Windows への NetBackup のインストール後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。

Windows への NetBackup のインストール中のディザスタリカバリパッケージのリストア

次の手順は、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を示しています。

NetBackup Appliance のディザスタリカバリパッケージをリストアするには、別の手順に従う必要があります。

p.290 の「Windows への NetBackup のインストール後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。

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 License Key and Server Type]画面で、[Disaster Recovery Master Server]オプションを選択します。

3. [NetBackup 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。

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

---

5 (該当する場合) 災害前のカタログバックアップ時に、NetBackup ドメインで外部 CA が署名した証明書が使用されていた場合は、次の点に注意してください。DR のインストール中に、インストーラは CRL (証明書失効リスト) を構成するための警告メッセージを表示します。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 CDP (CRL 配布ポイント) 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 証明書ストアを使用して外部 CA が署名した証明書を格納し、それらが DR パッケージにバックアップされていない場合は、次の点に注意してください。外部 CA が署名した証明書を構成する必要があることを示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、プライマリ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

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。

- (該当する場合) 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、touch ファイルを削除します。
  NetBackup サービスが起動されます。

6 (該当する場合) 災害の前にプライマリサーバーで KMS (キーマネージメントサービス) が構成されていた場合は、次のコマンドを実行して KMS サービスを起動します。

```
Install_path¥bin¥nbkmscmd -discoverNBKMS
```

7 『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。

Windows への NetBackup のインストール後のディザスタリカバリパッケージのリストア

次の手順は、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を示しています。

NetBackup Appliance のディザスタリカバリパッケージをリストアするには、このオプションを使用します。

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 次のコマンドを使用して、CRL (証明書失効リスト) を更新します。

```
nbcertcmd -getcrl
```

4 災害の前にプライマリサーバーで KMS (キーマネージメントサービス) が構成されていた場合は、次のコマンドを実行して KMS サービスを起動します。

```
Install_path¥bin¥nbkmscmd -discoverNBKMS
```

5 次のシナリオで NetBackup 証明書ファイルを削除するには、指定された手順を実行します。

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。

次のコマンドを使用して NetBackup 証明書ファイルを削除します。

```
configureWebServerCerts -removeNBCert
```

Linux 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。このパッケージは、カタログバックアップ時に作成され、NetBackup プライマリサーバーホスト ID が含まれます。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

ディザスタリカバリパッケージのリストアとカタログリカバリについては、次の点に注意してください。

- 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した後、カタログをリカバリできます。
- ディザスタリカバリパッケージ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。
- クラスタ化されたプライマリサーバーをリカバリする場合は、次の点に注意してください。
  - ディザスタリカバリパッケージには、仮想名のみの 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。

- 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.351 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。

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、次の点に注意してください。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
- 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。
- 災害前にプライマリサーバーで外部証明書を構成した場合、DR のインストールに失敗する場合があります。外部証明書の構成を修正する環境変数を設定できます。
  p.286 の「DR_PKG_MARKER_FILE 環境変数について」を参照してください。

Linux でのディザスタリカバリパッケージのリストアオプション

NetBackup プライマリ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。

p.292 の「Linux への NetBackup のインストール中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.294 の「Linux への NetBackup のインストール後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 への NetBackup のインストール中のディザスタリカバリパッケージのリストア

次の手順は、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を示しています。

NetBackup Appliance のディザスタリカバリパッケージをリストアするには、別の手順に従う必要があります。

p.294 の「Linux への NetBackup のインストール後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。

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. 入力を求めるメッセージが表示されたら、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 (該当する場合) 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 CDP (CRL 配布ポイント) 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。
- (該当する場合) 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、touch ファイルを削除します。
  NetBackup サービスが起動されます。

7 (該当する場合) 災害の前にプライマリサーバーで KMS (キーマネージメントサービス) が構成されていた場合は、次のコマンドを実行して KMS サービスを起動します。

```
/usr/openv/netbackup/bin/nbkmscmd -discoverNBKMS
```

8 『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。

Linux への NetBackup のインストール後のディザスタリカバリパッケージのリストア

次の手順は、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を示しています。

NetBackup Appliance のディザスタリカバリパッケージをリストアするには、このオプションを使用します。

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. 次のコマンドを使用して、CRL (証明書失効リスト) を更新します。

   ```
   nbcertcmd -getcrl
   ```

4. 災害の前にプライマリサーバーで KMS (キーマネージメントサービス) が構成されていた場合は、次のコマンドを実行して KMS サービスを起動します。

   ```
   /usr/openv/netbackup/bin/nbkmscmd -discoverNBKMS
   ```

5. 次のシナリオで NetBackup 証明書ファイルを削除するには、指定された手順を実行します。

   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。

   次のコマンドを使用して NetBackup 証明書ファイルを削除します。

   ```
   configureWebServerCerts -removeNBCert
   ```

NetBackup カタログをリカバリするためのオプション

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	Cohesity 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.303 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。 この種類のリカバリでは、NetBackup データベース (BMRDB、NBAZDB、NBDB) のデータとメタデータもリストアされるため、これ以降のリカバリ処理に利用できます。 p.315 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。

