NetBackup™ アップグレードガイド

リリース 10.1

VERITAS™

NetBackup™ アップグレードガイド

最終更新日: 2022-10-28

法的通知と登録商標

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

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

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

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

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

世界共通 (日本を除く)	CustomerCare@veritas.com
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、Veritasの Web サイトで入手できます。

https://sort.veritas.com/documents

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

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 10.1 アップグレードガイド』について

『NetBackup 10.1 アップグレードガイド』は、NetBackup 10.1 へのアップグレードの計画と実行を支援するために提供されます。『NetBackup 10.1 アップグレードガイド』では、NetBackup バージョン 7.7.x 以降から NetBackup 10.1 へのアップグレードパスについて説明しています。このガイドの最新版は、NetBackup アップグレードポータルから入手できます。

NetBackup 環境では、異なるバージョンの NetBackup を混在させることができます。複数バージョンの NetBackup がサポートされるため、サーバーを一度に 1 台ずつアップグレードできます。このアップグレードプロセスでは、システム全体のパフォーマンスへの影響が最小限に抑えられます。バージョン混在のサポートに関する詳しい情報を参照できます。

Veritas は、10.1 リリースでの NetBackup の変更について詳しくは、『NetBackup リリースノート』を参照することをお勧めします。

p.165 の「NetBackup のバージョン間の互換性について」を参照してください。

Veritas Services and Operations Readiness Tools (SORT) は、アップグレード準備に役立つリソースです。SORT に関する詳しい情報を参照できます。

p.26 の「Veritas Services and Operations Readiness Tools について」を参照してください。

NetBackup のサポート終了 (EOSL) バージョンから NetBackup 10.1 へのアップグレード

NetBackup 7.6.x 以前はサポート終了 (EOSL) になっています。NetBackup の EOSL バージョンの必要なアップグレード手順は、『NetBackup 10.1 アップグレードガイド』に記載されていません。NetBackup の EOSL バージョンから 9.1 に直接アップグレードするには、次のことが必要です。

- 『NetBackup 8.0 リリースノート』を参照して、NetBackup への変更点について理解します。
- 『NetBackup 8.0 アップグレードガイド』に一覧表示されているアップグレード手順を参照します。
- NetBackup 8.0 のアップグレード手順を、『NetBackup 10.1 アップグレードガイド』のアップグレード手順と組み合わせます。

Veritas は、ご使用の ESOL バージョンから NetBackup 10.1 までの各リリースの『NetBackup リリースノート』と『NetBackup アップグレードガイド』を参照することをお勧めします。

これらのマニュアルでは、正常にアップグレードするために役立つアップグレード手順と必要条件に関して詳しく説明しています。

これらのマニュアルのコピーについては、NetBackup マニュアルのランディングページを参照してください。

利用可能な NetBackup アップグレード方式

表 1-1 および 表 1-2 に、NetBackup のアップグレード方式の詳細を示します。使用環境に最適なアップグレード方式をよりよく理解するには、次の点を考慮してください。

- 対話形式: アップグレードプロセス中にユーザーが UI を介して入力する必要があります。
- サイレントまたはネイティブ: Windows コマンドファイルを使用するアップグレード、または UNIX および Linux のネイティブパッケージマネージャを直接呼び出すアップグレード。
- プッシュまたはリモート: VxUpdate、Chef、SCCM などのオプションが含まれます。さらに、Windows ではリモートアップグレードを実行でき、UNIX と Linux では `ssh` または `sftp` を使用できます。

表 1-1 UNIX と Linux のアップグレードおよび EEB

方式	プライマリ	メディア	クライアント
対話形式	p.58 の「NetBackup 10.1 への Linux サーバーソフトウェアのアップグレード」を参照してください。	p.77 の「NetBackup 10.1 への NetBackup メディアサーバーのアップグレード」を参照してください。 p.105 の「VxUpdate について」を参照してください。	可能。プライマリサーバーについての情報を参照してください。 p.105 の「VxUpdate について」を参照してください。
サイレントまたはネイティブ	p.64 の「Linux での NetBackup プライマリサーバーソフトウェアのサイレントアップグレード」を参照してください。	p.80 の「Linux での NetBackup メディアサーバーソフトウェアのサイレントアップグレード」を参照してください。 p.105 の「VxUpdate について」を参照してください。	p.91 の「ネイティブインストーラによる UNIX と Linux のクライアントバイナリのアップグレード」を参照してください。 p.105 の「VxUpdate について」を参照してください。
プッシュまたはリモート	アップグレード: 不可 EEB: EEB のプッシュアップグレードは、サードパーティの配備ツールを使用すれば可能な場合があります。Veritas から提供される Chef および SCCM のテンプレートも使用できます。	p.105 の「VxUpdate について」を参照してください。	p.179 の「サーバーのアップグレード後のクライアントのアップグレード」を参照してください。 Chef および SCCM のテンプレート https://sort.veritas.com/utility/netbackup/deployment p.105 の「VxUpdate について」を参照してください。

表 1-2 Windows のアップグレードおよび EEB

方式	プライマリ	メディア	クライアント
対話形式	p.42 の「Windows システムでローカルサーバー、リモートサーバー、クラスタサーバーのアップグレードを実行する」を参照してください。	p.77 の「NetBackup 10.1 への NetBackup メディアサーバーのアップグレード」を参照してください。 p.105 の「VxUpdate について」を参照してください。	可能。プライマリサーバーについての情報を参照してください。 p.105 の「VxUpdate について」を参照してください。
サイレント	p.54 の「Windows システムでのサイレントアップグレードの実行」を参照してください。	p.54 の「Windows システムでのサイレントアップグレードの実行」を参照してください。 p.105 の「VxUpdate について」を参照してください。	可能。プライマリサーバーについての情報を参照してください。 p.105 の「VxUpdate について」を参照してください。

方式	プライマリ	メディア	クライアント
プッシュまたはリモート	アップグレード: p.42 の「Windows システムでローカルサーバー、リモートサーバー、クラスタサーバーのアップグレードを実行する」を参照してください。 EEB: EEB のプッシュアップグレードは、サードパーティの配備ツールを使用すれば可能な場合があります。Veritas から提供される Chef および SCCM のテンプレートも使用できます。	p.77 の「NetBackup 10.1 への NetBackup メディアサーバーのアップグレード」を参照してください。 p.105 の「VxUpdate について」を参照してください。	可能。プライマリサーバーについての情報を参照してください。 Chef および SCCM のテンプレート https://sort.veritas.com/public/netbackup/deployment p.105 の「VxUpdate について」を参照してください。

VxUpdate について

VxUpdate は、メディアサーバーとクライアント向けのポリシーベースのオンデマンドアップグレードツールを提供します。ポリシー形式により、メディアサーバーおよびクライアントのアップグレード用のツールが簡略化されます。オンデマンド機能は、必要に応じた即時のアップグレードを可能にします。

VxUpdate は、バックアップポリシーに類似した、使い慣れたポリシーベース形式の構成になっています。配備ポリシーを使用して、Veritas から提供される緊急エンジニアリングバイナリのインストールを自動化できます。配備ポリシーを使用すると、配備アクティビティをスケジュールに従って構成および実行したり、クライアントホストの所有者がオンデマンドでアップグレードを実行したりできます。Veritas は、可能な場合はプッシュまたはリモートアップグレードに VxUpdate を使用することをお勧めします。

NetBackup 10.1 の変更について

NetBackup バージョン 10.1 の重要な変更をいくつか次に記述します。詳しくはバージョン 10.1 のNetBackup『 リリースノート』を参照してください。

NetBackup 9.1 以降のインストールとアップグレードに関する Windows コンパイラとセキュリティの要件

NetBackup 9.1 以降の Windows では、Visual Studio 2019 コンパイラと Windows 10 SDK (Software Development Kit) を使用します。インストールとアップグレードプロセスでは、Microsoft 再頒布可能ユーティリティを使用して、Visual Studio 2019 C++ ランタイムライブラリがまだインストールされていない Windows ホストにインストールします。すべてのセキュリティ更新プログラムが適用されていないと、これらのユーティリティがホストで失敗したり、予期しない動作をする可能性があります。Windows ホストで、NetBackup

9.1 以降をインストールするか 9.1 以降にアップグレードする前に、すべてのセキュリティ更新プログラムを適用する必要があります。

Microsoft 再頒布可能ユーティリティについて詳しくは、次を参照してください。
https://visualstudio.microsoft.com/downloads/

次に、失敗と予期しない動作の例を示します。

- NetBackup のインストールまたはアップグレードプロセスが開始直後に失敗し、Visual Studio 2019 C++ ランタイムライブラリを配備できないというメッセージが表示される。
- NetBackup のインストールまたはアップグレードプロセスによって実行された `nbcertcmdtool` アプリケーションが予期せず失敗する。このエラーは、セキュリティ構成が無効または不十分であるために発生する `nbcertcmdtool` エラーと区別することが困難です。
- NetBackup のインストールまたはアップグレードプロセスの終了間際に、MSDP アプリケーションが予期せず失敗する。

この問題を回避するには、インストールまたはアップグレードを試みる前に、すべての Windows セキュリティ更新プログラムを適用します。

Windows Server 2012 R2 および Windows 8.1 の場合、必要なセキュリティ更新プログラムのリストには、KB 2919355 (https://support.microsoft.com/en-us/topic/windows-rt-8-1-windows-8-1-and-windows-server-2012-r2-update-april-2014-3c9d820b-7079-359d-8660-21de648fa31d) が含まれます。

Windows Server 2012 R2、2008 Service Pack 2、Windows 8.1、その他すべての以前にサポートされていたバージョンの場合は、Windows 更新プログラムのユニバーサル C ランタイムをインストールする必要があります。この更新により、NetBackup を正しく実行できます。適切な C++ ランタイムバイナリが確実に存在する最小パッチレベルは、Microsoft KB 3118401 です。これ以降のその他のパッチにもこの修正が含まれているはずです。

この要件について詳しくは、次を参照してください。
https://support.microsoft.com/ja-jp/topic/update-for-universal-c-runtime-in-windows-322bf30f-4735-bb94-3949-49f5c49f4732

一部のコンピュータでは Java GUI と JRE のインストールは省略可能

NetBackup 8.3 以降、Linux メディアサーバーと Windows メディアサーバー、および UNIX クライアントと Linux クライアントでは、Java GUI と JRE パッケージはオプションです。

以前のリリースと同様に、Java GUI および JRE パッケージは必須であるため、すべてのプライマリサーバーに自動的にインストールされます。Java GUI と JRE は、Windows クライアントのデフォルトインストールの一部ではありません。Windows クライアントでこの機能が必要な場合は、Java リモート管理コンソールをインストールしてください。

NetBackup のさまざまなインストール方法が用意されているため、ユーザーは Java GUI や JRE のパッケージをインストールするかどうかを選択できます。インストールまたはアップグレード後の Java GUI や JRE のインストールについての詳しい情報も参照できます。

p.131 の「アップグレード後の Java GUI と JRE の追加または削除」を参照してください。

ログディレクトリの権限はロールバック時にリセットが必要

NetBackup 8.3 Windows のアップグレードが失敗し、以前のバージョンにロールバックする必要がある場合は、`mklogdir` コマンドを使ってログフォルダの権限をリセットする必要があります。NetBackup 8.3 のアップグレードによって、ログフォルダの権限が変更されます。これらの権限は、NetBackup の以前のバージョンとは互換性がありません。NetBackup をロールバックした後、`mklogdir.bat -fixFolderPerm` を実行して、ログフォルダの権限を 8.3 より前の権限に戻します。この要件は、Windows プラットフォームにのみ適用されます。`mklogdir` コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

NetBackup 7.6.0.4 以前からのアップグレードの非サポート

NetBackup をあるリリースから別のリリースにアップグレードするためには、相当なロジックが必要です。効率の観点から、NetBackup 7.6.0.4 以前に固有のアップグレードロジックは廃棄されます。これらのリリースの NetBackup のサポート期間は終了し、サポートされなくなります。NetBackup 7.6.0.4 以前から 10.1 にアップグレードを試みると、インストール前の検査は失敗し、アップグレードを続行できません。

これらのバージョンのいずれかの NetBackup を実行している場合で、NetBackup 10.1 にアップグレードする場合は、踏み台として中間リリースを使用します。サポートされる NetBackup のバージョンの詳細を、次の場所から参照できます。

https://www.veritas.com/content/support/en_US/eosl

NetBackup 8.2 以降でサポートされる外部認証局の証明書

NetBackup は NetBackup 8.2 で外部認証局証明書のサポートを導入しました。この変更により、ホストの検証とセキュリティのため、NetBackup 認証局の代替手段が提供されます。PEM、DER、P7B 形式の証明書をサポートしています。

NetBackup の外部 CA のサポートと CA が署名した証明書について詳しくは、『NetBackup セキュリティ暗号化ガイド』を参照してください。

NetBackup 8.2 の外部認証局の制限事項

- UNC パスまたはネットワークドライブの割り当てが含まれている外部認証局の仕様は、リモートインストール方式を使用する Windows ホストでは失敗します。

リモートインストールを実行する Windows ホストでは、外部 CA 証明書仕様に UNC パスやネットワークドライブの割り当てを使用できません。リモートインストール方式には、VxUpdate とセットアップウィザードのプッシュインストールオプションが含まれます。UNC パスまたは割り当てられたネットワークドライブの使用を試みると、パスにアクセスできないため、事前チェックとインストール操作が失敗します。

Veritas Usage Insights について

Veritas Usage Insights は、NetBackup の配備の効率的な管理、傾向の認識、今後の計画の作成に役立ちます。正確なほぼリアルタイムのレポートで、バックアップされるデータの合計量を確認できます。Usage Insights は、ライセンス付与されている容量の制限を超過しそうになると警告します。Usage Insights には Veritas NetBackup 8.1.2 以降が必要です。

Usage Insights では次のものが提供されます。

- 保護対象テラバイトの正確でほぼリアルタイムのレポート
- グラフィカルに表示される使用傾向
- ライセンス済み容量が超過する前の使用量評価の警告
- 簡単な容量計画と予算策定
- 適用の急増または潜在的なギャップの識別

容量ライセンス (NDMP、限定版、または完全) を使用しているお客様の場合、Usage Insights を使用することで、容量の使用状況を正確に測定できます。この測定により、保護対象の各作業負荷のストレージ使用状況を包括的に把握でき、効率的な容量計画が可能になります。さらに、Usage Insights は必要な遠隔測定データを自動的に提供するため、これらのお客様は遠隔測定データを手動でVeritasにアップロードする必要がありません。

次の URL で、よく寄せられる質問への追加の回答を確認できます。

https://help.veritas.com/vxhelp6/#/?context=veritas_usage_insights_netbackup&token=vui_nbu_faqs

---

注意: Usage Insights は、Google Chrome および Mozilla Firefox と互換性があります。Microsoft Edge または Microsoft Internet Explorer では正しくレンダリングされない情報があるため、これらを使用することはお勧めしません。

---

p.14 の「Veritas Usage Insights のベストプラクティス」を参照してください。

Veritas Usage Insights について詳しくは、『Veritas Usage Insights for NetBackup スタートガイド』を参照してください。

Veritas Usage Insights のベストプラクティス

Veritasでは、Usage Insights ツールの使用に特定のベストプラクティスを推奨しています。

- Usage Insights は、Google Chrome および Mozilla Firefox と互換性があります。Microsoft Edge または Microsoft Internet Explorer では正しくレンダリングされない情報があるため、Veritasではこれらを使用することはお勧めしません。
- 対象となるサイトで、安全な Web トラフィックを伝送できることを確認します。Usage Insights では HTTPS を使用して関連情報を送信します。自動アップロード機能を活用するために、プライマリサーバーでアウトバウンド HTTPS トラフィックを許可する必要があります。手動アップロードには、アップロード場所からの HTTPSトラフィックが必要です。
- カスタマ登録キーはライセンスキーではありません。Usage Insights が機能するためには登録キーが必要ですが、これは NetBackup ライセンスキーではありません。カスタマ登録キーは、Usage Insights の Web サイトからダウンロードできる、Usage Insights に固有のものです。
- 複数のアカウント ID がある場合、カスタマ登録キーをダウンロードするときに、集計登録キーが含まれていることがあります。この集計登録キーには、すべてのアカウント ID が含まれます。すべてのプライマリサーバーに対して、この集計されたキーを使用できます。ただし、NetBackup では、特定のアカウントの ID を持つ特定のキーを特定のプライマリサーバーに割り当てるためのメッセージが表示されます。必要な場合は、すべてのプライマリサーバーに対して、この集計されたキーを使用できます。
- NetBackup 8.1.2 へのインストールとアップグレード中は、インストーラが `veritas_customer_registration_key.json` ファイルを最終的なインストール先にコピーするのを許可します。NetBackup はこの処理を介してファイルの権限と所有権を正しく設定できます。インストールまたはアップグレード以外の処理でこのファイルをシステムに配置すると、処理は正しく動作しない可能性があります。
- NetBackup では、カスタマ登録キーのファイル名に短いファイル名形式 (8.3 形式) を使用することはサポートされていません。
- よく寄せられる質問への回答について詳しくは、次の URL に移動してください。https://help.veritas.com/vxhelp6/#/?context=veritas_usage_insights_netbackup&token=vui_nbu_faqs

カスタマ登録キーをダウンロードするには

1 Google Chrome または Mozilla Firefox を使用して Veritas NetInsights コンソールにログインします。

https://netinsights.veritas.com

2 Veritas Usage Insights のページに移動します。

3 プライマリサーバーの適切なカスタマ登録キーをダウンロードします。

2

アップグレード計画

この章では以下の項目について説明しています。

一般的なアップグレードの計画について

アップグレードの計画について詳しくは、このセクションを確認してください。

NetBackup 10.1 のアップグレード計画について

現在インストールされているバージョンの NetBackup は、NetBackup 10.1 のアップグレード処理に影響します。NetBackup の任意のバージョンからのアップグレードでは、NBDB データベースの再構築と MSDP ローリング変換を計画する必要があります。表 2-1 には、アップグレードに対して実行する必要があるタスクに関する追加情報があります。

表 2-1　インストールされているバージョンに基づいた必要なアップグレードタスク

アップグレードタスク	タスクを実行する必要があるバージョン
NBDB データベースの再構築	すべてのバージョンで NBDB データベースの再構築を実行する必要があります。

アップグレードタスク	タスクを実行する必要があるバージョン
MSDP 変換	MSDP を使う NetBackup 8.0 以前のすべてのバージョンは、MSDP ローリング変換を実行する必要があります。 p.85 の「NetBackup 8.1 での MSDP のアップグレードの考慮事項」を参照してください。

アップグレードを始める前に、メディアキットまたは製品の電子的なイメージファイルに含まれている『NetBackup リリースノート』を確認することをベリタスがお勧めします。Veritas このマニュアルはアップグレードする前によく理解する必要がある、NetBackup 10.1 での重要な変更を記述したものです。

注意: NetBackup 10.1 への正常なアップグレードを確実にするために、次の SORT ページと NetBackup アップグレードポータルを参照してアップグレードの詳細のすべてを確認してください。

SORT ページ:

https://sort.veritas.com/netbackup

p.26 の「Veritas Services and Operations Readiness Tools について」を参照してください。

NetBackup アップグレードポータル:

https://www.veritas.com/support/en_US/article.100032801

---

p.17 の「NetBackup 10.1 へのアップグレードの計画方法」を参照してください。

NetBackup 10.1 へのアップグレードの計画方法

NetBackup 10.1 へのアップグレードの準備段階で複数の要素を検討する必要があります。

管理者以外のユーザーとして NetBackup デーモンおよびサービスの起動

NetBackup 9.1 では、ほとんどの NetBackup デーモンとサービスを root 以外のユーザーとして起動できるようになりました。Veritas は、root 以外のユーザーとして NetBackup サービスを開始することをお勧めします。権限の少ないユーザーを使用する場合は、それに応じて計画する必要があります。ユーザーアカウントが、ディザスタリカバリファイル、外部認証局 (ECA) ファイル、一時ファイルのパスにアクセスできることを確認します。

UNIX と Linux の場合、プライマリサーバーのアップグレード中に新しいプロンプトが表示されます。新しいプロンプトではサービスユーザー (root 以外にすることが望ましい) の

入力を求めるメッセージが表示されます。このユーザーは事前に作成する必要があり、セカンダリグループとして nbwebgrp を指定する必要があります。

Windows では、ローカルサービスの組み込みアカウントをサービスアカウントとして使用できます。このオプションは、プライマリサーバーの[カスタム (Custom)]アップグレードパスで利用可能です。

インストールの完了後に、nbserviceusercmd コマンドを使用してメディアサーバーとクライアントでサービスユーザーを変更できます。nbserviceusercmd 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。サービスユーザーアカウントについて詳しくは、https://www.veritas.com/support/en_US/article.100053035 を参照してください。

Windows では、NetBackup Legacy Network Service や NetBackup Client Service などのサービスが「ローカルシステム」以外の管理者アカウントとして実行されている場合、その[ログオン]の値は変更されません。

クラウド保護ポリシーの変更

ユーザーが NetBackup 9.1 より前の環境から NetBackup 9.1 以降の環境にアップグレードすると、クラウド保護計画が変更されます。アップグレード前の環境に、異なる種類のクラウドプロバイダの複数のクラウド資産を含む保護計画が 1 つある場合、その計画はアップグレード後にクラウドプロバイダの種類ごとに 1 つの保護計画に分割されます。資産は、クラウドプロバイダの種類に基づいて、新しい保護計画間で分散されます。たとえば、Amazon、Azure、Google 資産を含む WeeklyBackups 保護計画があった場合、次のように分割されます。

- WeeklyBackups: Amazon の資産のみが含まれます。
- WeeklyBackups_azure: Azure の資産のみが含まれます。
- WeeklyBackups_gcp: Google の資産のみが含まれます。

メディアサーバー重複排除プールのローリング変換

NetBackup 8.1 のアップグレードには、メディアサーバー重複排除プール (MSDP) のローリング変換が含まれています。

デフォルトでは、ローリング変換はシステムがビジー状態ではないときに実行されます。つまり変換は、バックアップ、リストア、CRQP、CRC チェック、圧縮などが非アクティブのときに実行されます。この変換では、通常のシステム操作への影響は予想されていません。ローリング変換が完了すると、変換後のシステムと新しいインストールの間で違いはありません。ローリング変換に関する詳しい情報を参照できます。

p.85 の「NetBackup 8.1 での MSDP のアップグレードの考慮事項」を参照してください。

p.86 の「MSDP ローリングデータ変換について」を参照してください。

RBAC のセキュリティ管理者の指定

役割ベースのアクセス制御 (RBAC) を使用する場合は、セキュリティ管理者を指定する必要があります。詳細情報を参照できます。

p.132 の「NetBackup Web ユーザーインターフェースについて」を参照してください。

『NetBackup Web UI 管理者ガイド』を参照してください。

NetBackup のインストールとアップグレードのための Web サービスのアカウントの追加

NetBackup 8.0 より、NetBackup プライマリサーバーには、重要なバックアップ操作をサポートするための構成済み Tomcat Web サーバーが含まれます。この Web サーバーは、権限が制限されているユーザーアカウント要素の下で動作します。これらのユーザーアカウント要素は、各プライマリサーバー (またはクラスタ化されたプライマリサーバーの各ノード) で使用できる必要があります。詳細情報を参照できます。

p.126 の「NetBackup プライマリサーバー Web サーバーのユーザーとグループの作成」を参照してください。

メモ: ベリタスは、NetBackup Web サービスに使用するユーザーアカウントの詳細を保存することを推奨します。プライマリサーバーのリカバリでは、NetBackup カタログのバックアップが作成されたときに使われたものと同じ NetBackup Web サービスのユーザーアカウントとクレデンシャルが必要です。

注意: セキュアモードで NetBackup PBX を実行する場合は、Web サービスユーザーを PBX の権限を持つユーザーとして追加します。PBX モードの判別と、正しくユーザーを追加する方法について詳しくは、次をご覧ください。

http://www.veritas.com/docs/000115774

NAT が有効になっている Linux クラスタ化された NetBackup 8.2 のアップグレード

NAT が有効になっている NetBackup 8.2 Linux クラスタのアップグレードによって NAT の状態が誤って識別されます。その結果、10.1 へのアップグレード後に NAT は無効になります。NetBackup 10.1 へのアップグレードが完了したら、NAT を再度有効にする必要があります。アップグレード後の手順に、より詳しい情報が含まれています。

p.68 の「NetBackup 10.1 へのアップグレードのインストール後の手順」を参照してください。

任意の btrfs ファイルシステムから NetBackup データベースへの移行

Veritas は、btrfs ファイルシステムでは NetBackup データベースのインストールまたはアップグレードをサポートしていません。NetBackup データベースが btrfs ファイルシステムに存在する場合、アップグレードを開始する前に、サポートされているファイルシステム (ext4 または xfs) にデータベースを移動します。データベースファイルは、プライマリサーバーのディレクトリ /usr/openv/db に存在します。アップグレード前のデータベースの移動について、詳しい情報を参照できます。p.38 の「NetBackup 10.1 へのアップグレードのプレインストール手順」を参照してください。

証明書キーサイズの環境変数

NetBackup は安全に通信するため、セキュリティ証明書を使用して NetBackup ホストを認証します。セキュリティ証明書は X.509 公開鍵基盤 (PKI) 標準に適合しています。NetBackup プライマリサーバーは、認証局 (CA) として動作し、ホストに電子証明書を発行します。NetBackup は、2048 ビット、3072 ビット、4096 ビット、および 8192 ビットの証明書キーサイズをサポートしています。

NetBackup 9.1 のアップグレードでは、キー強度が 2048 ビットの新しい root CA が配備されます。2048 ビットより大きい証明書キーサイズを使用するには、インストールを開始する前にプライマリサーバーの NB_KEYSIZE 環境変数を設定します。

例:

```
NB_KEYSIZE = 4096
```

NB_KEYSIZE に指定できる値は、2048、3072、4096、8192 のみです。

メモ: プライマリサーバーで FIPS モードが有効になっている場合は、NB_KEYSIZE 環境変数の値として指定できるのは 2048 ビットまたは 3072 ビットのみです。

注意: 使用環境のキーサイズは慎重に選択する必要があります。大きいキーサイズを選択すると、パフォーマンスが低下する場合があります。使用環境に適したキーサイズを判断するには、あらゆる要素を考慮する必要があります。

CA の移行と証明書キーサイズについて詳しくは、『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 2-2はアップグレード手順の概要を示しています。

表 2-2 アップグレード処理の概要

手順	詳細	詳細情報
1	オペレーティングシステムの必要条件を見直し、コンピュータがすべての必要条件を満たしていることを確認します。	p.166 の「UNIX および Linux の場合のアップグレード要件」を参照してください。 p.169 の「Windows および Windows クラスタのアップグレード要件」を参照してください。 p.176 の「Windows クラスタのアップグレードの要件」を参照してください。
2	Web サーバーのユーザーアカウントとグループアカウントが作成され、有効になっていることを確認します。	詳しくは以下を参照してください。 p.126 の「NetBackup プライマリサーバー Web サーバーのユーザーとグループの作成」を参照してください。
3	アップグレード処理を開始する	p.37 の「 プライマリサーバーのアップグレードについて 」を参照してください。

レガシーログディレクトリのセキュリティ更新

NetBackup 10.1 へのアップグレード中に、レガシーログディレクトリの権限は、新しい ALLOW_WORLD_READABLE_LOGS でより制限の厳しいレベルに設定されます。この変更は、機密情報が含まれている可能性のある NetBackup ログへの不正アクセスを防止することを目的としています。

デフォルト値は ALLOW_WORLD_READABLE_LOGS=NO です。この値は NetBackup レガシーログへのアクセスを制限します。

ALLOW_WORLD_READABLE_LOGS を YES に変更することで、ログファイルの権限を制限の少ない設定に変更できます。NetBackup 10.1 へのアップグレード時に制限の少ないログ権限を保持する場合は、アップグレードする前に nbsetconfig コマンドを使用して ALLOW_WORLD_READABLE_LOGS=YES を設定します。

レガシーログの権限を再度制限するには、nbsetconfig を使用して ALLOW_WORLD_READABLE_LOGS=NO を設定します。

nbsetconfig コマンドについては、『NetBackup コマンドリファレンスガイド』を参照してください。

ALLOW_WORLD_READABLE_LOGS 値について詳しくは、『NetBackup ログリファレンスガイド』を参照してください。

通知、メッセージ、耐性の構成情報がアップグレードされない

NetBackup 10.0 より前の環境から NetBackup 10.0 以降へのアップグレード中、以前の通知、メッセージ、および耐性の構成情報は移行されません。以前に追加された

Resiliency Domain は、NetBackup Web インターフェースの[耐性 (Resiliency)]タブに表示されなくなります。

[耐性 (Resiliency)]タブの耐性情報を再構成して再検出するには、参照先のテクニカルノートに示されている手順を実行します。[耐性 (Resiliency)]タブには、Veritas Resiliency Platform (VRP) の構成情報と、その Resiliency Domain に関連するすべてのデータ (管理対象および管理対象外の資産を含む) が表示されます。

Resiliency Domain データを再検出するには、アップグレードの完了後に再構成する必要があります。NetBackup を 10.0 にアップグレードした後に VRP を再構成する方法について詳しくは、参照されているテクニカルノートを参照してください。

https://www.veritas.com/support/ja_JP/article.100052464

NetBackup 10.0 へのアップグレードの一環として移行されない情報は、次のファイルに格納されます。

- `vrp-h2-store.mv.db`
- `messages-h2-store.mv.db`
- `notifications-h2-store.mv.db`

これらのファイルは、プライマリサーバー上の次のディレクトリに保持されます。削除しないかぎり、これらのファイルは指定した場所に残ります。これらのファイルは、NetBackup 10.0 以降の環境では使用できません。

- Windows ファイル:

  install_path¥NetBackup¥var¥global¥wmc¥h2stores¥vrp-h2-store.mv.db

  install_path¥NetBackup¥var¥global¥wmc¥h2stores¥messages¥messages-h2-store.mv.db

  install_path¥NetBackup¥var¥global¥wmc¥h2stores¥notifications¥notifications-h2-store.mv.db

- Linux ファイル:

  /usr/openv/var/global/wmc/h2stores/vrp-h2-store.mv.db

  /usr/openv/var/global/wmc/h2stores/messages/messages-h2-store.mv.db

  /usr/openv/var/global/wmc/h2stores/notifications/notifications-h2-store.mv.db

カタログバックアップの既知の制限事項

Veritas は、NetBackup のバージョンが混在するバックアップ環境をサポートします。ただし、NetBackup カタログのバックアップを作成する場合は制限事項があります。

プライマリサーバーが別のメディアサーバーにカタログのバックアップを実行する場合に、メディアサーバーでプライマリサーバーと同じバージョンの NetBackup を使う必要があり

ます。NetBackup カタログがプライマリサーバー上に存在するため、プライマリサーバーはカタログバックアップのクライアントであると見なされます。

そのため、メディアサーバーの NetBackup のバージョンはプライマリサーバーと同じである必要があります。

メディアサーバーの NetBackup と同じバージョンを使わないと、カタログデータが適切に保護されません。

バージョン混在のサポートに関する詳しい情報を参照できます。

p.165 の「NetBackup のバージョン間の互換性について」を参照してください。

NetBackup ホスト用のセキュリティ証明書について

NetBackup では、NetBackup ホストの認証にセキュリティ証明書を使用します。NetBackup セキュリティ証明書は、X.509 公開鍵基盤 (PKI) 標準に適合しています。プライマリサーバーは、NetBackup 認証局 (CA) として動作し、ホストに NetBackup 証明書を発行します。

NetBackup は、ホスト ID ベースとホスト名ベースの 2 種類の NetBackup ホストセキュリティ証明書を提供します。ホスト ID ベース証明書は、各 NetBackup ホストに割り当てられる UUID (Universal Unique Identifier) に基づいています。NetBackup プライマリサーバーは、これらの識別子をホストに割り当てます。

NetBackup 8.0 以前に生成されたすべてのセキュリティ証明書は、現在ホスト名ベースの証明書と呼ばれます。NetBackup は、これらの古い証明書を新しいホスト ID ベースの証明書に置き換える移行を進めています。この移行は今後のリリースで完了し、ホスト名ベース証明書は使用されなくなる予定です。ただし移行はその途上にあり、特定の処理では最新の NetBackup バージョンに引き続き過去のホスト名ベース証明書が必要です。

NetBackup では、NetBackup 認証局または外部認証局が発行した証明書をホストの認証に使用します。プライマリサーバーで外部証明書を使用する場合は、インストール後のプロセスで証明書を構成します。外部証明書を使用するメディアサーバーやクライアントでは、インストール時またはアップグレード時、あるいはインストール後またはアップグレード後に外部証明書を構成できます。

インストール後の処理について詳しくは、
https://www.veritas.com/support/en_US/article.100044300 を参照してください。

NetBackup での外部 CA のサポート、および外部 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。

アップグレードによるファイルの自動変更について

以前のバージョンの NetBackup からアップグレードする場合、特定のカスタマイズ可能なスクリプトが上書きされます。NetBackup では、これらのスクリプトを上書きする前にスクリプトのコピーが保存され、すべての変更が保持されます。

UNIX および Linux の場合

表 2-3 UNIX および Linux の保護パスおよびファイル

保護対象のパスまたはファイル	処理
/usr/openv/netbackup/bin/initbpdbm /usr/openv/netbackup/bin/initbprd	現在の NetBackup バージョンの番号がファイル名に追記されます。 例: initbpdbm.*version*
/usr/openv/netbackup/nblog.conf	アップグレード時に、ファイルに接尾辞が追加されます。詳しくは、アップグレードの完了後に /usr/openv/netbackup ディレクトリの内容を確認してください。
/usr/openv/msg/C /usr/openv/netbackup/bin/goodies /usr/openv/netbackup/bin/help /usr/openv/volmgr/help	ディレクトリ全体がディレクトリ名と現在のバージョン番号に移行されます。 例: /usr/openv/netbackup/ bin/goodies.*version*

Windows の場合

表 2-4 Windows の保護対象のパスとファイル

保護対象のパスまたはファイル	処理
install_path¥NetBackup¥nblog.conf	ファイルは *install_path*¥NetBackup¥ bin.*original_version* ディレクトリにコピーされます。 *original_version* 値は、アップグレードを開始する前の NetBackup のバージョンです。 例: *install_path*¥NetBackup¥bin.*version*

保護対象のパスまたはファイル	処理
install_path¥NetBackup¥bin¥goodies¥netbackup.adm *install_path*¥NetBackup¥bin¥goodies¥help_script.cmd *install_path*¥NetBackup¥bin¥goodies¥available_media.cmd *install_path*¥NetBackup¥bin¥goodies¥check_coverage.cmd *install_path*¥NetBackup¥bin¥goodies¥cleanstats.cmd *install_path*¥NetBackup¥bin¥goodies¥duplicate_images.cmd *install_path*¥NetBackup¥bin¥goodies¥verify_images.cmd *install_path*¥NetBackup¥bin¥goodies¥bpstart_notify *install_path*¥NetBackup¥bin¥goodies¥bpend_notify	ファイルは *install_path*¥NetBackup¥bin¥goodies.*release* ディレクトリにコピーされます。 ***release*** 値は NetBackup の現在のバージョンです。 例: *install_path*¥NetBackup¥bin¥goodies.*version*¥netbackup.adm

アップグレード前のジョブデータベースのサイズの削減

ジョブデータベースが Web サービスのメモリにキャッシュされるようになりました。アップグレード後に、資産レベルでのアクセス制御を可能にするため、既存の VMware ジョブと RHV (Red Hat Virtualization) ジョブに資産の名前空間が割り当てられます。この処理には時間がかかる場合があります。関連付けを実行し、Web サービスのパフォーマンスに与える影響を最小限に抑えるため、アップグレードの前にジョブデータベースのサイズを削減する必要があります。非常に大規模なジョブデータベースでは、ヒープ領域の高使用率に関連したアラートが表示される場合があります。ジョブデータベースのサイズの削減、または Web サービスの最大ヒープサイズの増加について詳しくは、次の記事を参照してください。

http://www.veritas.com/docs/100049808

SUSE Linux プライマリサーバーのアップグレードに関する既知の問題

まれに、SUSE Linux プライマリサーバーのインストール前チェッカーで、webservice ユーザーまたは webservice グループが存在しないと報告される場合があります。

ユーザーとグループが想定どおりに存在することを検証し、アップグレードを再実行してください。

問題が解決しない場合は、インストール前チェッカーのエラーを上書きするように環境変数を設定し、操作を再実行します。

```
NBPREINSTALL_CRITICAL_OVERRIDE=YES
```

パフォーマンスと調整に関する注意事項

『NetBackup Backup Planning and Performance Tuning ガイド』には、現場の経験に基づいた環境に関する推奨事項が記載されています。特定の環境では、異なる注意事項が必要になる場合があります。

管理者は、このガイドを使用して、特定の NetBackup 環境の NetBackup のパフォーマンスを分析、評価、調整する必要があります。表示される情報を使用して、次の項目を決定します。

- NetBackup プライマリサーバーのサイズ要件。
- 必要な CPU、ディスクドライブ、テープドライブの数。
- さまざまな作業負荷に対して NetBackup を最適化する最善の方法。
- バックアップパフォーマンスを最大にするための調整パラメータ。
- リカバリ時間を短縮するための適切な戦略。
- NetBackup によるデータの処理方法を理解するための利用可能なツール。

追加情報に関しては、『NetBackup Backup Planning and Performance Tuning ガイド』を参照してください。

アップグレードツールについて

SORT (Services and Operations Readiness Tools) やインストール前チェッカーなどのアップグレードツールについて詳しくは、このセクションを確認してください。

Veritas Services and Operations Readiness Tools について

Veritas Services and Operations Readiness Tools (SORT) は、Veritas エンタープライズ製品をサポートするスタンドアロンと Web ベースの強力なツールセットです。NetBackup では、SORT によって、複数の UNIX/Linux または Windows 環境にまたがってホストの設定を収集、分析、報告する機能が提供されます。このデータは、システムで NetBackup の最初のインストールまたはアップグレードを行う準備ができているかどうかを評価するのに役立ちます。

次の Web ページから SORT にアクセスします。

https://sort.veritas.com/netbackup

SORT ページに移動すると、次のようにより多くの情報を利用可能です。

- インストールとアップグレードのチェックリスト
  このツールを使うと、システムで NetBackup のインストールまたはアップグレードを行う準備ができているかどうかを確認するためのチェックリストを作成できます。このレポートには、指定した情報に固有のソフトウェアとハードウェアの互換性の情報がす

べて含まれています。さらに、製品のインストールまたはアップグレードに関する手順とその他の参照先へのリンクも含まれています。

- Hotfix と EEB Release Auditor
  このツールを使うと、インストールする予定のリリースに必要な Hotfix が含まれているかどうかを調べることができます。
- カスタムレポート
  このツールを使うと、システムと Veritas エンタープライズ製品に関する推奨事項を取得できます。
- NetBackup のプラットフォームと機能の今後の予定
  このツールを使用すると、今後 Veritas が新しい機能や改善された機能と置き換える項目に関する情報を入手できます。さらに、今後 Veritas が置き換えることなく廃止する項目に関する情報を入手することもできます。これらの項目のいくつかには NetBackup の特定の機能、サードパーティ製品の統合、Veritas 製品の統合、アプリケーション、データベースおよび OS のプラットフォームが含まれます。

SORT ツールのヘルプが利用可能です。SORT ホームページの右上隅にある[ヘルプ(Help)]をクリックします。次のオプションがあります。

- 実際の本のようにページをめくってヘルプの内容を閲覧する
- 索引でトピックを探す
- 検索オプションを使ってヘルプを検索する

SORT のアップグレードのための推奨手順

Veritas は現在の NetBackup ユーザーに対して、SORT の最初の導入時に一覧表示される 4 つの手順を実行することをお勧めします。このツールには他にも多くの機能が備わっていますが、これらの手順はすでに NetBackup を使っているユーザーにとって SORT の概要を知る上で役立ちます。さらに、これらの手順を実行することで、その他の SORT 機能に関する有用で基本的な知識が備わります。

表 2-5

手順	詳細
SORT Web ページに Veritas Account を作成します。	p.28 の「SORT ページに Veritas Account を作成する方法」を参照してください。
システム固有のインストールレポートを作成します。	p.29 の「システム固有のインストールレポートを作成する方法 (Windows の場合)」を参照してください。 p.29 の「システム固有のインストールレポートを作成する方法 (UNIX または Linux の場合)」を参照してください。

手順	詳細
今後のプラットフォームと機能の予定を確認します。	p.31 の「今後のプラットフォームの変更と機能の予定を確認する方法」を参照してください。
Hotfix と EEB Release Auditor の情報を確認します。	p.31 の「Hotfix と EEB の情報を確認する方法」を参照してください。

SORT ページに Veritas Account を作成する方法

1 Web ブラウザで、次の場所に移動します:

https://sort.veritas.com/netbackup

2 右上で[ログイン (Login)]をクリックしてから、[今すぐ登録 (Register now)]をクリックします。

3 要求された次のログインおよび連絡先情報を入力します:

電子メールアドレス (Email address)	電子メールアドレスを入力し、検証してください
パスワード (Password)	パスワードを入力し、検証してください
名 (First name)	名を入力してください
姓 (Last name)	姓を入力してください
会社名 (Company name)	会社名を入力してください
国 (Country)	国を入力してください
優先言語 (Preferred language)	優先言語を選択してください
CAPTCHA テキスト (CAPTCHA text)	表示される CAPTCHA テキストを入力してください。必要に応じて、イメージを更新してください。

4 [送信 (Submit)]をクリックします。

5 ログイン情報の受信時に SORT にログインしてカスタマイズした情報のアップロードを開始できます。

システム固有のインストールレポートを作成する方法 (Windows の場合)

1. SORT の Web サイトに移動します。

   https://sort.veritas.com/netbackup

2. [インストールとアップグレード (Installation and Upgrade)]セクションで、[SORT データコレクタによるインストールとアップグレードのカスタムレポート (Installation and Upgrade custom reports by SORT data collectors)]を選択します。

3. [データコレクタ]タブを選択します

4. [グラフィカルユーザーインターフェース (Graphical User Interface)]のラジオボタンを選択して、プラットフォームに対して適切なデータコレクタをダウンロードします。

   データコレクタは OS 固有です。Windows コンピュータに関する情報を収集するには、Windows データコレクタが必要です。UNIX または Linux コンピュータに関する情報を収集するには、UNIX または Linux データコレクタが必要です。

5. ダウンロードが終わったら、データコレクタを起動します。

6. [ようこそ (Welcome)]画面の[製品ファミリー (product family)]セクションで NetBackup を選択して、[次へ (Next)]をクリックします。

7. [システムの選択 (System Selection)]画面で、分析するすべてのコンピュータを追加します。[参照 (Browse)]をクリックすると、分析に追加可能なコンピュータのリストを確認できます。Veritas 管理者アカウントまたは root アカウントでツールを起動することをお勧めします。

8. すべてのシステムを選択したら、[システム名 (System names)]セクションを確認して[次へ (Next)]をクリックします。

9. [検証オプション (Validation Options)]画面の[検証オプション (Validation options)]下で、アップグレード後のバージョンを選択します。

10. [次へ (Next)]をクリックして続行します。

11. ユーティリティによって要求されたチェックが実行され、結果が表示されます。レポートをマイ SORT にアップロードできます。また結果を印刷したり保存できます。Veritas 分析を一元管理しやすくするために、結果はマイ SORT Web サイトにアップロードすることをお勧めします。[アップロード (Upload)]をクリックして、マイ SORT のログイン情報を入力すると、データがマイ SORT にアップロードされます。

12. 終了したら、[完了(Finish)]をクリックしてユーティリティを閉じます。

システム固有のインストールレポートを作成する方法 (UNIX または Linux の場合)

1. SORT の Web サイトに移動します。

   https://sort.veritas.com/netbackup

2. [インストールとアップグレード (Installation and Upgrade)]セクションで、[SORT データコレクタによるインストールとアップグレードのカスタムレポート (Installation and Upgrade custom reports by SORT data collectors)]を選択します。

3 [データコレクタ]タブを選択します。

4 プラットフォームに対して適切なデータコレクタをダウンロードします。

データコレクタは OS 固有です。Windows コンピュータに関する情報を収集するには、Windows データコレクタが必要です。UNIX または Linux コンピュータに関する情報を収集するには、UNIX または Linux データコレクタが必要です。

5 ダウンロード済みのユーティリティを含むディレクトリに変更します。

6 実行 (Run). `/sortdc`

ユーティリティによって、最新バージョンのユーティリティがインストールされていることを確認するためのチェックが実行されます。さらに、ユーティリティによって、最新のデータが含まれているかどうかがチェックされます。この処理の後、ユーティリティによって、このセッションのログファイルの場所がリストされます。

7 要求されたら、Enter キーを押して続行します。

8 メインメニューで[NetBackup ファミリー (NetBackup Family)]を選択します。

9 [何をしますか? (What task do you want to accomplish?)]というプロンプトが表示されたら、[インストール/レポートのアップグレード (Installation/Upgrade report)]を選択します。

カンマで項目を区切ることで、複数のオプションを選択できます。

10 レポートに含めるシステムを指定します (複数可)。

指定したシステムで以前にレポートを実行していた場合は、そのレポートを再び実行するようプロンプトが表示されます。[はい (Yes)]を選択すると、レポートが再実行されます。

ユーティリティによって、セッションのログファイルの場所が再びリストされます。

ユーティリティの進捗状況が画面に表示されます。

11 インストールまたはレポートをアップグレードする製品に関するプロンプトが表示されたら、NetBackup を指定します。

12 インストールする NetBackup のバージョンに対応する数字を入力します。

ユーティリティによって、セッションのログファイルの場所が再びリストされます。

ユーティリティの進捗状況が画面に表示されます。

13 ユーティリティによって、レポートをオンラインで確認する場合には SORT Web サイトにアップロードするよう促すプロンプトが表示されます。オンラインレポートを利用すると、システム上のテキストベースのレポートよりも詳細な情報を入手できます。

14 タスクが完了したら、ユーティリティを終了できます。オプションでツールに関するフィードバックを提供できます。Veritas はフィードバックを基にツールの改良を実施しています。

今後のプラットフォームの変更と機能の予定を確認する方法

1. Web ブラウザで、次の場所に移動します:

   https://sort.veritas.com/netbackup

2. [NetBackup のプラットフォームと機能の今後の予定 (NetBackup Future Platform and Feature Plans)]ウィジェットを見つけて選択します。
3. [情報の表示 (Display Information)]を選択します。
4. 表示される情報を確認します
5. 任意 - サインインによる通知の作成 - [サインインによる通知の作成 (Sign in and create notification)]をクリックします。

Hotfix と EEB の情報を確認する方法

1. Web ブラウザで、次の場所に移動します:

   https://sort.veritas.com/netbackup

2. [NetBackup Hotfix と EEB Release Auditor (NetBackup Hot Fix and EEB Release Auditor)]ウィジェットを見つけて選択します。
3. Hotfix または緊急エンジニアリングバイナリ (EEB) の情報を入力します。
4. [検索 (Search)]をクリックします。
5. 新しいページに、以下の列が含まれた表が表示されます。

EEB 識別子の Hotfix (Hot fix of EEB Identifier)	前の画面で入力した Hotfix または EEB 番号が表示されます。
説明 (Description)	Hotfix または EEB に関連付けられた問題の説明が表示されます。
解決済みのバージョン (Resolved in Versions)	この問題が解決された NetBackup のバージョンが示されます。

NetBackup インストール前チェッカーについて

NetBackup インストーラにはインストール前チェッカーが含まれています。この機能を使用すると、コンピュータの正常なインストールまたはアップグレードの準備ができているか判断しやすくなります。

このチェックは、アップグレードを開始する際に自動的に実行されます。チェックの結果は次のポイントで示されます。

このチェックは、プライマリサーバーまたはメディアサーバーでインストールまたはアップグレードを開始する際に自動的に実行されます。チェックの結果は次のポイントで示されます。

- Linux のアップグレードスクリプト
  エンドユーザー使用許諾契約に同意してから、インストールを開始するまでの間。
- Windows のインストールウィザード
  [Installation Summary]が表示される[Ready to Install the Program]画面

また、インストール前チェッカーは VxUpdate から実行することもできます。p.105 の「VxUpdate について」を参照してください。

NetBackup は、インストールまたはアップグレードの開始時にチェックを行うインストール前プログラムを使用します。このチェックでは、正常に運用するために削除できる既知の問題を調べることができます。実行されるチェックは、インストール時やアップグレード時に発生した以前の問題に関して、お客様からいただいたご意見に基づいて開発されました。お客様から新たにフィードバックをいただいた場合、ベリタスはこのチェッカーを更新する可能性があります。更新は、NetBackup のリリースには依存しません。サーバーが telemetry.veritas.com に接続できる場合、インストールやアップグレードを開始すると、NetBackup がチェッカーを最新のバージョンに自動的に更新します。

実行されるテストの 1 つは、ローカルにインストールされた EEB（Emergency Engineering Binary の略で、緊急エンジニアリングバイナリの意味）の更新とインストール中の NetBackup のバージョンに含まれている修正の比較です。インストール前テストのうちいずれかが失敗すると、必要な操作の種類を示すメッセージが表示されます。

一部のテスト失敗は軽微なものと見なされ、アップグレードの続行が許可されます。重要なテスト失敗があると、インストールまたはアップグレードの実行が妨げられます。この出力は、インストールまたはアップグレードを安全に続行する前に他の処置を講じる必要があることが通知されます。

インストール前チェックの結果は次の場所に格納されます。

- Linux
  次のパスにあるインストールトレースファイル
  `/usr/openv/tmp`
- Windows
  bpimage コマンドは次のディレクトリにファイルを作成します。
  `%ALLUSERSPROFILE%¥Veritas¥NetBackup¥InstallSummary¥`

アップグレードに関する注意事項および制限事項

アップグレードの操作に関する注意事項、制限事項、要件について詳しくは、このセクションを確認してください。

NetBackup Web サーバーをサポートするユーザーアカウントの作成

NetBackup 8.0 より、NetBackup プライマリサーバーには、重要なバックアップ操作をサポートするための構成済み Web サーバーが含まれます。この Web サーバーは、権限

が制限されているユーザーアカウント要素の下で動作します。これらのユーザーアカウント要素は、各プライマリサーバー (またはクラスタ化されたプライマリサーバーの各ノード) で使用できる必要があります。

多数の手順を実行すると、オペレーティングシステムでユーザーとグループを作成できます。特定のいくつかの方法を示していますが、他の方法でも同じ目標を達成できる可能性があります。ホームディレクトリのパス、ユーザー名、およびグループ名はハードコードされていないため、変更することができます。デフォルトのローカルユーザー名は nbwebsvc、デフォルトのローカルグループ名は nbwebgrp です。

メモ: Linux プラットフォームの場合、UID はクラスタ環境の各ローカルアカウントと同じである必要があります。すべてのクラスタノードでローカルアカウントが一貫して定義されていることを確認します。

Linux でユーザーアカウントとユーザーグループを作成する方法

1. 次のコマンドでローカルグループを作成します。

   コマンド: `# groupadd group_name`

   例: `# groupadd nbwebgrp`

2. 次のコマンドでローカルユーザーアカウントを作成します。

   コマンド: `# useradd -g group_name -c comment -d /usr/openv/wmc user_name`

   例: `# useradd -g nbwebgrp -c 'NetBackup Web Services application account' -d /usr/openv/wmc nbwebsvc`

Windows でユーザーアカウントとユーザーグループを作成する方法

メモ: Windows 上のクラスタ環境のドメインアカウントを使う必要があります。

メモ: Web サービスのユーザーアカウント名は 20 文字に制限されます。

---

1. 次のコマンドでローカルユーザーアカウントを作成します。

   コマンド: `C:¥>net user user_name StrongPassword /add` (*StrongPassword* はアカウントに関連付ける強いパスワードです)

   例: `C:¥>net user nbwebsvc 1U*s7lQ# /add`

2. 次のコマンドでローカルグループを作成します。

   コマンド: `C:¥>net localgroup group_name /add`

   例: `C:¥>net localgroup nbwebgrp /add`

3 次のコマンドで新しいユーザーを新しいグループのメンバーにします。

コマンド: `C:¥>net localgroup group_name user_name /add`

例: `C:¥>net localgroup nbwebgrp nbwebsvc /add`

4 次のように、新しいユーザーに[サービスとしてログオン]の権限を付与します。

- [コントロールパネル]、[管理ツール]、[ローカルセキュリティポリシー]の順に進みます。
- 次に[セキュリティの設定]で、[ローカルポリシー]から[ユーザー権利の割り当て]をクリックします。
- [サービスとしてログオン]を右クリックして[プロパティ]を選択します。
- ローカルユーザーを追加します。
- 変更を保存して[サービスとしてログオン]のプロパティのダイアログボックスを閉じます。

これらの要件のいずれかが満たされていない場合、NetBackup プライマリサーバーのインストールは失敗します。Windows では、インストールプロセスの一部として、ユーザーアカウントのパスワードを指定するように求められます。

NetBackup 10.1 による RHEL 7.5 以降でのファイバートランスポートメディアサーバーのサポートについて

RHEL 7.5 以降でファイバートランスポートメディアサーバー (FTMS) を使用する計画がある場合は、必ず NetBackup を 8.1.2 以降にアップグレードしてください。また、NetBackup 8.1.2 以降が配備された新しい RHEL 7.5 以降のリリースのシステムを使用することもできます。

RHEL を 7.5 以降のリリースにアップグレードする前に、次の手順を実行します。

1 FTMS を無効にします。

2 NetBackup を 8.1.2 以降にアップグレードします。

3 RHEL を 7.5 以降のリリースにアップグレードし、その後 FTMS を再構成します。

FTMS の再構成について詳しくは、『NetBackup SAN クライアントおよびファイバートランスポートガイド』を参照してください。

NetBackup 8.1 での MSDP の変更

NetBackup 7.7.x または 8.0 から 8.1 へのアップグレードには、メディアサーバー重複排除プール (MSDP) のローリングデータ変換が含まれています。この変換はバックグラウンドで動作し、既存のすべてのデータコンテナを AES 暗号化と SHA2 指紋アルゴリズムに変換します。`crcontrol` コマンドを使用してローリングデータ変換を管理および監視できます。`crcontrol` コマンドの使用についての詳しい情報を参照できます。『Veritas

NetBackup 重複排除ガイド』のローリングデータ変換のセクションを参照してください。さらに、『NetBackup コマンドリファレンスガイド』の crcontrol コマンドを参照してください。

ローリング変換は、システムがビジー状態ではないときに実行されます。つまり変換は、バックアップ、リストア、CRQP、CRC チェック、圧縮などが非アクティブのときに実行されます。この変換では、通常のシステム操作への影響は予想されていません。ローリング変換が完了すると、変換後のシステムと新しいインストールの間で違いはありません。

NetBackup のアップグレード中に変換プロセスの明示的な手順は不要です。アップグレード後、ローリング変換はバックグラウンドで動作を開始します。ローリング変換が開始されると、元の NetBackup バージョンに戻すことはできません。ローリング変換に関する詳しい情報を参照できます。『Veritas NetBackup 重複排除ガイド』のローリングデータ変換のセクションを参照してください。

NetApp クラスタに必要になる可能性のある変更

10.1 アップグレードの一環として、任意の NetApp クラスタの設定を見直します。クラスタモードが Node Scope Mode に設定されている場合は、Veritas と NetApp 社の両方が、Vserver 対応モードへの変更を推奨しています。アップグレードの一環として Vserver 対応モードへの移行を計画する場合は、ファイラそれぞれに対する詳細なイメージレポートを作成します。bpimagelist コマンドを使って、このリストを生成します。環境のサイズによっては、この操作に時間がかかる場合があります。詳細情報を参照できます。

p.158 の「NetApp クラスタのためのアップグレード前の追加手順」を参照してください。

Bare Metal Restore 情報がエラー自動イメージレプリケーションを使って複製されるときのエラー

BMR (Bare Metal Restore) 情報の正常な AIR (Auto Image Replication の略で自動イメージレプリケーションの意味) には 2 つのことが必要です。1 つは、ターゲットドメインのプライマリサーバーで BMR が有効になっている必要があります。2 つ目に、ターゲットドメインのプライマリサーバーは BMR 情報を送信するあらゆるクライアントと同等以上の NetBackup のバージョンである必要があります。たとえば、ターゲットドメインのプライマリサーバーが NetBackup 10.1 で元のドメインのクライアントが 7.7.3 である場合には、AIR は正しく機能します。

元のドメインのクライアントが NetBackup 10.1 でターゲットドメインのプライマリが 7.7.3 である場合には、BMR 情報は複製できません。他の情報はすべて正常に送信され、BMR 情報だけが複製されません。クライアントの内容はリストアできますが、BMR を使うことはできません。

このトピックに関する詳細情報を参照できます。

http://www.veritas.com/docs/TECH211267

バージョン 8.1 より前のクライアントと 8.1 以降のメディアサーバーでのアップグレードの問題

NetBackup 8.1 のアップグレードで、指紋をとるアルゴリズムは MD5 から SHA2 にアップグレードされ、セキュリティの脆弱性に対する保護が向上しました。Veritas では、既存の MD5 の指紋データを SHA2 に変換するために、ローリング変換とインライン変換の 2 つの変換方式が導入されました。問題は、次の条件下で発生します。

- クライアントがバージョン 8.1 より前の NetBackup
- クライアントで Client Direct (クライアントで重複排除を実行する) を使用している
- NetBackup 8.1 以降のメディアサーバーでクライアントのバックアップを作成している

これらの条件下では、指紋の変換はインラインで行われます。その結果、バックアップパフォーマンスに悪影響が与えられ、メディアサーバーで CPU の処理負荷が増加します。メディアサーバーで、MD5 の情報を再ハッシュして SHA2 の指紋を作成する必要があります。

この問題を防ぐには、次の操作を行います。

- バージョン 8.1 より前のクライアントの場合、NetBackup 8.1 以降のメディアサーバーでメディアサーバー重複排除 (MSDP) を使用するようにバックアップを変更します。この処理により、バックアップでのインライン変換の実行を防ぎます。
- 8.1 以降のメディアサーバーでバックアップが作成されている 8.1 より前のクライアントで、Client Direct を使用しないでください。

3

プライマリサーバーのアップグレード

この章では以下の項目について説明しています。

プライマリサーバーのアップグレードについて

使用環境の他のコンピュータの NetBackup をアップグレードする場合は、まずプライマリサーバーの NetBackup をアップグレードします。プライマリサーバーのアップグレードが終了したらメディアサーバーをアップグレードし、次にクライアントをアップグレードします。NetBackup は、バージョンが混在する環境をサポートします。このトピックに関する詳細情報を参照できます。

p.165 の「NetBackup のバージョン間の互換性について」を参照してください。

プライマリサーバーのアップグレード方法として、NetBackup アップグレードスクリプトによる方法と、UNIX および Linux のネイティブインストーラによる方法の 2 種類をサポートしています。NetBackup アップグレードスクリプトによる方法は標準的なアップグレード方法で、新規ユーザーにお勧めです。UNIX および Linux のネイティブインストーラによる方法は難易度が高い場合があり、追加の手順も必要です。

NetBackup には、NetBackup のサポート対象バージョンすべての管理コンソールが含まれています。NetBackup のサポート対象バージョンについて詳しくは、次を参照してください。

https://sort.veritas.com/eosl

メモ: NetBackup のサーバーソフトウェアをインストールまたはアップグレードした後に、ホストにあるリモート管理コンソール (Windows と Java) の古いバージョンをアンインストールすることをお勧めします。ネイティブの Windows 版 NetBackup 管理コンソールがある場合は、NetBackup サーバーソフトウェアをインストールまたはアップグレードするときに自動的にその管理コンソールがアンインストールされます。

---

p.165 の「NetBackup のバージョン間の互換性について」を参照してください。

アップグレードに進みます。

p.38 の「NetBackup 10.1 へのアップグレードのプレインストール手順」を参照してください。

NetBackup 10.1 へのアップグレードのプレインストール手順

プライマリサーバーを NetBackup 10.1 にアップグレードするには、次の手順を実行します。

ガイド付き方式に必要な追加手順を実行できるようにするいくつかのツールを使用できます。詳しくは、Business Critical Services (BCS) の担当者にお問い合わせください。

NetBackup アップグレードに RHEL 7.5 へのアップグレードが含まれており、ファイバートランスポートメディアサーバー (FTMS) を使用する場合には、追加の手順が必要になります。詳細情報を参照できます。

p.34 の「NetBackup 10.1 による RHEL 7.5 以降でのファイバートランスポートメディアサーバーのサポートについて」を参照してください。

メモ: Global Cluster Option (GCO) を使ってグローバルにクラスタ化されたプライマリサーバーを含む NetBackup のインストールでは、このマニュアルのアップグレード計画のガイドラインに従ってください。これらのサーバーをアップグレードする手順については、次のドキュメントを参照してください:
https://www.veritas.com/support/en_US/article.100041191

NetBackup 10.1 にアップグレードしてイメージメタデータの移行を完了するためのインストール前手順

1 SORT ツールを使用して環境チェックを実行します。

p.27 の「SORT のアップグレードのための推奨手順」を参照してください。

2 Veritas Usage Insights のカスタマ登録キーをダウンロードします。Veritas Usage Insights に関する詳しい情報を参照できます。

p.13 の「Veritas Usage Insights について」を参照してください。

NetBackup 10.1 へのインストールとアップグレード中は、インストーラが `veritas_customer_registration_key.json` ファイルを最終的なインストール先にコピーするのを許可してください。NetBackup はこの処理を介してファイルの権限と所有権を正しく設定できます。インストールまたはアップグレード以外の処理でこのファイルをシステムに配置すると、処理は正しく動作しない可能性があります。

3 (該当する場合) Linux で、NetBackup データベースファイルが `btrfs` ファイルシステムに存在する場合、アップグレードの前に、サポートされているファイルシステム (`ext4` または `xfs` など) にデータベースファイルを移動します。`btrfs` ファイルシステムに NetBackup データベースを配置することはサポートされていません。データベースファイルは、プライマリサーバーのディレクトリ `/usr/openv/db` に存在します。

Linux で NetBackup データベースファイルを移動するには:

- カタログバックアップを実行します。
- すべての NetBackup デーモンを停止します。
  `/usr/openv/netbackup/bin/bp.kill_all`
- SQL Anywhere デーモンを起動します。
  `/usr/openv/netbackup/bin/nbdbms_start_stop start`
- 既存のデータ、インデックス、トランザクションログファイルを移動します。
  `/usr/openv/db/bin/nbdb_move -data` *`data_directory`* `-index` *`index_directory`* `-tlog` *`log_directory`*
  ミラー化されたトランザクションログを使用する場合、次のコマンドを使用します。
  `/usr/openv/db/bin/nbdb_move -data` *`data_directory`* `-index` *`index_directory`* `-tlog` *`log_directory`* `-mlog` *`log_mirror_directory`*
- すべての NetBackup デーモンを起動します。

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

- カタログバックアップを実行します。

4 (該当する場合) Windows の場合は、すべてのオペレーティングシステムの更新プログラムとセキュリティ更新プログラムを適用してください。詳細情報を参照できます。

p.10 の「NetBackup 9.1 以降のインストールとアップグレードに関する Windows コンパイラとセキュリティの要件」を参照してください。

5 NetBackup の各自の環境に応じて通常実行するアップグレード前のタスクを実行します。次に例を示します。

- すべてのカスタマイズされたスクリプトやサードパーティのスクリプトを停止します。
- クラスタ固有のタスクを実行します。
- ホットカタログバックアップを実行します。
- すべてのストレージライフサイクルポリシー (SLP) を無効にします。
- NetBackup のすべてのポリシーを無効にします。
- NetBackup 7.5.*x* より前のすべての環境ですべてのディスクステージングストレージユニットを無効にします。
- VMware と RHV (Red Hat Virtualization) 環境では、アップグレードする前にジョブデータベースのサイズを削減します。アップグレード後に、資産レベルでのアクセス制御を可能にするため、既存の VMware ジョブと RHV ジョブに資産の名前空間が割り当てられます。この処理には時間がかかる場合があります。このプロセスに関する詳細情報を参照できます。
  p.25 の「 アップグレード前のジョブデータベースのサイズの削減 」を参照してください。
- クラスタシステムの場合のみ、次の NetBackup リソースをオフラインにします。
  - Windows Server Failover Clusters (WSFC): ディスク、仮想名、仮想 IP アドレスを除くすべての NetBackup グループのリソースをオフラインにします。クラスタアドミニストレータインターフェースを使用して NetBackup グループのリソースをオフラインにする方法については、Microsoft のクラスタアドミニストレータに関するマニュアルを参照してください。
  - Veritas Cluster Server (VCS) クラスタ: NetBackup リソースをオフラインにします。
    次のコマンドで NetBackup オプションを使用して `-persist` グループを固定します。

    ```
    hagrp -freeze NetBackup_service_group -persistent
    ```

  これらのリソースをオフラインで取得するコマンドについて詳しくは、『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。

6 (該当する場合) NetApp クラスタをノードスコープモードから Vserver モードに変更する場合は、各ファイラの詳しいイメージレポートを作成します。このレポートは bpimagelist コマンドを使って生成できます。次に利用可能なオプションの一例を挙げます。環境に合わせて必要なオプションを使います。

```
bpimagelist -client ndmp_host_name
```

7 NetBackup 8.0 より、NetBackup プライマリサーバーには、重要なバックアップ操作をサポートするための構成済み Tomcat Web サーバーが含まれます。この Web サーバーは、権限が制限されているユーザーアカウント要素の下で動作します。これらのユーザーアカウント要素は、各プライマリサーバー (またはクラスタ化されたプライマリサーバーの各ノード) で使用できる必要があります。詳細情報を参照できます。

p.126 の「NetBackup プライマリサーバー Web サーバーのユーザーとグループの作成」を参照してください。

メモ: ベリタスは、NetBackup Web サービスに使用するユーザーアカウントの詳細を保存することを推奨します。プライマリサーバーのリカバリでは、NetBackup カタログのバックアップが作成されたときに使われたものと同じ NetBackup Web サービスのユーザーアカウントとクレデンシャルが必要です。

メモ: セキュアモードで NetBackup PBX を実行する場合は、Web サービスユーザーを PBX の権限を持つユーザーとして追加します。PBX モードの判別と、正しくユーザーを追加する方法について詳しくは、次をご覧ください。

http://www.veritas.com/docs/000115774

8 (該当する場合) Tomcat Web サーバーの設定をカスタマイズした場合は、それらの設定がアップグレード後も維持されるかどうかを確認します。詳細情報を参照できます。

p.155 の「維持される Java Virtual Machine のオプション」を参照してください。

9 NetBackup とやり取りするシステムのすべてのアプリケーションを停止します。この手順には、バックアップ中のデータベースまたはシステムコンポーネントが含まれます。これらのアプリケーションの停止に失敗すると、予期しない動作が発生する可能性があります。観測される動作には中止されたアップグレードやアプリケーションエラーが含まれます。

Oracle ユーザーの場合は、バックアップが実行されていないことを確認します。NetBackup をインストールする前に、RMAN のプロセスを停止します。AIX を使用する場合、RMAN プロセスを停止した後、root ユーザーとして `/usr/bin/slibclean` を実行する必要があります。

Oracle データベースを停止できない場合、手順は Oracle データベースがアクティブのままで NetBackup をインストールできる手順を利用できます。このトピックに関する詳細情報を参照できます。

http://www.veritas.com/docs/TECH158276

10 NetBackup のすべてのサービスを停止します。

- UNIX システムの場合: `/usr/openv/netbackup/bin/bp.kill_all`
- Windows システムの場合: *install_path*¥NetBackup¥bin¥bpdown -f

プレインストール手順は完了です。ご使用のプラットフォームに従って、NetBackup のバイナリのアップグレードに進みます。このトピックについて詳しくは、以下のページを参照してください。

- p.42 の「Windows システムでローカルサーバー、リモートサーバー、クラスタサーバーのアップグレードを実行する」を参照してください。
- p.54 の「Windows システムでのサイレントアップグレードの実行」を参照してください。
- p.58 の「NetBackup 10.1 への Linux サーバーソフトウェアのアップグレード」を参照してください。

Windows システムでローカルサーバー、リモートサーバー、クラスタサーバーのアップグレードを実行する

ローカルコンピュータ、リモートコンピュータ、クラスタコンピュータで NetBackup 10.1 にアップグレードするには次の手順を実行します。

Windows でローカルサーバー、リモートサーバー、クラスタサーバーの NetBackup バイナリをアップグレードする方法

1 NetBackup のアップグレードを開始するシステムにログオンします。管理者権限でログオンしてください。

- ローカルの Windows システムをアップグレードする場合は、コンソールでコンピュータに直接ログオンします。
- リモートの Windows システムをアップグレードする場合は、NetBackup をインストールするホストすべてにネットワークアクセスが可能なシステムにログオンします。
- クラスタの Windows システムをアップグレードする場合は、アクティブノード (共有ディスクが存在するノード) にログオンします。

2 ESD イメージ (ダウンロード済みファイル) が保存されているディレクトリに移動して、`Browser.exe` を実行して NetBackup インストールウィザードを起動します。

3 ブラウザの初期画面 ([ホーム (Home)]) で、[Installation]をクリックします。

4 [Installation]画面で、[Server Software Installation]をクリックします。

5 [ようこそ (Welcome)]画面で内容を確認して[次へ (Next)]をクリックします。

6 (該当する場合) 以前にこのホストに NetBackup 10.1 をインストールしている場合、[プログラムのメンテナンス (Program Maintenance)]ダイアログが表示されます。

- [変更 (Modify)]を選択してローカルホストのインストール設定を変更するか、ローカルホストをリモートホストへのプッシュインストールを実行するためのプラットフォームとして使用します。
- [修復 (Repair)]を選択して、NetBackup 10.1 をローカルホストで元の状態にリストアします。
- NetBackup 10.1 をローカルホストから削除するには、[削除 (Remove)]を選択します。

7 [使用許諾契約 (License Agreement)]画面で、次の操作を行います。

- [I agree to and accept the terms of the license agreement]にチェックマークを付けます。
  ソフトウェアをアップグレードするにはこの項目を選択する必要があります。
- [次へ (Next)]をクリックします。

8 ［Veritas NetBackup Installation Type］画面で以下の情報を入力します。

Where to install	ローカルアップグレードの場合は、［Install to this computer only］を選択します。 リモートアップグレードの場合は、［Install to multiple computers on your network］を選択します。 クラスタアップグレードの場合は、［Install a clustered primary server］が唯一のオプションです。
Typical	デフォルト設定の NetBackup をアップグレードするには、このオプションを選択します。 メディアサーバーのみ: デフォルトでは、Typical オプションはメディアサーバーの構成を調べ、Java GUI と JRE パッケージが存在している場合のみアップグレードします。現在のメディアサーバーの状態以外の状態を強制的に実行する場合は、Custom を選択します。Java GUI と JRE を除外することを選択した場合は、以前のすべてのバージョンが削除されます。
Custom	NetBackup のデフォルト設定を強制変更するには、このオプションを選択します。

［次へ (Next)］をクリックします。

9 ［NetBackup のライセンスとサーバーの種類 (NetBackup License and Server Type)］画面で、次の情報を入力します。

- ライセンス
  アップグレードの場合、すでにインストールされている製品のライセンスによって、選択可能なコンポーネントが決定されます。

メモ: リモートアップグレードの場合は、ここに入力したライセンスが他のノードにプッシュ型で転送されます。ライセンスによってアドオン製品を使用できるようになります。アドオン製品がすでにインストールされているノードに NetBackup をプッシュインストールした場合、ライセンスはアドオン製品に対して機能します。

リモートアップグレードまたはクラスタアップグレードの場合は、アップグレード処理中にアップグレードを実行する適切なクレデンシャルを所有していることを検証するために次の処理が実行されます。

- アップグレード先のクラスタシステムを選択すると、NetBackup はクラスタのすべてのノードに対する適切な管理クレデンシャルを所有しているかどうかを確認します。適切なクレデンシャルを所有していない場合は、そのシステムはリストに追加されません。

- 適切なクレデンシャルを所有している場合は、NetBackup によるセカンドチェックでライセンスが必要かどうかが判断されます。必要なライセンスが入力されなかった場合は、そのシステムはリストに追加できません。そのノードでアップグレードするには有効なライセンスを入力する必要があります。無効なライセンスを入力すると、この画面は有効なライセンスを入力するまで表示されたままになります。

- ［NetBackup プライマリサーバー (NetBackup Primary Server)］をクリックしてプライマリサーバーソフトウェアのアップグレードを続行します。
- ［NetBackup メディアサーバー (NetBackup Media Server)］をクリックしてメディアサーバーソフトウェアのアップグレードを続行します。メディアサーバーのアップグレードにライセンスは必要ありません。

10 (該当する場合) リモートアップグレードでは、［NetBackup での FIPS 準拠 (FIPS Compliance in NetBackup)］ダイアログが表示されます。

NetBackup では、アップグレード中の FIPS モードの変更はサポートされていません。既存の NetBackup のバージョンで FIPS がサポートされている場合は、アップグレードの前に FIPS モードを有効にします。それ以外の場合は、アップグレード後に有効にします。

Windows のリモートアップグレード中に FIPS モードを有効または無効にしても、リモートホストの NetBackup の構成で既存の FIPS モード値が変更されることはありません。

FIPS 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。

11 ［カスタマ登録キー (Customer Registration Key)］画面で、カスタマ登録キーの場所を入力します。このファイルを Veritas Usage Insights サイトからダウンロードし、適切なプライマリサーバーに配置します。Veritas Usage Insights に関する詳しい情報を参照できます。

p.13 の「Veritas Usage Insights について」を参照してください。

NetBackup 10.1 へのインストールとアップグレード中は、インストーラが `veritas_customer_registration_key.json` ファイルを最終的なインストール先にコピーするのを許可してください。NetBackup はこの処理を介してファイルの権限と所有権を正しく設定できます。インストールまたはアップグレード以外の処理でこのファイルをシステムに配置すると、処理は正しく動作しない可能性があります。

メモ: NetBackup では、カスタマ登録キーのファイル名に短いファイル名形式 (8.3 形式) を使用することはサポートされていません。

---

12 ［NetBackup Web サービス (NetBackup Web Services)］画面で、［Web サービスパスワード (Web Services Password)］を入力します。

これは、NetBackup Web サービスのユーザーアカウントのパスワードです。このアカウントは、プライマリサーバーをインストールする前に作成する必要があります。詳細情報を参照できます。

[NetBackup Web サービス (NetBackup Web Services)]画面で、アカウントの種類とアカウントの詳細を指定します。

どの種類のアカウントを使用する必要がありますか? (What types of acccounts should we use?)	[ローカル (Local)]または[ドメイン (Active Directory) (Domain (Active Directory))]を選択します。 Web サーバーを、ローカルホストに存在するユーザーおよびグループアカウントに関連付ける場合は[ローカル (Local)]を選択します。 Web サーバーを、信頼済みの Windows ドメインに存在するユーザーおよびグループアカウントに関連付ける場合は[ドメイン (Active Directory) (Domain (Active Directory))]を選択します。
既存のアカウントの詳細とは何ですか (What are the existing account details)	次に示すように、情報を指定します。 ■ [ドメイン (Domain)]: アカウントの種類の選択を[ドメイン (Active Directory) (Domain (Active Directory))]にする場合は、ユーザーおよびグループアカウントが属するドメインの名前を指定します。 ■ [グループ (Group)]: Web サーバーに関連付けるグループアカウントの名前を指定します。 ■ [ユーザー (User)]: Web サーバーに関連付けるユーザーアカウントの名前を指定します。セキュリティ上の理由により、ホストの管理者権限を持つユーザーアカウントを指定しないでください。 ■ [パスワード (Password)]: [ユーザー (User)]フィールドでユーザーアカウントのパスワードを指定します。

詳細情報を参照できます。

p.169 の「Windows および Windows クラスタのアップグレード要件」を参照してください。

13 この手順はカスタムアップグレードにのみ適用されます。[Typical]インストールの場合は、次の手順へスキップします。

この手順では、[NetBackup Features]、[NetBackup Port Numbers]、および[NetBackup Services]を選択し構成する方法について記述します。

- Java GUI および JRE オプション
  (該当する場合: メディアサーバーのみ) アップグレードの内容に応じて、次のオプションが表示されます。

- ［Java GUI および JRE を含める (Include Java GUI and JRE)］: 指定したコンピュータで Java GUI と JRE コンポーネントをインストールまたはアップグレードします。
- ［Java GUI および JRE を除外する (Exclude Java GUI and JRE)］: 指定したコンピュータから Java GUI と JRE コンポーネントを除外します。既存の Java GUI および JRE コンポーネントは削除されます。
- ［既存の構成と合わせる (Match Existing Configuration)］: Java GUI と JRE コンポーネントの現在の状態を保持します。アップグレード前のシステムにコンポーネントが存在する場合、コンポーネントはアップグレードされます。アップグレード前のシステムにコンポーネントが存在しない場合、コンポーネントはインストールされません。

- NetBackup ポート番号
  構成に必要な場合は、この画面からポート番号を変更できます。
  NetBackup と他社製品が同じポートを共有しようとして競合が発生した場合、ポート番号の変更が必要になることがあります。また、ファイアウォールでセキュリティの問題を引き起こすポートの競合が発生している場合にも変更できます。
  ポート番号を変更するには、置き換えるポート番号を選択し、新しい番号を入力します。
  ［次へ (Next)］をクリックします。
- NetBackup サービス
  この画面で、次の NetBackup サービスの起動アカウントおよび起動の種類を指定します。

特権アカウントの詳細 (Privileged Account Details)

［ローカルシステムアカウント (Local System account)］または［カスタムアカウント (Custom account)］を指定します。

デフォルトでは、［ローカルシステムアカウント (Local System account)］が選択されるので、NetBackup は組み込みシステムアカウントを使います。このオプションを選択すると、その下のフィールドは無効になります。

異なるシステムアカウントを指定する方法

- ［カスタムアカウント (Custom account)］を選択します。
- 次のフィールドにアカウント情報を入力します。
  ドメイン (Domain)
  ユーザー名 (Username)
  パスワード (Password)

特権のないアカウントの詳細 (Non-Privileged Account Details)	先ほど指定した特権アカウントと同じアカウントまたはローカルサービスアカウントを指定します。 ローカルサービスアカウントを使用する場合、1 回限りの変換を行う必要があります。この変換により、カタログサイズに応じてアップグレード時間が大幅に増加する場合があります。 特権のないサービスユーザーアカウントについて詳しくは、次を参照してください。 https://www.veritas.com/docs/100048220 この情報は、プライマリサーバーのアップグレードにのみ適用されます。
スタートアップの種類 (Startup Type)	このオプションは、NetBackup ホストを再起動する必要がある場合、NetBackup サービスが自動的に開始するかどうかを判断します。デフォルトは[自動 (Automatic)]です。 再起動後、NetBackup サービスを手動で開始するには、[Manual]を選択します。
インストール後にジョブに関連する NetBackup サービスを起動する (Start job-related NetBackup services following installation)NetBackup	デフォルトでは、アップグレードが完了したらジョブに関連するサービスを自動的に開始する設定になっています。 ジョブに関連するサービスが自動的に開始しないようにするには、ボックスをクリックしてチェックマークをはずします。
安全な中止オプション (Safe Abort Option)	このオプションは、アップグレードの一環として再起動が必要な場合にアップグレードを続行する方法を決めます。 このオプションを選択すると、アップグレード処理で再起動が必要であると判断された場合にアップグレードは停止します。システムは元の状態にロールバックされます。 このオプションを選択しないと、アップグレード処理で再起動が必要であると判断されてもアップグレードは続行されます。