リカバリオプション	説明
NetBackup データベースをリカバリします。	NetBackup は NetBackup データベース (NBDB) に情報を格納します。メタデータには、バックアップ済みのデータと、データの保存場所についての情報が含まれます。 NetBackup データベースが破損または消失しても有効なカタログイメージファイルがある場合は、データベースをリカバリします。 p.330 の「NetBackup データベースのリカバリについて」を参照してください。

NetBackup カタログの構成要素は、『NetBackup Web UI 管理者ガイド』に記載されています。

特別な使用例のための他の手順もあります。

p.342 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。

NetBackup カタログまたは NetBackup カタログイメージファイルのリカバリの前提条件

注意: NetBackup カタログリカバリは重要なプロセスです。カタログリカバリの処理中は、NetBackup Web UI や NetBackup 管理コンソールを使用して他の操作を実行しないでください。処理中は、NetBackup データベースとすべてのサービスは停止します。

注意: NetBackup カタログまたはカタログイメージファイル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。

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.351 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 カタログまたは NetBackup カタログイメージファイルのリカバリを実行する前に、次の要件と情報を確認します。

- 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。
- NetBackup でリカバリデバイスを構成します。

- 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 プライマリ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。
- カタログをリカバリするプライマリサーバーにログオンする必要があります。
- 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。
- Web UI からカタログをリカバリするには、管理者の役割または同様の権限が必要です。`bprecover` コマンドを使用するには、root (管理) 権限が必要です。
- 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.297 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。
- ディザスタリカバリファイルの場所があることを確認します。
  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。このファイルには、NetBackup プライマリサーバーのホスト ID が含まれています。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ており、カタログバックアップ中にファイルに保存されます。
  p.299 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.344 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。

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プライマリ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。

NAT メディアサーバーとの接続を確立するには

1. プライマリサーバーで `configureMQ` コマンドを実行します。
2. `nbsetconfig` コマンドを使用して、プライマリサーバーで次の構成オプションを設定します。
   - カタログ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 プライマリサーバーでサービスを再起動します。

4 プライマリサーバーと 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。

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 プライマリサーバーがインストールされている。プライマリ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 NetBackup 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 ディレクトリの下の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。

クラスタ化されたプライマリサーバーのカタログのリカバリ	クラスタ化されたプライマリサーバーからディザスタリカバリサイトの単一のプライマリサーバーに NetBackup 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/openv/netbackup/db -> /opt/VRTSnbu/netbackup/db`
	`/usr/openv/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/openv -> /opt/openv`

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 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。

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:          Tuesday, June 13, 2023 04:42
To:            NetBackup Administrator
Subject:       NetBackup Catalog Backup successful on host
               primary.example.com status 0
Attachments:   cat_1686692545_FULL.drpkg
```

```
Server
 primary.example.com

NetBackup Version
 10.3

Date
 6/13/2023 04:42:20 PM

Policy
 cat

Catalog Backup Status
 the requested operation was successfully completed (status 0).


DR image file: /usr/openv/cat_1686692545_FULL

To ensure that the NetBackup catalog data is protected through
Tue 13 Jun 2023 04:42:20 PM CDT, 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_1686692540_FULL
 * media-server.example.com  @aaaab           cat_1686692545_FULL
 * media-server.example.com  @aaaab           cat_1686692545_FULL

DR file written to
 /usr/openv/cat_1686692545_FULL

DR Package file written to
 /usr/openv/cat_1686692545_FULL.drpkg

The CA configuration at the time of catalog backup is as follows:


The primary server primary.example.com is configured to use NetBackup certificates.

 ECA_CRL_PATH_SYNC_HOURS = 1
 ECA_CRL_REFRESH_HOURS = 24
 ECA_CRL_CHECK = LEAF
```

```
The primary server is configured to use service account: root

The primary server is configured to run with FIPS mode set to: DISABLE


* - 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 web UI or the nbseccmd command.
- If the catalog backup is encrypted using keys from an External KMS, configure
  the External KMS in NetBackup after the installation completes and before
  starting recovery. See the NetBackup Security and Encryption Guide for
  information on how to configure an external KMS.
  http://www.veritas.com/docs/DOC5332
- If this catalog backup is encrypted using a keys from the NetBackup KMS,
  configure the NetBackup KMS and restore the required keys after the installation
  completes and before starting recovery. See the NetBackup Security and
  Encryption Guide for information on how to backup and restore keys from the
  NetBackup KMS. http://www.veritas.com/docs/DOC5332
```

```
 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 "Are you currently
         performing a disaster recovery of a primary server? [y,n] (y)".
         Select "y"
      ii. On the Windows installer click the "Disaster Recovery Primary
         Server" button.
    b. The installation procedure prompts you for the primary server's DR
       Package
       (refer to the /usr/openv/cat_1686692545_FULL.drpkg mentioned earlier).
       Make sure that the primary server can access the attached DR package
       file.
    c. Type the passphrase associated with the DR Package,
       when prompted.
      i. The installer validates the DR package using the 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/100033743
      iii. If the external CA-signed certificates could not be backed up,
           configure the certificates on the host.
           Refer to the following article:
           http://www.veritas.com/docs/100044249
 2. Configure the devices necessary to read the media listed above.
 3. Inventory the media.
 4. Make sure that the primary server can access the attached DR image file.
 5. Start the NetBackup Recovery Wizard from the NetBackup web UI.  Or, start
    the wizard from a command line by entering bprecover -wizard.