[次へ (Next)]をクリックします。

14 [NetBackup System Names]画面で、次の情報を入力します。

プライマリサーバー名 (Primary Server Name)
プライマリサーバーのインストールの場合は、ローカルコンピュータの名前を入力します。

メディアサーバーのインストールの場合は、この名前を、そのメディアサーバーが構成されるプライマリサーバー名に変更する必要があります。

メモ: クラスタサーバーの場合は、このフィールドは[NetBackup Virtual Host Name]です。Veritas はこの値を変更しないことを推奨します。

追加サーバー (Additional Servers)
このサーバーと通信する追加の NetBackup プライマリサーバーおよびメディアサーバーの名前を入力します。後で NetBackup をインストールするコンピュータの名前を含めます。

複数の名前を入力するには、それぞれの名前をカンマで区切るか、それぞれの名前の後で Enter キーを押します。

メディアサーバー名 (Media server name)
このフィールドは NetBackup Enterprise メディアサーバーのインストールの場合にのみ表示されます。

メディアサーバーソフトウェアをインストールする場合、このフィールドはデフォルトでローカルサーバー名になります。

[次へ (Next)]をクリックします。

15 (該当する場合: メディアサーバーのみ) 環境で外部認証局を使用している場合、[外部証明書 (External Certificate)]画面が表示されます。[外部証明書 (External Certificate)]画面で、外部認証局 (ECA) を構成する方法に基づいて、3 つのラジオボタンのいずれかを選択します。選択した方法に応じて、異なる情報を入力する必要があります。

- [Windows 証明書ストアの使用 (Use Windows certificate store)]
  証明書の場所は、*Certificate Store Name*¥*Issuer Distinguished Name*¥*Subject Distinguished Name* のように入力する必要があります。

  メモ: 証明書ストアを指定するときは、任意の名前に対して `$hostname` 変数を使用できます。実行時に `$hostname` 変数はローカルホストの名前を評価します。このオプションを使用すると、NetBackup ソフトウェアを多数のクライアントにプッシュインストールするときに柔軟性が高まります。

  あるいは、Windows 証明書の場所をカンマ区切りのリストで指定できます。たとえば、`MyCertStore¥IssuerName1¥SubjectName, MyCertStore¥IssuerName2¥SubjectName2, MyCertStore4¥IssuerName1¥SubjectName5` のように指定できます。
  次に、表示されるラジオボタンから、証明書失効リスト (CRL) オプションを選択します。

- ［証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)］: 追加の情報は不要です。
- ［次のパスにある CRL を使用する (Use the CRL at the following path)］: CRL のパスを入力するように求められます。
- ［CRL は使用しない (Do not use a CRL)］

- ［ファイルから証明書を使用する (Use certificate from a file)］
  このオプションを選択した後、次を指定します。
  - ［証明書ファイル (Certificate file)］: このフィールドには、証明書ファイルへのパスと証明書のファイル名を指定する必要があります。
  - ［トラストストアの場所 (Trust store location)］: このフィールドには、トラストストアへのパスとトラストストア名を指定する必要があります。
  - ［秘密鍵のパス (Private key path)］: このフィールドには、秘密鍵ファイルへのパスと秘密鍵のファイル名を指定する必要があります。
  - ［パスフレーズファイル (Passphrase file)］: このフィールドでは、パスフレーズファイルへのパスとパスフレーズのファイル名を指定する必要があります。このフィールドは必要に応じて指定します。
  - ［CRL オプション (CRL option)］: お使いの環境の正しい CRL オプションを指定します。
    - ［証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)］: 追加の情報は不要です。
    - ［次のパスにある CRL を使用する (Use the CRL at the following path)］: CRL のパスを入力するように求められます。
    - ［CRL は使用しない (Do not use a CRL)］
- ［セキュリティなしで続行 (Proceed without security)］
  潜在的な問題を一覧表示する警告メッセージが表示されます。現在のセキュリティ構成の状態に応じて、外部 CA 証明書が構成されるまで、NetBackup がバックアップやリストアを実行できない場合があります。

［次へ (Next)］をクリックして続行します。

16 リモートアップグレードの場合のみ、［Veritas NetBackup Remote Hosts］画面で NetBackup をインストールするホストを指定します。

- Windows Destination Systems
  ［Windows Destination Computers］を右クリックし、ドロップダウンメニューから選択するか、次の方式を使ってください。

参照 (Browse)

NetBackup をアップグレードするホストのネットワークを検索するには、ここをクリックします。

- ［Available Systems］ダイアログボックスで追加するコンピュータを選択し、［次へ (Next)］をクリックします。
- ［Remote Computer Login Credentials］ダイアログボックスで、リモートコンピュータで使う NetBackup のアカウントのユーザー名、パスワード、ドメインを入力します。
- 複数のリモートコンピュータをアップグレードする場合は、［Remember User Name and Password］の隣にあるチェックボックスにチェックマークを付けます。このオプションを選択すると、各リモートコンピュータにこの情報を入力する必要がなくなります。

  クレデンシャルを指定したらホストノードを選択し、［Windows Destination Systems］リストに追加します。NetBackup のリモートアップグレードは、これらのノードで実行されます。インストール先のシステムを選択する場合、ローカルホストも忘れずに選択してください。

  NetBackup では、システムを選択するたびに、システムおよびライセンスの確認が実行されます。たとえば、次のようにサーバーアップグレード先のシステムが選択した種類と一致するかどうかが確認されます。
  - NetBackup がインストールされていない場合: リモートは検証済みと見なされます。
  - NetBackup がすでにインストールされている場合: そのシステムのアップグレードの種類と要求しているアップグレードの種類を比較します。
  - 無効な組み合わせの場合: 問題があることが通知され、そのシステムは選択できません。無効な組み合わせの例として、すでにプライマリサーバーになっているリモートシステムにリモート管理コンソールをインストールしようとしている場合があります。
  - リモートシステムがサポート外のプラットフォームやレベルの場合: 問題が通知され、そのシステムは選択できません。

  アップグレード手順で、リモートシステムに対する適切な管理クレデンシャルを所有しているかどうかも検証されます。管理クレデンシャルを所有していない場合は、［Enter Network Password］画面が表示され、管理者のユーザー名およびパスワードの入力を求められます。

  ［OK］をクリックし、インストール先のシステムの選択を続けます。

  選択するノードごとに、この処理を繰り返します。ユーザー名およびパスワードは保持することができます。その場合、ユーザー名またはパスワードが無効な場合にのみ、そのユーザー名またはパスワードが求められるようになります。

  次に、クラスタ環境でのプッシュインストールに関連する注意事項を示します。
  - NetBackup は、複数のノードでアップグレードできます。ただし、クラスタのノード数に対する制限は、NetBackup ではなくクラスタサービスによって設定されます。
  - 言語パッケージとその他の NetBackup のアドオン製品は、プッシュ方式ではアップグレードできません。アドオン製品は、クラスタグループのノードごとにアップグレードする必要があります。これらの製品のアップグレード方法については、各製品の NetBackup マニュアルを参照してください。

参照 (Browse) (続き)

(続き)

- NetBackup は、アップグレードの開始時に入力したライセンスのみを他のノードにプッシュ型で転送します。ライセンスによってアドオン製品を使用できるようになります。アドオン製品がすでにインストールされているノードに NetBackup をプッシュインストールすると、ライセンスはその製品に対して機能します。
- ［OK］をクリックします。

インポート (Import)

ホスト名のリストを含んでいるテキストファイルをインポートするためにここをクリックします。テキストファイルを作成する場合、ホスト名は次の形式で定義する必要があります。

```
Domain¥ComputerName
```

追加 (Add)

ホストを手動で追加するためにここをクリックします。

- [Manual Remote Computer Selection]ダイアログボックスが表示されたら、[Domain]と[Computer Name]を入力し、[OK]をクリックします。
- [Remote Computer Login Credentials]ダイアログボックスで、リモートコンピュータでアップグレードを実行するために使うアカウントの[User Name]と[Password]を入力します。
  複数のリモートコンピュータに追加、アップグレードする場合は、[Remember User Name and Password]の隣にあるチェックボックスにチェックマークを付けます。このオプションを選択すると、各リモートコンピュータにこの情報を入力する必要がなくなります。
- [OK]をクリックします。

削除 (Remove)

[Destination Systems]リストからホストを削除するには、ホストを選択し、ここをクリックします。

変更 (Change)

選択したリモートホストの NetBackup ファイルのインストールの宛先を変更するためにここをクリックします。

- [次へ (Next)]をクリックします。

17 クラスタアップグレードの場合のみ、[Cluster Settings]画面に表示される情報を確認します。単なる情報として[パブリックネットワーク]以外のすべての情報が表示されます。パブリックネットワークを変更する必要がある場合は、ドロップダウンリストから正しいパブリックネットワークを選択します。

警告: このクラスタに割り当てられているプライベートネットワークは選択しないでください。

[Cluster Configuration]をクリックします。クラスタ構成が正常に行われたことを示すメッセージが表示されたら、[次へ (Next)]をクリックします。

18 (該当する場合: プライマリサーバーのみ) カタログのサイズによっては、無制限の保持変換を続行するように求められることがあります。

9.0 より前の NetBackup から NetBackup 9.0 以降へのアップグレードには、無制限の有効期限変換が含まれます。この変換は、2038 年より先の有効期限をサポートします。この変換によって、アップグレードを完了するために必要な時間が長くなる場合があります。詳しくは、次の記事を参照してください。

https://www.veritas.com/content/support/en_US/article.100048600

19 [Ready to Install the Program]画面で、前述の手順での選択を示す[Installation Summary]を確認します。

ECA 健全性チェックユーティリティで CSP (暗号サービスプロバイダ) または KSP (キーストレージプロバイダ) がセキュリティ記述子をサポートしていないことが示された場合、アップグレードは続行できません。

このフラグは、NetBackup サービスがローカルサービスユーザーアカウントのコンテキストで実行されている場合、プロバイダを使用できないことを示します。セキュリティ記述子をサポートしているプロバイダを使用するか、管理者アカウントを使用してすべての NetBackup サービスを実行してください。

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』の「NetBackup 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の Windows 証明書ストアの制限事項」の情報を参照してください。

20 次のオプションのいずれかを選択します。

- インストールを開始するには、[Install]をクリックします。
- 前の画面を表示して変更するには[Back]をクリックし、その後、この画面に戻って[Install]をクリックします。
- アップグレードを中止するには、[Cancel]をクリックします。

[Install]をクリックするとアップグレード処理が開始され、アップグレードの進捗状況を示す画面が表示されます。この処理には数分かかる場合があります。

リモートアップグレードまたはクラスタアップグレードの場合のみ、ダイアログボックスでシステムを右クリックしてアップグレードの状態を確認します。アップグレードは 5 つまで並行して行われます。1 つのアップグレードが完了すると別のアップグレードが開始し、最大 5 つのアップグレードが進行中になります。

21 リモートアップグレードの場合のみ、すべてのリモートアップグレードが完了したら[完了 (Finish)]をクリックします。

22 [Installation Complete]画面で、次のオプションから選択します。

Add Licenses

[Add Licenses]は、プライマリサーバーにのみ適用できます。

Veritas はインストールする他の NetBackup 製品の追加のライセンスをここに入力することをお勧めします。

- 追加のライセンスを入力するには、[Add Keys]をクリックします。
- [Current License Keys]のリストが表示されたら、[Add Key]をクリックして新規のライセンスキーを入力し、次に[Add]をクリックします。
- すべてのライセンスキーを入力したら、[Current License Keys]ウィンドウを閉じます。

View installation log file

アップグレードログファイルには、詳しいインストール情報とエラーが発生したかどうかが表示されます。このログには、Java GUI と JRE のオプションインストールについての情報が含まれています。

次の場所にあるアップグレードログを確認します。

```
%ALLUSERSPROFILE%¥Veritas¥NetBackup¥InstallLogs¥
```

メモ: 複数のコンピュータにリモートアップグレードを実行する場合は、このオプションを選択するとローカルコンピュータのログのみが表示されます。アップグレードするように選択した各コンピュータにそれぞれのアップグレードログファイルが作成されます。リモートコンピュータのログファイルを表示するためには、Windows エクスプローラのウィンドウを開き、¥¥<COMPUTERNAME> と入力します。

アップグレードログを検索し、次のエラーが表示されているかどうかを確認します。

- `Return Value 3` を含む文字列。
- 次のように色分けされている重大なログメッセージ:
  黄色 = 警告。
  赤 = エラー。

［完了 (Finish)］

アップグレードを完了するには次のいずれかの操作をします。

- すべてのサーバーのソフトウェアをアップグレードした場合は、［Launch NetBackup Administration Console now］の隣にあるチェックボックスにチェックマークを付けて［完了 (Finish)］をクリックします。
  NetBackup 管理コンソールを使用して構成ウィザードを起動すると、NetBackup 環境を構成できます。
- アップグレードするサーバーソフトウェアが他にも存在する場合は、［完了 (Finish)］をクリックします。
  次のコンピュータに移動して、必要なサーバーソフトウェアをアップグレードできます。

23 NetBackup クラスタ設定を手動で修正した場合や外部スクリプトで修正した場合は、NetBackup クラスタレジストリに変更が正しく反映されていることを確認してください。質問がある場合は、Veritas のテクニカルサポートにお問い合わせください。

24 バイナリが正常にインストールされました。インストール後の手順に進みます。

詳細情報を参照できます。

p.68 の「NetBackup 10.1 へのアップグレードのインストール後の手順」を参照してください。

Windows システムでのサイレントアップグレードの実行

サイレントアップグレードを実行すると、リモートアップグレードを実行する場合と同様に、対話形式での入力が不要になります。NetBackup サービスをローカルシステムではなく

特定のユーザーで実行する場合、NetBackup のサイレントインストールはサポートされません。

サイレントアップグレードを実行するには、最初に該当する NetBackup スクリプトを修正する必要があります。スクリプトの修正後に、そのスクリプトを実行してサイレントアップグレードを開始できます。

このスクリプトはアップグレードを開始できるようにすべての NetBackup サービスを終了します。他のシステムプロセスで NetBackup ファイルに対するハンドルが保持されていることをスクリプトが検出すると、アップグレードは失敗します。実行中の NetBackup プロセスを特定するには、次の場所にある NetBackup Install ログファイルを確認します。

```
%ALLUSERSPROFILE%¥Veritas¥NetBackup¥InstallLogs
```

特定した各プロセスを手動で停止したら、再びアップグレードスクリプトを実行できます。

メモ: Windows 2012/2012 R2/2016 Server Core システムでは、この手順で NetBackup のみをアップグレードできます。

NetBackup サーバーソフトウェアをサイレントアップグレードする方法

1. NetBackup をアップグレードするシステムに管理者としてログオンします。
2. ESD イメージ (ダウンロード済みファイル) が存在する場所に移動します。
3. Windows エクスプローラを開き、x64 ディレクトリの内容を、ハードドライブの一時ディレクトリにコピーします。インストールしたいプラットフォームの形式と関連付けられたディレクトリを選択します。
4. ソースファイルが読み取り専用であるので、コピーされたファイルの権限を変更して、インストールまたは更新できるようにします。
5. コピーされたファイルが存在する一時ディレクトリで、変更する適切なスクリプトを選択します。
   - プライマリサーバーをアップグレードするには、silentprimary.cmd を編集します。
   - メディアサーバーのアップグレード時: silentmedia.cmd
6. 次の行をインストールの必要に応じて編集します。
   - SET ADDITIONALSERVERS=media1,media2,media3

     このホストと通信する追加の NetBackup プライマリサーバーおよびメディアサーバーの名前を入力します。後で NetBackup をインストールするサーバーの名前を含めます。
     他のサーバーがこのホストと通信しない場合は、スクリプトからこの行を削除します。

- SET ABORT_REBOOT_INSTALL=0

  この行では、再起動が必要になった場合のアップグレードの続行方法を指定できます。次の設定から選択します。

  0 (デフォルト)
  デフォルトでは、再起動が必要であると判断された場合でもサイレントアップグレードは中止されません。この設定を 0 のままにした場合、次のタスクの 1 つを選択します。
  - アップグレードの完了後にインストールログを調べて再起動が必要かどうかを確認します。
    文字列 in use がログ内に表示されれば、システムを手動で再起動する必要があります。
  - アップグレードの完了後に自動再起動を強制します。
    自動再起動を強制するには、スクリプトを実行する前に、サイレントインストールのコマンドスクリプト (silent*.cmd) から次のオプションを削除します。

    ```
    REBOOT="ReallySuppress"
    ```

    警告: 強制再起動はユーザーに警告なしで起きます。アップグレードは取り消されず、システムが元の状態にロールバックされることもありません。

  1
  再起動が必要であると判断された場合にアップグレードを中止するにはこの設定を選択します。

  この設定を選択すると、再起動が必要な場合はアップグレードが取り消されてシステムが元の状態にロールバックされます。

- SET USAGE_INSIGHTS_FILE_PATH=*path*

  プライマリサーバーのみの場合、Veritas Usage Insights のカスタマ登録キーのパスを指定する必要があります。詳細情報を参照できます。p.13 の「Veritas Usage Insights について」を参照してください。

- SET ALLOW_PRE_90_UPGRADE=*value*

  このフィールドはプライマリサーバー専用です。この値は、9.0 より前のリリースの NetBackup からのアップグレードを続行できるかどうかを判定します。アップグレードの続行を許可する場合は 1 を指定します。アップグレードには、無制限の有効期限変換プロセスが含まれます。0 を指定すると、プライマリサーバーをアップグレードできません。

  NetBackup 9.0 以降のバージョンでは、2038 年より先の有効期限がサポートされています。NetBackup の以前のバージョンとの互換性を確保するために、無制限の有効期限が設定されたすべての項目は、新しい無制限の有効期限の値を反映するように更新されます。この変換によって、アップグレードを完了するた

めに必要な時間が長くなる場合があります。詳しくは、次の記事を参照してください。
https://www.veritas.com/content/support/en_US/article.100048600

- SET ECA_CERT_STORE=*cert_store_string*
  このフィールドは、メディアサーバーのみに表示されます。このフィールドを使用して、Windows 証明書ストアの外部証明書の場所を指定します。このフィールドは、「*store_name*¥*issuer_DN*¥*subject*」という形式で指定します。このフィールドは、Windows 証明書ストアから外部証明書を使用する場合に必要です。
- SET ECA_CERT_PATH=*path*
  このフィールドは、メディアサーバーのみに表示されます。このフィールドを使用して、外部証明書ファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
- SET ECA_TRUST_STORE_PATH=*path*
  このフィールドは、メディアサーバーのみに表示されます。このフィールドを使用して、トラストストアの場所を示すファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
- SET ECA_PRIVATE_KEY_PATH=*path*
  このフィールドを使用して、秘密鍵を示すファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
- SET ECA_CRL_CHECK_LEVEL=*value*
  このフィールドは、メディアサーバーのみに表示されます。このフィールドを使用して、CRL モードを指定します。このフィールドは必須です。サポートされる値は次のとおりです。
  - USE_CDP: 証明書に定義されている CRL を使用します。
  - USE_PATH: ECA_CRL_PATH で指定されたパスにある CRL を使用します。
  - DISABLED: CRL を使用しません。
- SET ECA_CRL_PATH=*path*
  このフィールドは、メディアサーバーのみに表示されます。このフィールドを使用して、外部 CA 証明書に関連付けられている CRL のパスとファイル名を指定します。このフィールドは、ECA_CRL_CHECK_LEVEL が USE_PATH に設定されている場合にのみ必要です。該当しない場合は、このフィールドを空のままにします。
- SET ECA_KEY_PASSPHRASEFILE=*path*
  このフィールドは、メディアサーバーのみに表示されます。このフィールドを使用して、キーストアにアクセスするためのパスフレーズを含むファイルのパスとファイル名を指定します。このフィールドは省略可能で、ファイルから外部証明書を設定する場合にのみ適用されます。
- SET INCLUDE_JAVA_GUI_AND_JRE=*value*

NetBackup Windows メディアサーバーのインストールでは、NetBackup Java GUI と JRE パッケージのインストールは省略可能です。このオプションは、Java GUI および JRE パッケージをインストール、アップグレード、または削除するかどうかを指定します。このオプションでサポートされる値は、次のとおりです。

- INCLUDE: NetBackup をインストールまたはアップグレードする際に Java GUI と JRE を含めます。
- EXCLUDE: NetBackup をインストールまたはアップグレードする際に Java GUI と JRE を除外します。既存の NetBackup Java GUI および JRE パッケージがすべて削除されます。
- MATCH: ホスト上の既存の構成を照合します。Java GUI および JRE コンポーネントがすでにあるホストは最新バージョンに更新されます。コンポーネントは他のすべてのホストについて除外されます。

7 スクリプトを保存して実行します。

8 次の場所にあるインストールログを確認します。

```
%ALLUSERSPROFILE%¥Veritas¥NetBackup¥InstallLogs¥
```

このログには、Java GUI と JRE のオプションインストールについての情報が含まれています。

インストールログを検索し、次のエラーが表示されているかどうかを確認します。

- `Return Value 3` を含む文字列。
- 重要なログメッセージは次のように色分けされます。
  黄色 = 警告。
  赤 = エラー。

9 バイナリが正常にインストールされました。インストール後の手順に進みます。詳細情報を参照できます。

p.68 の「NetBackup 10.1 へのアップグレードのインストール後の手順」を参照してください。

NetBackup 10.1 への Linux サーバーソフトウェアのアップグレード

バックアップが実行されない時間にアップグレードおよび再構成をスケジュールすることをお勧めします。ただし、アップグレードの手順では、バックアップがアップグレードの妨げにならないようにするため、すべてのポリシーを無効にするように指示されます。NetBackup のアップグレードおよび再構成中にバックアップが実行されないようにポリシーを一時的に変更することもできます。

Linux サーバーソフトウェアを 10.1 にアップグレードするには

1. root ユーザーとしてサーバーにログインします。
2. NetBackup 管理コンソールが開いている場合は、ここで閉じる必要があります。
3. (該当する場合) クラスタ環境では次のタスクを実行します。
   - 必要に応じて、bp.conf と vm.conf ファイルを次のように編集します。
     REQUIRED_INTERFACE エントリがある場合は、CLUSTER_NAME エントリに置換します。それ以外の場合は、新しい CLUSTER_NAME エントリを追加します。このエントリは仮想サーバー名として定義する必要があります。
     プライマリサーバーの場合は、最初の SERVER エントリが bp.conf ファイルの CLUSTER_NAME エントリに一致することを確認してください。
   - NetBackup サーバーリソース (*ServerResource*) をオフラインにします。以下に示すコマンドを使います。
     `/opt/VRTSvcs/bin/hares -offline ServerResource -sys $nodename`
   - 非アクティブノードのアップグレード中に移行が行われないようにするために、NetBackup グループを凍結します。以下に示すコマンドを使います。
     `/opt/VRTSvcs/bin/hagrp -freeze group -persistent`
   - VCS クラスタが構成されている場合、Cluster Manager インターフェースまたはコマンドラインを使用して NetBackup グループを凍結できます。
   - クラスタのアップグレードに進む前に、他のクラスタアップグレード要件について『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。
     http://www.veritas.com/docs/DOC5332
4. アップグレードスクリプトを実行すると第 1 章で説明していない修正済み NetBackup スクリプトが削除されます。このトピックに関する詳細情報を参照できます。

   p.24 の「アップグレードによるファイルの自動変更について」を参照してください。

   変更したファイルで、保持する必要があるファイルを保存します。
5. インストールイメージが存在する場所に移動します。次のコマンドを入力して、アップグレードスクリプトを開始します。

   ```
   ./install
   ```
6. インストールスクリプトのプロンプトに従って、NetBackup サーバーバイナリをインストールします。

7 (該当する場合:プライマリサーバーのみ)メッセージが表示されたら、無制限の有効期限変換に関する質問に答えます。

```
NetBackup 9.0 and later versions support the retention periods
that
extend beyond the year 2038. To ensure compatibility with previous

NetBackup versions, all items with an infinite expiration date
are
updated to reflect the new infinite expiration date value. This
conversion may extend the time that is required to complete the
upgrade.
Review the following article for more information:

https://www.veritas.com/content/support/en_US/article.100048600

Date of collection: date_time
NetBackup state: online|offline
Records found: records
Conversion time estimate: time (hh:mm)

Please see the linked article to obtain a more accurate estimate
 of how
long the conversion may take.

Would you like to continue with the upgrade? [y,n]
```

8 (該当する場合:プライマリサーバーのみ)メッセージが表示されたら、ほとんどのデーモンを起動するために使用するサービスユーザーアカウントの名前を指定します。このプロンプトは、インストーラが bp.conf ファイルからサービスユーザーの値を取得できない場合にのみ表示されます。

```
Enter the name of the service user account to be used to start
most of the daemons
```

以下の点にご注意ください。

- サービスのユーザー名は 32 文字を超えることはできません。英語の文字のみを含めることができます。
- Veritas では、root ユーザーをサービスユーザーとして使用することはお勧めしません。
- nbwebsvc ユーザーをサービスユーザーとして使用することはできません。
- nbwebgrp グループはサービスユーザーのセカンダリグループである必要があります。

- /usr/openv ディレクトリの所有権は、ここで指定する新しいサービスユーザーアカウントに変更されます。
- サービスアカウントを使用する場合、1 回限りの変換を行う必要があります。この変換により、カタログサイズに応じてアップグレード時間が大幅に増加する場合があります。
- インストール後にサービスユーザーアカウントを変更する場合は、nbserviceusercmd --changeUser コマンドを使用します。

サービスユーザーアカウントについて詳しくは、次を参照してください。
https://www.veritas.com/docs/100048220

9 (該当する場合: メディアサーバーのみ) 環境で外部認証局を使用する場合は、表示されたプロンプトで外部認証局情報を入力します。

```
Enter the certificate file path or q to skip security
configuration:
/usr/eca/cert_chain.pem

Enter the trust store location or q to skip security
configuration:
/usr/eca/trusted/cacerts.pem

Enter the private key path or q to skip security configuration:
/usr/eca/private/key.pem

Enter the passphrase file path or q to skip security configuration

(default: NONE): /usr/eca/private/passphrase.txt
```

メモ: パスフレーズファイルのパスの入力は任意です。

10 (該当する場合: メディアサーバーのみ) プロンプトが表示されたら、CRL 構成に必要な情報を入力します。

```
Should a CRL be honored for the external certificate?
1) Use the CRL defined in the certificate.
2) Use the CRL from a file path.
3) Do not use a CRL.
q) skip security configuration
CRL option (1):
```

11 (該当する場合: メディアサーバーのみ) [ファイルパスの CRL を使用 (Use the CRL from a file path)]を指定した場合、CRL の場所のパスを入力する必要があります。

```
Enter the CRL location path or q to skip security configuration:

/usr/eca/crl
```

12 (該当する場合: メディアサーバーのみ) インストーラは入力された構成情報を再表示し、外部証明書の詳細の取得を試みます。

```
External CA values entered:
Certificate file path:  /usr/eca/cert_chain.pem
Trust store file path:  /usr/eca/trusted/cacerts.pem
Private key file path:  /usr/eca/private/key.pem
 Passphrase file path:  /usr/eca/private/passphrase.txt
      CRL check level:  Use the CRL from a file path.
    CRL location path:  /usr/eca/crl

Getting external CA certificate details
         Issued By : CN=IITFRMNUSINT,O=Veritas,OU=iitf
      Subject Name : CN=cuomovm04,O=Veritas,OU=iitf
       Expiry Date : Oct 31 17:25:59 2019 GMT
  SHA1 Fingerprint : 62:B2:C3:31:D5:95:15:85:9D:C9:AE:C6:EA:C2:
                     DF:DF:6D:4B:92:5B
     Serial Number : 0x6c7fa2743072ec3eaae4fd60085d468464319a
  Certificate Path : /usr/eca/cert_chain.pem

Validating host ECA certificate.
NOTE: Depending on the network, this action may take a few
minutes.
      To continue without setting up secure communication, press
 Ctrl+C.
```

13 (該当する場合: メディアサーバーのみ) 外部証明書を登録するための事前チェックが正常に完了した場合は、1 を選択し、Enter キーを押して続行します。

```
The external certificate enrollment pre-check is successful.

The external certificate is valid for use with primary server
name
How do you want to proceed?
1) Continue the installation using this certificate.
2) Modify the external CA values entered.
3) Abort the installation.
Default option (1):
```

14 (該当する場合: メディアサーバーのみ) 外部証明書の登録の事前チェックが失敗した場合は、表示される選択肢から選択します。デフォルトは 2 です。

```
The external certificate enrollment pre-check failed.

The external certificate is not valid for use with primary server
 name
How do you want to proceed?
1) Continue the installation and set up external certificates
later.
2) Modify the external CA values entered.
3) Abort the installation.
Default option (2):
```

15 (該当する場合: メディアサーバーのみ) プロンプトが表示されたら、アップグレードで Java GUI と JRE バイナリをどのように処理するかを指定します。

```
The Java GUI and JRE packages are currently install_state on this
host.

The Java GUI and JRE can be optionally included with NetBackup.
The Java GUI and JRE enable the NetBackup Administration Console
and the Backup, Archive and Restore (BAR) GUI. Choose an option
from the list below.

1) Update the Java GUI and JRE.

2) Remove the Java GUI and JRE.
```

1 を指定すると、サーバーの状態に基づいて Java および JRE のバイナリがインストールまたはアップグレードされます。2 を指定すると、サーバーの状態に基づいて Java および JRE のバイナリが削除または除外されます。

16 スクリプトが終了したら、バイナリが正常にインストールされています。

インストール後の手順に進みます。

詳細情報を参照できます。

p.68 の「NetBackup 10.1 へのアップグレードのインストール後の手順」を参照してください。

Linux での NetBackup プライマリサーバーソフトウェアのサイレントアップグレード

ネイティブインストーラを使用して、NetBackup の Linux プライマリサーバーをアップグレードできます。NetBackup インストールスクリプトまたは優先するインストーラによる方法のいずれかを使用できます。

- Linux の場合: rpm、yum など

インストールまたはアップグレードに成功すると、/usr/openv/pack/install.history ファイルに記録されます。

メモ: パッケージ名の変更により、ネイティブインストーラによる方法でプライマリサーバーを NetBackup 7.7.3 以前から NetBackup 8.0 以降にアップグレードするには、追加の手順が必要です。プライマリサーバーを正しくアップグレードして Veritas パッケージに変換するには、次の 2 つのオプションがあります。NetBackup インストーラを使用してプライマリサーバーを新しい Veritas パッケージにアップグレードできます。または、ネイティブインストーラの手順に従って、該当する手順を実行します。詳細情報を参照できます。

p.65 の「ネイティブインストーラを使用して Linux プライマリサーバーバイナリをアップグレードするには:」を参照してください。

この両方のアップグレードオプションは同じ結果になります。Veritas パッケージに正常にアップグレードすると、その後のアップグレードは各自が選択するインストーラを使用して実行できます。

ネイティブインストーラを使用して Linux プライマリサーバーバイナリをアップグレードするには:

1. root ユーザーとしてサーバーにログインします。
2. NetBackup 管理コンソールが開いている場合は、ここで閉じる必要があります。
3. (該当する場合) クラスタ環境では次のタスクを実行します。
   - 必要に応じて、`bp.conf` と `vm.conf` ファイルを次のように編集します。
     `REQUIRED_INTERFACE` エントリがある場合は、`CLUSTER_NAME` エントリに置換します。それ以外の場合は、新しい `CLUSTER_NAME` エントリを追加します。このエントリは仮想サーバー名として定義する必要があります。
     プライマリサーバーの場合は、最初の `SERVER` エントリが `bp.conf` ファイルの `CLUSTER_NAME` エントリに一致することを確認してください。
   - NetBackup グループをオフラインにします。以下に示すコマンドを使います。
     `/opt/VRTSvcs/bin/hares -offline`
   - 非アクティブノードのアップグレード中に移行が行われないようにするために、NetBackup グループを凍結します。以下に示すコマンドを使います。
     `/opt/VRTSvcs/bin/hagrp -freeze group -persistent`
   - VCS クラスタが構成されている場合、Cluster Manager インターフェースまたはコマンドラインを使用して NetBackup グループを凍結できます。
   - クラスタのアップグレードに進む前に、他のクラスタアップグレード要件について『NetBackup マスターサーバーのクラスタ化管理者ガイド』を参照してください。
     http://www.veritas.com/docs/DOC5332

4 アップグレードスクリプトを実行すると第 1 章で説明していない修正済み NetBackup スクリプトが削除されます。このトピックに関する詳細情報を参照できます。

p.24 の「アップグレードによるファイルの自動変更について」を参照してください。

変更したファイルで、保持する必要があるファイルを保存します。

5 プライマリサーバーの一時ディレクトリに NetBackup インストール応答ファイル (NBInstallAnswer.conf) を作成してください。そのディレクトリは通常、/tmp ディレクトリです。応答ファイルとその内容に関する詳しい情報を参照できます。

p.133 の「NetBackup 応答ファイルについて」を参照してください。

6 (該当する場合) NetBackup 8.1.1 以前からプライマリサーバーをアップグレードする場合、NBInstallAnswer.conf に次の情報を指定します。

USAGE_INSIGHTS_FILE_PATH=*path*

7 NBInstallAnswer.conf ファイルに省略可能なパラメータを追加できます。次に示すパラメータは、追加できるパラメータの例です。Veritas は、このマニュアルに含まれている NetBackup 応答ファイルのセクションを確認することをお勧めします。

- LICENSE エントリ
  LICENSE エントリはプライマリサーバーでのみ必要です。
- SERVER エントリ

p.133 の「NetBackup 応答ファイルについて」を参照してください。

8 (該当する場合) ユーザーまたはユーザーグループに RBAC セキュリティおよびバックアップ管理者の役割を割り当てる場合は、NBInstallAnswer.conf に次の必要な情報を指定します。

- RBAC_DOMAIN_TYPE
  このフィールドを使用して、ユーザーまたはユーザーグループが属するドメイン形式を指定します。RBAC_DOMAIN_TYPE の NT, VX, UNIXPWD, LDAP 値がサポートされています。
- RBAC_DOMAIN_NAME
  このフィールドを使用して、ユーザーまたはユーザーグループが属するドメインの名前を指定します。
- RBAC_PRINCIPAL_TYPE
  このフィールドを使用して、USER または USERGROUP を指定します。
- RBAC_PRINCIPAL_NAME
  このフィールドを使用して、ユーザー名またはユーザーグループを指定します。

RBAC_* オプションに関する詳しい情報を参照できます。

p.156 の「RBAC ブートストラップについて」を参照してください。

p.133 の「NetBackup 応答ファイルについて」を参照してください。

9 十分な容量があるシステムに、サーバープラットフォームに一致するサーバーパッケージをダウンロードします。次に、そのサーバーパッケージファイルの内容を抽出します。

サーバーパッケージファイルの内容を抽出します。例:

- Linux Red Hat の場合:

```
tar -xzvf NetBackup_10.1_LinuxR_x86_64.tar.gz
```

- Linux SuSE の場合:

```
tar -xzvf NetBackup_10.1_LinuxS_x86_64.tar.gz
```

10 目的のオペレーティングシステムのディレクトリに移動し、サーバーのファイルをインストール先のコンピュータにコピーします。

オペレーティングシステムのディレクトリ:

- Linux Red Hat の場合:

```
NetBackup_10.1_LinuxR_x86_64/linuxR_x86/anb
```

- Linux SuSE の場合:

```
NetBackup_10.1_LinuxS_x86_64/linuxS_x86/anb
```

サーバーのファイルをインストール先のマシンにコピーします。

- Linux: `VRTSnetbp.rpm`、`VRTSnbslibs.rpm`、および `VRTSpddes.rpm`

11 クライアントバイナリを抽出し、プライマリサーバーにコピーします。

クライアントバイナリを抽出します。

```
tar -xzvf client_dist.tar.gz
```

目的のオペレーティングシステムのディレクトリに移動します。

- RedHat: `openv/netbackup/client/Linux/RedHat3.10.0`
- SuSE: `openv/netbackup/client/Linux/SuSE3.0.76`

以下に示すファイルをプライマリサーバーにコピーします。

Linux	`VRTSnbpck.rpm`
	`VRTSpbx.rpm`
	`VRTSnbclt.rpm`
	`VRTSnbclibs.rpm`
	`VRTSnbjre.rpm`
	`VRTSnbjava.rpm`
	`VRTSpddea.rpm`
	`VRTSnbcfg.rpm`

12 Veritas 事前チェックパッケージをインストールします。

- Linux: `rpm -U VRTSnbpck.rpm`

13 (該当する場合) NetBackup 8.0 より前のバージョンからアップグレードする場合は、古い SYMC* パッケージを削除します。次の例は、SYMC RPM パッケージの削除に使用するコマンドを示しています。このプロセスでは、NetBackup の構成が保持されます。

```
rpm -e SYMCnbjava
rpm -e SYMCpddea
rpm -e SYMCnbclt
rpm -e SYMCnbjre
rpm -e SYMCnetbp
rpm -e SYMCpddes
```

14 以下のコマンドを示されている順序で実行してファイルをインストールします。

Linux

```
rpm -U VRTSpbx.rpm
rpm -U VRTSnbclt.rpm
rpm -U VRTSnbclibs.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjava.rpm
rpm -U VRTSpddea.rpm
rpm -U VRTSpddes.rpm
rpm -U VRTSnbcfg.rpm
rpm -U VRTSnetbp.rpm
rpm -U VRTSnbslibs.rpm
```

15 インストールの完了後に Java GUI または JRE をインストールする場合は、追加情報が利用可能です。

p.131 の「アップグレード後の Java GUI と JRE の追加または削除」を参照してください。

NetBackup 10.1 へのアップグレードのインストール後の手順

「NetBackup 10.1 へのアップグレードのインストール後の手順」では、NetBackup をアップグレードしてイメージメタデータの移行を完了するためのインストール後の手順を説明します。

NetBackup 10.1 へのアップグレードのインストール後の手順

1 利用可能な NetBackup 10.1 メンテナンスリリースを確認します。メンテナンスリリースは NetBackup 10.1 の後にリリースされる非常に重要な修正が含まれます。Veritas はアップグレードアクティビティ時に最新の利用可能なメンテナンスリリースをインストールすることを推奨します。

最新の NetBackup 10.1 メンテナンスリリースにアクセスする方法

- NetBackup SORT の Web サイトに移動します。
  https://sort.veritas.com/netbackup
- [インストールとアップグレードのチェックリスト (Installation and Upgrade Checklist)]セクション:
  - [製品 (Product)]で、正しい製品 (NetBackup Enterprise Server または NetBackup Server) を選択します。
  - [これからインストールまたはアップグレードする製品のバージョン (Product version you are installing or upgrading to)]で、NetBackup 最新バージョンを指定します。
  - [プラットフォーム (Platform)]で、アップグレードするサーバーのプラットフォームを選択します。
  - [プロセッサ (Processor)]で、サーバーのプロセッサを指定します。
  - [アップグレードされる製品のバージョン (Product version you are upgrading from (Optional))]で、アップグレードするサーバーの NetBackup の現在のバージョンを選択します。
  - [チェックリストの生成 (Generate Checklist)]をクリックします。
- [アップグレード情報 (Upgrade Information)]に *version_number*[ダウンロードリンク (Download Links)] のハイパーリンクがあります。メンテナンスリリースのハイパーリンクをクリックします。
- メンテナンスリリースが利用できない場合は、`bprd` を終了後に再起動します。`bprd` が再起動したら続行します。
  Linux の場合: `/usr/openv/netbackup/bin/bprd`
  Windows の場合: *`install_path`*`¥NetBackup¥bin¥bprd`
- メンテナンスリリースが利用可能な場合は、すぐにダウンロードします。
- すべての NetBackup 処理およびサービスを停止して、インストールの準備をします。以下に示すコマンドを使います。
  UNIX および Linux の場合: `/usr/openv/netbackup/bin/bp.kill_all`
  Windows の場合: *`install_path`*`¥NetBackup¥bin¥bpdown -f`
- メンテナンスリリースをインストールします。