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. Run:
    Configure certificates for the media server that is associated with this
    catalog recovery by running the below commands on that host:
        nbcertcmd -getCACertificate
        nbcertcmd -getCertificate -force
 3.  Configure the devices necessary to read the media listed above.
```

4. Inventory the media.
5. Run
   To recover from copy 1:
   bpimport -create_db_info [-server name] -id /
6. Run:
   cat_export -client client1.example.com
7. Go to the following directory to find the DR image file
   cat_backup_1686692545_FULL:
   /usr/openv/netbackup/db.export/images/primary.example.com/1686000000
8. Open cat_backup_1686692545_FULL file and find the BACKUP_ID
   (for example: primary.example.com_1686692545).
9. Run:
   bpimport [-server name] -backupid primary.example.com_1686692545
10. Run:
    bprestore -T -w [-L progress_log] -C primary.example.com -t 35
    -p cat_backup -X -s 1686692545 -e 1686692545 /
11. Run the NetBackup web UI to restore the remaining image database
    if the DR image is a result of an incremental backup.
12. To recover the NetBackup relational database, run:
    bprecover -r -nbdb
13. Stop and start NetBackup.
14. Run:
    Re-configure the certificates on the primary server and the media server,
    because the database is restored to a previous point in time.
        Run the following set of commands on the primary server:
            nbcertcmd -getCACertificate -force
            nbcertcmd -createToken -reissue -host <primary/media>
            name <>
            nbcertcmd -getCertificate -token <> -force
        Run the following set of commands on the media server that is
        associated with this catalog recovery:
            nbcertcmd -getCACertificate -force
            nbcertcmd -getCertificate -force
15. Configure the devices if any device has changed since the last
    backup.
16. To make sure the volume information is updated, inventory the
    media to update the NetBackup database.

NetBackup カタログ全体のリカバリについて

Cohesity 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 データベースがリストアされます。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 データベースがリストアされます。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。その後、NetBackup Web UI または[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。

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。

- NetBackup カタログリカバリウィザード。
  p.304 の「NetBackup カタログリカバリウィザードを使用した NetBackup カタログ全体のリカバリ」を参照してください。
- `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.309 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。

NetBackup カタログリカバリウィザードを使用した NetBackup カタログ全体のリカバリ

この手順では、[NetBackup カタログリカバリウィザード (NetBackup catalog recovery wizard)]を使ってカタログ全体をリカバリする方法を示します。

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、Cohesity 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.315 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。

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。

NetBackup カタログリカバリウィザードを使用してカタログ全体をリカバリする方法

1 カタログリカバリを開始する前に、前提条件を確認します。

p.296 の「NetBackup カタログまたは NetBackup カタログイメージファイルのリカバリの前提条件」を参照してください。

2 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/openv/netbackup/bin/bp.start_all`
- Windows の場合:
  install_path¥NetBackup¥bin¥bpup

3 カタログをリカバリするプライマリサーバーにサインインします。管理者の役割または同様の権限が必要です。

4 NetBackup の Web UI を起動します。

5 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。

- 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
- 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、`nbdevconfig` コマンドを使用して、プライマリサーバーの構成にストレージサーバーを追加します。
  MSDP プールからの NetBackup カタログのリカバリについて詳しくは、記事を参照してください。
- 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。

6 上部で[設定 (Settings)]、[NetBackup カタログリカバリ (NetBackup catalog recovery)]をクリックします。

7 ディザスタリカバリファイルが保存される場所を指定します。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。ディザスタリカバリファイルは、Web UI を開いたローカルコンピュータ上で利用可能である必要があります。

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。

8 NetBackup は、カタログのリカバリに必要なメディアを検索します。その後、進捗状況が通知され、ディザスタリカバリイメージの必要なバックアップ ID が特定されます。メディアが検出されなかった場合、NetBackup はデータベースの更新が必要なメディアを示します。

必要に応じて、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。表示される情報は、完全バックアップと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。

必要なすべてのメディアソースが見つかったら、[次へ (Next)]をクリックします。

9 デフォルトでは、[NetBackup カタログ全体をリカバリする (Recover entire catalog)]オプションが選択されています。

必要に応じて、[ジョブ優先度 (Job priority)]を選択し、[次へ (Next)]をクリックしてリカバリを開始します。[キャンセル (Cancel)]をクリックすると、NetBackup カタログリカバリの処理を停止できます。

10 NetBackup 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。

11 リカバリが完了したら、[完了 (Finish)]をクリックします。

12 重要: 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。パスフレーズは、カタログリカバリ中にリカバリされません。

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。

- 上部で、[設定 (Settings)]、[グローバルセキュリティ設定 (Global security settings)]の順にクリックします。[ディザスタリカバリ (Disaster Recovery)]タブで、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。

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.351 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、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てください。
- 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する必要があります。そうしないと、NetBackup によってメディアが上書きされる可能性があります。

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 次のように、プライマリ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/openv/netbackup/bin/bp.kill_all
/usr/openv/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 Web UI 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停止されます。

16 サービスを再起動したら、次のコマンドのいずれかを実行します。

- 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/openv/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/openv/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/openv/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/openv/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.352 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。

17 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ていないと、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 カタログリカバリウィザードの代わりに使用できます。

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、Cohesity 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.315 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。

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 カタログリカバリを開始する前に、前提条件を確認します。

p.296 の「NetBackup カタログまたは NetBackup カタログイメージファイルのリカバリの前提条件」を参照してください。

2 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。

3 次のコマンドを使って NetBackup を起動します。

- UNIX および Linux の場合:

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

- Windows の場合:

  `install_path``¥NetBackup¥bin¥bpup.exe`

4 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。

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、プライマリ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

5 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/openv/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)
```

6 [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:
```

7 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)。また、以前のバージョンのカタログ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。

8 [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 データベース (NBDB および NBAZDB 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 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
```

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 データベース (NBDB および NBAZDB 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。

10 重要: 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。

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。

- Web UI を開きます。上部で、[設定 (Settings)]、[グローバルセキュリティ設定 (Global security settings)]の順にクリックします。[ディザスタリカバリ (Disaster Recovery)]タブで、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。

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.351 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、Cohesity 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、プライマリ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/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

- Windows の場合:

```
install_path¥NetBackup¥bin¥bpdown
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/openv/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/openv/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/openv/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/openv/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.352 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。

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ていないと、必要な WORM 保護が新しいバックアップに適用されません。

カタログリカバリ後の NetBackup ジョブ ID 番号の指定

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。カタログリカバリ後に、NetBackup ジョブ ID 番号を指定できます。

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. NetBackup `jobid` ファイルを編集し、リカバリカタログにある最後のジョブ ID の数字より 1 つ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/openv/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。
2. NetBackup カタログをリカバリします。

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。
- NetBackup データベース (BMRDB、NBAZDB、NBDB) のデータとメタデータがリストアされるため、必要な場合に、これ以降のリカバリ処理に利用できます。
  p.340 の「ステージングでの NetBackup 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 は部分的なリカバリに含まれているファイルのリストです。

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プライマリ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.299 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。

Cohesity 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 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。
- 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、構成ファイルを、通常のリカバリオプションを使用して NetBackup Web UI でリストアできます。または、[バックアップ、アーカイブおよびリストア (Backup, Archive and Restore)]インターフェースを使用できます。
- 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/openv/netbackup/bp.conf	なし
/usr/openv/netbackup/db/*	install_path¥NetBackup¥db¥*
/usr/openv/netbackup/db/class/*(オプション)	*install_path*¥NetBackup¥db¥class¥*(オプション)
/usr/openv/netbackup/vault/sessions*	*install_path*¥NetBackup¥vault¥sessions¥*
/usr/openv/var/*(オプション)	*install_path*¥NetBackup¥var¥*(オプション)

UNIX および Linux	Windows の場合
/usr/openv/volmgr/database/*	*install_path*¥Volmgr¥database¥*
/usr/openv/volmgr/vm.conf	*install_path*¥Volmgr¥vm.conf

NetBackup 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、[NetBackup カタログリカバリウィザード (NetBackup catalog recovery wizard)]を使って NetBackup カタログイメージファイルをリカバリする方法を示します。

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。

NetBackup 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. nbgetconfig コマンドを実行し、出力を保存します。この出力は、カタログリカバリ中に上書きされたホスト固有の情報をリカバリするために、カタログリカバリの後で使用できます。

   例:

   ```
   ./nbgetconfig > sample.txt
   ```

2. カタログリカバリを開始する前に、前提条件を確認します。

   p.296 の「NetBackup カタログまたは NetBackup カタログイメージファイルのリカバリの前提条件」を参照してください。

3. 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/openv/netbackup/bin/bp.start_all
     ```

   - Windows の場合:

     install_path¥NetBackup¥bin¥bpup

4. 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。

   - NetBackup で必要なリカバリデバイスを構成します。
   - 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。

- 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.299 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。

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。

5 NetBackup Web UI を開きます。

6 上部で[設定 (Settings)]、[NetBackup カタログリカバリ (NetBackup catalog recovery)]をクリックします。

7 ディザスタリカバリファイルが保存される場所を指定します。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。

8 NetBackup は、カタログのリカバリに必要なメディアを検索します。その後、進捗状況が通知され、ディザスタリカバリイメージの必要なバックアップ ID が特定されます。メディアが検出されなかった場合、NetBackup はデータベースの更新が必要なメディアを示します。

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見つかったら、[次へ (Next)]をクリックします。

9 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。

必要に応じて、[ジョブ優先度 (Job priority)]を選択し、[次へ (Next)]をクリックしてリカバリを開始します。

10 NetBackup 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。

11 リカバリが完了したら、[サインアウト (Sign Out)]をクリックします。

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。

12 NetBackup データベース全体をリカバリせずにイメージヘッダー情報をリカバリする場合は、次の手順を実行します。

- 手順 a - ターゲットデータベースをバックアップします。次のコマンドを実行します。

  `nbdb_backup -online directory`

  出力ディレクトリとしてステージングフォルダを指定しないようにします。(ステージングフォルダには、カタログバックアップの NetBackup データベースのスキーマデータと構成データが含まれています。イメージ `.f` と構成ファイルは最終的な宛先にリカバリされます。)

- 手順 b - ステージングディレクトリから NetBackup データベースをリカバリします。