- 以下のコマンドで NetBackup を再起動します。
  UNIX および Linux システムの場合:
  `/usr/openv/netbackup/bin/bp.start_all`
  Windows システムの場合: *install_path*¥NetBackup¥bin¥bpup -f

2 ディザスタリカバリパッケージのパスフレーズを設定します。パスフレーズを設定しないと、カタログバックアップが失敗します。詳細情報を参照できます。『NetBackup トラブルシューティングガイド』にある、パスフレーズについての情報を参照してください。

3 役割ベースのアクセス制御 (RBAC) を使用する場合は、セキュリティ管理者を指定する必要があります。詳細情報を参照できます。

p.132 の「NetBackup Web ユーザーインターフェースについて」を参照してください。

『NetBackup Web UI 管理者ガイド』を参照してください。

4 NetBackup とやり取りするシステムのアプリケーションを開始します。この手順には、バックアップ中のデータベースまたはシステムコンポーネントが含まれます。

5 (該当する場合) クラスタ化されたプライマリサーバーがある場合は、安全な通信のため非アクティブノードで証明書を生成します。詳細情報を参照できます。

p.128 の「クラスタ化されたプライマリサーバーの非アクティブノードで証明書を生成する」を参照してください。

6 (該当する場合) このサーバーがクラスタサーバーの場合は、クラスタ内の他のノードを更新します。次に示す標準のクラスタアップグレード処理により、クラスタ内のその他のプライマリサーバーノードを NetBackup 10.1 に更新できます。詳しくは、『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。

NetBackup リソースがオンラインでない場合はオンラインにします。

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

7 (該当する場合) 外部認証局 (ECA) を使用するプライマリサーバーまたは ECA 構成をスキップするメディアサーバーの場合は、今すぐ ECA を構成してください。詳細情報を参照できます。

https://www.veritas.com/support/en_US/article.100044300

詳しくは、『NetBackup セキュリティおよび暗号化ガイド』で外部 CA と外部証明書の章を参照してください。

8 NetBackup 10.1 にアップグレードする必要があるメディアサーバーがある場合には、この時点でアップグレードできます。メディアサーバーのアップグレードを開始したら、メディアサーバーのアップグレードが完了するまでこの手順を続行しないでください。

メモ: NetBackup では、特定のユースケースで正しく機能するようにメディアサーバーでセキュリティ証明書が必要です。このトピックに関する詳細情報を参照できます。

p.23 の「NetBackup ホスト用のセキュリティ証明書について」を参照してください。

このトピックに関する詳細情報を参照できます。

p.77 の「NetBackup 10.1 への NetBackup メディアサーバーのアップグレード」を参照してください。

9 次の項目をこの順序で再度有効にします。

- すべてのディスクステージングストレージユニット。
- すべての NetBackup ポリシー。
- すべてのストレージライフサイクルポリシー (SLP)。

10 (該当する場合) お客様の環境でクラウドストレージを使用している場合、読み取りおよび書き込みのバッファサイズを更新する必要があります。詳細情報を参照できます。

p.178 の「Amazon クラウドストレージサーバーのアップグレード後の手順」を参照してください。

11 (該当する場合) NetApp クラスタを使っている場合は、追加の手順が必要なことがあります。詳細情報を参照できます。

p.158 の「NetApp クラスタのためのアップグレード前の追加手順 」を参照してください。

12 (該当する場合) SSL が有効なクラウドとストレージサーバーについては、CRL の検証はデフォルトで有効になっています。ストレージサーバーが実行中で、CRL 機能が正しく動作していることを確認します。詳細情報を参照できます。

『NetBackup クラウド管理者ガイド』を参照してください。

13 (該当する場合) Amazon の構成では、NetBackup と CloudPoint を最新バージョンにアップグレードした後、クレデンシャルを更新する必要があります。`tpconfig -update` コマンドを実行します。アップグレード後に、クレデンシャルが AWS IAM ロールのみをサポートするように更新されます。詳細情報を参照できます。

『NetBackup Web UI クラウド管理者ガイド』を参照してください。

14 バックアップ環境を監視し、通常の NetBackup 操作が再開されていることを確認します。

15 所要時間とバックアップ時間帯の許容範囲内で、まだアップグレードしていないメディアサーバーとクライアントをアップグレードします。クライアントをアップグレードする前に、メディアサーバーをアップグレードしてください。NetBackup 8.1 クライアントを 8.1 以前のメディアサーバーにバックアップまたはリストアすることはできません。

p.77 の「NetBackup 10.1 への NetBackup メディアサーバーのアップグレード」を参照してください。

クライアントのアップグレードはクライアントのインストールと同じです。インストールのヘルプについては、『NetBackup インストールガイド - UNIX および Windows』を参照してください。

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

メモ: すべてのスクリプトは、ローカルに格納してローカルで実行する必要があります。すべてのユーザーにスクリプトの書き込み権限を与えることは推奨しません。ネットワークまたはリモートの場所からスクリプトを実行することは許可されません。NetBackup をアンインストールする際は、NetBackup の `db_ext` (UNIX の場合) または `dbext` (Windows の場合) に格納されている作成済みのスクリプトを保護する必要があります。

承認を受けた場所とスクリプトについて詳しくは、ナレッジベースの記事を参照してください。

http://www.veritas.com/docs/000126002

お使いのデータベースエージェントについて詳しくは、当該エージェントに関するマニュアルを確認してください。

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

---

16 (該当する場合) NAT が有効になっている NetBackup 8.2 Linux クラスタを最新バージョンにアップグレードする場合、アップグレードによって NAT が無効になります。NAT を有効にし、NetBackup クラスタグループに追加された `nbmqbroker` サービスをクラスタで監視できるようにするには、次のコマンドを実行します。

- デフォルトのポートを使用して構成するには:

  ```
  configureMQ -enableCluster -defaultPorts
  ```

- 特定のポートを使用して構成するには:

```
configureMQ -enableCluster -externalPort port1 -internalPorts
port2port3port4
```

17 その他のアップグレード手順を実行します。このトピックに関する詳細情報を参照できます。

p.74 の「アップグレード後のシステムの更新」を参照してください。

NetBackup の起動と停止のスクリプトについて

NetBackup をインストールするとき、インストールスクリプトは起動と停止のスクリプトの構成も実行します。起動スクリプトを使用して、システムがブートする際に NetBackup デーモンを自動的に起動することができます。停止スクリプトを使用して、システムを停止する際に起動スクリプトを自動的に終了することができます。

インストール処理はオペレーティングシステムの適切な場所に NetBackup の起動と停止のスクリプトをコピーします。

非クラスタ環境でのアップグレードの場合、既存の NetBackup 関連の起動および停止スクリプトは保存され、新しいバージョンのスクリプトがインストールされます。

表 3-1には、NetBackup のインストール中にインストールされる各種のプラットフォームの起動スクリプトとシャットダウンスクリプトのリンクがリストされます。

表 3-1 プラットフォーム別の NetBackup の起動と停止のスクリプトのリンク

プラットフォーム	リンク

AIX	`/etc/rc.netbackup.aix`
	■ レベル 2 でのブート中にこのスクリプトが呼び出されるように、NetBackup のインストールスクリプトによって `/etc/inittab` ファイルが編集され、次に示すエントリが追加されました。
	`netbackup:2:wait:/etc/rc.netbackup.aix`
	■ 停止するには、次に示す行を `/etc/rc.shutdown` ファイルに追加します。
	`/etc/rc.netbackup.aix stop`

Linux Debian	`/etc/rc0.d/K01netbackup ->/etc/init.d/netbackup`
	`/etc/rc1.d/K01netbackup ->/etc/init.d/netbackup`
	`/etc/rc2.d/S95netbackup ->/etc/init.d/netbackup`

プラットフォーム	リンク
Red Hat Linux	/etc/rc.d/rc0.d/K01netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc1.d/K01netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc2.d/S77netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc3.d/S77netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc5.d/S77netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc6.d/K01netbackup ->/etc/rc.d/init.d/netbackup
SuSE Linux	/etc/init.d/rc0.d/K01netbackup ->/etc/init.d/netbackup /etc/init.d/rc2.d/S77netbackup ->/etc/init.d/netbackup /etc/init.d/rc3.d/S77netbackup ->/etc/init.d/netbackup /etc/init.d/rc5.d/S77netbackup ->/etc/init.d/netbackup /etc/init.d/rc6.d/K01netbackup ->/etc/init.d/netbackup
Solaris	/etc/rc0.d/K01netbackup ->/etc/init.d/netbackup /etc/rc1.d/K01netbackup ->/etc/init.d/netbackup /etc/rc2.d/S77netbackup ->/etc/init.d/netbackup

アップグレード後のシステムの更新

サーバーおよびクライアントのアップグレード後に、NetBackup 環境の更新を完了するには、追加作業が必要となる場合があります。

ご使用の NetBackup 環境で、次のいずれかの手順を実行します。

プライマリサーバーの権限	root 以外のユーザーが NetBackup を管理することを許可されているプライマリサーバーをアップグレードした場合は、権限とグループを再構成する必要があります。新しくインストールされたファイルのデフォルトの権限およびグループでは、root ユーザーだけが NetBackup の管理を実行できます。
ターゲットの自動イメージレプリケーション (AIR) のリモートプライマリサーバー間の信頼関係を更新します。	ソースとターゲットの両方のプライマリサーバーを 8.0 以前から 8.1 以降にアップグレードした後に、信頼関係を更新する必要があります。NetBackup 8.1 から以降のバージョンにアップグレードする場合、信頼関係を再確立する必要はありません。信頼関係を再確立するには、ソースとターゲットの両方のプライマリサーバーで表示されているコマンドを実行します。 `nbseccmd -setuptrustedmaster -update` 詳細情報を参照できます。『NetBackup コマンドリファレンスガイド』を参照してください。
アドオン製品	アップグレードされたすべてのクライアント上のアドオン製品 (NetBackup 言語パッケージなど) をアップグレードします。すべてのアドオン製品は NetBackup クライアントと同じバージョンである必要があります。
NetBackup スクリプト	アップグレード前に NetBackup スクリプトを変更した場合は、それらの変更を新しくアップグレードしたスクリプトに適用します。
外部認証局	外部認証局を構成します。セキュリティ構成をスキップすることを選択した場合、または環境で ECA を使用する場合は、ECA の構成が必要になる場合があります。ECA を構成する方法について詳しくは、次を参照してください。 https://www.veritas.com/support/en_US/article.100044300 詳しくは、『NetBackup セキュリティおよび暗号化ガイド』で外部 CA と外部証明書の章を参照してください。

ストレージサーバーの更新	NetBackup は、ストレージが変更されるたびにストレージサーバーやディスクプールなどのオブジェクトを更新するわけではありません。ストレージの変更は、NetBackup MSDP の変更や、サードパーティの OST ベンダーソフトウェアのアップグレードによって発生する可能性があります。さらに、SLP レプリケーションで使用されるストレージ定義のレプリケーショントポロジーの変更や、インポート操作には更新が必要です。ユーザーは、`updatests` コマンドや `updatedp` コマンドを使用して、これらの変更を事前に確認する必要があります。NetBackup のアップグレードでは、使用環境で活用できる新機能が導入されることがあります。この新機能を使用するストレージサーバーやディスクプールで `updatests` コマンドや `updatedp` コマンドを実行することをお勧めします。`updatests` および `updatedp` 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 アクセス制御または拡張監査	環境内で NetBackup アクセス制御または拡張監査が有効になっている場合は、プライマリサーバー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。

4

メディアサーバーのアップグレード

この章では以下の項目について説明しています。

NetBackup 10.1 への NetBackup メディアサーバーのアップグレード

メディアサーバーのアップグレード方法は、NetBackup アップグレードスクリプトによる方法、Linux のネイティブインストーラによる方法、VxUpdate による方法の 3 種類があります。NetBackup アップグレードスクリプトによる方法は標準的なアップグレード方法で、新規ユーザーにお勧めです。Linux のネイティブインストーラによる方法は難易度が高い場合があり、追加の手順も必要です。VxUpdate は、リモートインストール機能とユーザー定義のスケジュールによるアップグレード機能を備えています。

MSDP を使うメディアサーバーのアップグレードには、ローリングデータ変換が含まれます。ローリング変換は、システムがビジー状態ではないときに実行されます。つまり変換は、バックアップ、リストア、CRQP、CRC チェック、圧縮などが非アクティブのときに実行されます。この変換では、通常のシステム操作への影響は予想されていません。ローリング変換が完了すると、変換後のシステムと新しいインストールの間で違いはありません。

NetBackup では、メディアサーバーが正しく機能するためにセキュリティ証明書を必要とします。このトピックに関する詳細情報を参照できます。

p.23 の「NetBackup ホスト用のセキュリティ証明書について」を参照してください。

NetBackup には、NetBackup のサポート対象バージョンすべての管理コンソールが含まれています。NetBackup のサポート対象バージョンについて詳しくは、次を参照してください。

https://sort.veritas.com/eosl

NetBackup 8.1.2 アップグレードに RHEL 7.5 へのアップグレードが含まれており、ファイバートランスポートメディアサーバー (FTMS) を使用する場合には、追加の手順が必要になります。詳細情報を参照できます。

p.34 の「NetBackup 10.1 による RHEL 7.5 以降でのファイバートランスポートメディアサーバーのサポートについて」を参照してください。

表 4-1　　メディアサーバーの移行手順

手順	作業	完了
1	メディアサーバーのアップグレードがプライマリサーバーのアップグレードに含まれる場合は、次のステップに進みます。 含まれない場合は、メディアサーバーを無効にします。	
2	NetBackup のすべてのサービスを停止します。 ■ Linux システムの場合: `/usr/openv/netbackup/bin/bp.kill_all` ■ Windows システムの場合: *install_path*¥NetBackup¥bin¥bpdown -f	
3	NetBackup バイナリをアップグレードします。このトピックについて詳しくは、以下のページを参照してください。 ■ p.42 の「Windows システムでローカルサーバー、リモートサーバー、クラスタサーバーのアップグレードを実行する」を参照してください。 ■ p.54 の「Windows システムでのサイレントアップグレードの実行」を参照してください。 ■ p.58 の「NetBackup 10.1 への Linux サーバーソフトウェアのアップグレード」を参照してください。 ■ p.80 の「Linux での NetBackup メディアサーバーソフトウェアのサイレントアップグレード」を参照してください。 ■ p.105 の「VxUpdate について」を参照してください。	
4	セキュリティ証明書を取得しなかった場合は、証明書を生成します。このトピックに関する詳細情報を参照できます。 p.23 の「NetBackup ホスト用のセキュリティ証明書について」を参照してください。	

手順	作業	完了
5	利用可能な NetBackup 10.1 メンテナンスリリースを確認します。メンテナンスリリースは NetBackup 10.1 の後にリリースされる非常に重要な修正が含まれます。ベリタスはアップグレードアクティビティ時に最新の利用可能なメンテナンスリリースをインストールすることを推奨します。 最新の NetBackup 10.1 メンテナンスリリースにアクセスする方法 **1** Veritas SORT の Web サイトに移動します。 https://sort.veritas.com/netbackup **2** [インストールとアップグレードのチェックリスト (Installation and Upgrade Checklist)] セクション: ■ [製品 (Product)] で、正しい製品 (NetBackup Enterprise Server または NetBackup Server) を選択します。 ■ [これからインストールまたはアップグレードする製品のバージョン (Product version you are installing or upgrading to)] で、NetBackup 最新バージョンを指定します。 ■ [プラットフォーム (Platform)] で、アップグレードするサーバーのプラットフォームを選択します。 ■ [プロセッサ (Processor)] で、サーバーのプロセッサを指定します。 ■ [アップグレードされる製品のバージョン (Product version you are upgrading from (Optional))] で、アップグレードするサーバーの NetBackup の現在のバージョンを選択します。 ■ [チェックリストの生成 (Generate Checklist)] をクリックします。 **3** [アップグレード情報 (Upgrade Information)] に *version_number* [ダウンロードリンク (Download Links)] のハイパーリンクがあります。メンテナンスリリースのハイパーリンクをクリックします。 **4** メンテナンスリリースが利用可能ではない場合は手順 6 に進みます。 **5** メンテナンスリリースが利用可能な場合は、すぐにダウンロードします。 **6** すべての NetBackup 処理およびサービスを停止して、インストールの準備をします。以下に示すコマンドを使います。 Linux の場合: `/usr/openv/netbackup/bin/bp.kill_all` Windows の場合: *`install_path`*`¥NetBackup¥bin¥bpdown -f` **7** メンテナンスリリースをインストールします。 **8** 以下のコマンドで NetBackup を再起動します。 Linux システムの場合: `/usr/openv/netbackup/bin/bp.start_all` Windows システムの場合: *`install_path`*`¥NetBackup¥bin¥bpup -f`	

手順	作業	完了
6	(該当する場合) メディアサーバーのアップグレードがプライマリサーバーのアップグレードに含まれる場合は、このステップはスキップします。 メディアサーバーを再度アクティブにします。	
7	(該当する場合) メディアサーバーのアップグレードがプライマリサーバーのアップグレードに含まれる場合は、プライマリサーバーのアップグレード手順を再開します。	

Linux での NetBackup メディアサーバーソフトウェアのサイレントアップグレード

ネイティブインストーラを使用して、NetBackup の Linux メディアサーバーをアップグレードできます。NetBackup インストールスクリプトまたは優先するインストーラによる方式のいずれかを使用できます。

Linux の場合: `rpm`、`yum` など

インストールまたはアップグレードに成功すると、`/usr/openv/pack/install.history` ファイルに記録されます。

注意: ネイティブインストーラを使用して NetBackup Red Hat と SUSE Linux をアップグレードする前に、NetBackup Nutanix プラグインパッケージを削除する必要があります。Nutanix プラグインと NetBackup は同じライブラリを同じ場所にインストールするため、削除しないとアップグレードに失敗します。アップグレードが失敗すると、「`install of package_name conflicts with file from package package_name`」というエラーメッセージが表示されます。

NetBackup をアップグレードする前に、次のコマンドを使用してプラグインをアンインストールします。

```
rpm -e VRTSnbntnxahv*
```

ネイティブインストーラを使用して Linux メディアサーバーバイナリをアップグレードするには:

1. メディアサーバーの /tmp ディレクトリに NetBackup インストール応答ファイル (NBInstallAnswer.conf) を作成してください。応答ファイルとその内容に関する詳しい情報を参照できます。

   p.133 の「NetBackup 応答ファイルについて」を参照してください。

2. (該当する場合) お使いの環境で NetBackup 認証局を使用しており、メディアサーバーがすでに NetBackup 認証局に対して構成されている場合、4 に進みます。それ以外の場合は、NBInstallAnswer.conf に次の必要な情報を指定します。

   CA_CERTIFICATE_FINGERPRINT=*fingerprint*

   例 (指紋の値は読みやすくするため折り返されています):

   ```
   CA_CERTIFICATE_FINGERPRINT=01:23:45:67:89:AB:CD:EF:01:23:45:67:
   89:AB:CD:EF:01:23:45:67
   ```

   お使いの NetBackup 環境のセキュリティ構成に応じて、応答ファイルに AUTHORIZATION_TOKEN オプションを追加する必要があります。AUTHORIZATION_TOKEN オプションに関する詳しい情報を参照できます。

   p.133 の「NetBackup 応答ファイルについて」を参照してください。

3. (該当する場合) お使いの環境で外部認証局を使用しており、メディアサーバーがすでに外部認証局に対して構成されている場合、4 に進みます。それ以外の場合は、NBInstallAnswer.conf に次の必要な情報を指定します。

   - ECA_CERT_PATH
     このフィールドを使用して、外部証明書ファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
   - ECA_TRUST_STORE_PATH
     このフィールドを使用して、トラストストアの場所を示すファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
   - ECA_PRIVATE_KEY_PATH
     このフィールドを使用して、秘密鍵を示すファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
   - ECA_KEY_PASSPHRASEFILE
     このフィールドを使用して、キーストアにアクセスするためのパスフレーズを含むファイルのパスとファイル名を指定します。このフィールドは省略可能で、ファイルから外部証明書を設定する場合にのみ適用されます。
   - ECA_CRL_CHECK_LEVEL

このフィールドを使用して、CRL モードを指定します。このフィールドは必須です。サポートされる値は次のとおりです。

- USE_CDP: 証明書に定義されている CRL を使用します。
- USE_PATH: ECA_CRL_PATH で指定されたパスにある CRL を使用します。
- DISABLED: CRL を使用しません。

- ECA_CRL_PATH
  このフィールドを使用して、外部 CA 証明書に関連付けられている CRL へのパスを指定します。このフィールドは、ECA_CRL_CHECK_LEVEL が USE_PATH に設定されている場合にのみ必要です。該当しない場合は、このフィールドを空のままにします。

4 また、NBInstallAnswer.conf ファイルに表示される省略可能なパラメータを追加できます。

- 追加の SERVER エントリ

各オプションに関する詳細情報を参照できます。

p.133 の「NetBackup 応答ファイルについて」を参照してください。

5 十分な容量があるシステムに、サーバープラットフォームに一致するサーバーパッケージをダウンロードします。次に、必要なサーバーパッケージを抽出します。

サーバーパッケージファイルの内容を抽出します。例:

- Linux Red Hat の場合:
  ```
  tar -xzvf NetBackup_10.1_LinuxR_x86_64.tar.gz
  ```
- Linux SuSE の場合:
  ```
  tar -xzvf NetBackup_10.1_LinuxS_x86_64.tar.gz
  ```

6 目的のオペレーティングシステムのディレクトリに移動し、サーバーのファイルをメディアサーバーにコピーします。

オペレーティングシステムのディレクトリ:

- Linux Red Hat の場合:
  ```
  NetBackup_10.1_LinuxR_x86_64/linuxR_x86/anb
  ```
- Linux SuSE の場合:
  ```
  NetBackup_10.1_LinuxS_x86_64/linuxS_x86/anb
  ```

サーバーのファイルを、インストール先のコンピュータにコピーします。

- Linux: VRTSnetbp.rpm、VRTSnbslibs.rpm、および VRTSpddes.rpm
- Linux Red Hat: VRTSpddei.rpm

7 クライアントバイナリを抽出し、メディアサーバーにコピーします。

クライアントバイナリを抽出します。

```
tar -xzvf client_dist.tar.gz
```

目的のオペレーティングシステムのディレクトリに移動します。

- Red Hat: `openv/netbackup/client/Linux/RedHat3.10.0`
- SuSE: `openv/netbackup/client/Linux/SuSE3.0.76`

以下に示すファイルをメディアサーバーにコピーします。

メモ: Java GUI と JRE のアップグレードは省略可能です。アップグレードしない場合は、`VRTSnbjava` と `VRTSnbjre` パッケージのコピーとインストールを省略します。

アップグレードしないことを選択した場合、Veritas は、古い Java GUI および JRE パッケージを削除することをお勧めします。

p.131 の「アップグレード後の Java GUI と JRE の追加または削除」を参照してください。

Linux の場合:

```
VRTSnbpck.rpm
VRTSpbx.rpm
VRTSnbclt.rpm
VRTSnbclibs.rpm
VRTSnbjre.rpm
VRTSnbjava.rpm
VRTSpddea.rpm
VRTSnbcfg.rpm
```

8 Veritas 事前チェックパッケージをインストールします。

Linux: `rpm -U VRTSnbpck.rpm`

9 (該当する場合) NetBackup 8.0 より前のバージョンからアップグレードする場合は、古い `SYMC*` パッケージを削除します。次の例は、`SYMC` RPM パッケージの削除に使用するコマンドを示しています。このプロセスでは、NetBackup の構成が保持されます。

```
rpm -e SYMCnbjava
rpm -e SYMCpddea
rpm -e SYMCnbclt
rpm -e SYMCnbjre
rpm -e SYMCpddes
rpm -e SYMCnetbp
```

10 以下のコマンドを示されている順序で実行してファイルをインストールします。

メモ: Java GUI と JRE のアップグレードは省略可能です。アップグレードしない場合は、VRTSnbjava と VRTSnbjre パッケージのコピーとインストールを省略します。

アップグレードしないことを選択した場合、Veritas は、古い Java GUI および JRE パッケージを削除することをお勧めします。

p.131 の「アップグレード後の Java GUI と JRE の追加または削除」を参照してください。

Linux

```
rpm –U VRTSpbx.rpm
rpm –U VRTSnbclt.rpm
rpm –U VRTSnbclibs.rpm
rpm –U VRTSnbjre.rpm
rpm –U VRTSnbjava.rpm
rpm –U VRTSpddea.rpm
rpm –U VRTSpddes.rpm
rpm –U VRTSpddei.rpm
rpm –U VRTSnbcfg.rpm
rpm –U VRTSnetbp.rpm
rpm –U VRTSnbslibs.rpm
```

VRTSpddei.rpm は Linux Red Hat でのみ使用される点に注意してください。

11 古いバージョンの Java GUI と JRE を使う予定がない場合は、削除することをお勧めします。

- Linux の場合:

```
rpm -e VRTSnbjava.rpm
rpm -e VRTSnbjre.rpm
```

5

NetBackup の MSDP のアップグレード

この章では以下の項目について説明しています。

NetBackup 8.1 での MSDP のアップグレードの考慮事項

NetBackup 8.1 での MSDP の指紋アルゴリズムの変更により、アップグレードパスの計画時に MSDP 環境を検討する必要があります。指紋アルゴリズムが刷新されるため、NetBackup 8.0 以前のホストは NetBackup 8.1 の MSDP にアクセスできません。NetBackup ジョブの失敗は、この条件を計画しなかったことによるものである可能性があります。

8.1 MSDP ストレージサーバーのメディアサーバーリストに 8.0 以前のサーバーが含まれる場合、アルゴリズムが刷新されたことにより不具合が生じる可能性があります。8.1 と 8.0 のサーバーの共通のメディアサーバーが 8.0 のサーバーである場合、ジョブが失敗する可能性があります。Client Direct を使用する場合、クライアントを 8.1 にアップグレードする必要があります。アップグレードしない場合、Client Direct リストアでエラーが発生する可能性があります。これらの不具合は、8.0 以前のホストが 8.1 のサーバーにアクセスできないことが原因です。

MSDP 環境の一部として複数のメディアサーバーが存在する場合、アップグレードを計画するときに次に示すオプションを検討します。

- アクセス権を相互に共有するすべての MSDP メディアサーバーをアップグレードします。これらの MSDP ディスクプールへの Client Direct を使用するすべてのクライアントをアップグレードします。
  このオプションでは、環境で中断が発生することはありません。
- 環境で Client Direct を使用できて設定を変更しない場合、Client Direct を使用して MSDP メディアサーバーとクライアントをアップグレードします。
  選択した共通メディアサーバーが NetBackup 8.1 サーバーではない場合、リストア、検証、インポート、最適化複製が失敗するリスクがあります。古いクライアントで Client Direct を使用する場合、Client Direct リストアでエラーが発生する可能性があります。この不具合は、アルゴリズムが変更されたことにより発生します。
- 環境で Client Direct を使用できる場合、Client Direct を使用して MSDP メディアサーバーとクライアントをアップグレードします。アップグレードされるストレージサーバーが NetBackup 8.1 サーバーのみ含むように、クレデンシャルを持つメディアサーバーリストを修正します。
  この処理によって、アップグレードされないサーバーがアップグレードされるサーバーにアクセスする権限が効果的に無効になります。アクセス権限の変更により、以前設定された操作が動作を停止するリスクがあります。このオプションを選択する場合、すべてのメディアサーバーがアップグレードされた後、変更を戻せるように、設定変更を詳細に書き留めてください。
  複製ジョブが 8.1 MSDP から 8.0 以前の MSDP に複製する場合、以前の MSDP のストレージユニットを作成します。その新しいストレージユニットの[メディアサーバー (Media Servers)]リストを 8.1 ホストに制限します。ストレージライフサイクルポリシー (SLP) が管理する複製ジョブが 8.0 以前の MSDP ホストから 8.1 MSDP ホストに複製する場合、それらのジョブを変更する必要があります。複製ステージの[代替読み込みサーバー (Alternate Read Server)]を 8.1 メディアサーバーに設定します。

MSDP ローリングデータ変換について

NetBackup 8.0 では、既存の Blowfish アルゴリズムに置き換わる AES 暗号化アルゴリズムが導入されました。NetBackup 8.1 では、既存の MD5 のようなアルゴリズムに換わる SHA2 指紋アルゴリズムが導入されました。暗号化と指紋アルゴリズムの双方へのアップグレードは、データのセキュリティを向上させるために設計されています。

NetBackup 8.1 にアップグレードされた環境には、新しい形式に変換する必要がある Blowfish で暗号化されたデータと MD5 のような指紋が含まれている場合があります。変換を処理してデータを保護するには、新しい内部タスクで現在のデータコンテナを AES 暗号化と SHA-2 指紋アルゴリズムに変換します。この新しいタスクは、ローリングデータ変換と呼ばれます。

ローリングデータ変換は、すべての既存のデータコンテナを処理します。Blowfish アルゴリズムを使ってデータが暗号化されている場合、データは AES アルゴリズムを使って再暗号化されます。それから、新しい SHA-2 指紋が生成されます。変換後、データコン

テナには、.bhd と .bin ファイルに加えて、.map 拡張子を持つ新しいファイルが収められます。.map ファイルには、SHA-2 と MD5 に似たアルゴリズムの指紋間のマッピングが含まれています。.bhd ファイルには、SHA-2 指紋が含まれています。

NetBackup 8.1 の新規インストールでは、ローリングデータ変換は[完了 (Finished)]としてマークされ、それ以降は起動しません。NetBackup 8.1 へのアップグレード場合は、ローリングデータ変換はデフォルトでは有効であり、MSDP 変換の完了後にバックグラウンドで動作します。変換されるのは、アップグレードの前に存在していたデータのみです。すべての新しいデータは新しい SHA-2 の指紋を使用するため、変換の必要がありません。

crcontrol コマンドを使用してローリングデータ変換を管理および監視できます。使用方法に関する詳細情報を参照できます。

『NetBackup 重複排除ガイド』および『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

MSDP 指紋アルゴリズムの変更について

NetBackup 8.1 では、メディアサーバー重複排除プール (MSDP) でよりセキュアな指紋アルゴリズムが導入されます。既存の MD5 のようなアルゴリズムは、SHA2 アルゴリズムに換わりました。NetBackup 8.1 は両方の指紋の種類を処理できるため、新しいサーバーは古いクライアントおよび古いサーバーと互換性があります。変換は、古いクライアントおよび古いサーバーと新しいサーバー間の通信中に発生します。指紋の変換には、追加の計算時間が必要になります。古いクライアントと古いサーバーおよび新しいサーバー間の通信は、クライアントとサーバーの両方が新しい場合よりも低速になります。

MD5 のようなアルゴリズムと SHA-2 アルゴリズムの両方を使用する混在環境のメディアサーバーの場合、最初のバックアップでは重複排除率が低下する可能性があります。アルゴリズムによりメディアサーバーを分割して、それぞれのサーバーに異なるストレージユニットを作成することを推奨します。

詳細情報を参照できます。

『NetBackup 重複排除ガイド』

6

クライアントのアップグレード

この章では以下の項目について説明しています。

クライアントのアップグレードについて

クライアントコンピュータのプライマリサーバーとメディアサーバーをアップグレードすると、クライアントコンピュータをアップグレードできます。関連付けられたプライマリサーバーとメディアサーバーをアップグレードする前に、クライアントコンピュータをアップグレードしないでください。

Veritas は、クライアントコンピュータのアップグレードには、わずかながら問題があると考えています。クライアントコンピュータには最小の NetBackup バイナリしか存在せず、NetBackup データベースは存在しませんが、お客様によっては、クライアントコンピュータでミッションクリティカルなデータベースまたはビジネス固有の一意のアプリケーションをホストできると考える場合もあります。そのため、クライアントコンピュータを確認し、重要なデータベースやアプリケーションへのアクセスが中断されないように、リソースを追加する必要があるかどうかを判断してください。

Veritas は、次の 3 つのクライアントアップグレード方法をサポートしています。

- NetBackup アップグレードスクリプト。NetBackup アップグレードスクリプトによる方法は標準的なアップグレード方法で、新規ユーザーにお勧めです。詳細情報を参照できます。

p.42 の「Windows システムでローカルサーバー、リモートサーバー、クラスタサーバーのアップグレードを実行する」を参照してください。
p.89 の「NetBackup アップグレードスクリプトによる UNIX および Linux クライアントのアップグレード」を参照してください。

- UNIX および Linux のネイティブインストーラ。UNIX および Linux のネイティブインストーラによる方法は難易度が高い場合があり、追加の手順も必要です。詳細情報を参照できます。
  p.91 の「ネイティブインストーラによる UNIX と Linux のクライアントバイナリのアップグレード」を参照してください。
- VxUpdate。VxUpdate は LiveUpdate に代わるもので、クライアントコンピュータのクライアントアップグレードをスケジュール設定できます。詳細情報を参照できます。
  p.105 の「VxUpdate について」を参照してください。

NetBackup アップグレードスクリプトによる UNIX および Linux クライアントのアップグレード

UNIX および Linux クライアントで NetBackup 10.1 にアップグレードするには、次の手順を使用します。

NetBackup アップグレードスクリプトを使用して UNIX および Linux クライアントをアップグレードするには

1. root ユーザーとしてクライアントにログインします。
2. ESD イメージ (ダウンロード済みファイル) がある場所に移動し、次のコマンドを入力します。

   ```
   ./install
   ```

3 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。

```
Veritas Installation Script
Copyright (c) 2019 Veritas Technologies LLC. All rights reserved.


                Installing NetBackup Client Software


Please review the VERITAS SOFTWARE LICENSE AGREEMENT located on
the installation media before proceeding. The agreement includes
details on the NetBackup Product Improvement Program.

For NetBackup installation and upgrade information specific to
your
platform and to find out if your installed EEBs or hot fixes are
contained in this release, check the Installation and Upgrade
checklists
and the Hot Fix and EEB Release Auditor, both available on the
Veritas
Services and Operations Readiness Tools (SORT) page:
https://sort.veritas.com/netbackup.

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

4 NetBackup で必要なシステム条件を確認したら、Enter キーを押して続行します。

```
Do you want to install the NetBackup client software for this
client? [y,n] (y)
```

5 (該当する場合) 環境で NetBackup 認証局を使用する場合は、インストーラによって証明書の詳細が取得され、情報の確認を求められます。認証局の情報を確認すると、認証トークンの情報の入力を求められます。

6 環境で外部認証局を使用する場合は、表示されたプロンプトで外部認証局の情報を入力します。

```
Enter the certificate file path or q to skip security
configuration:
/usr/eca/cert_chain.pem

Enter the trust store location or q to skip security
configuration:
/usr/eca/trusted/cacerts.pem

Enter the private key path or q to skip security configuration:
/usr/eca/private/key.pem

Enter the passphrase file path or q to skip security configuration
(default: NONE): /usr/eca/private/passphrase.txt
```

メモ: パスフレーズファイルのパスの入力は任意です。

7 プロンプトが表示されたら、アップグレードで Java GUI と JRE バイナリをどのように処理するかを指定します。

```
The Java GUI and JRE packages are currently install_state on this
host.

The Java GUI and JRE can be optionally included with NetBackup.
The Java GUI and JRE enable the Backup, Archive and Restore (BAR)
GUI. Choose an option from the list below.

1) Update the Java GUI and JRE.