  ```
  nbdb_restore -recover -staging
  ```

- 手順 c - バックアップからインポートするイメージヘッダーデータをエクスポートします。

  たとえば、次のコマンドを実行すると、すべてのイメージヘッダーデータがエクスポートされます。データは `netbackup/db.export` ディレクトリにエクスポートされます。

  ```
  cat_export -all
  ```

- 手順 d - 次のコマンドを実行して NetBackup データベースをリカバリします。

  `nbdb_restore -recover directory`

  手順 a と同じディレクトリを指定していることを確認します。

- 手順 e - `cat_import` コマンドを実行して、手順 c で抽出したイメージヘッダーデータをインポートします。

```
cat_import -all -replace_destination -delete_source
```

コマンドは、以下を実行します。

- netbackup/db.export ディレクトリのすべてのイメージヘッダーデータをインポートします。
- ターゲットデータベースにすでに存在するエクスポートされたイメージヘッダーデータを置き換えます。
- netbackup/db.export ディレクトリにあるイメージヘッダーデータを削除します。

- 手順 f - ディスクデバイスからカタログをリカバリした場合は、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。次のコマンドを実行します。

```
nbcatsync -sync_dr_file DR file path -dryrun
```

カタログ DR ファイルへのパスで *DR file path* を置き換えます。

- 手順 g - ドライランの結果が十分な場合は、次のコマンドを実行します。

```
nbcatsync -sync_dr_file DR file path
```

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.351 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、Cohesity 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、カタログのデータベース部分をリカバリする必要があります。
p.330 の「NetBackup 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 手順 1 でバックアップしたホスト設定をリカバリします。次のコマンドを実行します。

```
./nbsetconfig sample.txt
```

15 次のように、プライマリサーバーで 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/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

- Windows の場合:

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

16 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/openv/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/openv/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.352 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。

17 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

bprecover -wizard コマンドは、NetBackup カタログリカバリウィザードの代わりに使用できます。

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.315 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。

bprecover -wizard 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. nbgetconfig コマンドを実行し、出力を保存します。この出力は、カタログリカバリ中に上書きされたホスト固有の情報をリカバリするために、カタログリカバリの後で使用できます。

   例:

   ```
   ./nbgetconfig > sample.txt
   ```

2. カタログリカバリを開始する前に、前提条件を確認します。

   p.296 の「NetBackup カタログまたは NetBackup カタログイメージファイルのリカバリの前提条件」を参照してください。

3. 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。
   - 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.299 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。

4. 次のコマンドを入力してプライマリサーバーの 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/openv/netbackup/bin/bp.start_all

5 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)
```

6 [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:
```

7 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)。また、以前のバージョンのカタログ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)
```

8 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)
```

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。

```
Do you also want to include licensing data?(Y/N)
```

10 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...

Gathering configuration information.
Waiting for the security services to start operation.
Generating identity for host 'vm2.example.com_1318309224'
Setting up security on target host: vm2.example.com_1318309224
nbatd is successfully configured on NetBackup Primary Server.
Operation completed successfully.

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 "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.

WRN - Local or global-level settings that you have configured on
 the
master server before catalog recovery are overwritten.
It is recommended that you re-configure the required settings
after
the services are restarted.

For more information, please review the log file:
/usr/openv/netbackup/logs/user_ops/root/logs/Recover1318357550.log
```

11 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。

12 NetBackup データベース全体をリカバリせずにイメージヘッダー情報をリカバリする場合は、次の手順を実行します。

- 手順 a - ターゲットデータベースをバックアップします。次のコマンドを実行します。

  ```
  nbdb_backup -online directory
  ```

  出力ディレクトリとしてステージングフォルダを指定しないようにします。(ステージングフォルダには、カタログバックアップの NetBackup データベースのスキーマデータと構成データが含まれています。イメージ `.f` と構成ファイルは最終的な宛先にリカバリされます。)

- 手順 b - ステージングディレクトリから NetBackup データベースをリカバリします。

  ```
  nbdb_restore -recover -staging
  ```

- 手順 c - バックアップからインポートするイメージヘッダーデータをエクスポートします。
  たとえば、次のコマンドを実行すると、すべてのイメージヘッダーデータがエクスポートされます。データは `netbackup/db.export` ディレクトリにエクスポートされます。

  ```
  cat_export -all
  ```

- 手順 d - 次のコマンドを実行して NetBackup データベースをリカバリします。

  ```
  nbdb_restore -recover directory
  ```

  手順 a と同じディレクトリを指定していることを確認します。

- 手順 e - `cat_import` コマンドを実行して、手順 c で抽出したイメージヘッダーデータをインポートします。

  ```
  cat_import -all -replace_destination -delete_source
  ```

  コマンドは、以下を実行します。

  - `netbackup/db.export` ディレクトリのすべてのイメージヘッダーデータをインポートします。
  - ターゲットデータベースにすでに存在するエクスポートされたイメージヘッダーデータを置き換えます。
  - `netbackup/db.export` ディレクトリにあるイメージヘッダーデータを削除します。

- 手順 f - ディスクデバイスからカタログをリカバリした場合は、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。次のコマンドを実行します。

```
nbcatsync -sync_dr_file DR file path -dryrun
```

カタログ DR ファイルへのパスで *DR file path* を置き換えます。

- 手順 g - ドライランの結果が十分な場合は、次のコマンドを実行します。

```
nbcatsync -sync_dr_file DR file path
```

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.351 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、Cohesity 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、カタログのデータベース部分をリカバリする必要があります。
p.330 の「NetBackup 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 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 手順 1 でバックアップしたホスト設定をリカバリします。次のコマンドを実行します。

```
./nbsetconfig sample.txt
```

16 次のように、プライマリ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¥bpdown
install_path¥NetBackup¥bin¥bpup
```

- UNIX の場合:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/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/openv/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/openv/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、以下の手順を実行します。
  非クラスタ設定の場合:
  UNIX の場合:

  ```
  /usr/openv/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/openv/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.352 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 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 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 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.330 の「NetBackup データベース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.336 の「NetBackup データベースのステージングからのリカバリ」を参照してください。

NetBackup データベースのバックアップからのリカバリ

NBDB (NetBackup)、NBAZDB (NetBackup Authorization)、または BMRDB (Bare Metal Restore) データベースをバックアップからリカバリできます。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	データベースが利用可能で、NetBackup Scale-Out Relational Database サーバーが実行されている場合は、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 10 およびステップ 12 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 データベース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/openv/netbackup/bin/bp.kill_all
```

Windows の場合:
```
install_path¥NetBackup¥bin¥bpdown
```

2 NBDB、NBAZDB または BMRDB をデータベースディレクトリから一時ディレクトリに移動します。

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。

```
install_path¥NetBackupDB¥data¥nbdb
install_path¥NetBackupDB¥data¥nbazdb
install_path¥NetBackupDB¥data¥bmrdb
```

```
/usr/openv/db/data/nbdb
/usr/openv/db/data/nbazdb
/usr/openv/db/data/bmrdb
```

3 次のように、NetBackup Scale-Out Relational Database サーバーを起動します。

UNIX の場合:
```
/usr/openv/netbackup/bin/nbdbms_start_stop start
```

Windows の場合:
```
install_path¥NetBackup¥bin¥bpup -e vrtsdbsvc_psql
```

4 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。

次のディレクトリからコマンドを実行します。

UNIX の場合: `/usr/openv/db/bin`

Windows の場合: *install_path*¥NetBackup¥bin

通常のシナリオ	`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	`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	`create_nbdb -drop -data VXDBMS_NB_DATA -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。

5 次のように NetBackup サービスを開始します。

UNIX の場合:	`/usr/openv/netbackup/bin/bp.start_all`
Windows の場合:	*install_path*¥NetBackup¥bin¥bpup

6 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/openv/volmgr/bin/tpext -loadEMM`
Windows の場合:	*install_path*¥Volmgr¥bin¥tpext -loadEMM

7 nbdb_move コマンドを使って NetBackup データベースを再配置した場合は、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が移動されるデフォルトの場所を示します。

install_path¥NetBackupDB¥data¥nbdb
install_path¥NetBackupDB¥data¥nbazdb
install_path¥NetBackupDB¥data¥bmrdb

/usr/openv/db/data/nbdb
/usr/openv/db/data/nbazdb
/usr/openv/db/data/bmrdb

8 次のように、NetBackup プライマリサーバー上の NetBackup Device Manager を起動します。

UNIX の場合:	/usr/openv/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)。

9 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

10 プライマリ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 の場合: `/usr/openv/netbackup/bin/admincmd/bprecover -r -nbdb`

Windows の場合: *`install_path`*`¥NetBackup¥bin¥admincmd¥bprecover -r -nbdb`

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、プライマリ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 の場合:
```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

Windows の場合:
```
install_path¥NetBackup¥bin¥bpdown
install_path¥NetBackup¥bin¥bpup
```

13 サービスが再起動したら、証明書を更新します。

- 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/openv/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/openv/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/openv/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/openv/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.352 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 データベースのステージングからのリカバリ

カタログバックアップ中に、NetBackup データベース (BMRDB、NBAZDB、NBDB) のデータとメタデータがステージングディレクトリにコピーされます。イメージファイルと構成ファイルをリストアするリカバリオプションは、NetBackup データベースのデータとメタデータもステージングディレクトリにリストアします。

p.315 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。

NetBackup データベース (BMRDB、NBAZDB、NBDB) は、ステージングディレクトリからリカバリできます。

p.340 の「ステージングでの NetBackup データベースの処理について」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.337 の「データベースが壊れていない場合に NetBackup データベースをステージングからリカバリする方法」を参照してください。
データベースが壊れている場合	p.337 の「データベースが壊れている場合に NetBackup データベースをステージングからリカバリする方法」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 NetBackup データベースをステージングからリカバリする方法

1. ステージングから NBDB をリカバリするには、プライマリサーバーで次のコマンドを実行します。

   UNIX: `/usr/openv/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/openv/netbackup/bin/bp.kill_all
   /usr/openv/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 NetBackup データベースをステージングからリカバリする方法

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/openv/netbackup/bin/bp.kill_all`

   Windows の場合: *install_path*¥NetBackup¥bin¥bpdown

2. NBDB、NBAZDB または BMRDB をデータベースディレクトリから一時ディレクトリに移動します。

   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。

   ```
   install_path¥NetBackupDB¥data¥nbdb
   install_path¥NetBackupDB¥data¥nbazdb
   install_path¥NetBackupDB¥data¥bmrdb

   /usr/openv/db/data/nbdb
   /usr/openv/db/data/nbazdb
   /usr/openv/db/data/bmrdb
   ```