2) Remove the Java GUI and JRE.
```

1 を指定すると、サーバーの状態に基づいて Java および JRE のバイナリがインストールまたはアップグレードされます。2 を指定すると、サーバーの状態に基づいて Java および JRE のバイナリが削除または除外されます。

8 問題がない場合、インストーラはエラーなしで終了します。

ネイティブインストーラによる UNIX と Linux のクライアントバイナリのアップグレード

ネイティブインストーラを使用して、NetBackup の UNIX および Linux クライアントをアップグレードできます。NetBackup インストールスクリプトまたは優先するインストーラによる

方法のいずれかを使用できます。ただし、Debian パッケージを使用するクライアントには当てはまりません。これらのクライアントは、NetBackup インストールスクリプトを使用してアップグレードする必要があります。

- AIX の場合: `lslpp`、`installp`
- Linux の場合: `rpm`、`yum` など
- Solaris の場合: `pkginfo`、`pkgadd`

インストールまたはアップグレードに成功すると、`/usr/openv/pack/install.history` ファイルに記録されます。

注意: ネイティブインストーラを使用して NetBackup Red Hat と SUSE Linux をアップグレードする前に、NetBackup Nutanix プラグインパッケージを削除する必要があります。Nutanix プラグインと NetBackup は同じライブラリを同じ場所にインストールするため、削除しないとアップグレードに失敗します。アップグレードが失敗すると、「`install of package_name conflicts with file from package package_name`」というエラーメッセージが表示されます。

NetBackup をアップグレードする前に、次のコマンドを使用してプラグインをアンインストールします。

```
rpm -e VRTSnbntnxahv*
```

ネイティブインストーラを使用して UNIX または Linux クライアントバイナリをアップグレードするには

1. クライアントの /tmp ディレクトリに NetBackup インストール応答ファイル (NBInstallAnswer.conf) を作成してください。応答ファイルとその内容に関する詳しい情報を参照できます。

   p.133 の「NetBackup 応答ファイルについて」を参照してください。

2. (該当する場合) お使いの環境で NetBackup 認証局を使用しており、クライアントがすでに NetBackup 認証局に対して構成されている場合、5 に進みます。それ以外の場合は、NBInstallAnswer.conf に必要な情報 () を指定します。

   CA_CERTIFICATE_FINGERPRINT=*fingerprint*

   例 (指紋の値は読みやすくするため折り返されています):

   CA_CERTIFICATE_FINGERPRINT=01:23:45:67:89:AB:CD:EF:01:23:45:67:
   89:AB:CD:EF:01:23:45:67

   お使いの NetBackup 環境のセキュリティ構成に応じて、応答ファイルに AUTHORIZATION_TOKEN オプションを追加する必要があります。AUTHORIZATION_TOKEN オプションに関する詳しい情報を参照できます。

   p.133 の「NetBackup 応答ファイルについて」を参照してください。

3. (該当する場合) お使いの環境で外部認証局を使用しており、クライアントがすでに外部認証局に対して構成されている場合、5 に進みます。それ以外の場合は、NBInstallAnswer.conf に必要な情報 () を指定します。

   - SET ECA_CERT_PATH=*path*
     このフィールドを使用して、外部証明書ファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
   - SET ECA_TRUST_STORE_PATH=*path*
     このフィールドを使用して、トラストストアの場所を示すファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
   - SET ECA_PRIVATE_KEY_PATH=*path*
     このフィールドを使用して、秘密鍵を示すファイルのパスとファイル名を指定します。このフィールドは、ファイルから外部証明書を設定する場合に必要です。
   - SET ECA_KEY_PASSPHRASEFILE=*path*
     このフィールドを使用して、キーストアにアクセスするためのパスフレーズを含むファイルのパスとファイル名を指定します。このフィールドは省略可能で、ファイルから外部証明書を設定する場合にのみ適用されます。
   - SET ECA_CRL_CHECK_LEVEL=*value*

このフィールドを使用して、CRL モードを指定します。このフィールドは必須です。サポートされる値は次のとおりです。

- USE_CDP: 証明書に定義されている CRL を使用します。
- USE_PATH: ECA_CRL_PATH で指定されたパスにある CRL を使用します。
- DISABLED: CRL を使用しません。

- SET ECA_CRL_PATH=*path*
  このフィールドを使用して、外部 CA 証明書に関連付けられている CRL へのパスを指定します。このフィールドは、ECA_CRL_CHECK_LEVEL が USE_PATH に設定されている場合にのみ必要です。該当しない場合は、このフィールドを空のままにします。

4 (該当する場合) ネットワークアドレス変換 (NAT) クライアントをサポートするように NetBackup プライマリサーバーが構成されている場合、次の必要な情報を NBInstallAnswer.conf に入力します。

```
ACCEPT_REVERSE_CONNECTION=TRUE
```

詳細情報を参照できます。p.133 の「NetBackup 応答ファイルについて」を参照してください。

5 また、NBInstallAnswer.conf ファイルに表示される省略可能なパラメータを追加できます。

- SERVICES=no
- MERGE_SERVER_LIST=*value*

各オプションに関する詳細情報を参照できます。

p.133 の「NetBackup 応答ファイルについて」を参照してください。

6 適切なクライアントパッケージから必要なクライアントファイルを抽出して、クライアントコンピュータにコピーします。

- 十分な容量があるシステムに UNIX クライアント用の CLIENTS1 パッケージをダウンロードする
- 十分な容量があるシステムに Linux クライアント用の CLIENTS2 パッケージをダウンロードする
- CLIENTS1 ファイルまたは CLIENTS2 ファイルの内容を抽出する
  例:

AIX	`gunzip NetBackup_10.1_CLIENTS1.tar.gz; tar -xvf NetBackup_10.1_CLIENTS1.tar`
Linux	`tar -xzvf NetBackup_10.1_CLIENTS2.tar.gz`
Solaris	`tar -xzvf NetBackup_10.1_CLIENTS1.tar.gz`

- 目的のオペレーティングシステムのディレクトリに移動します。
  例:

AIX

```
CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/RS6000/AIX7/
```

Linux

Linux Red Hat の場合:

```
CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux/RedHat2.6.18/
```

Linux SuSE の場合:

```
CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux/SuSE3.0.76
```

Linux - s390x

Linux-s390x Red Hat の場合:

```
CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/
Linux-s390x/IBMzSeriesRedHat2.6.18/
```

Linux-s390x SuSE の場合:

```
CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/
Linux-s390x/IBMzSeriesSuSE3.0.76
```

Linux - ppc64le

Linux-ppc64le Red Hat の場合:

```
CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/
Linux-ppc64le/IBMpSeriesRedHat3.10.0/
```

Linux-ppc64le SuSE の場合:

```
CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/
Linux-ppc64le/IBMpSeriesSuSE4.4.21
```

Solaris

Solaris SPARC の場合:

```
CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/Solaris/Solaris10/
```

Solaris x86 の場合:

```
CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/Solaris/Solaris_x86_10_64/
```

- 以下に示すファイルをクライアントコンピュータにコピーします。

メモ: Java GUI と JRE のアップグレードは省略可能です。アップグレードしない場合は、VRTSnbjava と VRTSnbjre パッケージのコピーとインストールを省略します。

アップグレードしないことを選択した場合は、古い Java GUI および JRE パッケージを削除することをお勧めします。

p.131 の「アップグレード後の Java GUI と JRE の追加または削除」を参照してください。

AIX

```
VRTSnbpck.image
VRTSpbx.image.gz
VRTSnbclt.image.gz
VRTSnbclibs.image.gz
VRTSnbjre.image.gz
VRTSnbjava.image.gz
VRTSpddea.image.gz
VRTSnbcfg.image.gz
```

Linux

```
VRTSnbpck.rpm
VRTSpbx.rpm
VRTSnbclt.rpm
VRTSnbclibs.rpm
VRTSnbjre.rpm
VRTSnbjava.rpm
VRTSpddea.rpm
VRTSnbcfg.rpm
```

メモ: VRTSnbjre.rpm、VRTSnbjava.rpm、VRTSpddea.rpm の各ファイルは、IBM pSeries クライアントではサポートされません。

Solaris

```
.pkg_defaults
VRTSnbpck.pkg.gz
VRTSpbx.pkg.gz
VRTSnbclt.pkg.gz
VRTSnbclibs.pkg.gz
VRTSnbjre.pkg.gz
VRTSnbjava.pkg.gz
VRTSpddea.pkg.gz
VRTSnbcfg.pkg.gz
```

メモ: Solaris クライアントバイナリには .pkg_defaults という非表示の管理ファイルが含まれます。この管理ファイルには、デフォルトのインストール処理が含まれています。

メモ: z/Architecture クライアント用の VRTSpddea.rpm はないことに注意してください。

メモ: VRTSnbjre.rpm、VRTSnbjava.rpm、VRTSpddea.rpm の各ファイルは、IBM pSeries クライアントではサポートされません。

7 (該当する場合) Solaris および AIX でのみ、次のコマンドを使用して圧縮パッケージファイルを抽出します。

```
gunzip VRTS*.*
```

この処理で、以下に示すすべてのパッケージファイルが抽出されます。

```
VRTSnbpck.pkg
VRTSpbx.pkg
VRTSnbclt.pkg
VRTSnbclibs.pkg
VRTSnbjre.pkg
VRTSnbjava.pkg
VRTSpddea.pkg
VRTSnbcfg.pkg
```

8 Veritas 事前チェックパッケージをインストールします。

- AIX: `installp -ad VRTSnbpck.image all`
- Linux: `rpm -U VRTSnbpck.rpm`
- Solaris: `pkgadd -a .pkg_defaults -d VRTSnbpck.pkg VRTSnbpck`

9 (該当する場合) NetBackup 8.0 より前のバージョンからアップグレードする場合は、古い SYMC* パッケージを削除します。次の例は、SYMC RPM パッケージの削除に使用するコマンドを示しています。このプロセスでは、NetBackup の構成が保持されます。

```
rpm -e SYMCnbjava
rpm -e SYMCpddea
rpm -e SYMCnbclt
rpm -e SYMCnbjre
```

10 以下のコマンドを示されている順序で実行してファイルをインストールします。

メモ: Java GUI と JRE のアップグレードは省略可能です。アップグレードしない場合は、VRTSnbjava と VRTSnbjre パッケージのコピーとインストールを省略します。

アップグレードしないことを選択した場合は、古い Java GUI および JRE パッケージを削除することをお勧めします。

p.131 の「アップグレード後の Java GUI と JRE の追加または削除」を参照してください。

AIX

```
installp -ad VRTSpbx.image all
installp -ad VRTSnbclt.image all
installp -ad VRTSnbclibs.image all
installp -ad VRTSnbjre.image all
installp -ad VRTSnbjava.image all
installp -ad VRTSpddea.image all
installp -ad VRTSnbcfg.image all
```

次のコマンドのみを使用してすべてのパッケージをインストールすることもできます。

```
installp -ad folder_name all
```

Linux

```
rpm -U VRTSpbx.rpm
rpm -U VRTSnbclt.rpm
rpm -U VRTSnbclibs.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjava.rpm
rpm -U VRTSpddea.rpm
rpm -U VRTSnbcfg.rpm
```

メモ: VRTSnbjre.rpm、VRTSnbjava.rpm、VRTSpddea.rpm の各ファイルは、IBM pSeries クライアントではサポートされません。

Solaris

以下に示す pkgadd -a *admin* -d *device* [*pkgid*] コマンドを使用してファイルをインストールします。

```
pkgadd -a .pkg_defaults -d VRTSpbx.pkg VRTSpbx
pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt
pkgadd -a .pkg_defaults -d VRTSnbclibs.pkg VRTSnbclibs
pkgadd -a .pkg_defaults -d VRTSnbjre.pkg VRTSnbjre
pkgadd -a .pkg_defaults -d VRTSnbjava.pkg VRTSnbjava
pkgadd -a .pkg_defaults -d VRTSpddea.pkg VRTSpddea
pkgadd -a .pkg_defaults -d VRTSnbcfg.pkg VRTSnbcfg
```

- -a オプションでは、デフォルトの管理ファイルの代わりに使用する特定の admin (.pkg_defaults) を指定します。管理ファイルにはデフォルトのインストール処理が含まれます。
- -d デバイスオプションでは、ソフトウェアパッケージのソースを指定します。デバイスには、デバイス、ディレクトリ、またはスプールディレクトリのパスを指定できます。
- pkgid パラメータを使用して、インストールするパッケージの名前を指定します。このパラメータは必要に応じて指定します。

11 (該当する場合)応答ファイルがないか、正しく構成されていない場合は、次のエラーメッセージが表示されます。

```
WARNING: There is no answer file present and no valid bp.conf.
Therefore, security configuration is not complete. Manual steps
are required before backups and restores can occur. For more
information:
https://www.veritas.com/support/en_US/article.000127129
```

/usr/openv/netbackup/bin/private ディレクトリに変更し、nb_init_cfg コマンドを実行して bp.conf ファイルを構成します。手動で bp.conf ファイルを構成することもできます。セキュリティと証明書の構成を手動で設定しなければならない場合があります。詳細情報を参照できます。

https://www.veritas.com/support/en_US/article.000127129

12 古いバージョンの Java GUI と JRE を使う予定がない場合は、削除することをお勧めします。

- Linux の場合:

```
rpm -e VRTSnbjava.rpm
rpm -e VRTSnbjre.rpm
```

- Solaris の場合:

```
pkgrm VRTSnbjava
pkgrm VRTSnbjre
```

- AIX

```
installp -u VRTSnbjre
installp -u VRTSnbjava
```

UNIX クライアントと Linux クライアントに NetBackup インストールスクリプトを使用する場合は、インストールの動作に 1 つだけ変更点があります。NetBackup インストールスクリプトは、インストールパッケージをクライアントの /usr/openv/pack/ ディレクトリにコピーしなくなりました。インストールまたはアップグレードに成功すると、/usr/openv/pack/install.history ファイルに記録されます。

UNIX、Linux のインストールエラーメッセージ、エラーの原因、その解決策

ここに示されている手順とは異なるインストールを試みると、エラーメッセージが表示されることがあります。表 6-1に、処理およびそれによって生成されるメッセージをいくつか示します。

表 6-1　インストールのエラーメッセージと解決策

インストール処理	エラーメッセージ	解決方法
AIX の場合		
同じバージョンのバイナリが存在するのにバイナリをインストールしようとする。	`# installp -ad VRTSnbpck.image all` `package VRTSnbpck.image is already installed`	`lslpp -L package_name` コマンドを使ってインストールされているパッケージの名前を特定します。このパッケージをアンインストールしてから操作を再試行します。

誤った順序でバイナリをインストールしようとする。	`# installp -ad VRTSnbcfg.image all`
	`error: Failed dependencies:`
	`VRTSnbclt >= 8.1.0.0 is needed by VRTSnbcfg-version-platform`
		イメージパッケージの正しいインストール順序については、マニュアルを参照してください。依存パッケージの一覧表示のエラーで、詳しい情報を取得することもできます。
		p.93 の「ネイティブインストーラを使用して UNIX または Linux クライアントバイナリをアップグレードするには」を参照してください。

新しいバージョンのバイナリが存在する場合に古いバージョンのバイナリをインストールしようとする。	`# installp -d VRTSnbclt.image all`
	`WARNING:`
	`file /usr/openv/lib/java/nbvmwaretags.jar from install of VRTSnbclt-version-platform conflicts with file from package VRTSnbclt-version-platform`
		`lslpp -L package_name` コマンドを使ってインストールされているパッケージの名前を特定します。このパッケージをアンインストールしてから操作を再試行します。

Linux の場合		

インストール処理	エラーメッセージ	解決方法
同じバージョンのバイナリが存在するのにバイナリをインストールしようとする。	`# rpm -U VRTSnbpck.rpm` `package VRTSnbpck.rpm-version-platform is already installed`	rpmコマンドを使ってインストールされているパッケージの名前を特定します。このパッケージをアンインストールしてから操作を再試行します。

誤った順序でバイナリをインストールしようとする。	`# rpm -U VRTSnbcfg.rpm`
	`error: Failed dependencies:`
	`VRTSnbclt >= 8.1.0.0 is needed by VRTSnbcfg-version-platform`
		マニュアルを参照して、RPMの正しいインストール順序を確認します。詳細情報を参照できます。
		p.93 の「ネイティブインストーラを使用して UNIX または Linux クライアントバイナリをアップグレードするには」を参照してください。

新しいバージョンのバイナリが存在する場合に古いバージョンのバイナリをインストールしようとする。	`# rpm -U VRTSnbclt.rpm` `file /usr/openv/lib/java/nbvmwaretags.jar from install of VRTSnbclt-version-platform conflicts with file from package VRTSnbclt-version-platform`	rpmコマンドを使ってインストールされているパッケージの名前を特定します。このパッケージをアンインストールしてから操作を再試行します。
Solaris の場合		

インストール処理	エラーメッセージ	解決方法
同じバージョンのバイナリが存在するのにバイナリをインストールしようとする		pkginfoコマンドを使用して、現在インストールされているパッケージの名前を特定します。このパッケージをアンインストールしてから操作を再試行します。 または、パッケージに付属する管理ファイルを使用して、パッケージを再インストールします。

インストール処理	エラーメッセージ	解決方法
	pkgadd -a .pkg_defaults -d VRTSnbpck.pkg VRTSnbpck Processing package instance <VRTSnbpck> from </root/packages/Solaris/Solaris_x86_10_64/VRTSnbpck.pkg> NetBackup Pre-Check(i386) 8.1.0.0 This appears to be an attempt to install the same architecture and version of a package which is already installed. This installation will attempt to overwrite this package. Copyright 2017 Veritas Technologies LLC. All rights reserved. ## Executing checkinstall script. Using </> as the package base directory. ## Processing package information. ## Processing system information. 6 package pathnames are already properly installed. ## Verifying disk space requirements. Installing NetBackup Pre-Check as <VRTSnbpck> ## Executing preinstall script. Wednesday, May 10, 2017 03:15:44 PM IST: Installing package VRTSnbpck.	

インストール処理	エラーメッセージ	解決方法
	Installing NB-Pck. ## Installing part 1 of 1. [verifying class <NBclass>] ## Executing postinstall script. Wednesday, May 10, 2017 03:15:45 PM IST: Install of package VRTSnbpck was successful.	
誤った順序でバイナリをインストールしようとする。	# pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt ERROR: VRTSnbpck >=8.1.0.0 is required by VRTSnbclt. checkinstall script suspends	パッケージの正しいインストール順序については、マニュアルを参照してください。詳細情報を参照できます。 p.93 の「ネイティブインストーラを使用して UNIX または Linux クライアントバイナリをアップグレードするには」を参照してください。
新しいバージョンのバイナリが存在する場合に古いバージョンのバイナリをインストールしようとする。	# pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt Processing package instance <VRTSnbclt> from </root/80packages/Solaris/Solaris_x86_10_64/VRTSnbclt.pkg> NetBackup Client(i386) 8.0.0.0 The following instance(s) of the <VRTSnbclt> package are already installed on this machine: 1 VRTSnbclt NetBackup Client (i386) 8.1.0.0 Do you want to overwrite this installed instance [y,n,?,q]	pkginfo コマンドを使用して、現在インストールされているパッケージの名前を特定します。このパッケージをアンインストールしてから操作を再試行します。

7

VxUpdate を使用した NetBackup 配備の管理

この章では以下の項目について説明しています。

VxUpdate について

VxUpdate は、メディアサーバーとクライアント向けのポリシーベースのアップグレードツールを提供します。Veritas はメディアサーバーおよびクライアントのアップグレード用の簡略化されたツールを提供します。追加の外部ツールを必要とせず、バックアップポリシーに類似した、使い慣れたポリシーベース形式の構成になっています。署名済みパッケージが検証され、プライマリサーバー上の VxUpdate リポジトリにインストールされます。パッケージがインストールされると、配備ポリシーで利用可能になります。さらに、配備ポリシーを使用して、Veritas から提供される緊急エンジニアリングバイナリのインストールを自動化できます。

配備ポリシーを使用すると、配備アクティビティをスケジュールに従って構成および実行したり、クライアントホストの所有者が、必要に応じてアップグレードを実行したりできます。さらに、配備アクティビティを細分化して、小規模のタスクに分割できます。事前チェック、

ステージング、インストールのタスクを、それぞれに固有の配備時間帯を設定した異なるスケジュールを持つ個別のアクティビティとしてスケジュール設定できます。

メモ: キューに登録された配備ジョブのみをキャンセルできます。VxUpdate ジョブがアクティブ状態になるとキャンセルできません。

配備ポリシーは、NetBackup 管理コンソールの他のポリシーと同じ場所にはありません。配備ポリシーは、NetBackup 管理コンソールの[配備の管理 (Deployment Management)]、[配備ポリシー (Deployment Policies)]にあります。

配備ポリシーを正常に作成して使用するためにVeritasが推奨する方法は次のとおりです。

表 7-1

手順	処理	追加情報
1	NetBackup リポジトリへの配置	p.107 の「リポジトリの管理」を参照してください。
2	配備ポリシーの作成	p.110 の「配備ポリシーの管理」を参照してください。
3	(オプション)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からのアップグレードの手動による実行	p.115 の「VxUpdate を使用したプライマリサーバーからのアップグレードの手動による開始」を参照してください。 p.120 の「VxUpdate を使用したメディアサーバーまたはクライアントからのアップグレードの手動による開始」を参照してください。

VxUpdate で使用するコマンド

NetBackup では、2 つのコマンドを使用して NetBackup パッケージリポジトリを変更し、コマンドラインからポリシーを開始できます。コマンドラインを使用したポリシーの開始は、スクリプトが使用されている環境で役立ちます。コマンドは次のとおりです。

- `nbrepo`

  `nbrepo` コマンドは、NetBackup パッケージリポジトリの管理に使用します。パッケージの追加、検証、削除ができるほか、リポジトリ内のパッケージ識別子や、パッケージに関するその他の情報を取得できます。このコマンドはプライマリサーバーにのみあります。

- `nbinstallcmd`

nbinstallcmd コマンドは、コマンドラインから配備ポリシーを開始するために使用します。オンデマンドの配備ジョブを開始するためにも、このコマンドを使用できます。このコマンドは、NetBackup 環境内のすべてのホストにあります。

これらのコマンドと、その他の関連するコマンドの詳細が利用可能です。

『NetBackup コマンドリファレンスガイド』

リポジトリの管理

VxUpdate はプライマリサーバー上に存在するリポジトリを使用します。リポジトリには、メディアサーバーとクライアントにデプロイできるすべてのパッケージが含まれています。リポジトリには、アップグレードパッケージ、エンジニアリングバイナリ、Hotfix を含めることができます。VxUpdate では、nbrepo コマンドがパッケージリポジトリの管理を制御します。nbrepo コマンドを使用せずに、手動でリポジトリを変更または更新しないでください。追加されたパッケージに応じて、リポジトリが大きくなる可能性があります。ご使用の環境に必要なすべてのパッケージに対して、プライマリサーバーに十分な領域があることを確認します。プライマリサーバー上のリポジトリディレクトリを監視し、リポジトリから不要なパッケージを削除します。Linux の場合、リポジトリは /usr/openv/var/global/repo にあります。Windows の場合、リポジトリは *install_path*¥NetBackup¥var¥global¥repo にあります。

nbrepo コマンドは、リポジトリを検証し、NetBackup パッケージを配置します。Veritas は、VxUpdate パッケージに署名します。非公式または署名のない NetBackup パッケージをリポジトリに配置しようとすると、失敗します。これらのパッケージは、ターゲットホストに NetBackup をインストールする配備ポリシーで参照されます。nbrepo コマンドを使用してリポジトリへの配置を行う場合は、必要なディスク容量に注意してください。プライマリサーバーには、配備ポリシーで指定された NetBackup のバージョンとプラットフォーム向けパッケージを格納するために十分なディスク容量が確保されている必要があります。

リポジトリにロードできるパッケージには、次の種類があります。

- VxUpdate メディアサーバーとクライアントパッケージ
  VxUpdate を使用して、NetBackup メディアサーバーとクライアントを新しいバージョンの NetBackup にアップグレードできます。これらのパッケージは、標準の NetBackup メディアサーバーおよびクライアントパッケージとは少し異なります。さまざまな VxUpdate 操作をサポートするための追加コンポーネントがパッケージに含まれます。
- 緊急バイナリ (EEB) と Hotfix
  VxUpdate を使用して、緊急バイナリと Hotfix を NetBackup 8.1.2 以降のメディアサーバーとクライアントに配備できます。従来の EEB を取得するのと同じ方法で、VxUpdate 形式の EEB をサポートから取得できます。これらの EEB は、NetBackup バージョン 8.1.2 以降専用です。Veritas が NetBackup 8.1.2 以降のリリース向けに作成したすべてのメディアサーバーおよびクライアントの Hotfix には、VxUpdate 形式の修正が含まれています。

Veritas NetBackup 承認済みメディアサーバーおよびクライアントパッケージのダウンロード

VxUpdate 形式のパッケージは、myveritas.com のライセンスポータルから入手できます。緊急バイナリと Hotfix は、標準の場所から取得できます。これらのパッケージの VxUpdate バージョンをダウンロードし、プライマリサーバーにアクセスできる場所に配置する必要があります。プライマリサーバーにアクセス可能になったら、NetBackup パッケージリポジトリにパッケージを配置します。

1. myveritas.com ライセンスポータルに移動します。
2. ユーザー名およびパスワードを入力します。
3. [ライセンス (Licensing)]を選択します。
4. アカウント番号を選択または入力します。
5. [フィルタの適用 (Apply Filters)]を選択します。
6. 表示されるテーブルから、アカウント番号を選択します。

   この処理により、資格の一覧が表示されます。ここから、関連するソフトウェアをダウンロードできます。
7. [ダウンロード (Downloads)]を選択します。
8. フィルタオプションを使用して、NetBackup 製品ラインと該当する製品のバージョンに結果を絞り込みます。

   フィルタを追加して、[フィルタの適用 (Apply Filters)]を選択します。
9. [処理 (Actions)]からダウンロードアイコンを選択します。
10. 表示されるテーブルで VxUpdate パッケージを選択し、[ダウンロード (Download)]を選択します。

    メディアサーバーとクライアントの両方のバイナリが含まれているパッケージの命名規則は、`vxupdate_nb_version_operatingsystem_platform.sja` です。
11. ファイルをダウンロードして、コンピュータの一時的な場所に抽出します。

関連するすべてのパッケージをコンピュータにダウンロードし、抽出が完了したら、NetBackup パッケージリポジトリにパッケージを追加します。このトピックに関する詳細情報を参照できます。

p.108 の「NetBackup パッケージリポジトリへのパッケージの追加」を参照してください。

NetBackup パッケージリポジトリへのパッケージの追加

VxUpdate では、NetBackup パッケージリポジトリに追加した、Veritas の署名済みパッケージのみを使用できます。`nbrepo` コマンドを使用してリポジトリにパッケージを追加します。このコマンドは、EMM データベースにメタデータを追加し、ファイルシステム上のリポジトリのディレクトリ構造にパッケージを配置します。`nbrepo` コマンドを使用して、パッケージリポジトリの内容や、個々のパッケージに関する詳細を一覧表示できます。

1 コマンドプロンプトから admincmd ディレクトリに移動します。

Linux の場合: /usr/openv/netbackup/bin/admincmd

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

2 nbrepo オプションを指定して -a コマンドを使用します。

nbrepo -a *package_path*

例: nbrepo -a C:¥temp¥nbclient_8.1.2_windows_x64.sja

3 パッケージが正常に検証されリポジトリに追加されると、コマンドは成功メッセージを返します。

4 nbrepo コマンドについての詳細情報を参照できます。

『NetBackup コマンドリファレンスガイド』

5 使われなくなったパッケージがリポジトリ内に存在する場合は、パッケージを削除します。詳細情報を参照できます。

p.109 の「NetBackup パッケージリポジトリからのパッケージの削除」を参照してください。

NetBackup パッケージリポジトリからのパッケージの削除

パッケージが不要になった場合や、ディスク容量を節約するために、リポジトリからパッケージを削除できます。たとえば、すべてのクライアントが NetBackup 8.1.2 バージョンにアップグレードされたら、このバージョンのパッケージを削除します。nbrepo コマンドを使用して、パッケージを削除します。-pkgDetails オプションを使用すると、ファイルシステムのパスやその他のパッケージ属性などの、パッケージの詳細が表示されます。パッケージが削除されたことを確認するには、nbrepo コマンドを使用して、すべてのパッケージを一覧表示します。パッケージがリポジトリになくなったことを確認できます。パッケージがファイルシステムのパスになくなったことも確認できます。

1 コマンドプロンプトから admincmd ディレクトリに移動します。

Linux の場合: /usr/openv/netbackup/bin/admincmd

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

2 -l オプションを指定して nbrepo コマンドを使用し、すべてのパッケージとそれらの識別子を一覧表示します。

nbrepo -l

3 -d オプションを指定して nbrepo コマンドを使用し、使用されていないパッケージを削除します。

```
nbrepo -d package_identifier
```

例: `nbrepo -d 6`

4 nbrepo コマンドについての詳細情報を参照できます。

『NetBackup コマンドリファレンスガイド』

配備ポリシーの管理

以下に示す手順を使用して、配備ポリシーを作成、変更、削除します。

配備ポリシーの作成

メモ: 作業用配備ポリシーを作成する前に、VxUpdate リポジトリにパッケージを追加する必要があります。リポジトリ内にパッケージを追加せずに配備ポリシーを作成できますが、このようなポリシーは正常に実行できません。VxUpdate リポジトリの管理についての詳細情報を参照できます。

p.107 の「リポジトリの管理」を参照してください。

---

1 NetBackup 管理コンソールの左ペインで、[配備の管理 (Deployment Management)]、[配備ポリシー (Deployment Policies)]の順に選択します。

2 [処理 (Actions)]メニューで[新しい配備ポリシー (New Deployment Policy)]を選択します。

3 新しいポリシー用の一意の名前を[新しい配備ポリシーの追加 (Add a New Deployment Policy)]ダイアログボックスに入力します。

4 [OK]をクリックします。

5 [配備ポリシーの変更 (Change Deployment Policy)]ウィンドウの[属性 (Attributes)]タブに表示されている情報を指定します。

- [パッケージ (Package)]: 配備するパッケージをドロップダウンメニューから選択します。

  メモ: 外部認証局の証明書をサポートするパッケージを指定すると、[セキュリティ (Security)]という追加タブが表示されます。このタブについては、この手順で後ほど説明します。

- [メディアサーバー (Media server)]: メディアサーバーをドロップダウンメニューから指定します。指定したメディアサーバーは、ポリシーに含まれている

NetBackup ホストに接続してファイルを転送するために使用します。メディアサーバーは NetBackup リポジトリからファイルのキャッシュも行います。メディアサーバーは、NetBackup 8.1.2 以降のバージョンでなければなりません。リポジトリはプライマリサーバーに存在するため、メディアサーバーフィールドのデフォルト値はプライマリサーバーになります。

メディアサーバーをアップグレードするとき、[メディアサーバー (Media server)] ドロップダウンは自動的にプライマリサーバーに設定され、変更できません。

- Java GUI および JRE: ターゲットシステムで Java GUI と JRE をアップグレードするかどうかを指定します。3 つのオプションがあります。
  - [インクルード (INCLUDE)]: 指定したコンピュータで Java GUI と JRE コンポーネントをインストールまたはアップグレードします。
  - [除外 (EXCLUDE)]: 指定したコンピュータから Java GUI と JRE コンポーネントを除外します。既存の NetBackup Java GUI および JRE パッケージがすべて削除されます。
  - [一致 (Match)]: Java GUI と JRE コンポーネントの現在の状態を保持します。アップグレード前のシステムにコンポーネントが存在する場合、コンポーネントはアップグレードされます。アップグレード前のシステムにコンポーネントが存在しない場合、コンポーネントはインストールされません。
- (該当する場合): [同時ジョブ数の制限 (Limit simultaneous jobs)]オプションを選択し、[ジョブ (Jobs)]の値を指定して、一度に実行できる同時ジョブの合計数を制限します。最小値は 1 で、最大値は 999 です。

  チェックボックスにチェックマークが付いている場合、デフォルト値は 3 です。

  チェックボックスのチェックマークをはずした場合は、アップグレードの同時ジョブに制限は適用されません。

  コマンドラインインターフェースで値を 0 に設定すると、同時アップグレードジョブを無制限に設定できます。
- [ホストを選択 (Select hosts)]: [利用できるホスト (Available hosts)]リストからホストを選択し、[追加 (Add)]を選択して配備ポリシーにホストを追加します。リストは、ホストデータベースとバックアップポリシーのホストから生成されます。[追加 (Add)]を選択すると、[選択したホスト (Selected hosts)]にホストが表示されます。

  配備ポリシーには、メディアサーバーまたはクライアントのいずれかを含められますが、両方は含められません。インストールが必要なパッケージを選択するときは、利用可能なホストのリストが、メディアサーバーまたはクライアントにフィルタ処理されます。

メモ: 7.7.x または 8.0 メディアサーバーをアップグレードするには、メディアサーバーがバックアップポリシーに含まれている必要があります。ポリシーがアクティブである必要はありません。また、ポリシーを実行する必要はありません。メディアサーバーを NetBackup 8.1 以降にアップグレードしたら、ポリシーを削除できます。ポリシーは、クライアントリストにメディアサーバーを含めるためだけに必要です。ファイルリスト、スケジュール、またはその他のポリシー属性を指定する必要はありません。

ポリシー内にメディアサーバーが含まれていない場合、メディアサーバーのオペレーティングシステムが[不明 (Unknown)]として表示されます。この問題はパッケージの不足であることがツールのヒントで示されます。選択されたホストのオペレーティングシステム用のパッケージがありません。nbrepo コマンドラインを使用して、不足している必要なパッケージをリポジトリに追加してください。実際にリポジトリにパッケージがない可能性がありますが、メディアサーバーをバックアップポリシーに追加する必要もあります。メディアサーバーをポリシーに追加してもツールのヒントが表示される場合は、必要なパッケージの追加が必要な可能性があります。

6 [配備ポリシーの変更 (Change Deployment Policy)]ウィンドウの[スケジュール (Schedules)]タブを選択します。

そのポリシー内の、すべてのスケジュールの概略を確認できます。

7 [新規 (New)]を選択します。

8 [配備スケジュールの追加 (Add Deployment Schedule)]ウィンドウに表示される情報を指定します。

- [名前 (Name)]: 新しいスケジュールの名前を入力します。
- [形式 (Type)]: 作成するスケジュールの形式を指定します。

  スケジュール形式:

  - 事前チェック
    更新のための十分な領域がクライアントにあるかどうかの確認など、さまざまな事前チェック操作を実行します。事前チェックのスケジュール形式は、EEB パッケージ向けには存在しません。
  - 段階
    更新パッケージをクライアントに移動します。インストールは行いません。事前チェック操作も実行します。
  - インストール
    指定したパッケージをインストールします。また、事前チェック操作とステージパッケージ操作も実行します。ステージパッケージ操作を実行済みの場合、インストールスケジュールによってパッケージが再度移動されることはありません。

メモ: 複数の異なるスケジュール形式を、同じ配備スケジュール時間帯に追加すると、予測できない結果が生じることに注意してください。VxUpdate には、最初にどのスケジュール形式を実行するかを判断するための動作が定義されていません。単一の配備スケジュール時間帯に事前チェック、ステージ、およびインストールのジョブがある場合、それらの実行順序を指定する方法はありません。事前チェックまたはステージのスケジュールが失敗することはありますが、インストールは正常に完了します。事前チェック、ステージ、インストールのスケジュールを使うことを計画している場合は、それぞれに個別のスケジュールと時間帯を作成することをお勧めします。

- [開始 (Starts)]: ポリシーの開始日時を、テキストフィールドに、または日時のスピナを使用して指定します。カレンダーアイコンをクリックして表示されるウィンドウで、日時を指定することもできます。ウィンドウ下部に表示される 3 カ月のカレンダー上でクリックおよびドラッグすると、スケジュールを選択できます。
- [終了 (Ends)]: 開始時刻を指定したように、ポリシーを終了する日時を指定します。
- [期間 (Duration)]: 必要に応じて、ポリシーの終了時刻ではなく、日、時間、分、秒で期間を指定できます。最小値は 5 分で、最大値は 99 日です。
- [追加 (Add)]または[OK]を選択すると、スケジュールが作成されます。[OK]を選択して、ポリシーを保存して作成します。

9 [セキュリティ (Security)]タブは、外部認証局のサポートを含む配備パッケージを選択すると表示されます。

デフォルトでは、[可能な場合は既存の証明書を使用します。(Use existing certificates when possible)]オプションが選択されています。このオプションは、既存の NetBackup CA 証明書または外部 CA 証明書が利用可能な場合はそれを使用するように NetBackup に指示します。

メモ: このオプションを指定した状態で証明書が使用できない場合、アップグレードは失敗します。

[可能な場合は既存の証明書を使用します (Use existing certificates when possible)]オプションを選択解除すると、UNIX/Linux コンピュータおよび Windows コンピュータの外部認証局情報の場所を指定できます。

このオプションを選択解除すると、ユーザーはアップグレード中にセキュリティ構成の設定を変更できません。

10 Windows クライアントはデフォルトで、[Windows 証明書ストアの使用 (Use Windows certificate store)]が選択されています。

証明書の場所は、*Certificate Store Name*¥*Issuer Distinguished Name*¥*Subject Distinguished Name* のように入力する必要があります。

メモ: 証明書ストアを指定するときは、任意の名前に対して `$hostname` 変数を使用できます。実行時に `$hostname` 変数はローカルホストの名前を評価します。このオプションを使用すると、NetBackup ソフトウェアを多数のクライアントにプッシュインストールするときに柔軟性が高まります。

あるいは、Windows 証明書の場所をカンマ区切りのリストで指定できます。たとえば、`MyCertStore¥IssuerName1¥SubjectName, MyCertStore¥IssuerName2¥SubjectName2, MyCertStore4¥IssuerName1¥SubjectName5` のように指定できます。

次に、表示されるラジオボタンから、証明書失効リスト (CRL) オプションを選択します。

- ［CRL は使用しない (Do not use a CRL)］: 追加の情報は不要です。
- ［証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)］: 追加の情報は不要です。
- ［次のパスにある CRL を使用する (Use the CRL at the following path)］: CRL のパスを入力するように求められます。

11 ［証明書ファイルパスから (ファイルベースの証明書の場合) (From certificate file path (for file-based certificates))］オプションを選択しているメディアサーバーとクライアントの両方に対して、次のように情報を指定します。

- ［証明書ファイル (Certificate file)］: このフィールドには、証明書ファイルへのパスと証明書のファイル名を指定する必要があります。
- ［トラストストアの場所 (Trust store location)］: このフィールドには、トラストストアへのパスとトラストストア名を指定する必要があります。
- ［秘密鍵のパス (Private key path)］: このフィールドには、秘密鍵ファイルへのパスと秘密鍵のファイル名を指定する必要があります。
- ［パスフレーズファイル (Passphrase file)］: このフィールドでは、パスフレーズファイルへのパスとパスフレーズのファイル名を指定する必要があります。このフィールドは必要に応じて指定します。
- お使いの環境の正しい CRL オプションを指定します。
  - ［CRL は使用しない (Do not use a CRL)］: 追加の情報は不要です。
  - ［証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)］: 追加の情報は不要です。

- ［次のパスにある CRL を使用する (Use the CRL at the following path)］: CRL のパスを入力するように求められます。

配備ポリシーを変更するには

1. 配備ポリシーを右クリックして、［変更 (Change)］を選択します。
2. 配備ポリシーの各タブを参照して、ポリシーに必要な変更を加えます。
3. ［OK］を選択すると、ポリシーが更新されます。

配備ポリシーの削除

1. 配備ポリシーを右クリックして、［削除 (Delete)］を選択します。
2. ［OK］を選択します。
3. ポリシーの削除を確認します。

VxUpdate を使用したプライマリサーバーからのアップグレードの手動による開始

2 つの方法のいずれかを使用して、VxUpdate でアップグレードを手動で開始できます。既存のポリシーに基づいて、アップグレードを手動で開始できます。また、ポリシーを関連付けずにアップグレードを開始することもできます。

ローカルでプライマリサーバーにログインし、即時に更新を強制実行する必要がある場合は、配備ポリシーを手動で開始します。または、緊急バイナリ用に、即時のアップグレードを開始できます。VxUpdate を使用すると、コマンドラインを使用してメディアサーバーまたはクライアントからもアップグレードを起動できます。詳細情報を参照できます。

p.120 の「VxUpdate を使用したメディアサーバーまたはクライアントからのアップグレードの手動による開始」を参照してください。

管理コンソールからポリシー内のすべてのメディアサーバーまたはクライアントのアップグレードを手動で開始するには

1. NetBackup 管理コンソールで、［配備の管理 (Deployment Management)］、［配備ポリシー (Deployment Policies)］の順に移動します。
2. 中央ペインで、プライマリサーバーを展開して、実行するポリシーを選択します。
3. 開始するポリシーを右クリックして、［手動配備 (Manual Deployment)］を選択します。
4. または、実行するポリシーを選択したら、［処理 (Actions)］、［手動配備 (Manual Deployment)］の順に選択できます。

管理コンソールからポリシー内の特定のホストのアップグレードを手動で開始するには

1. NetBackup 管理コンソールで、[NetBackup の管理 (NetBackup Management)]、[ホストプロパティ (Host Properties)]、[メディアサーバー (Media Servers)]または[NetBackup の管理 (NetBackup Management)]、[ホストプロパティ (Host Properties)]、[クライアント (Clients)]の順に選択します。
2. 右ペインで、アップグレードするホストを右クリックします。
3. [ホストをアップグレード (Upgrade Host)]を選択します。
4. [ホストをアップグレード (Upgrade Host)]ダイアログボックスで、次のようにします。
   - [パッケージ (Package)]ドロップダウンリストから、使用するパッケージを選択します。

     メモ: 外部認証局証明書がサポートされているパッケージを指定すると、追加の[構成 (Configure)]ボタンが表示されます。このボタンについては、次の手順で説明します。

   - [形式 (Type)]ドロップダウンリストから、実行するスケジュール形式を指定します。
   - [メディアサーバー (Media server)]ドロップダウンリストから、使用するメディアサーバーを選択します。
     メディアサーバーをアップグレードするとき、[メディアサーバー (Media server)]ドロップダウンは自動的にプライマリサーバーに設定され、変更できません。
   - アップグレードするホストが[選択したホスト (Selected hosts)]にあることを確認します。

5 (該当する場合) 存在する場合、[構成 (Configure)]ボタンをクリックして、外部認証局情報を構成します。

デフォルトでは、[可能な場合は既存の証明書を使用します。(Use existing certificates when possible)]オプションが選択されています。このオプションは、証明書が利用可能な場合、既存の NetBackup CA または外部 CA 証明書を使用するように NetBackup に指示します。

メモ: このオプションを指定して証明書が利用できない場合、アップグレードは失敗します。

[可能な場合は既存の証明書を使用します (Use existing certificates when possible)]オプションを選択解除すると、UNIX/Linux コンピュータおよび Windows コンピュータの外部認証局情報の場所を指定できます。

このオプションを選択解除すると、ユーザーはアップグレード中にセキュリティ構成の設定を変更できません。

6 Windows クライアントはデフォルトで、[Windows 証明書ストアの使用 (Use Windows certificate store)]が選択されています。

証明書の場所は、*Certificate Store Name*¥*Issuer Distinguished Name*¥*Subject Distinguished Name* のように入力する必要があります。

メモ: 証明書ストアを指定するときは、任意の名前に対して `$hostname` 変数を使用できます。実行時に `$hostname` 変数はローカルホストの名前を評価します。このオプションを使用すると、NetBackup ソフトウェアを多数のクライアントにプッシュインストールするときに柔軟性が高まります。

あるいは、Windows 証明書の場所をカンマ区切りのリストで指定できます。たとえば、`MyCertStore¥IssuerName1¥SubjectName, MyCertStore¥IssuerName2¥SubjectName2, MyCertStore4¥IssuerName1¥SubjectName5` のように指定できます。

次に、表示されるラジオボタンから、証明書失効リスト (CRL) オプションを選択します。

- [CRL は使用しない (Do not use a CRL)]: 追加の情報は不要です。
- [証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)]: 追加の情報は不要です。
- [次のパスにある CRL を使用する (Use the CRL at the following path)]: CRL のパスを入力するように求められます。

7 [証明書ファイルパスから (ファイルベースの証明書の場合)]オプションを選択している UNIX および Linux クライアント、Windows クライアントの両方に対して、次のように情報を指定します。

- [証明書ファイル (Certificate file)]: このフィールドには、証明書ファイルへのパスと証明書のファイル名を指定する必要があります。
- [トラストストアの場所 (Trust store location)]: このフィールドには、トラストストアへのパスとトラストストア名を指定する必要があります。
- [秘密鍵のパス (Private key path)]: このフィールドには、秘密鍵ファイルへのパスと秘密鍵のファイル名を指定する必要があります。
- [パスフレーズファイル (Passphrase file)]: このフィールドでは、パスフレーズファイルへのパスとパスフレーズのファイル名を指定する必要があります。このフィールドは必要に応じて指定します。
- お使いの環境の正しい CRL オプションを指定します。
  - [CRL は使用しない (Do not use a CRL)]: 追加の情報は不要です。
  - [証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)]: 追加の情報は不要です。
  - [次のパスにある CRL を使用する (Use the CRL at the following path)]: CRL のパスを入力するように求められます。

8 [OK]を選択して、アップグレードを起動します。

メモ: NetBackup 管理コンソールの[ポリシー (Policies)]セクションからも、クライアントのアップグレードジョブを起動できます。NetBackup 管理コンソールで[NetBackup の管理 (NetBackup Management)]、[ポリシー (Policies)]の順に選択します。中央ペインで、[クライアント (Clients)]を選択します。右ペインでアップグレードするクライアントを右クリックして、[ホストをアップグレード (Upgrade Host)]を選択します。示されている手順に従います。この手順は、メディアサーバーではなくクライアントにのみ適用できます。

ポリシー内のすべてのメディアサーバーまたはクライアントに対してコマンドラインからアップグレードを手動で開始するには

ポリシー内のすべてのメディアサーバーまたはクライアントのアップグレードを手動で開始するには、この手順を使用します。

メモ: この手順は、指定したポリシーのすべてのメディアサーバーまたはクライアントのアップグレードを開始します。選択したメディアサーバーまたはクライアントで、アップグレードを開始できます。詳細情報を参照できます。

「ポリシー内の選択したホストに対してコマンドラインからアップグレードを手動で開始するには」

1 コマンドプロンプトを開いて、次のディレクトリに移動します。

Windows の場合: *install_path*¥netbackup¥bin

UNIX または Linux の場合: /usr/openv/netbackup/bin

2 次に示すように、nbinstallcmd コマンドを使用してポリシーを起動します。

```
nbinstallcmd -policy policy_name -schedule schedule
[-master_server primary]
```

ここで、*policy_name* は配置ポリシーの名前、*schedule* はスケジュールの名前、*primary* はプライマリサーバーの名前です。

ポリシー内の選択したホストに対してコマンドラインからアップグレードを手動で開始するには

ポリシー内の選択したホストのアップグレードを手動で開始するには、この手順を使用します。

メモ: この手順は、指定したポリシーの選択したメディアサーバーとクライアントのアップグレードを開始します。ポリシー内のすべてのメディアサーバーとクライアントのアップグレードを開始できます。詳細情報を参照できます。

「ポリシー内のすべてのメディアサーバーまたはクライアントに対してコマンドラインからアップグレードを手動で開始するには」

1 コマンドプロンプトを開いて、次のディレクトリに移動します。

Windows の場合: *install_path*¥netbackup¥bin

UNIX または Linux の場合: /usr/openv/netbackup/bin

2 次に示すように、nbinstallcmd コマンドを使用します。

```
nbinstallcmd -policy policy_name -schedule schedule
{-host_filelist filename|-hosts client1, client2, clientN}
```

以下はその説明です。

- *policy_name* は配備ポリシーの名前です。
- *schedule* はスケジュールの名前です。

- *filename* は、アップグレードするメディアサーバーまたはクライアントのリストが含まれるファイルの名前です。
- *client1*、*client2*、*clientN* は、アップグレードするメディアサーバーまたはクライアントのリストです。

ポリシーを関連付けずにコマンドラインから 1 つのクライアントのアップグレードを手動で開始できます。nbinstallcmd コマンドに対して必要なオプションは、セキュリティの構成によって異なります。すべての利用可能なオプションとコマンドの使用例のリストについては、nbinstallcmd コマンドのマニュアルを参照してください。

『NetBackup コマンドリファレンスガイド』

VxUpdate を使用したメディアサーバーまたはクライアントからのアップグレードの手動による開始

ローカルでメディアサーバーまたはクライアントにログインし、即座に更新を強制実行するには、配備ジョブを手動で開始します。配備ポリシーを使用してすぐにアップグレードを開始するか、ポリシーを関連付けずにアップグレードを指定できます。アップグレードは、NetBackup バージョンの更新、または緊急バイナリなどの他のアップグレードの目的で使用できます。

VxUpdate を使用してメディアサーバーまたはクライアントからアップグレードを開始する理由には、特定の保守期間が設けられたミッションクリティカルシステムがあります。このようなシステムの一例は、ダウンタイムが限られているデータベースサーバーです。

メモ: 更新は、ローカルメディアサーバーまたはクライアントでのみ起動できます。メディアサーバーまたはクライアントで nbinstallcmd コマンドを使用し、他のメディアサーバーまたはクライアント上でジョブを起動することはできません。他のメディアサーバーまたはクライアントで更新を起動するには、プライマリサーバーからそれらを開始する必要があります。

VxUpdate を使用すると、コマンドラインを使用してプライマリサーバーからアップグレードを起動することもできます。詳細情報を参照できます。

p.115 の「VxUpdate を使用したプライマリサーバーからのアップグレードの手動による開始」を参照してください。

ターゲットクライアントまたはメディアサーバーで非ポリシーベースのアップグレードを直接開始した場合、旧バージョンのホストの nbinstallcmd バージョンは現在の nbinstallcmd バージョンではありません。nbinstallcmd コマンドの正確な形式については、現在インストールされているバージョンの NetBackup についての『NetBackup コマンドリファレンスガイド』を参照してください。

この古いバージョンの nbinstallcmd により、通常の VxUpdate 動作で次のような例外が発生します。

- プライマリサーバーで NetBackup 証明書と外部証明書の両方を使用しており、ターゲットメディアサーバーまたはクライアントが NetBackup 8.1.2 にある場合、ターゲットホストで非ポリシーベースのアップグレードを直接実行することはサポートされていません。次に示すオプションのいずれかを使用してアップグレードする必要があります。
  - VxUpdate を使用して、プライマリサーバーからクライアントまたはメディアサーバーをアップグレードします。
  - プライマリサーバー上でポリシーを作成します。次に、ターゲットクライアントまたはメディアサーバーでポリシーベースの nbinstallcmd を実行します。
  - ターゲットホストで非ポリシーベースのアップグレードを開始する前に、プライマリサーバーの外部証明書を無効にします。外部証明書は、アップグレードが正常に完了した後で有効にできます。
- クライアントまたはメディアサーバーが NetBackup 8.2 以前のバージョンにある場合、-components フラグは利用できません。このフラグは、NetBackup Java GUI と JRE のオプションインストールを有効にするために NetBackup 8.3 で導入されました。NetBackup 8.2 以前のクライアントまたはメディアサーバーでアドホックの nbinstallcmd を実行すると、-components javagui_jre オプションはデフォルト値の MATCH に設定されます。この値を指定すると、アップグレード前のホストの Java GUI と JRE の状態と一致するようにアップグレードされます。アップグレード前のホストに Java GUI と JRE がインストールされている場合、アップグレード後もインストールされたままになります。アップグレード前のホストに Java GUI と JRE がインストールされていない場合、アップグレード後もインストールされません。

既存のポリシーに基づいてメディアサーバーまたはクライアントが開始した配備ジョブを開始するには

1. コマンドプロンプトからバイナリのディレクトリに移動します。

   UNIX または Linux の場合: `/usr/openv/netbackup/bin`

   Windows の場合: *install_path*¥netbackup¥bin

2. `nbinstallcmd` を次のように使用します。

   `nbinstallcmd -policy` *policy* `-schedule` *schedule* `-master_server` *name*

   例: `nbinstallcmd -policy all_clients -schedule install812 -master_server primary1`

   ジョブが正常に開始された場合は、エラーメッセージは表示されずにコマンドプロンプトに戻ります。

   メモ: `nbinstallcmd` コマンドを使用してメディアサーバーのアップグレードを開始する場合、`-master_server` と `-media_server` の両方のオプションを含める必要があります。この場合、これら両方のオプションの値が同じである必要があります。

3. NetBackup 管理者とともに、NetBackup 管理コンソールのアクティビティモニターを使用してアップグレード状態を監視します。

コマンドラインから、ポリシーを関連付けずにメディアサーバーまたはクライアントが開始した配備ジョブを起動できます。`nbinstallcmd` コマンドに必要なオプションは、セキュリティ構成およびアップグレードするコンピュータの NetBackup バージョンによって異なります。すべての利用可能なオプションとコマンドの使用例のリストについては、`nbinstallcmd` コマンドのマニュアルを参照してください。

『NetBackup コマンドリファレンスガイド』

配備ジョブの状態

NetBackup 管理コンソールのアクティビティモニターで、配備ジョブの状態を監視および確認します。配備ジョブ形式は、VxUpdate ポリシーの新しい形式です。状態コード 0 (ゼロ) で終了する配備ポリシーの親ジョブは、すべての子ジョブが正常に完了したことを示します。状態コード 1 で終了する親ジョブは、1 つ以上の子ジョブが成功し、少なくとも 1 つが失敗したことを示します。その他の状態コードは、エラーを示します。子ジョブの状態を確認して、失敗した理由を判断します。それ以外は、配備ジョブとその他の NetBackup ジョブとの間に違いはありません。

配備コードの状態コードが 224 になる場合もあります。このエラーは、クライアントのハードウェアとオペレーティングシステムが誤って指定されていることを示します。このエラー

は、次の場所にある bpplclients コマンドを使用して配備ポリシーを変更することで修正できます。

Linux の場合: /usr/openv/netbackup/bin/admincmd

Windows の場合: *install_path*¥netbackup¥bin¥admincmd

次の構文を使用します。

bpplclients *deployment_policy_name* -modify *client_to_update* -hardware *new_hardware_value* -os *new_os_value*

配備ポリシーは、オペレーティングシステムとハードウェアの値に、簡素化した命名スキームを使用します。bpplclients コマンドに示すように値を使用します。

表 7-2　配備ポリシーのオペレーティングシステムとハードウェア

オペレーティングシステム	ハードウェア
debian	x64
redhat	x64
suse	x64
redhat	ppc64le
suse	ppc64le
redhat	zseries
suse	zseries
aix	rs6000
solaris	sparc
solaris	x64
windows	x64

[証明書配備のセキュリティレベル (Security Level for certificate deployment)]が[最高 (Very High)]に設定されている場合、セキュリティ証明書は VxUpdate アップグレードの一環としては配置されません。この設定は、NetBackup 管理コンソールの NetBackup の[グローバルセキュリティ設定 (Global Security Settings)]にあります。

クライアントのアップグレードに VxUpdate を使用した後で、クライアントと通信できなくなった場合は、アップグレード中に適切なセキュリティ証明書が発行されたことを確認してください。証明書の手動配備が必要な場合があります。詳しくは、次の記事を参照してください。

https://www.veritas.com/content/support/en_US/article.100039650

配備ジョブの状態コードが 7207 になる場合もあります。このエラーは、NetBackup 事前チェックまたはアップグレードのプロセスが完了するまでに予想より長い時間がかかる、または完了しない場合に発生する可能性があります。プライマリサーバーの NetBackup 構成で次の値を定義すると、ジョブが状態 7207 で終了するまでに VxUpdate が待機する時間を構成できます。

VXUPDATE_CLIENT_READ_TIMEOUT_SECONDS

この値は、事前チェック操作とクライアントのアップグレード操作に許容される時間 (秒) を制御します。デフォルト値は 1800 (30 分) です。最短 600 (10 分)、または最長 3600 (60 分) まで設定できます。

VXUPDATE_SERVER_READ_TIMEOUT_SECONDS

この値は、サーバーのアップグレード操作に許容される時間 (秒) を制御します。デフォルト値は 2700 (45 分) です。最短 600 (10 分)、または最長 5400 (90 分) まで設定できます。

bpsetconfig コマンドを使用してプライマリサーバーの NetBackup 構成に値を追加する方法について詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

A

参照先

この付録では以下の項目について説明しています。

- NetBackup プライマリサーバー Web サーバーのユーザーとグループの作成
- クラスタ化されたプライマリサーバーの非アクティブノードで証明書を生成する
- NetBackup Java Runtime Environment について
- アップグレード後の Java GUI と JRE の追加または削除
- NetBackup Web ユーザーインターフェースについて
- NetBackup 応答ファイルについて
- 維持される Java Virtual Machine のオプション
- RBAC ブートストラップについて
- NetBackup ソフトウェアの入手について
- NetApp クラスタのためのアップグレード前の追加手順
- Replication Director を使用した NetApp ディスクアレイの使用
- NetBackup のバージョン間の互換性について
- UNIX および Linux の場合のアップグレード要件
- Windows および Windows クラスタのアップグレード要件
- Windows クラスタのアップグレードの要件
- 新しいメディアサーバーに全データを移行してクラスタ化されたメディアサーバーを削除する
- Amazon クラウドストレージサーバーのアップグレード後の手順
- サーバーのアップグレード後のクライアントのアップグレード

- アップグレードエラーのロールバック手順
- NetBackup プライマリサーバーとドメインのサイズについてのガイダンス

NetBackup プライマリサーバー Web サーバーのユーザーとグループの作成

NetBackup 8.0 より、NetBackup プライマリサーバーには、重要なバックアップ操作をサポートするための構成済み Web サーバーが含まれます。この Web サーバーは、権限が制限されているユーザーアカウント要素の下で動作します。これらのユーザーアカウント要素は、各プライマリサーバー (またはクラスタ化されたプライマリサーバーの各ノード) で使用できる必要があります。

メモ: セキュリティのため、管理者またはスーパーユーザー権限を持つ Web サーバーユーザーまたはグループは作成しないでください。

多数の手順を実行すると、オペレーティングシステムでユーザーとグループを作成できます。特定のいくつかの方法を示していますが、他の方法でも同じ目標を達成できる可能性があります。ホームディレクトリのパス、ユーザー名、およびグループ名はハードコードされていないため、変更することができます。デフォルトのローカルユーザー名は `nbwebsvc`、デフォルトのローカルグループ名は `nbwebgrp` です。ユーザーとグループには、デーモンを実行するための十分なアクセス権がある必要があります。

このトピックに関する詳細情報を参照できます。

p.166 の「UNIX および Linux の場合のアップグレード要件」を参照してください。

オペレーティングシステム固有のアカウントとグループの要件に注意してください。

- Linux のクラスタ環境では、すべてのクラスタノードでローカルアカウントが一貫して定義されていることを確認します。UID は、ローカルアカウントごとに同じである必要があります。UNIX で LDAP アカウントを使うことができます。
- Windows のクラスタ化されたプライマリサーバーでは、ドメインアカウントを使用する必要があります。非クラスタ環境ではドメインアカウントを使用できますが、必須ではありません。
- Windows のクラスタ化されたプライマリサーバーでは、ドメイングループを使用する必要があります。

これらの要件のいずれかが満たされない場合、NetBackup プライマリサーバーのインストールは失敗します。Windows では、インストールプロセスの一部として、ユーザーアカウントのパスワードを指定するように求められます。

メモ: Web サーバーアカウントに関連付けられたパスワードの期限が初期構成後に切れた場合、NetBackup はパスワードの期限が切れたことを通知しません。アカウントとパスワードはオペレーティングシステムが管理するため、この動作は正常であり、想定どおりです。

Web サーバーがアクティブなままであるかぎり、アカウントと Web サーバーは正常に動作し続けます。

Web サーバーを再起動したときや、nbwmc サービスを再起動しようとした場合、サービスは期限切れのパスワードが原因で失敗します。オペレーティングシステムの該当する領域に移動し、正しいパスワードを入力して、サービスを再起動します。

Web サービスアカウントとグループに関する詳しい情報を参照できます。『NetBackup セキュリティおよび暗号化ガイド』および Web サービスアカウントのセクションを参照してください。

ユーザーアカウントとローカルグループを作成する方法:

1. ローカルグループを作成します。
   - Linux の場合: `# groupadd nbwebgrp`
   - Windows の場合: `C:¥>net localgroup nbwebgrp /add`
2. ローカルユーザーを作成します。
   - Linux の場合: `# useradd -g nbwebgrp -c 'NetBackup Web Services account' -d /usr/openv/wmc nbwebsvc`
   - Windows の場合: `C:¥>net user nbwebsvc strong_password /add`
3. (該当する場合) Windows の場合のみ、ユーザーをグループのメンバーにします。

   `C:¥>net localgroup nbwebgrp nbwebsvc /add`
4. (該当する場合) Windows の場合のみ、[サービスとしてログオン]権限をユーザーに付与します。
   - [コントロールパネル]、[管理ツール]、[ローカルセキュリティポリシー]の順に進みます。
   - [セキュリティの設定]で、[ローカルポリシー]、[ユーザー権利の割り当て]の順にクリックします。
   - [サービスとしてログオン]を右クリックして[プロパティ]を選択します。
   - ローカルユーザーを追加します。デフォルトのローカルユーザー名は nbwebsvc です。
   - 変更を保存して[サービスとしてログオン]の[プロパティ]ダイアログボックスを閉じます。

クラスタ化されたプライマリサーバーの非アクティブノードで証明書を生成する

クラスタ化されたプライマリサーバーのインストールまたはアップグレードが完了したら、すべての非アクティブノードで証明書を生成する必要があります。この手順は、クラスタの非アクティブノードのバックアップおよびリストアを成功させるために必要です。

クラスタ化されたプライマリサーバーの非アクティブノードで証明書を生成する

メモ: 特に明記しない限り、すべてのコマンドは非アクティブノードから発行します

---

1. (該当する場合) 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。

2. `nbcertcmd` コマンドを実行し、非アクティブノードに認証局の証明書を格納します。

   Linux の場合: `/usr/openv/netbackup/bin/nbcertcmd -getCACertificate`

   Windows の場合: *install_path*`¥NetBackup¥bin¥nbcertcmd -getCACertificate`

3. `nbcertcmd` コマンドを実行し、非アクティブノードでホスト証明書を生成します。

   ```
   nbcertcmd -getCertificate
   ```

4. (該当する場合) `nbcertcmd -getCertificate` コマンドが失敗し、トークンが必要なことを示すエラーメッセージが表示される場合は、認証局からのトークンが必要です。表示されている手順を使用してトークンを取得し、正しく使用します。

   - アクティブノードで、必要な変更を許可するように、示されているとおりに `bpnbat` コマンドを使用します。認証ブローカーを要求す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
     ```

   - アクティブノードで、`nbcertcmd` コマンドを使用してトークンを作成します。

     ```
     nbcertcmd -createToken -name token_name
     ```

     この手順ではトークン名は重要ではありません。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。次のコマンドで必要になるため、この値をメモします。

   - 非アクティブノードで、`nbcertcmd` コマンドとともに認証トークンを使用して、ホスト証明書を格納します。

     ```
     nbcertcmd -getCertificate -token
     ```

     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。

証明書に関する詳しい情報を参照できます。『NetBackup セキュリティおよび暗号化ガイド』で、プライマリサーバーノードでの証明書の配備に関するセクションを参照してください。

NetBackup Java Runtime Environment について

次の製品のいずれかをインストールするときに、Veritasはカスタマイズされたバージョンの Java Runtime Environment (JRE) をインストールします。カスタマイズされたバージョンの JRE には、標準 JRE インストールに含まれる man、plugin など、すべてのディレクトリが含まれているわけではありません。

JRE をインストールする製品は、次のとおりです。

- NetBackup プライマリサーバー、メディアサーバー、UNIX および Linux クライアントソフトウェア
- NetBackup Java リモート管理コンソール

NetBackup 8.3 以降、Linux メディアサーバーと Windows メディアサーバー、および UNIX クライアントと Linux クライアントでは、Java GUI と JRE パッケージはオプションです。

以前のリリースと同様に、Java GUI および JRE パッケージは必須であるため、すべてのプライマリサーバーに自動的にインストールされます。Java GUI と JRE は、Windows クライアントのデフォルトインストールの一部ではありません。Windows クライアントでこの機能が必要な場合は、Java リモート管理コンソールをインストールしてください。

NetBackup のさまざまなインストール方法が用意されているため、ユーザーは Java GUI や JRE のパッケージをインストールするかどうかを選択できます。インストールまたはアップグレード後の Java GUI や JRE のインストールまたは削除についての詳しい情報も参照できます。

p.131 の「アップグレード後の Java GUI と JRE の追加または削除」を参照してください。

以前は、NetBackup と共にインストールされる JRE パッケージは、ソフトウェアを以降のリリースにアップグレードした場合にのみ更新されました。nbcomponentupdate ユーティリティを使用して、JRE を以下の製品でサポートされているバージョンに更新することができます。

- NetBackup プライマリサーバー、メディアサーバー、UNIX および Linux クライアントソフトウェア
- NetBackup Java リモート管理コンソール

メモ: このユーティリティを使用して、NetBackup Plug-in for VMware vCenter の JRE を更新することはできません。

システムで NetBackup 8.0 以降を実行している場合、表 A-1 を使用して、nbcomponentupdate ユーティリティの場所を特定します。

表 A-1 JRE 更新ユーティリティの場所

製品	オペレーティングシステム	パス
NetBackup	Windows	*install_path*¥netbackup¥java¥nbcomponentupdate.exe
	UNIX または Linux	/usr/openv/java/nbcomponentupdate
NetBackup Java リモート管理コンソール	Windows	*install_path*¥java¥nbcomponentupdate.exe

NetBackup 7.7.x 以前がある場合、以下の場所から nbcomponentupdate ユーティリティをダウンロードします。

https://www.veritas.com/support/en_US/article.000115043

nbcomponentupdate コマンドとそのパラメータに関する詳細情報を参照できます。

『NetBackup コマンドリファレンスガイド』

NetBackup とともにインストールされる JRE は、その NetBackup リリースに対してサポートされているメジャーバージョンです。サポートされているメジャー JRE バージョンのマイナーバージョンに更新するには、このユーティリティを使用します。たとえば、NetBackup 8.0 が JRE 1.8.0.31 をインストールした場合、サポート対象のメジャーバージョンは 1.8 です。JRE 1.8.0.92 に更新するには、このユーティリティを使用します。

Veritas は、JRE ベンダーがインストール済みの JRE バージョンに対し End-of-Life を宣言した場合にのみ別のメジャー JRE バージョンに更新することを推奨します。お使いの環境にインストール済みの JRE バージョンでもある JRE 1.8 に対し、JRE ベンダーが End-of-Life を宣言した場合は、JRE 1.9 に更新します。

JRE を更新しようとする前に、NetBackup などの製品を終了します。更新時に製品が実行中である場合、ユーティリティが終了し、製品を終了するように求めるエラーメッセージが表示されます。

注意: JRE 更新が進行中の場合、ユーティリティを停止しないでください。このアクションにより、JRE を使用する NetBackup などの製品が不安定になる可能性があります。

追加バージョンの JRE がその他のアプリケーションに対してシステムにインストールされている場合、NetBackup JRE はそれらの JRE と干渉しません。NetBackup JRE は Web ブラウザとの統合を行ったり、Java アプレットまたは Web Start の実行を許可した

りするものではありません。したがって、NetBackup JRE は Java アプレットまたは Web Start の脆弱性を利用するタイプのブラウザベースの攻撃で使用されることがありません。

NetBackup JRE アラートに関する詳しい情報を参照できます。

http://www.veritas.com/docs/TECH50711

アップグレード後の Java GUI と JRE の追加または削除

アップグレード操作が完了したら、Java GUI と JRE パッケージを追加または削除できます。

Java GUI および JRE の追加

パッケージを追加するには、次に示すオプションのいずれかを使用します。

- VxUpdate ポリシー (アドホック操作) を作成して実行し、Java GUI および JRE パッケージを含めるように指定します。
- UNIX の場合は、アップグレードメディアにアクセスし、次に示すコマンドを実行します。

Linux	`rpm -U VRTSnbjre.rpm` `rpm -U VRTSnbjava.rpm`
Solaris	`pkgadd -a .pkg_defaults -d VRTSnbjre.pkg VRTSnbjre` `pkgadd -a .pkg_defaults -d VRTSnbjava.pkg VRTSnbjava`
AIX	`installp -ad VRTSnbjre.image all` `installp -ad VRTSnbjava.image all`
Debian	Debian インストールスクリプトを再実行し、正しい値を指定して、Java GUI と JRE パッケージを追加します。

- Windows の場合は、インストールメディアにアクセスし、次に示すパッケージを実行します。
  - `Veritas NetBackup JRE.msi`
  - `Veritas NetBackup Java GUI.msi`

Java GUI および JRE の削除

パッケージを削除するには、次に示すオプションのいずれかを使用します。

- VxUpdate ポリシー (アドホック操作) を作成して実行し、Java GUI および JRE パッケージを除外するように指定します。
- UNIX の場合、次のコマンドを実行します。

Linux	`rpm -e VRTSnbjava.rpm` `rpm -e VRTSnbjre.rpm`
Solaris	`pkgrm VRTSnbjava` `pkgrm VRTSnbjre`
AIX	`installp -u VRTSnbjre` `installp -u VRTSnbjava`
Debian	Debian インストールスクリプトを再実行し、正しい値を指定して、Java GUI と JRE パッケージを削除します。

- Windows の場合
  - スタートメニューで[設定]、[コントロールパネル]の順に選択します。
  - [コントロールパネル]ウィンドウで、インストール済みのプログラムとアプリケーションの適切なユーティリティを選択します。
  - [現在インストールされているプログラム]のリストで[Veritas NetBackup Java]を選択し、[削除]をクリックします。
  - [現在インストールされているプログラム]のリストで[Veritas NetBackup JRE]を選択し、[削除]をクリックします。

NetBackup Web ユーザーインターフェースについて

バージョン 8.1.2 で、Veritas は NetBackup と併用する新しい Web ユーザーインターフェースを導入しました。新しいインターフェースは、使いやすさと機能が向上するように設計されています。現時点で、NetBackup 管理コンソールの一部の機能は、新しいインターフェースで利用可能になっていません。

NetBackup は、新しいインターフェースの通信を暗号化するために、トランスポート層セキュリティ (TLS) プロトコルを使用します。NetBackup Web サーバーで TLS を有効にするには、NetBackup ホストを識別する TLS 証明書が必要です。NetBackup は、クライアントとホストの検証に自己署名証明書を使用します。自己署名証明書は、Web ブラウザと NetBackup Web サーバー間の TLS 通信を有効にするため、インストール時に自動的に生成されます。NetBackup Web サービスをサポートするために、サードパーティの証明書を作成して実装して、自己署名証明書の代わりに使用できます。証明書は

TLS 暗号化と認証で使用されます。詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

NetBackup Web UI から NetBackup プライマリサーバーへの初回サインイン

NetBackup のインストール後に、root ユーザーまたは管理者が NetBackup Web UI に Web ブラウザからサインインして、ユーザー向けに RBAC の役割を作成する必要があります。役割は、組織のユーザーの役割に基づいて、Web UI を通じて NetBackup 環境にアクセスするためのアクセス権をユーザーに付与します。一部のユーザーは、デフォルトで Web UI にアクセスできます。

権限を持つユーザー、役割の作成、Web UI へのサインインとサインアウトについて詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

NetBackup 応答ファイルについて

NetBackup では、事前定義された一連の設定オプションを使用して、無人インストール、サイレントインストール、アップグレードを実行する方法を提供します。これらのオプションを使うと、次のことが可能になります。

- 一部のデフォルト値を上書きします。
- 対話式のインストール時の質問への回答を回避します。

UNIX と Linux では、プライマリ、メディア、およびクライアントのテンプレートは、ベリタスからダウンロードした、NetBackup インストールイメージの最上位で利用可能です。これらのテンプレートは、必要に応じて変更し、インストール時とアップグレード時に使用できるように `/tmp/NBInstallAnswer.conf` に配置する必要があります。

Windows では、プライマリ、メディア、およびクライアントのテンプレートは、ベリタスからダウンロードした、NetBackup インストールイメージの最上位にある `windows_x64` ディレクトリで利用可能です。これらのテンプレートはそれぞれ、`silentprimary.cmd`、`silentmedia.cmd`、`silentclient.cmd` と呼ばれます。

メディアとクライアントのテンプレートは、Veritas からダウンロードした、NetBackup インストールイメージの最上位で利用可能です。

インストールスクリプトを実行する前にターゲットホストに NetBackup 応答ファイルを設定します。ファイルが存在しない場合はファイルを作成します。サポート対象のエントリを関連する情報とともに示します。

表 A-2 テンプレートのすべてのオプションと必要なコンピュータ

オプション	NetBackup の役割	プラットフォーム	アップグレードに必要かどうか
「ABORT_REBOOT_INSTALL」	プライマリ、メディア、およびクライアント	Windows	不要
「ACCEPT_EULA」	プライマリ、メディア、およびクライアント	UNIX および Linux	不要
「ACCEPT_REVERSE_CONNECTION」	クライアント	すべて	不要
「ADDITIONALSERVERS」	プライマリ、メディア、およびクライアント	Windows	不要
「ALLOW_PRE_90_UPGRADE」	プライマリ	すべて	詳しくは、オプションを参照してください。
「AUTHORIZATION_TOKEN」	メディアおよびクライアント	すべて	詳しくは、「セキュリティ構成の注意事項について」を参照してください。
「CA_CERTIFICATE_FINGERPRINT」	メディアおよびクライアント	すべて	詳しくは、「セキュリティ構成の注意事項について」を参照してください。
「CLIENT」	クライアント	Windows	必要
「CLIENT_NAME」	メディアおよびクライアント	UNIX および Linux	不要
「ECA_CERT_PATH」	メディアおよびクライアント	すべて	詳しくは、「セキュリティ構成の注意事項について」を参照してください。
「ECA_CERT_STORE」	メディアおよびクライアント	Windows	詳しくは、「セキュリティ構成の注意事項について」を参照してください。
「ECA_CRL_CHECK_LEVEL」	メディアおよびクライアント	すべて	詳しくは、「セキュリティ構成の注意事項について」を参照してください。
「ECA_CRL_PATH」	メディアおよびクライアント	すべて	ECA_CRL_CHECK_LEVEL=USE_PATH が指定された場合のみ。
「ECA_KEY_PASSPHRASEFILE」	メディアおよびクライアント	すべて	不要
「ECA_PRIVATE_KEY_PATH」	メディアおよびクライアント	すべて	詳しくは、「セキュリティ構成の注意事項について」を参照してください。
「ECA_TRUST_STORE_PATH」	メディアおよびクライアント	すべて	詳しくは、「セキュリティ構成の注意事項について」を参照してください。

オプション	NetBackup の役割	プラットフォーム	アップグレードに必要かどうか
「INCLUDE_JAVA_GUI_AND_JRE」	メディアおよびクライアント	すべて	UNIX および Linux のメディアサーバーとクライアント: 不要 Windows メディアサーバー: 必要
「INSTALL_PATH」	メディアおよびクライアント	すべて	不要
「INSTALLDIR」	プライマリ、メディア、およびクライアント	Windows	不要
「LICENSE」	プライマリ	UNIX および Linux	不要
「LICENSEKEY」	プライマリ	Windows	不要
「MACHINE_ROLE」	メディアおよびクライアント	UNIX および Linux	不要
「MEDIA_SERVER」	クライアント	UNIX および Linux	不要
「MEDIASERVER」	メディア	Windows	不要
「MERGE_SERVERS_LIST」	クライアント	UNIX および Linux	不要
「PRIMARYSERVER」	プライマリ、メディア、およびクライアント	Windows	必要
「PROCEED_WITH_INSTALL」	プライマリ、メディア、およびクライアント	UNIX および Linux	不要
「RBAC_DOMAIN_NAME」	プライマリ	Linux	不要
「RBAC_DOMAIN_TYPE」	プライマリ	Linux	不要
「RBAC_PRINCIPAL_NAME」	プライマリ	Linux	不要
「RBAC_PRINCIPAL_TYPE」	プライマリ	Linux	不要
「SECURITY_CONFIGURATION」	メディアおよびクライアント	すべて	不要
「SERVER」	メディアおよびクライアント	UNIX および Linux	不要
「SERVICES」	クライアント	UNIX および Linux	不要
「SERVICESTARTTYPE」	プライマリ、メディア、およびクライアント	Windows	不要

オプション	NetBackup の役割	プラットフォーム	アップグレードに必要かどうか
「SERVICE_USER」	プライマリ	Linux	必要
「START_JOB_DAEMONS」	プライマリ	Linux	不要
「STOP_NBU_PROCESSES」	プライマリ、メディア、およびクライアント	Windows	不要
「USAGE_INSIGHTS_FILE_PATH」	プライマリ	Windows および Linux	可能性あり
「VNETD_PORT」	プライマリ、メディア、およびクライアント	Windows	不要
「WEBSVC_DOMAIN」	プライマリ	Windows	必要
「WEBSVC_GROUP」	プライマリ	すべて	UNIX および Linux: 不要 Windows: 必要
「WEBSVC_PASSWORD_PLAIN」	プライマリ	Windows	必要
「WEBSVC_USER」	プライマリ	すべて	UNIX および Linux: 不要 Windows: 必要

プラットフォームおよび役割別の応答ファイルオプション

これらの表には、プラットフォームと役割に基づいて利用可能な応答ファイルオプションが示されています。一覧に示されているオプションの一部は必須ではありません。詳しくは、表 A-2 またはオプションの詳細を参照してください。

表 A-3 Windows コンピュータ

プライマリ	メディア	クライアント
ABORT_REBOOT_INSTALL ADDITIONALSERVERS ALLOW_PRE_90_UPGRADE INSTALLDIR LICENSEKEY PRIMARYSERVER SERVICESTARTTYPE STOP_NBU_PROCESSES USAGE_INSIGHTS_FILE_PATH VNETD_PORT WEBSVC_DOMAIN WEBSVC_GROUP WEBSVC_PASSWORD_PLAIN WEBSVC_USER	ABORT_REBOOT_INSTALL ADDITIONALSERVERS AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT ECA_CERT_PATH ECA_CERT_STORE ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INSTALL_PATH INSTALLDIR MEDIASERVER PRIMARYSERVER SERVICESTARTTYPE STOP_NBU_PROCESSES VNETD_PORT	ABORT_REBOOT_INSTALL ACCEPT_REVERSE_CONNECTION ADDITIONALSERVERS AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT CLIENT ECA_CERT_PATH ECA_CERT_STORE ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INSTALL_PATH INSTALLDIR PRIMARYSERVER SERVICESTARTTYPE STOP_NBU_PROCESSES VNETD_PORT

表 A-4 UNIX および Linux コンピュータ

プライマリ	メディア	クライアント
ACCEPT_EULA ALLOW_PRE_90_UPGRADE CLIENT_NAME INSTALL_PATH LICENSE MACHINE_ROLE MEDIA_SERVER PROCEED_WITH_INSTALL RBAC_DOMAIN_NAME RBAC_DOMAIN_TYPE RBAC_PRINCIPAL_NAME RBAC_PRINCIPAL_TYPE SERVER SERVICE_USER START_JOB_DAEMONS USAGE_INSIGHTS_FILE_PATH WEBSVC_GROUP WEBSVC_USER	ACCEPT_EULA AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT CLIENT_NAME ECA_CERT_PATH ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INSTALL_PATH MACHINE_ROLE PROCEED_WITH_INSTALL SERVER	ACCEPT_EULA ACCEPT_REVERSE_CONNECTION AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT CLIENT_NAME ECA_CERT_PATH ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INSTALL_PATH MACHINE_ROLE MEDIA_SERVER MERGE_SERVERS_LIST PROCEED_WITH_INSTALL SERVER SERVICES

セキュリティ構成の注意事項について

NetBackup のバージョンおよび実行される操作によって、テンプレートファイルに必要なセキュリティパラメータが決まります。

初期インストールまたは 8.1 より前のバージョンのアップグレードでのセキュリティ構成に関する注意事項

この操作が初回インストール、または 8.1 より前のバージョンからのアップグレードの場合は、少なくとも 1 セットのセキュリティ構成パラメータを指定する必要があります。セキュリティ構成はスキップできますが、スキップした場合は、インストールまたはアップグレード後に各ターゲットホストで手順を手動で実行する必要があります。

NetBackup プライマリサーバーを認証局として使用するには、プライマリサーバーの CA_CERTIFICATE_FINGERPRINT を指定する必要があります。プライマリサーバーのセキュリティレベル、またはこのコンピュータがプライマリサーバーですでに構成されているかどうかに応じて、AUTHORIZATION_TOKEN オプションが必要になることがあります。詳しくは、https://www.veritas.com/support/en_US/article.000127129 を参照してください。

UNIX および Linux で外部認証局を使用するには、ECA_CERT_PATH、ECA_CRL_CHECK_LEVEL、ECA_PRIVATE_KEY_PATH、ECA_TRUST_STORE_PATH の値が必須です。詳しくは、https://www.veritas.com/support/en_US/article.100044300 を参照してください。

詳しくは、『NetBackup セキュリティおよび暗号化ガイド』で外部 CA と外部証明書の章を参照してください。

Windows で外部認証局を使用するには、ECA_CERT_STORE と ECA_CRL_CHECK_LEVEL の値を指定するか、UNIX と Linux で以前に指定したすべての値を指定します。

ECA_CRL_PATH と ECA_KEY_PASSPHRASEFILE の値は省略可能です。詳しくは、https://www.veritas.com/support/en_US/article.100044300 を参照してください。

詳しくは、『NetBackup セキュリティおよび暗号化ガイド』で外部 CA と外部証明書の章を参照してください。

NetBackup 8.1 以降のアップグレードのセキュリティ構成に関する注意事項

すでに安全な通信が構成されているバージョンの NetBackup からアップグレードする場合 (NetBackup 8.1 以降)、CA_CERTIFICATE_FINGERPRINT と AUTHORIZATION_TOKEN の値は無視されます。

NetBackup 8.2 以降のアップグレードのセキュリティ構成に関する注意事項

ECA がすでに構成されているバージョンの NetBackup からアップグレードする場合 (NetBackup 8.2 以降)、すべての ECA* パラメータは無視されます。

外部認証局の構成のスキップについて

認証局を構成せずにインストールまたはアップグレードを続行するには、SECURITY_CONFIGURATION キーを含め、そのキーを SKIP に設定します。CA_CERTIFICATE_FINGERPRINT、AUTHORIZATION_TOKEN、およびすべての ECA_ 値を応答ファイルから削除します。必要な認証局コンポーネントを構成せずにインストールまたはアップグレードを続行すると、バックアップとリストアが失敗します。

ABORT_REBOOT_INSTALL

- 説明: このオプションは、再起動が必要な場合にインストールまたはアップグレードを停止します。有効な値は 0 (停止しない) または 1 (停止) です。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: 0
- 必要/不要: 不要。
- ABORT_REBOOT_INSTALL 0 | 1
- 表 A-2 に戻ります。

ACCEPT_EULA

- 説明: このオプションは、EULA の条項に同意し、インストールまたはアップグレードを続行するかどうかを指定します。
- 該当するプラットフォーム: UNIX および Linux
- デフォルト値: なし
- 必要/不要: 不要
- `ACCEPT_EULA = yes | no`
- 表 A-2 に戻ります。

ACCEPT_REVERSE_CONNECTION

- 説明: NAT クライアントと NetBackup ホストとの接続方法を識別する場合に、このオプションを使用します。許可される値は `TRUE` と `FALSE` です。NetBackup で NAT をサポートする場合はこのオプションを `TRUE` に、それ以外の場合は `FALSE` に設定します。次の場合、`ACCEPT_REVERSE_CONNECTION=FALSE` を設定します。
  - NetBackup で NAT クライアントをサポートしない場合。
  - NetBackup クライアントがファイアウォールの背後に存在しない場合。
- 該当するプラットフォーム: UNIX と Windows の両方。
- デフォルト値: `FALSE`
- `ACCEPT_REVERSE_CONNECTION=TRUE | FALSE`
- 表 A-2 に戻ります。

ADDITIONALSERVERS

- 説明: このオプションは、プライマリサーバーにセキュリティ要求をプロキシするために使用される NetBackup メディアサーバーを含める場合に使用します。このホストの前回のインストール以降に追加されたサーバーのみを一覧表示します。インストール処理では、既存のサーバーのセットが新しいものと統合されています。IP アドレスの使用はサポートされていません。有効な入力値は、完全修飾コンピュータ名のカンマで区切られたリストです。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 不要。
- `ADDITIONALSERVERS` *`server1,server2,servern`*
- 表 A-2 に戻ります。

ALLOW_PRE_90_UPGRADE

- 説明: このフィールドはプライマリサーバーのみを対象としています。この値は、9.0 より前のリリースの NetBackup から NetBackup 9.0 以降へのアップグレードを続行できるかどうかを判定します。アップグレードには、無制限の有効期限変換プロセスが含まれます。この変換は、9.0 より前の NetBackup から 9.0 以降の NetBackup にアップグレードするときにのみ行われます。アップグレードの動作とこのオプションの必要性は、プライマリサーバーのプラットフォームによって異なります。
  - Windows
    この値は、Windows プライマリサーバーのサイレントアップグレードに必要です。アップグレードを続行する場合は `1` を指定し、アップグレードを停止する場合は `0` を指定します。この値は、対話形式の Windows プライマリサーバーのアップグレード中は無視されます。NetBackup カタログのサイズと必要な変換時間によっては、アップグレードを続行するかどうかを確認するメッセージが表示されることがあります。
  - Linux
    Linux プライマリサーバーの場合は、`yes` または `no` を指定するとユーザーに確認メッセージが表示されなくなります。無制限の有効期限変換によってアップグレードプロセスが延長されることが予想される場合、値 `yes` はアップグレードを続行することを意味します。値 `no` はアップグレードが停止することを意味します。この値を指定しない場合、アップグレードを続行するかどうかを確認するメッセージが NetBackup によって表示されます。

  NetBackup 9.0 以降のバージョンでは、2038 年より先の有効期限がサポートされています。NetBackup の以前のバージョンとの互換性を確保するために、無制限の有効期限が設定されたすべての項目は、新しい無制限の有効期限の値を反映するように更新されます。この変換によって、アップグレードを完了するために必要な時間が長くなる場合があります。詳しくは、次の記事を参照してください。
  https://www.veritas.com/content/support/en_US/article.100048600
- 該当するプラットフォーム: UNIX と Windows の両方。
- デフォルト値: なし
- 必要/不要: プラットフォームおよびアップグレード方法に依存します。
- `ALLOW_PRE_90_UPGRADE=yes|no` (UNIX)
  `ALLOW_PRE_90_UPGRADE=1|0` (Windows)
- 表 A-2 に戻ります。

AUTHORIZATION_TOKEN

- 説明: このオプションは、NetBackup がホスト証明書の取得時に認証トークンまたは再発行トークンを自動的に使用するかを指定します。`AUTHORIZATION_TOKEN` は大文字で 16 文字です。一部の環境では、バックアップおよびリストアが正常に動作す

るために認証トークンが必要です。この情報が必要な場合に、応答ファイルに指定されていないと、インストールは失敗します。SKIP を指定すると、インストーラはトークンを含まずにホスト証明書を取得しようとします。環境によっては、この選択により、インストール後に手動による追加の手順が必要となる場合があります。

AUTHORIZATION_TOKEN は、次のいずれかの条件では無視されることに注意してください。

- ECA がプライマリサーバーで使用されている
- プライマリサーバーのセキュリティレベルが High より低い値に設定されている

- 該当するプラットフォーム: UNIX と Windows の両方。
- デフォルト値: なし。
- 必要/不要: 詳しくは、「セキュリティ構成の注意事項について」を参照してください。
- AUTHORIZATION_TOKEN=*ABCDEFGHIJKLMNOP* | SKIP
- 表 A-2 に戻ります。

CA_CERTIFICATE_FINGERPRINT

- 説明: このオプションは、認証局 (CA) 証明書の指紋を指定します。SHA-1 指紋と SHA-256 指紋の両方がサポートされます。証明書の指紋は、インストールまたはアップグレード中に CA から取得されます。指紋形式は 59 文字または 95 文字であり、0 から 9 の数字、A から F の英字およびコロンの組み合わせです。たとえば、01:23:45:67:89:AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23:45:67 となります。指紋の値は、最初の SERVER=*server_name* オプションに指定されているサーバーの指紋と一致する必要があります。

  CA_CERTIFICATE_FINGERPRINT は、次のいずれかの条件では無視されることに注意してください。

  - ECA がプライマリサーバーで使用されている
  - プライマリサーバーのセキュリティレベルが High より低い値に設定されている

- 該当するプラットフォーム: UNIX と Windows の両方。
- デフォルト値: なし。
- 必要/不要: 詳しくは、「セキュリティ構成の注意事項について」を参照してください。
- CA_CERTIFICATE_FINGERPRINT=*fingerprint*
- 表 A-2 に戻ります。

CLIENT

- 説明: このオプションは、NetBackup がこのクライアントホストの識別に使用する名前を指定します。%COMPUTERNAME% 値により、ローカルホストがコンピュータ名を提供で

きるようになります。この値を使用すると、単一のプライマリサーバードメイン内のすべてのコンピュータに同じ応答ファイルを使用できます。IP アドレスの使用はサポートされていません。

- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 必要。
- CLIENT=*client_name* | %COMPUTERNAME%
- 表 A-2 に戻ります。

CLIENT_NAME

- 説明: このオプションは、NetBackup がこのコンピュータの識別に使用する名前を指定します。XLOCALHOSTX 値により、ローカルホストがコンピュータ名を提供できるようになります。この値を使用すると、単一のプライマリサーバードメイン内のすべてのコンピュータに同じ応答ファイルを使用できます。この値は、bp.conf ファイルに追加されます。
  アップグレードで CLIENT_NAME が指定されている場合、応答ファイルで指定される名前が bp.conf ファイルで構成されている値と一致することを検証するチェックが行われます。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: なし。
- 必要/不要: 不要
- CLIENT_NAME=*name* | XLOCALHOSTX
- 表 A-2 に戻ります。

ECA_CERT_PATH

- 説明: このオプションは、外部証明書ファイルのパスとファイル名を指定します。
  ECA がホストですでに構成されている場合、またはプライマリサーバーで NBCA のみが使用されている場合、アップグレード時に ECA_CERT_PATH オプションは無視されます。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。
- 必要/不要: 詳しくは、「セキュリティ構成の注意事項について」を参照してください。
- ECA_CERT_PATH=*path_and_file_name*
- 表 A-2 に戻ります。

ECA_CERT_STORE

- 説明: このオプションは、Windows 証明書ストアの外部証明書の場所を指定します。このオプションは、Windows 証明書ストアから外部証明書を設定する場合に必要です。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 詳しくは、「セキュリティ構成の注意事項について」を参照してください。
- ECA_CERT_STORE=*store_name*¥*issuer_distinguished_name*¥*subject*
- 表 A-2 に戻ります。

ECA_CRL_CHECK_LEVEL

- 説明: このオプションは CRL モードを指定します。サポートされる値は次のとおりです。
  - USE_CDP: 証明書に定義されている CRL を使用します。
  - USE_PATH: ECA_CRL_PATH で指定されたパスにある CRL を使用します。
  - DISABLED: CRL を使用しません。
  - ECA がホストですでに構成されている場合、またはプライマリサーバーで NBCA のみが使用されている場合、アップグレード時に ECA_CERT_PATH オプションは無視されます。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。
- 必要/不要: 詳しくは、「セキュリティ構成の注意事項について」を参照してください。
- ECA_CRL_CHECK_LEVEL=*value*
- 表 A-2 に戻ります。

ECA_CRL_PATH

- 説明: このオプションは、外部 CA 証明書に関連付けられている CRL のパスとファイル名を指定します。
  ECA がホストですでに構成されている場合、またはプライマリサーバーで NBCA のみが使用されている場合、アップグレード時に ECA_CERT_PATH オプションは無視されます。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。
- 必要/不要: ECA_CRL_CHECK_LEVEL=USE_PATH が指定された場合のみ。

- ECA_CRL_PATH=*path*
- 表 A-2 に戻ります。

ECA_KEY_PASSPHRASEFILE

- 説明: このオプションは、キーストアにアクセスするためのパスフレーズを含むファイルのパスとファイル名を指定します。
  ECA がホストですでに構成されている場合、またはプライマリサーバーで NBCA のみが使用されている場合、アップグレード時に ECA_CERT_PATH オプションは無視されます。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。
- 必要/不要: 不要
- ECA_KEY_PASSPHRASEFILE=*path/filename*
- 表 A-2 に戻ります。

ECA_PRIVATE_KEY_PATH

- 説明: このオプションは、秘密鍵を示すファイルのパスとファイル名を指定します。
  ECA がホストですでに構成されている場合、またはプライマリサーバーで NBCA のみが使用されている場合、アップグレード時に ECA_CERT_PATH オプションは無視されます。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。
- 必要/不要: 詳しくは、「セキュリティ構成の注意事項について」を参照してください。
- ECA_PRIVATE_KEY_PATH=*path/filename*
- 表 A-2 に戻ります。

ECA_TRUST_STORE_PATH

- 説明: このオプションは、トラストストアの場所を示すファイルのパスとファイル名を指定します。
  ECA がホストですでに構成されている場合、またはプライマリサーバーで NBCA のみが使用されている場合、アップグレード時に ECA_CERT_PATH オプションは無視されます。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。
- 必要/不要: 詳しくは、「セキュリティ構成の注意事項について」を参照してください。

- ECA_TRUST_STORE_PATH=*path/filename*
- 表 A-2 に戻ります。

INCLUDE_JAVA_GUI_AND_JRE

- 説明: インストール時またはアップグレード時にオプションの Java および JRE コンポーネントを処理する方法を決定するために使用します。サポートされる値は次のとおりです。
  - INCLUDE: Java GUI と JRE をインストールまたはアップグレードの一部として含めます。
  - EXCLUDE: Java GUI と JRE を除外します。このオプションを指定すると、以前のすべてのバージョンの Java GUI と JRE がホストに存在する場合、それらも削除されます。
  - MATCH: ホスト上の既存の構成を照合します。初期インストールでこのオプションを指定すると、コンポーネントはインストールされません。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし
- 必要/不要: UNIX および Linux の場合は不要、Windows メディアサーバーの場合は必要。
- 表 A-2 に戻ります。

INSTALL_PATH

- 説明: このオプションは、NetBackup バイナリをインストールする場所を指定します。このオプションに必要なのは、ベースディレクトリへの絶対パスのみです。インストーラは /openv を自動的に追加します。このオプションは、アップグレード中に NetBackup の場所を変更する目的では使用できません。
  アップグレード時に、INSTALL_PATH オプションが無視されることに注意してください。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: /usr
- 必要/不要: 不要
- INSTALL_PATH = *path*
- 表 A-2 に戻ります。

INSTALLDIR

- 説明: このオプションは、NetBackup をインストールする場所を指定します。ベースディレクトリへの完全修飾パスが必要です。

- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 必要
- `INSTALLDIR=C:¥Program Files¥Veritas`
- 表 A-2 に戻ります。

LICENSE

- 説明: このオプションは、プライマリサーバーに適用するライセンスキー文字列を指定します。ライセンスをさらに適用する場合は、追加の「`LICENSE = key_string`」行を追加できます。このオプションはキーの追加のみ実行し、既存のキーは削除されません。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: なし。
- 必要/不要: 不要。
- `LICENSE = key_string`
- 表 A-2 に戻ります。

LICENSEKEY

- 説明: このオプションは、プライマリサーバーインストール用の NetBackup ライセンスキーを指定します。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 必要 (プライマリサーバーの場合)。メディアサーバーとクライアントの場合は不要。
- `LICENSEKEY=NetBackup_license_key`
- 表 A-2 に戻ります。

MACHINE_ROLE

- 説明: このオプションは、このコンピュータでインストールおよび構成を実行するための NetBackup の役割を指定します。アップグレードの場合、この値はコンピュータに構成されている役割と一致する必要があります。
- デフォルト値: なし。サポートされる値は、`PRIMARY`、`MEDIA`、`CLIENT` です。
- 該当するプラットフォーム: UNIX および Linux のみ。
- 必要/不要: 不要。

- MACHINE_ROLE = PRIMARY | MEDIA | CLIENT
- 表 A-2 に戻ります。

MEDIA_SERVER

- 説明: このオプションは、指定したホストを NetBackup が使用してこのクライアントに対するセキュリティ保護された Web 要求をトンネリングするように指定します。クライアントとプライマリサーバー上の NetBackup Web サービスの間の通信が遮断される場合、トンネルが必要です。この通信は、NetBackup のインストールまたはアップグレード時にホスト証明書を入手するために必要です。応答ファイルには複数の MEDIA_SERVER エントリを含めることができます。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: なし。
- 必要/不要: 不要。
- MEDIA_SERVER=*media_server_name*
- 表 A-2 に戻ります。

MEDIASERVER

- 説明: このオプションは、このコンピュータがメディアサーバーとして認識するホストの名前を指定します。IP アドレスの使用はサポートされていません。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 不要。
- MEDIASERVER=*media_server_name*
- 表 A-2 に戻ります。

MERGE_SERVERS_LIST

- 説明: プライマリ上の bp.conf にあるサーバーを、このクライアントの bp.conf に格納されているサーバーリストに統合します。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: NO
- 必要/不要: 不要。
- MERGE_SERVERS_LIST = yes | no
- 表 A-2 に戻ります。

PRIMARYSERVER

- 説明: このオプションは、このコンピュータが現在の NetBackup プライマリサーバーとして認識するサーバー名を指定します。このホストがプライマリサーバーの場合は、%COMPUTERNAME% を値に使用できます。IP アドレスの使用はサポートされていません。ADDITIONALSERVERS オプションを使用すると、追加のプライマリサーバーを指定できます。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 必要。
- PRIMARYSERVER=*primary_server_name*
- 表 A-2 に戻ります。

PROCEED_WITH_INSTALL

- 説明: このオプションを使用すると、インストール前チェックの後にインストールを続行または停止できます。続行する前に、失敗した重要でないチェックの一部を解決することが必要な場合があります。重要なチェックエラーがあると、インストールまたはアップグレードは引き続き中止されます。
- 該当するプラットフォーム: UNIX および Linux
- デフォルト値: なし
- 必要/不要: 不要
- PROCEED_WITH_INSTALL = yes | no
- 表 A-2 に戻ります。

RBAC_DOMAIN_NAME

- 説明: このオプションは、管理者の役割に、役割ベースのアクセス制御 (RBAC) 権限が構成されているプリンシパルのドメイン名を指定します。
- デフォルト値: なし。
- 該当するプラットフォーム: UNIX および Linux のみ。
- 必要/不要: 不要
- RBAC_DOMAIN_NAME = *domain_name*
- 表 A-2 に戻ります。

RBAC_DOMAIN_TYPE

- 説明: このオプションは、管理者の役割に、役割ベースのアクセス制御 (RBAC) 権限が構成されているプリンシパルのドメイン形式を指定します。

- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: なし。
- 必要/不要: 不要
- `RBAC_DOMAIN_TYPE = domain_type`
- 表 A-2 に戻ります。

RBAC_PRINCIPAL_NAME

- 説明: このオプションは、管理者の役割に、役割ベースのアクセス制御 (RBAC) 権限が構成されているプリンシパルの名前を指定します。このユーザーまたはユーザーグループがシステムに存在する必要があります。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: なし。
- 必要/不要: 不要
- `RBAC_PRINCIPAL_NAME = principal_name`
- 表 A-2 に戻ります。

RBAC_PRINCIPAL_TYPE

- 説明: このオプションは、管理者の役割に、役割ベースのアクセス制御 (RBAC) 権限が構成されているプリンシパルの形式を指定します。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: なし。
- 必要/不要: 不要
- `RBAC_PRINCIPAL_TYPE = USER | USERGROUP`
- 表 A-2 に戻ります。

SECURITY_CONFIGURATION

- 説明: ホストで NetBackup 認証局も外部認証局も構成されていない場合にのみ適用できます。NBCA または ECA を使用するようにホストを構成せずにインストールまたはアップグレードを続行するには、このオプションを `SKIP` に設定します。セキュリティをスキップした場合は、インストールまたはアップグレードが完了したときにすべてのターゲットホストで追加の手順を手動で実行する必要があります。このオプションが `SKIP` に設定されている場合、`CA_CERTIFICATE_FINGERPRINT`、`AUTHORIZATION_TOKEN`、`ECA_` オプションには値を指定できません。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。

- 必要/不要: 不要。
- SECURITY_CONFIGURATION = SKIP
- 表 A-2 に戻ります。

SERVER

- 説明: このオプションは、このコンピュータが現在の NetBackup プライマリサーバーとして認識するサーバー名を指定します。認識する必要のあるサーバーが他にある場合は、追加の SERVER= 行を追加できます。SERVER= 行が複数ある場合、最初に表示されるのがプライマリサーバーです。これらのエントリは、bp.conf ファイルに追加されます。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: なし。
- 必要/不要: 不要。
- SERVER=*primary_server_name*
- 表 A-2 に戻ります。

SERVICES

- 説明: このオプションは、クライアントのインストールまたはアップグレードの完了時に NetBackup サービスを起動するかどうかを指定します。起動しないことを指定すると、NetBackup サービスは起動しません。インストールまたはアップグレードの終了後、NetBackup サービスが起動する前に、手動による追加手順の実行が必要になる場合があります。
- 該当するプラットフォーム: UNIX および Linux のみ。
- デフォルト値: YES
- 必要/不要: 不要。
- SERVICES=no
- 表 A-2 に戻ります。

SERVICESTARTTYPE

- 説明: このオプションは、ホストサーバーの再起動後に、NetBackup サービスを再起動するかどうかを指定します。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: Automatic
- 必要/不要: 不要。
- SERVICESTARTTYPE=Automatic | Manual

- 表 A-2 に戻ります。

SERVICE_USER

- 説明: このオプションは、プライマリサーバー上でほとんどの NetBackup サービスまたはデーモンを起動するために使用するサービスユーザーアカウントを指定します。次の点に注意してください。
  - Veritas では、root ユーザーをサービスユーザーとして使用しないことをお勧めします。
  - Veritas では、nbwebsvc ユーザーをサービスユーザーとして使用しないことをお勧めします。
  - nbwebgrp グループはサービスユーザーのセカンダリグループである必要があります。
  - /usr/openv ディレクトリの所有権は、このオプションで指定する新しいサービスユーザーアカウントに変更されます。
  - インストール後にこのユーザーを変更するには、nbserviceusercmd --changeUser コマンドを使用します。
  - クラスタサーバーの場合、すべてのクラスタノードでサービスユーザーとサービスユーザー ID が同じである必要があります。
  - SERVICE_USER 値が応答ファイルに指定され、bp.conf ファイルに存在する場合、値が一致する必要があります。
  - サービスユーザーアカウントについて詳しくは、次を参照してください。 https://www.veritas.com/docs/100048220
- 該当するプラットフォーム: Linux のみ。
- デフォルト値: なし。
- 必要/不要: 必要。
- SERVICE_USER=*name*
- 表 A-2 に戻ります。

START_JOB_DAEMONS

- 説明: このオプションは、ジョブの実行を制御する NetBackup デーモンを開始するかどうかを指定します。
- 該当するプラットフォーム: Linux のみ。
- デフォルト値: yes
- 必要/不要: 不要。
- START_JOB_DAEMONS=yes|no

- 表 A-2 に戻ります。

STOP_NBU_PROCESSES

- 説明: このオプションは、インストール処理でアクティブな NetBackup プロセスが検出された場合、そのプロセスを自動的に停止するかどうかを指定します。インストールまたはアップグレードの前に、実行中の NetBackup ジョブがないことと、すべての NetBackup データベースが停止していることを確認します。有効な入力値は、0 (停止しない) および 1 (停止) です。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: `0`
- 必要/不要: 不要。
- `STOP_NBU_PROCESSES = 0 | 1`
- 表 A-2 に戻ります。

USAGE_INSIGHTS_FILE_PATH

- 説明: このオプションは、Usage Insights のカスタマ登録キーファイルのパスとファイル名を指定します。
- 該当するプラットフォーム: すべて。
- デフォルト値: なし。
- 必要/不要: NetBackup 8.1.2 より前のバージョンからのアップグレードでは、このオプションが必要です。8.1.2 以降からのアップグレードでは、このオプションは必要ありません。
- `USAGE_INSIGHTS_FILE_PATH = path_and_file_name`
- 表 A-2 に戻ります。

VNETD_PORT

- 説明: このオプションは、NetBackup の `vnetd` プロセスが使用するポートを指定します。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: `13724`
- 必要/不要: 不要。
- `VNETD_PORT=port_number`
- 表 A-2 に戻ります。

WEBSVC_DOMAIN

- 説明: このオプションは、Web サーバーをドメイン (Active Directory) アカウントと関連付ける場合に使用します。このフィールドにドメイン名を指定します。Web サーバーをローカルアカウントに関連付ける場合は、このフィールドを空白のままにします。
- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- 必要/不要: 不要。
- WEBSVC_DOMAIN=*domain_name*
- 表 A-2 に戻ります。

WEBSVC_GROUP

- 説明: このオプションは、NetBackup Web サーバーが使用するアカウントのグループ名を指定します。このグループはシステムに存在している必要があります。
- WEBSVC_GROUP 値が応答ファイルに指定され、bp.confファイルに存在する場合、値が一致する必要があります。
- 該当するプラットフォーム: すべて。
- デフォルト値: nbwebgrp
- 必要/不要: 不要 (Linux プライマリサーバーの場合)、必要 (Windows プライマリサーバーの場合)。
- WEBSVC_GROUP=*custom_group_account_name*
- 表 A-2 に戻ります。

WEBSVC_PASSWORD_PLAIN

- 説明: このオプションは、Windows WEBSVC_USER アカウントのパスワードを指定します。websvc のパスワードに特殊文字が含まれている場合 (`(% ^ & < > | ' ` , ; = ( ) ! " ¥ [ ] . * ?`) は、パスワードに適切なエスケープ文字を追加します。たとえば、websvc のパスワードが abc% の場合は、abc%% と入力する必要があります。

  注意: このオプションは、このアカウントのパスワードを平文にします。そのため、セキュリティ上の問題になる可能性があります。

- 該当するプラットフォーム: Windows のみ。
- デフォルト値: なし。
- WEBSVC_PASSWORD_PLAIN=*password*

- 表 A-2 に戻ります。

WEBSVC_USER

- 説明: このオプションは、NetBackup Web サーバーが使用するアカウントのユーザー名を指定します。このユーザーはシステムに存在している必要があります。
  WEBSVC_USER 値が応答ファイルに指定され、bp.confファイルに存在する場合、値が一致する必要があります。
- 該当するプラットフォーム: すべて。
- デフォルト値: nbwebsvc
- 必要/不要: 不要 (Linux プライマリサーバーの場合)、必要 (Windows プライマリサーバーの場合)。
- WEBSVC_USER=*custom_user_account_name*
- 表 A-2 に戻ります。

維持される Java Virtual Machine のオプション

NetBackup 9.0 より前では、NetBackup のアップグレード時に、Web サービス Java Virtual Machine (JVM) のすべての調整値 (メモリの割り当てなど) が上書きされます。NetBackup 9.0 で、Veritasはアップグレードで維持される一連の Web サーバー JVM の調整オプションを定義しました。これらのオプションは、ローカルホストに格納されている実行可能シェルスクリプトで環境変数として定義されています。スクリプトの内容によって、初期設定の JVM の調整オプションが上書きされます。このスクリプトは、NetBackup 9.0 以降の Web サービスが起動されたときにのみ実行されます。デフォルト値を上書きするオプションを構成できます。このスクリプトはいつでも定義できます。値を定義したら、以降のアップグレード時に再定義する必要はありません。

維持される JVM の調整オプションを定義するには、次のようにします。

1 適切な NetBackup 構成ディレクトリに `wmcConfig` スクリプトを作成します。

Windows の場合:
install_path¥Veritas¥NetBackup¥var¥global¥wsl¥config¥wmcConfig.bat

UNIX および Linux の場合:
/usr/openv/var/global/wsl/config/wmcConfig.sh

2 サポートされている変数のリストから目的の変数を含めるように、スクリプトを編集します。各値は個別の行にする必要があります。サポートされる変数は次のとおりです。