3 次のように、NetBackup Scale-Out Relational Database サーバーを起動します。

UNIX の場合: `/usr/openv/netbackup/bin/nbdbms_start_stop start`

Windows の場合: *install_path*¥NetBackup¥bin¥bpup -e vrtsdbsvc_psql

4 次のとおり、空のデータベースを作成します:

UNIX の場合: `/usr/openv/db/bin/create_nbdb -drop`

Windows の場合: *install_path*¥NetBackup¥bin¥create_nbdb -drop

5 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/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

Windows の場合:

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

6 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/openv/volmgr/bin/tpext -loadEMM`

Windows の場合: *install_path*¥Volmgr¥bin¥tpext -loadEMM

7 `nbdb_move` コマンドを使用して NetBackup データベース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が配置されていたディレクトリを再作成します。

8 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/openv/volmgr/bin/ltid -v`

Windows の場合: Device Manager サービスを起動します。

9 ステージングから NBDB をリカバリするには、プライマリサーバーで次のコマンドを実行します。

UNIX: `/usr/openv/db/bin/nbdb_restore -dbn NBDB -recover -staging`

Windows: *install_path*¥NetBackup¥bin¥nbdb_restore -dbn NBDB -recover -staging

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、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/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

Windows の場合:

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

12 サービスが再起動したら、証明書を更新します。

- 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/openv/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/openv/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/openv/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/openv/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.352 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 NetBackup データベースの処理について

警告: Cohesityでは、Cohesity Technical Supportの指示による場合のみ、NetBackup NetBackup データベースを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、Cohesity 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

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。

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

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 データベース (BMRDB、NBAZDB および NBDB) のデータとメタデータ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。

`nbdb_restore -staging`	ステージングディレクトリから NetBackup データベースをリカバリするには、`nbdb_restore -staging` を使います。 p.336 の「NetBackup データベースのステージングからのリカバリ」を参照してください。

データベース接続の終了

`nbdb_unload` を実行する前に NetBackup をシャットダウンして、データベースへのすべてのアクティブな接続を終了してください。NetBackup をシャットダウンすると、起こりうる並列実行の問題が回避されます。

Windows でデータベース接続を終了する方法

1. 次のコマンドを入力するとすべての NetBackup サービスが停止します。

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

2. Windows のサービスマネージャで、NetBackup Scale-Out Relational Database Manager という名前のサービスを再起動します。

3 データベース接続を終了するために次のいずれかの方法を使用します。

- NetBackup データベース管理ユーティリティを使用します。
- 出力の内容 (データベース名、表またはスキーマのみ) および出力先ディレクトリを指定して、nbdb_unload を実行します。

4 NetBackup Scale-Out Relational Database Manager サービスを、次のコマンドを使用して停止します。

```
install_path¥NetBackup¥bin¥bpdown -e vrtsdbsvc_psql
```

5 次のコマンドを入力して NetBackup のすべてのサービスを起動します。

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

UNIX でデータベース接続を終了する方法

1 次のコマンドを入力して、すべての NetBackup デーモンを停止します。

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

2 次のコマンドを使用して NetBackup データベースデーモンを起動します。

```
/usr/openv/netbackup/bin/nbdbms_start_stop start
```

3 データベースサーバーだけを起動します。`/usr/openv/netbackup/bin/nbdbms_start_stop start`

4 データベース接続を終了するために次のいずれかの方法を使用します。

- NetBackup データベース管理ユーティリティを使用します。
- 出力の内容 (データベース名、表またはスキーマのみ) および出力先ディレクトリを指定して、nbdb_unload を実行します。

5 データベースサーバーを停止します。`/usr/openv/netbackup/bin nbdbms_start_stop stop`

6 NetBackup Scale-Out Relational Database Manager サービスを、次のコマンドを使用して停止します。

```
/usr/openv/netbackup/bin/nbdbms_start_stop stop
```

7 次のコマンドを入力することによって NetBackup のすべてのデーモンを起動します。

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

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	手順詳細
手順 1	NBAC が構成されて稼働中であるプライマリ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。 http://www.veritas.com/docs/DOC5332
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.303 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。 http://www.veritas.com/docs/DOC5332
手順 4	NetBackup を再起動します。	`/usr/openv/netbackup/bin/bp.kill_all` `/usr/openv/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	手順詳細
手順 1	NBAC が構成されて稼働中であるプライマリ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。 http://www.veritas.com/docs/DOC5332
手順 2	NetBackup サービスを停止します。	*install_path*¥Veritas¥NetBackup¥bin¥bpdown.exe

手順	作業	手順詳細
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。	*install_path*¥Veritas¥NetBackup¥bin¥bpup.exe
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.303 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 7	NBAC を使うように NetBackup を構成します。	手順は環境によって次のように異なります。 ■ Windows Server フェールオーバークラスタ環境の NetBackup プライマリサーバーの場合は、アクティブノードの NetBackup プライマリサーバーで次のコマンドを実行します。 `bpnbaz -setupmaster` 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 Windows レジストリをプロビジョニングします。 ■ 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 NetBackup プライマリサーバーで実行します。 `bpnbaz -setupmaster` ■ 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。 『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。 http://www.veritas.com/docs/DOC5332
手順 8	NetBackup を再起動します。	*install_path*¥Veritas¥NetBackup¥bin¥bpdown.exe *install_path*¥Veritas¥NetBackup¥bin¥bpup.exe

p.295 の「NetBackup カタログをリカバリするためのオプション」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 NetBackup