```
WMC_HEAP
WMC_METASPACE
WMC_NEW_RATIO
WMC_SURVIVOR_RATIO
WMC_GC_CONFIG
WMC_HEAP_DUMP_CONFIG
```

変数とその適切な範囲について詳しくは、Oracle の JVM マニュアルを参照してください。

3 Web サービスを再起動して、構成の変更を適用します。

RBAC ブートストラップについて

Linux 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時に、RBAC ブートストラップで、ユーザーまたはユーザーグループに、役割ベースのアクセス制御 (RBAC) 権限を割り当てることができます。Linux インストーラで `bpnbaz -AddRBACPrincipal` コマンドを使用して、`/tmp/NBInstallAnswer.conf` ファイルに指定したユーザーまたはユーザーグループに、管理者の役割の権限を付与します。

メモ: RBAC ブートストラップは、以前にユーザーまたはユーザーグループが特定のオブジェクトへのアクセスを制限されていた場合でも、指定したユーザーまたはユーザーグループにすべてのオブジェクトへのアクセスを提供します。たとえば、既存のユーザー Tester1 がデフォルトの VMware 管理者の役割に割り当てられているとします。RBAC ブートストラップに Tester1 を指定すると、Tester1 に管理者の役割が割り当てられます。

インストールまたはアップグレード後に、Windows と Linux の両方のプラットフォームで、`bpnbaz -AddRBACPrincipal` コマンドをスタンドアロンで実行して RBAC 権限を割り当てることができます。このコマンドはプライマリサーバーでのみ利用できます。このコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

Linux プラットフォームにおけるインストール時およびアップグレード時の RBAC ブートストラップ:

インストールパッケージから入手できる応答ファイルテンプレート NBInstallAnswer-primary.template を使用して、/tmp/NBInstallAnswer.conf ファイルを作成します。インストールまたはアップグレードを実行する前に、作成したファイルに次のエントリを追加します。

RBAC_DOMAIN_TYPE = *domain_type*

RBAC_DOMAIN_NAME = *domain_name*

RBAC_PRINCIPAL_TYPE = USER | USERGROUP

RBAC_PRINCIPAL_NAME = *principal_name*

RBAC_DOMAIN_TYPE には、NT, VX, UNIXPWD, LDAP の値を指定できます。

メモ: RBAC_* オプションについて詳しくは、次のページを参照してください。

p.133 の「NetBackup 応答ファイルについて」を参照してください。

すべてのエントリが空または存在しない場合、RBAC ブートストラップは実行されません。この場合、インストールトレースファイルに「Answer file did not contain any RBAC entries」というメッセージが記録されます。インストール処理は常に、RBAC ブートストラップが成功したかどうかにかかわらず続行されます。SEC_CONFIG カテゴリに、監査レコードが作成されます。

RBAC ブートストラップが成功した場合は、次のメッセージが表示されます。

Successfully configured the RBAC permissions for *principal_name*.

ユーザーまたはユーザーグループに管理者の RBAC の役割がすでに割り当てられている場合も、このメッセージが表示されます。

応答ファイルに 1 つ以上の RBAC エントリが存在しても、応答ファイルに必要なエントリが存在しない場合は、次のメッセージが表示されます。

Warning: Unable to configure the RBAC permissions. One or more required fields are missing in /tmp/NBInstallAnswer.conf.

RBAC ブートストラップに他の問題がある場合は、次のメッセージが表示されます。

Warning: Failed to configure the RBAC permissions for *principal_name*. Refer to logs in /usr/openv/netbackup/logs/admin for more information.

RBAC ブートストラップが成功し、監査が失敗した場合は、次のメッセージが表示されます。

Successfully configured the RBAC permissions for *user_or_usergroup_name*.

```
WARNING: Auditing of this operation failed.
Refer to logs in /usr/openv/netbackup/logs/admin for more information.
```

インストールまたはアップグレードの完了後、指定したユーザーまたはユーザーグループに、管理者の役割と対応する RBAC アクセス権が割り当てられます。ユーザーは、API と Web UI にアクセスできるようになります。

NetBackup ソフトウェアの入手について

NetBackup 10.1 は、MyVeritas の Web ページからダウンロード用 ESD イメージとして利用できます。イメージは 1.8G のサイズ制限に従っています。

ESD のダウンロードを正しく行うために、一部の製品イメージがより小さく管理しやすいファイルに分割されています。ファイルを解凍する前に、`1 of 2`、`2 of 2` として識別できる分割されたイメージファイルを最初に結合する必要があります。`MyVeritas` 上の Download Readme.txt ファイルには、ファイルを結合する方法が記述されています。

NetApp クラスタのためのアップグレード前の追加手順

NetBackup のアップグレード後、すべてが問題なく機能するように、NetApp クラスタ構成を確認するという追加手順が必要になる場合があります。表 A-5 に、さまざまな構成と続行方法を示します。

注意: アップグレードの後にモードが Node Scope から Vserver 対応に変わる場合、追加手順が必要になります。追加手順を実行しないと、データリスクの原因になります。

表 A-5 追加で必要な NetApp クラスタの変更

アップグレード時の NetApp クラスタモード	アップグレード後の NetApp クラスタモードへの変更	詳細情報
Node scope mode	変更なし	Veritas と NetApp 社は、早い段階での Vserver 対応モードへの変更を推奨しています。
Node scope mode	Vserver 対応モードへの変更	追加手順が必要です。 p.159 の「Node Scope Mode から Vserver 対応モードに変わるための追加手順」を参照してください。

アップグレード時の NetApp クラスタモード	アップグレード後の NetApp クラスタモードへの変更	詳細情報
Vserver 対応モード	なし	追加手順が必要です。 p.160 の「Vserver 対応モードの NetApp クラスタに必要な追加の変更」を参照してください。

メモ: メディアサーバーが Vserver 対応モードを検出すると、以前のリリースの NetBackup を実行している他のメディアサーバーでは、それ以上のバックアップアクティビティが実行されません。

Node Scope Mode から Vserver 対応モードに変わる場合は、次のことを行う必要があります。

Node Scope Mode から Vserver 対応モードに変わるための追加手順

1. Node Scope Mode を無効にすることにより、クラスタ上の Vserver 対応モードを有効にします。
2. クラスタノードにテープデバイスが接続されている場合、その再設定が必要です。デバイス構成用 NDMP ホストとしてクラスタ管理論理インターフェース (LIF) を使用するようにテープデバイスを設定します。NetBackup は、デバイス構成用にノード名の使用をサポートしません。

   詳しくは、『NetBackup for NDMP 管理者ガイド』を参照してください。
3. バックアップで使用するすべての LIF に信用証明を付与します。

   このアクティビティには、バックアップポリシー用に使われる Vserver データ LIF に加えてクラスタ管理 LIF も含まれます。

   詳しくは、『NetBackup for NDMP 管理者ガイド』を参照してください。
4. 環境内のすべての既存 NDMP ホストに対してデータベースを更新します。次のコマンドを使って、データベースを更新します。

   ```
   tpautoconf -verify NDMP_host_name
   ```
5. クラスタ LIF を使うのにクラスタのノード名を使用するストレージユニットを更新するか、置換します。
6. クラスタをバックアップする既存のポリシーを更新するか、置換します。

   クライアント名としてデータ LIF かクラスタ管理 LIF のいずれかを使用する必要があります。NetBackup はクライアント名としてノード名の使用をサポートしません。バックアップ選択項目も修正の必要がある場合があります。

7 クラスタ管理 LIF をホストしない各ノードに対してクラスタ間管理 LIF を追加します。

NetApp クラスタでは、NDMP 3-Way バックアップまたは NDMP リモートバックアップの実行にこのアクティビティが必要です。この LIF がない場合は、クラスタ管理 LIF と同じノードでホストされていないボリュームからのすべての 3-Way バックアップまたはリモートバックアップが失敗します。

8 古いイメージをリストア、検証、複製するには、代替読み取りホストを使用することが必要になる場合があります。

Vserver 対応モードの NetApp クラスタに必要な追加の変更

1 各 Vserver で `tpautoconf` コマンドを実行します。このコマンドは Vserver に対するクレデンシャルを備えているメディアサーバーから実行する必要があります。

```
tpautoconf -verify ndmp_host
```

コマンドが正常に実行されれば、次のような `nbemmcmd` 出力が表示されます。

```
servername1@/>nbemmcmd -listsettings -machinename machinename123
 -
machinetype ndmp
NBEMMCMD, Version: 7.7
The following configuration settings were found:
NAS_OS_VERSION="NetApp Release 8.2P3 Cluster-Mode"
NAS_CDOT_BACKUP="1"
Command completed successfully.