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。

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. カタログリカバリを開始する前に、前提条件を確認します。

   p.296 の「NetBackup カタログまたは NetBackup カタログイメージファイルのリカバリの前提条件」を参照してください。

2. 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、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
     ```

3. 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/openv/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_FULL。

   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.299 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および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、プライマリ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. 各プライマリ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中に使用されたのと同じ構成に設定します。プライマリ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の各プロパティが、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。

`master_server`	NetBackup 構成で指定されているプライマリサーバーの正確な名前を使用します。
`media_server`	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。
`timestamp`	DR ファイル名の先頭 4 桁の数字の後に 0 (ゼロ) を 6 つ付けたもの。
`media`	ディザスタリカバリファイルの FRAGMENT 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。
`backup_id`	DR ファイル内の BACKUP_ID に指定されています。

   例:

   file: Hot_Backup_1122502016_INCR

   timestamp: 1122000000

4 プライマリサーバー上に DR リカバリディレクトリを作成します。

UNIX の場合:

```
/usr/openv/netbackup/db/images/primary_server/timestamp/tmp
```

Windows の場合:

```
C:¥Program Files¥VERITAS¥NetBackup¥db¥images¥primary_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/primary_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 primary_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 primary_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 Web UI を開き、[リカバリ (Recovery)]をクリックします。[標準リカバリ (Regular recovery)]カードで[リカバリの開始 (Start recovery)]をクリックします。または、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]クライアントインターフェースを使用します。
- ポリシー形式に[NBU-Catalog]を選択します。
- プライマリサーバーにソースクライアントおよび宛先クライアントを設定します。

- 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/*primary_server*

- プライマリ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 重要なデータをリストアします。

- NetBackup Web UI を開き、[リカバリ (Recovery)]をクリックします。[標準リカバリ (Regular recovery)]カードで[リカバリの開始 (Start recovery)]をクリックします。または、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]クライアントインターフェースを使用します。
- ポリシー形式に[NBU-Catalog]を選択します。
- プライマリサーバーにソースクライアントおよび宛先クライアントを設定します。
- ([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) ビューを更新します。
- 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。
- プライマリサーバーで次のディレクトリを参照します。

  install_path/netbackup/db/images

- 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。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。

- NetBackup Web UI を開き、[リカバリ (Recovery)]をクリックします。[標準リカバリ (Regular recovery)]カードで[リカバリの開始 (Start recovery)]をクリックします。または、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]クライアントインターフェースを使用します。
- リストアするデータと一致するポリシー形式を選択します。
- データをバックアップしたクライアントに合わせて、ソースクライアントおよび宛先クライアントを設定します。
- ([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) ビューを更新します。

11 NetBackup 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 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 primary_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 各プライマリ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 Web UI を開き、[リカバリ (Recovery)]をクリックします。[標準リカバリ (Regular recovery)]カードで[リカバリの開始 (Start recovery)]をクリックします。または、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]クライアントインターフェースを使用します。
- ポリシー形式に[NBU-Catalog]を選択します。
- プライマリサーバーにソースクライアントおよび宛先クライアントを設定します。
- リストアする追加のサーバーごとに、ソースクライアントと宛先クライアントをそのサーバーに設定します。
- 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 サービスが再起動したら、証明書を更新します。

- 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/openv/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/openv/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/openv/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/openv/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.352 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 Web UI または[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特定のファイルをリカバリできます。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.295 の「NetBackup カタログをリカバリするためのオプション」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 Web UI を開きます。または、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]クライアントインターフェースを使用します。
2. [リカバリ (Recovery)]をクリックします。[標準リカバリ (Regular recovery)]カードで[リカバリの開始 (Start recovery)]をクリックします。
3. ポリシー形式に[NBU-Catalog]を選択します。
4. プライマリサーバーにソースクライアントおよび宛先クライアントを設定します。
5. 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凍する方法を記述します。

p.295 の「NetBackup カタログをリカバリするためのオプション」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. プライマリサーバー上で、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. プライマリサーバーで次のコマンドを実行します。

   ```
   bpimport
   ```

3. プライマリサーバー上で、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/openv/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
     次の手順に進みます。

2. プライマリ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. プライマリサーバーの Client_Name キーの値に注意してください。クラスタ化されたプライマリサーバーの場合は、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/openv/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 プライマリサーバーのホスト 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

クラスタ化されたプライマリサーバーの場合は、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-xxxxxxxxx
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 プライマリサーバーに対し、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 Web UI でも、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 (Security)]、[ホストマッピング (Host mappings)] の順に選択します。

6 証明書を更新するには次の操作を行います。

- プライマリサーバーの 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

  クラスタ化されたプライマリサーバーの場合は、次のコマンドを実行します。

  install_path¥netbackup¥bin¥nbcertcmd -renewCertificate -cluster