NAS_OS_VERSION displays the NetApp Version.
NAS_CDOT_BACKUP tells us if NetBackup uses the new cDOT
capabilities.
```

新しい Vserver が追加される場合、`tpautoconf -verify ndmp_host` コマンドは必須ではありません。

2 必要に応じて NDMP クラスタにデバイスを追加し、クラスタ管理 LIF を使ってアクセスします。デバイスを追加する場合は、そのデバイスを検出する必要があります。

3 新しく検出されたデバイスに対してストレージユニットを追加します。

4 クラスタをバックアップする既存のポリシーを更新します。

クライアント名としてデータ LIF かクラスタ管理 LIF のいずれかを使用する必要があります。NetBackup はクライアント名としてノード名の使用をサポートしません。バックアップ選択項目も修正の必要がある場合があります。

Replication Director を使用した NetApp ディスクアレイの使用

Replication Director は、2 つの異なる状況で NetApp ディスクアレイのスナップショットをレプリケートできます。

- 非クラスタモード: 7-Mode は、NAS および SAN におけるスナップショットのレプリケートに使われています。プラグインは、OCUM (OnCommand Unified Manager) サーバー (図 A-1) にインストールする必要があります。
- クラスタモード: clustered Data ONTAP (cDOT) は、ストレージの仮想マシン間 (SVM または vServer) におけるスナップショットのレプリケートに使います。サポート対象は、NAS のみです。
  プラグインは、OCUM サーバー、プライマリサーバー、またはあらゆるメディアサーバー (図 A-2) 以外の Windows コンピュータまたは Linux コンピュータにインストールする必要があります。

モードは両方とも同じトポロジーをサポートします。

表 A-6 では、NetBackup バージョンと NetApp プラグインの間の関連について説明します。

表 A-6 バージョンの互換性

NetBackup のバージョン	NetApp プラグイン バージョン	説明	OCUM サーバーに対するプライマリサーバーの比	サポート対象のポリシー形式
7.7 以降	1.1	7-Mode のサポートがすべての NetBackup Replication Director 機能に提供されます。	1 つのプライマリサーバーが多数の OCUM サーバーをサポートします。 プラグインは、OCUM (OnCommand Unified Manager) サーバーにインストールする必要があります。	MS-Windows、標準、NDMP、VMware、Oracle
	1.1 P1	7-Mode のサポートがすべての NetBackup Replication Director 機能に提供されます。	1 つのプライマリサーバーが多数の OCUM サーバーをサポートします。	MS-Windows、標準、NDMP、VMware、Oracle
	2.0	cDOT サポートを提供します。	1 つのプライマリサーバーが多数の OCUM サーバーをサポートします。 プラグインは、OCUM サーバー、プライマリサーバー、またはあらゆるメディアサーバー以外の Windows コンピュータまたは Linux コンピュータにインストールする必要があります。	MS-Windows、標準、NDMP、VMware、Oracle

メモ: プラグインをアップグレードする前に NetBackup 環境全体をアップグレードする必要があります。すべてのプライマリサーバー、メディアサーバー、クライアント、プラグインと通信するホストをアップグレードします。

図 **A-1** NetBackup と NBUPlugin for 7-Mode 間の通信

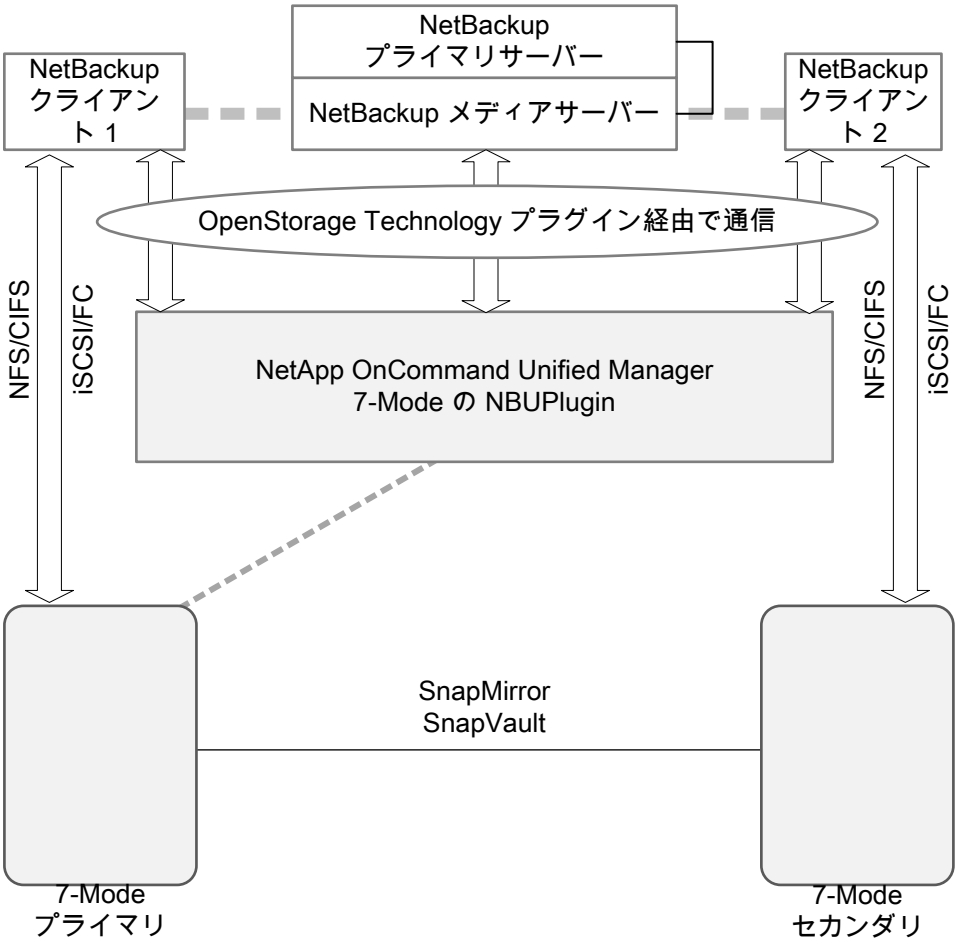
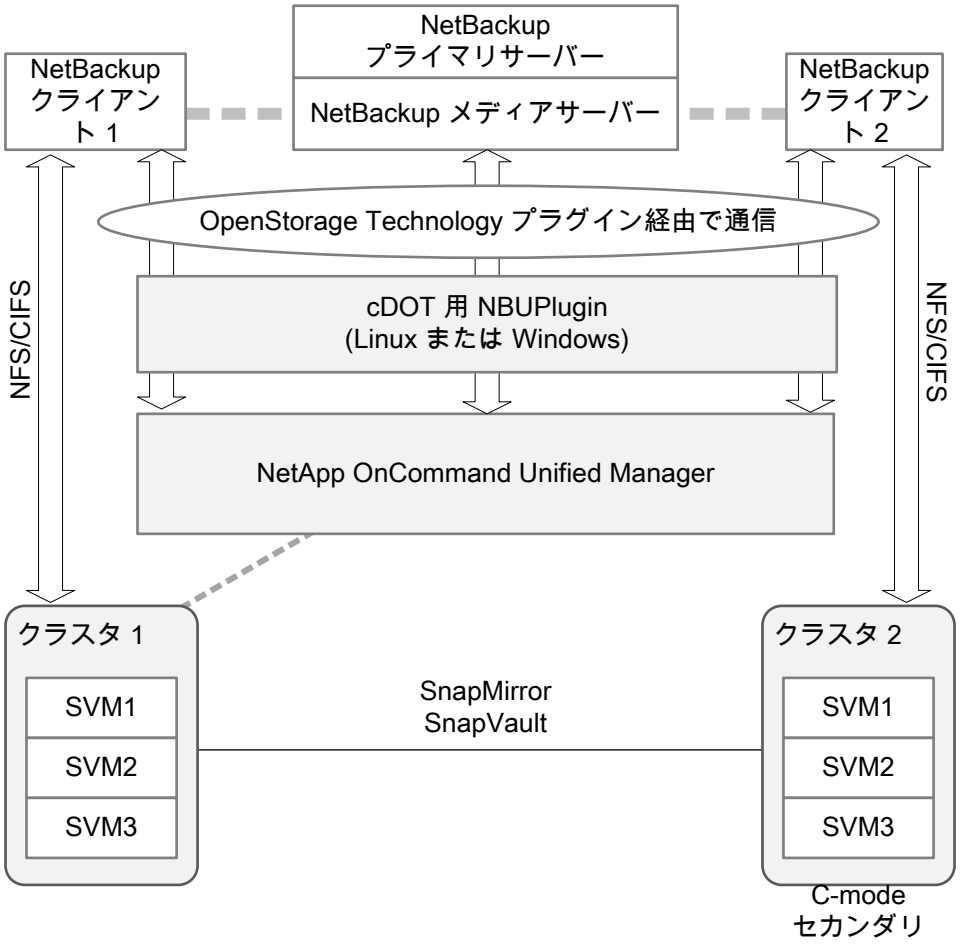


図 **A-2** NetBackup と NBUPlugin for clustered Data ONTAP 間の通信



プラグインのバージョンの判断

NBUPlugin のバージョンを判断するには、NBUPlugin がインストールされているシステムで次のバージョンファイルを検索します。

Windows の場合: *Install_path*¥Program Files¥Netapp¥NBUPlugin¥version.txt

UNIX の場合: /usr/NetApp/NBUPlugin/version.txt

ファイルの内容には、製品名、ビルドの日付、NBUPlugin のバージョンが記載されています。複数のプラグインがインストールされている場合は、両方のリストに表示されます。

プラグインのアップグレード

NetApp Plug-in for Veritas NetBackup をアップグレードするには、古いプラグインを使用するすべてのストレージライフサイクルポリシージョブがアップグレード前に完了していることを確認してください。

ストレージライフサイクルポリシーに関連付けられたすべてのジョブの完了、処理中、または未開始を判断するには、次のコマンドを使用します。

Windows の場合: *install_path*¥NetBackup¥bin¥admincmd>nbstlutil.exe stlilist -U

UNIX の場合: /usr/openv/netbackup/bin/admincmd/nbstlutil stlilist -U

NetBackup のバージョン間の互換性について

プライマリサーバー、メディアサーバー、およびクライアントの間で、バージョンが異なる NetBackup を実行できます。この旧バージョンのサポートによって、NetBackup サーバーを 1 つずつアップグレードして、全体的なシステムパフォーマンスに与える影響を最小限に抑えることができます。

Veritas ではサーバーとクライアントの特定の組み合わせのみがサポートされています。バージョンが混在する環境では、特定のコンピュータが最新のバージョンである必要があります。具体的には、バージョンの順序をプライマリサーバー、メディアサーバー、クライアントのようにします。たとえば、10.0 プライマリサーバー > 9.0 メディアサーバー > 8.3.0.1 クライアントというシナリオがサポートされます。

NetBackup バージョンはすべて 4 桁の長さです。NetBackup 10.0 リリースは 10.0.0.0 リリースです。同様に、NetBackup 9.1 リリースは NetBackup 9.1.0.0 リリースです。サポート目的では、4 番目の数字は無視されます。9.1 プライマリサーバーは 9.1.0.1 メディアサーバーをサポートします。サポートされない例は、9.1 プライマリサーバーと 10.0 メディアサーバーの組み合わせです。

NetBackup カタログはプライマリサーバー上に存在します。したがって、プライマリサーバーはカタログバックアップのクライアントであると見なされます。NetBackup 構成にメディアサーバーが含まれている場合は、プライマリサーバーと同じ NetBackup バージョンを使ってカタログバックアップを実行する必要があります。

NetBackup バージョン間の互換性について詳しくは、Veritas SORT Web サイトを参照してください。

Veritas は EOSL 情報をオンラインで確認することをお勧めします。

UNIX および Linux の場合のアップグレード要件

表 A-7は NetBackup のアップグレードのために UNIX と Linux システムを準備するための要件を記述します。各項目に対応するためにチェックリストとしてこの表を使ってください。

インストールの必要条件に関する最新情報について詳しくは Veritas SORT Web サイトを参照してください。SORT に関する詳しい情報を参照できます。

p.26 の「Veritas Services and Operations Readiness Tools について」を参照してください。

表 A-7 UNIX および Linux の場合の NetBackup の要件

チェック	要件	詳細
	オペレーティングシステム	■ UNIX と Linux の互換性のあるオペレーティングシステムの完全なリストについては、次の Web サイトで『Software Compatbility List（SCL）』を参照してください。 http://www.netbackup.com/compatibility https://sort.veritas.com/netbackup
	メモリ	サーバーのサイズを正しく設定するには、次に示す情報を使用します。 ■ SORT の Web サイト。p.26 の「Veritas Services and Operations Readiness Tools について」を参照してください。 ■ NetBackup 環境のサイズを設定する方法に関する一般的な詳細。p.184 の「NetBackup プライマリサーバーとドメインのサイズについてのガイダンス」を参照してください。 ■ NetBackup 環境の計画とチューニングについての詳しい情報を参照できます。詳しくは『NetBackup バックアップ計画とパフォーマンスチューニングガイド』を参照してください。
	ディスク容量	■ 必要となる正確な空き領域はハードウェアプラットフォームによって決まります。このトピックに関する詳細情報を参照できます。 NetBackup リリースノート 10.1 ■ NetBackup カタログには、バックアップについての情報が含まれているため、製品の使用に伴ってサイズが大きくなります。カタログに必要なディスク領域は、主に、次のバックアップ構成によって異なります。 ■ バックアップ対象のファイル数。 ■ バックアップの間隔。 ■ バックアップデータの保持期間。 空き容量など、領域に問題がある場合は、NetBackup を代替のファイルシステムにインストールできます。インストールの際に、代替のインストール場所を選択して、/usr/openv からの適切なリンクを作成できます。 **メモ:** ディスク領域の値は初回インストール用です。NetBackup カタログはプライマリサーバーが本番環境になっているときにかなり多くの領域を必要とします。

チェック	要件	詳細
	一般要件	■ gzip および gunzip コマンドがローカルシステムにインストールされていることを確認してください。これらのコマンドがインストールされているディレクトリは、ルートユーザーの PATH 環境変数設定に含まれている必要があります。 ■ すべてのサーバーに対する、すべての NetBackup インストール ESD イメージ、有効なライセンス、およびルートユーザーのパスワード。 ■ サポートされているハードウェアでサポートされているバージョンのオペレーティングシステム (パッチを適用済みであること) を稼働しているサーバー、十分なディスク領域、およびサポートされている周辺装置。これらの要件について詳しくは、『NetBackup リリースノート 10.1』を参照してください。 ■ すべての NetBackup サーバーがクライアントシステムを認識し、またクライアントシステムから認識されている必要があります。一部の環境では、それぞれの /etc/hosts ファイルに対して、もう一方の定義を行う必要があります。また、他の環境の場合は、ネットワーク情報サービス (NIS) またはドメインネームサービス (DNS) を使用することになります。 ■ 画面解像度には 1024 x 768、256 色以上が必要です。
	クラスタシステム	■ NetBackup クラスタ内の各ノードで ssh コマンドまたは同等のコマンドを実行できることを確認します。ルートユーザーとして、パスワードを入力せずにクラスタ内の各ノードにリモートログオンできる必要があります。このリモートログオンは、NetBackup サーバー、NetBackup エージェントおよび別ライセンス製品のインストールと構成を行うときに必要です。インストールおよび構成を完了した後は不要になります。 ■ NetBackup をインストールする前に、クラスタフレームワークをインストールして構成し、起動しておく必要があります。 ■ DNS、NIS、/etc/hosts ファイルを使って、仮想名を定義しておく必要があります。IP アドレスも同時に定義します。(仮想名は IP アドレスのラベルです。) ■ アクティブノードからアップグレードを開始し、それから非アクティブノードをアップグレードします。 クラスタ要件に関する詳細情報を参照できます。 『NetBackup マスターサーバーのクラスタ化管理者ガイド』
	NFS の互換性	Veritas NFS マウントされたディレクトリへの NetBackup のインストールはサポートされていません。NFS マウントしたファイルシステムのファイルロックは確実でない場合があります。
	カーネルの再構成	一部の周辺機器およびプラットフォームでは、カーネルの再構成が必要です。 詳しくは、『NetBackup デバイス構成ガイド』を参照してください。
	Linux	NetBackup をインストールする前に、次に示すシステムライブラリが存在することを確認します。いずれかのライブラリが存在しない場合は、オペレーティングシステムよって指定されるシステムライブラリをインストールします。 ■ libnsl.so.1 ■ libXtst
	Red Hat Linux	Red Hat Linux の場合、サーバー用のネットワーク構成にする必要があります。

チェック	要件	詳細
	他のバックアップソフトウェア	Veritasこの製品をインストールする前に、現在システムに構成されている他のベンダーのバックアップソフトウェアをすべて削除することをお勧めします。他のベンダーのバックアップソフトウェアによって、NetBackupのインストールおよび機能に悪影響が及ぼされる場合があります。
	Web サービス	NetBackup 8.0 より、NetBackup プライマリサーバーには、重要なバックアップ操作をサポートするための構成済み Tomcat Web サーバーが含まれます。この Web サーバーは、権限が制限されているユーザーアカウント要素の下で動作します。これらのユーザーアカウント要素は、各プライマリサーバー (またはクラスタ化されたプライマリサーバーの各ノード) で使用できる必要があります。これらの必須アカウント要素は、インストールの前に作成しておく必要があります。詳しくは以下を参照してください。 p.126 の「NetBackup プライマリサーバー Web サーバーのユーザーとグループの作成」を参照してください。 **メモ:** ベリタスは、NetBackup Web サービスに使用するユーザーアカウントの詳細を保存することを推奨します。プライマリサーバーのリカバリでは、NetBackup カタログのバックアップが作成されたときに使われたものと同じ NetBackup Web サービスのユーザーアカウントとクレデンシャルが必要です。 **メモ:** セキュアモードで NetBackup PBX を実行する場合は、Web サービスユーザーを PBX の権限を持つユーザーとして追加します。PBX モードの判別と、正しくユーザーを追加する方法について詳しくは、次をご覧ください。 http://www.veritas.com/docs/000115774 デフォルトでは、UNIX インストールスクリプトは、Web サーバーをユーザーアカウント `nbwebsvc` およびグループアカウント `nbwebgrp` に関連付けようとします。これらのデフォルト値は、NetBackup インストール応答ファイルに上書きできます。UNIX のインストールスクリプトを開始する前に、ターゲットホストに NetBackup インストール応答ファイルを設定する必要があります。NetBackup インストール応答ファイルにカスタム Web サーバーアカウント名を次に示すように設定します。 **1** ルートユーザーとしてサーバーにログインします。 **2** 任意のテキストエディタでファイル /tmp/NBInstallAnswer.conf を開きます。ファイルが存在しない場合はファイルを作成します。 **3** 次に示す行を追加して、デフォルトの Web サーバーユーザーアカウント名を上書きします。 `WEBSVC_USER=`*`custom_user_account_name`* **4** 次に示す行を追加して、デフォルトの Web サーバーグループアカウント名を上書きします。 `WEBSVC_GROUP=`*`custom_group_account_name`* **5** ファイルを保存して閉じます。

チェック	要件	詳細
	Veritas Usage Insights のカスタマ登録キー	NetBackup 8.1.2 以降、Veritas Usage Insights のカスタマ登録キーを指定する必要があります。Veritas Usage Insights に関する詳しい情報を参照できます。 p.13 の「Veritas Usage Insights について」を参照してください。 NetBackup 8.1.2 へのインストールとアップグレード中は、インストーラが `veritas_customer_registration_key.json` ファイルを最終的なインストール先にコピーするのを許可してください。NetBackup はこの処理を介してファイルの権限と所有権を正しく設定できます。インストールまたはアップグレード以外の処理でこのファイルをシステムに配置すると、処理は正しく動作しない可能性があります。 **メモ:** NetBackup では、カスタマ登録キーのファイル名に短いファイル名形式 (8.3 形式) を使用することはサポートされていません。

Windows および Windows クラスタのアップグレード要件

「表 A-8」に、NetBackup のインストールのために Windows システムを準備するための要件が記述されています。各項目に対応するためにチェックリストとしてこの表を使ってください。

インストールの必要条件に関する最新情報について詳しくは Veritas SORT Web サイトを参照してください。SORT に関する詳しい情報を参照できます。

p.26 の「Veritas Services and Operations Readiness Tools について」を参照してください。

注意: ベリタスでは、インストールまたはアップグレードの後、`nbdb_move` コマンドを使って Windows クラスタ上のデフォルト以外の場所に NetBackup カタログを移動することがサポートされます。ただし、アップグレードを成功させるためには、アップグレードの前に NetBackup カタログをデフォルトの場所に戻す必要があります。カタログがデフォルトの場所にない場合、NetBackup のアップグレードは行わないでください。アップグレードの前にデータベースをデフォルトの場所に移動しなかった場合、プライマリサーバーが使用できなくなります。nbdb_move についての詳しい情報を参照できます。

『NetBackup コマンドリファレンスガイド』

表 A-8 Windows および Windows クラスタでの NetBackup 要件

チェック	要件	詳細
	オペレーティングシステム	■ セキュリティ更新プログラムを含む、最新のオペレーティングシステムパッチと更新プログラムを適用したことを確認します。オペレーティングシステムが最新のものかどうか不明な場合は、ご購入先にお問い合わせのうえ、最新のパッチおよび更新版を入手してください。 ■ Windows の互換性のあるオペレーティングシステムの完全なリストについては、次の Web サイトで『Software Compatibility List (SCL)』を参照してください。 http://www.netbackup.com/compatibility
	メモリ	サーバーのサイズを正しく設定するには、次に示す情報を使用します。 ■ SORT の Web サイト。p.26 の「Veritas Services and Operations Readiness Tools について」を参照してください。 ■ NetBackup 環境のサイズを設定する方法に関する一般的な詳細。p.184 の「NetBackup プライマリサーバーとドメインのサイズについてのガイダンス」を参照してください。 ■ NetBackup 環境の計画とチューニングについての詳しい情報を参照できます。詳しくは『NetBackup バックアップ計画とパフォーマンスチューニングガイド』を参照してください。
	ディスク容量	■ NTFS パーティション。 ■ サーバーソフトウェアおよび NetBackup カタログに対応するために必要となる正確な空き領域は、ハードウェアプラットフォームによって決まります。このトピックに関する詳細情報を参照できます。 NetBackup リリースノート 10.1 ■ アップグレードでは、NetBackup が代替の場所にインストールされている場合でも、プライマリドライブに追加の領域が必要になります。プライマリドライブは、Windows がインストールされているドライブです。 ■ サーバーをアップグレードする場合、NetBackup を代替ドライブの場所にインストールするときに、Veritasでは、プライマリ Windows ドライブに 2.8 GB の空き容量を用意するように求めます。 ■ クライアントをアップグレードする場合、NetBackup を代替ドライブの場所にインストールするときに、Veritasでは、プライマリ Windows ドライブに 1.7 GB の空き容量を用意するように求めます。 ■ NetBackup カタログには、バックアップについての情報が含まれているため、製品の使用に伴ってサイズが大きくなります。カタログに必要なディスク領域は、主に、次のバックアップ構成によって異なります。 ■ バックアップ対象のファイル数。 ■ バックアップの間隔。 ■ バックアップデータの保持期間。 ■ Veritas ディスクストレージユニットボリュームまたはファイルシステムで 5% 以上の利用可能なディスク容量を確保することを推奨します。 **メモ:** ディスク領域の値は初回インストール用です。NetBackup カタログはプライマリサーバーが本番環境になっているときにかなり多くの領域を必要とします。

チェック	要件	詳細
	一般要件	以下の項目すべてがあることを確認します。 ■ NetBackup インストール ESD イメージ ■ 適切なライセンスキー ■ すべてのサーバーの管理者アカウントとパスワード ■ 画面解像度は 1024 x 768、256 色以上に設定してください。 **メモ:** Windows 2012 R2、UAC が有効な Windows 2012、Windows Server 2016、Windows 2019、および Windows 2022 環境で NetBackup をインストールするには、正規の管理者としてログオンする必要があります。管理者グループに割り当て済みであり、正規の管理者ではないユーザーは、UAC が有効な環境で NetBackup をインストールできません。管理者グループのユーザーが NetBackup をインストールできるようにするには、UAC を無効化します。

チェック	要件	詳細
	リモートインストールおよびクラスタインストール	

チェック	要件	詳細
		リモートインストールおよびクラスタインストールには、前述のすべてのインストール要件に加えて、次のガイドラインが適用されます。 ■ クラスタ内のすべてのノードで、同じバージョンのオペレーティングシステム、Service Pack および NetBackup を実行している必要があります。サーバーのオペレーティングシステムに異なるバージョンを混在させることはできません。 ■ インストールのアカウントには、すべてのリモートシステムまたはクラスタ内のすべてのノードの管理者権限が必要です。 ■ インストール元のシステム (またはプライマリノード) では、Windows 2012/2012 R2/Windows 2016 のいずれかを実行している必要があります。 ■ インストール先のコンピュータ (またはクラスタノード) に Windows 2012/2012 R2/Windows 2016 のいずれかがインストールされている必要があります。 ■ Remote Registry サービスはリモートシステムで開始する必要があります。 NetBackup のインストーラはリモートシステムの Remote Registry サービスを有効にし、開始できます。Remote Registry サービスが開始されない場合、インストールは次のエラーメッセージを受信します。 `Attempting to connect to server server_name failed with the following error: Unable to connect to the remote system. One possible cause for this is the absence of the Remote Registry service. Please ensure this service is started on the remote host and try again.` ■ NetBackup の仮想名と IP アドレス NetBackup で利用可能な仮想名および IP アドレスを用意します。インストール中に、この情報を入力する必要があります。 ■ メディアサーバーのクラスタのサポートの変更 クラスタ化されたメディアサーバーの新しいインストールを実行することはできません。 ■ Windows Server Failover Clustering (WSFC) ■ NetBackup グループによって使用される共有ディスクがクラスタ内で構成され、アクティブノードでオンラインになっている必要があります。 ■ NetBackup を共有ディスクが存在するノード (アクティブノード) からインストールします。 ■ コンピュータ名またはホスト名は 15 文字より長い名前には設定できません。 ■ Cluster Server (VCS) のクラスタ: NetBackup をインストールする前に、すべての NetBackup ディスクリソースを、Veritas Enterprise Administrator (VEA) で構成しておく必要があります。 ■ クラスタノードのデバイス構成とアップグレード クラスタをアップグレードする場合、`ltid` およびロボットデーモンは、特定のクラスタノードのデバイス構成を EMM データベースから取得します。EMM データベースでのデバイス構成の格納または取得は、クラスタノード名 (`gethostname` を使用して表示) によって行われます。クラスタノード名は、デバイス構成の更新時 (`ltid` によるドライブ状態の更新時など) に使われます。クラスタノード名は、デバイスの接続先を示す場合にのみ使用されます。NetBackup の仮想名は、ロボット制御ホストなど、他の目的にも使用されます。 クラスタ要件に関する詳細情報を参照できます。

チェック	要件	詳細
		『NetBackup マスターサーバーのクラスタ化管理者ガイド』
	リモート管理コンソールのホスト名	プライマリサーバーのインストール中に、リモート管理コンソールホストの名前を入力する必要があります。
	NetBackup 通信	ネットワークがすべてのサーバーおよびクライアントから認識され、相互に通信できるように構成されていることを確認します。 通常は、ping コマンドを実行してサーバーからクライアントにアクセスできるように設定されていれば、NetBackup でも正しく動作します。 ■ NetBackup サービスおよびポート番号は、ネットワーク全体で同じである必要があります。 ■ Veritas はデフォルトのポート設定を NetBackup サービスとインターネットサービスのポートに使うことを推奨します。ポート番号を変更する場合は、すべてのプライマリサーバー、メディアサーバーおよびクライアントに対して同じ値を設定する必要があります。ポートエントリは、次のファイルに格納されています。 `%SYSTEMROOT%¥system32¥drivers¥etc¥services`。デフォルト設定を変更するには、NetBackup のカスタムインストールを行うか、`services` ファイルを手動で編集する必要があります。
	CIFS マウントされたファイルシステム	Veritas CIFS マウントされたディレクトリへの NetBackup のインストールはサポートされていません。CIFS マウントしたファイルシステムのファイルロックは確実でない場合があります。
	ストレージデバイス	ロボットおよびスタンドアロンテープドライブなどのデバイスが製造元の指示どおりに取り付けられ、Windows ソフトウェアから認識されている必要があります。
	サーバー名	サーバー名の入力を求められたら、適切なホスト名を常に入力してください。IP アドレスを入力しないでください。
	バージョンの混在	使用を計画しているクライアントの最新バージョンと同じかそれ以上のリリースレベルの NetBackup サーバーをインストールしてください。サーバーソフトウェアのバージョンが古い場合、新しいバージョンのクライアントソフトウェアとともに使用すると、問題が発生する可能性があります。 p.165 の「NetBackup のバージョン間の互換性について」を参照してください。
	Windows 2012/2012 R2 Server Core/Windows 2016 でのインストール	NetBackup はこれらのコンピュータにサイレントインストール方式でのみインストールできます。 p.54 の「Windows システムでのサイレントアップグレードの実行」を参照してください。
	他のバックアップソフトウェア	現在システムに構成されている他のベンダーのバックアップソフトウェアをすべて削除します。他のベンダーのバックアップソフトウェアによって、NetBackup のインストールおよび機能に悪影響が及ぼされる場合があります。

チェック	要件	詳細
	Web サービス	NetBackup 8.0 より、NetBackup プライマリサーバーには、重要なバックアップ操作をサポートするための構成済み Tomcat Web サーバーが含まれます。この Web サーバーは、権限が制限されているユーザーアカウント要素の下で動作します。これらのユーザーアカウント要素は、各プライマリサーバー (またはクラスタ化されたプライマリサーバーの各ノード) で使用できる必要があります。詳しくは以下を参照してください。 p.126 の「NetBackup プライマリサーバー Web サーバーのユーザーとグループの作成」を参照してください。 **メモ:** ベリタスは、NetBackup Web サービスに使用するユーザーアカウントの詳細を保存することを推奨します。プライマリサーバーのリカバリでは、NetBackup カタログのバックアップが作成されたときに使われたものと同じ NetBackup Web サービスのユーザーアカウントとクレデンシャルが必要です。 **メモ:** セキュアモードで NetBackup PBX を実行する場合は、Web サービスユーザーを PBX の権限を持つユーザーとして追加します。PBX モードの判別と、正しくユーザーを追加する方法について詳しくは、次をご覧ください。 http://www.veritas.com/docs/000115774
	CA 証明書の指紋	(該当する場合) メディアサーバーとクライアントのみの場合: NetBackup 認証局 (CA) を使用する場合、インストール時にプライマリサーバーの CA 証明書の指紋を把握している必要があります。この要件は、NetBackup 認証局を使用する場合にのみ適用されます。CA 証明書の指紋と、セキュリティ証明書の生成時のこの指紋の役割について詳しくは、次を参照してください。 https://www.veritas.com/support/en_US/article.000127129
	認証トークン	(該当する場合) メディアサーバーとクライアントのみの場合: 場合によっては、セキュリティ証明書を正常に配備するために、インストーラの実行時に認証トークンが必要です。認証トークンと、セキュリティ証明書の生成時のこのトークンの役割について詳しくは、次を参照してください。 NetBackup 認証局 (CA) を使用すると、場合によっては、セキュリティ証明書を正常に配備するために、インストーラの実行時に認証トークンが必要になります。認証トークンと、セキュリティ証明書の生成時のこのトークンの役割について詳しくは、次を参照してください。 https://www.veritas.com/support/en_US/article.000127129
	外部認証局	プライマリサーバー (クラスタを含む) の場合: 外部認証局の構成は、インストール後のアクティビティです。 メディアサーバーおよびクライアントの場合: インストール処理中、またはインストールの完了後に ECA を構成できます。インストール後の構成について詳しくは、次の記事を参照してください。 https://www.veritas.com/support/en_US/article.100044300

チェック	要件	詳細
	Veritas Usage Insights のカスタマ登録キー	NetBackup 8.1.2 以降、Veritas Usage Insights のカスタマ登録キーを指定する必要があります。Veritas Usage Insights に関する詳しい情報を参照できます。 p.13 の「Veritas Usage Insights について」を参照してください。 NetBackup 8.1.2 へのインストールとアップグレード中は、インストーラが `veritas_customer_registration_key.json` ファイルを最終的なインストール先にコピーするのを許可してください。NetBackup はこの処理を介してファイルの権限と所有権を正しく設定できます。インストールまたはアップグレード以外の処理でこのファイルをシステムに配置すると、処理は正しく動作しない可能性があります。 **メモ:** NetBackup では、カスタマ登録キーのファイル名に短いファイル名形式 (8.3 形式) を使用することはサポートされていません。

p.166 の「UNIX および Linux の場合のアップグレード要件」を参照してください。

Windows クラスタのアップグレードの要件

通常のサーバー要件に加えて、NetBackup のクラスタアップグレードは特別な配慮を必要とします。

次に、Windows システムで NetBackup のクラスタアップグレードを行う場合のガイドラインについて説明します。

表 A-9　インストールとアップグレードに関する Windows クラスタの要件

項目	要件
サーバーのオペレーティングシステム	セキュリティ更新プログラムを含む、最新のオペレーティングシステムパッチと更新プログラムを適用したことを確認します。オペレーティングシステムが最新のものかどうか不明な場合は、ご購入先にお問い合わせのうえ、最新のパッチおよび更新版を入手してください。 互換性のあるオペレーティングシステムの完全なリストについては、次の Web サイトで『Software Compatibility List (SCL)』を参照してください。 ■ http://www.netbackup.com/compatibility ■ https://sort.veritas.com/netbackup
権限	クラスタインストールを実行するには、クラスタ内のすべてのリモートノードの管理者権限を持っている必要があります。Veritas クラスタ内のすべてのノードと各ノードの既存のソフトウェアを記録しておくことをお勧めします。

項目	要件
NetBackup の仮想名と IP アドレス	NetBackup で利用可能な仮想名および IP アドレスを用意します。インストール中に、この情報を入力する必要があります。
ノードのオペレーティングシステム	すべてのクラスタノードで、同じバージョンのオペレーティングシステム、同じ Service Pack レベル、および同じバージョンの NetBackup を使用する必要があります。クラスタ環境では、異なるバージョンのサーバーは実行できません。
メディアサーバーのクラスタのサポートの変更	クラスタ化されたメディアサーバーはサポートされません。
Windows Server Failover Clustering (WSFC)	セキュリティ更新プログラムを含む、最新のオペレーティングシステムパッチと更新プログラムを適用したことを確認します。オペレーティングシステムが最新のものかどうか不明な場合は、ご購入先にお問い合わせのうえ、最新のパッチおよび更新版を入手してください。 互換性のあるオペレーティングシステムの完全なリストについては、次の Web サイトで『Software Compatibility List (SCL)』を参照してください。 ■ http://www.netbackup.com/compatibility ■ https://sort.veritas.com/netbackup
Cluster Server (VCS) のクラスタ	■ NetBackup をインストールする前に、すべての Veritas ディスクリソースを、NetBackup Enterprise Administrator (VEA) で構成しておく必要があります。 ■ インストールまたはアップグレードを開始する前に、VCS NetBackup リソースをオフラインにする必要があります。 **メモ:** アクティブノードのインストールまたはアップグレード時に共有ディスクと IP リソースがオンラインであることを確認してください。
クラスタノードのデバイス構成とアップグレード	クラスタをアップグレードする場合、`ltid` およびロボットデーモンは、特定のクラスタノードのデバイス構成を EMM データベースから取得します。EMM データベースでのデバイス構成の格納または取得は、クラスタノード名 (`gethostname` を使用して表示) によって行われます。クラスタノード名は、デバイス構成の更新時 (`ltid` によるドライブ状態の更新時など) に使われます。クラスタノード名は、デバイスの接続先を示す場合にのみ使用されます。NetBackup の仮想名は、ロボット制御ホストなど、他の目的にも使用されます。

新しいメディアサーバーに全データを移行してクラスタ化されたメディアサーバーを削除する

NetBackup 環境からクラスタ化されたメディアサーバーを削除できます。すべてのデータをクラスタから新しいスタンドアロンサーバーに移行してから古いクラスタサーバーを廃止する必要があります。

すべての NetBackup リソースを移行してメディアサーバーを廃止するために必要な手順については、で詳しく説明しています。http://www.veritas.com/docs/DOC5332『NetBackup 管理者ガイド Vol. 1』で「メディアサーバーの廃止方法について」を参照してください。http://www.veritas.com/docs/DOC5332

Amazon クラウドストレージサーバーのアップグレード後の手順

NetBackup 8.1 から、Amazon (S3) と Amazon GovCloud ストレージサーバーのオブジェクトのサイズが変更されています。この変更は、これらのクラウドストレージサーバーの読み取りおよび書き込みバッファサイズの有効範囲に影響します。プライマリサーバーで NetBackup 管理コンソールを使用して、NetBackup 8.1 より前のサーバーの読み取りおよび書き込みバッファサイズの値を更新する必要があります。メディアサーバーに関連付けられている各クラウドストレージサーバーのこれらの設定を更新します。

有効範囲については、『NetBackup クラウド管理者ガイド』の `READ_BUFFER_SIZE` と `WRITE_BUFFER_SIZE` の情報を参照してください。

NetBackup 管理者コンソールの Amazon (S3) および Amazon GovCloud の読み取りおよび書き込みバッファサイズを更新するには

1. NetBackup 管理コンソールを開きます。
2. [メディアおよびデバイスマネージャ (Media and Device Manager)]、[クレデンシャル (Credentials)]、[ストレージサーバー (Storage Server)]の順に移動します。
3. Amazon (S3) および Amazon GovCloud ストレージサーバーの場合。
   - 右側のペインでストレージサーバーをダブルクリックして[ストレージサーバーの変更 (Change Storage Server)]ダイアログボックスを開きます。
   - [ストレージサーバーの変更 (Change Storage Server)]ダイアログボックスで、[プロパティ (Properties)]タブをクリックします。
   - 表示されるパラメータの値を更新します。これらの値はバイト単位で入力します。

```
READ_BUFFER_SIZE
WRITE_BUFFER_SIZE
```

4 ［保存 (Save)］をクリックします。

コマンドラインから次のコマンドを使用して読み取りおよび書き込みバッファサイズを更新します。

1 `nbdevconfig -getconfig -stype storage_server_type -storage_server storage_server_name -configlist filename`

2 表示されるパラメータの値を更新します。これらの値はバイト単位で入力します。

```
READ_BUFFER_SIZE
WRITE_BUFFER_SIZE
```

3 `nbdevconfig -setconfig -stype storage_server_type -storage_server storage_server_name -configlist filename`

サーバーのアップグレード後のクライアントのアップグレード

update_clients インストールスクリプトによって、クライアントにクライアントソフトウェアのプッシュインストールを実行できます。NetBackup メディアサーバーまたはプライマリサーバーであるリモートクライアントには、クライアントソフトウェアのプッシュインストールは実行できません。これは、1 つのホスト上のサーバーソフトウェアおよびクライアントバイナリが同じバージョンである必要があるためです。

メモ: インストールスクリプト update_clients を使用して NetBackup 8.2 以降のクライアントをプッシュできないことに注意してください。VxUpdate を使用する必要があります。

---

update_clients インストールスクリプトを使用すると、サーバーに構成されている完全なクライアントリストを確認できます。パラメータを指定せずに実行すると、/usr/openv/netbackup/bin/admincmd/bpplclients に基づいて、すべてのクライアントの更新が試行されます。一部のクライアントをアップグレードする場合は、一部のクライアントを指定できます。ハードウェアおよびオペレーティングシステムのパラメータを使用するか、-ClientList パラメータを使用します。

メディアサーバーから update_clients を実行できます。この場合、-ClientList パラメータを使用する必要があります。このコマンドを使用すると、メディアサーバーおよび一連のクライアントを、プライマリサーバーよりも前のバージョンに保持できます。このコマンドを使用するには、予定外のクライアントをアップグレードしないように、プライマリサーバー

およびメディアサーバーでの update_clients -ClientList コマンドの使用に熟知している必要があります。

クラスタ環境の場合、クライアントソフトウェアのプッシュインストールを実行できるのは、アクティブノードからだけです。

メモ: セキュアな環境でクライアントを配備し、クライアントがプライマリサーバーに直接接続されていない場合は、追加の手順が必要になります。このトピックに関する詳細情報を参照できます。NetBackup『セキュリティおよび暗号化ガイド』で、プライマリサーバーに未接続でクライアントに証明書を配備する方法についてのトピックを参照してください。

クライアントのアップグレードの間に、新しいクライアントファイルがクライアントの /tmp 内のディレクトリに書き込まれます。このディレクトリには、正常にアップグレードを行うために新しいクライアントファイルを一時的に保存するための十分な領域がなければなりません。十分な領域が利用可能でない場合、アップグレードスクリプトで /tmp ディレクトリ内の場所に書き込みを行うことができなかったという状態メッセージが表示されます。この問題を解決するには、/tmp ディレクトリにより多くの領域を割り当てて、アップグレード手順を再び実行します。一時ディレクトリはアップグレードが完了すると削除されます。

サーバーのアップグレード後にクライアントをアップグレードする方法

1 インストールスクリプトを開始するには、次のいずれかの方法を使用します。

ESD イメージ (ダウンロード済みファイル)	■ インストールイメージが存在する場所に移動します。 ■ 次のコマンドを入力します。 `./install`
ネイティブインストールツール	NetBackup では、ネイティブインストーラによる UNIX と Linux のクライアントバイナリのインストールとアップグレードがサポートされます。詳細情報を参照できます。 p.91 の「ネイティブインストーラによる UNIX と Linux のクライアントバイナリのアップグレード」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。

```
Installing NetBackup Client Software.
Do you wish to continue? (y/n) [y]
```

クライアントのバイナリは、バイナリがコンパイルされたオペレーティングシステムのバージョンを表します。通常、バイナリは、より新しいバージョンのオペレーティングシステム上で問題なく動作します。たとえば、Solaris 10 のバイナリは Solaris 11 レベルのオペレーティングシステムでも使用されます。

3 インストールするクライアント形式を選択し、プロンプトに従ってそのクライアント形式をインストールします。目的のクライアント形式がすべてインストールされるまで、必要に応じて繰り返します。

このサーバーからプッシュするすべての形式の UNIX クライアントのソフトウェアをインストールしたことを確認してください。これを行わない形式の UNIX クライアントは、NetBackup のポリシー構成に追加できません。

4 NetBackup プライマリサーバー上で、root ユーザーとして次のコマンドを入力して、bprd が動作しているかどうかを確認します。

```
/usr/openv/netbackup/bin/bpps
```

bprd が動作している場合は、次のコマンドを実行して停止します。

```
/usr/openv/netbackup/bin/admincmd/bprdreq -terminate
```

5 バックアップまたはリストアが実行中ではないことを確認するには、次のコマンドを入力します。

```
/usr/openv/netbackup/bin/admincmd/bpdbjobs
```

6 update_clients スクリプトを実行することによって UNIX クライアントソフトウェアを更新します。クライアントのリストには、仮想名ではなく各ノードのホスト名を指定します。

次のいずれかのコマンドを使用します。

-ClientList ファイルを使わない場合	/usr/openv/netbackup/bin/update_clients
-ClientList ファイルを使う場合	/usr/openv/netbackup/bin/update_clients -ClientList *filename*

メディアサーバーでは、-ClientList パラメータを使用する必要があります。

クライアントが 30 を超える場合、リストを複数のファイルに分割して、各ファイルに対して update_clients を実行できます。

クライアントリストファイルを作成するには、次の手順を実行します。

- 次のように NetBackup admincmd ディレクトリに変更します。

  ```
  cd /usr/openv/netbackup/bin/admincmd
  ```

- bpplclients コマンドを使用して、現在 NetBackup データベースに構成されているクライアントのリストが含まれるファイルを作成します。このコマンドで使用するオプションは、次に示すように、プライマリサーバーまたはメディアサーバーのどちらからプッシュインストールを行うかによって異なります。

プライマリサーバーからプッシュインストールを行う場合 `./bpplclients -allunique -noheader > file`

メディアサーバーからプッシュインストールを行う場合 `./bpplclients -allunique -noheader -M ¥ m_server_name > file`

オプションの説明は、次のとおりです。

`m_server_name` 環境内の NetBackup プライマリサーバーの名前。

`file` 一意のクライアントのリストを含めるファイルの名前。NetBackup データベース内でクライアントが構成されていない場合、ファイルは空になります。

`bpplclients` コマンドは、次の形式で `file` に出力を書き込みます。

```
hardware os client
```

`hardware` ハードウェアの名前。たとえば、ディレクトリ `/usr/openv/netbackup/client` では、`ls` コマンドを実行します。

`os` オペレーティングシステムの名前。たとえば、ディレクトリ `ls`**hardware**`/usr/openv/netbackup/client/`*`hardware`*`.` コマンドを実行します。

`client` クライアントの名前。

`file` の内容は、次の例のようになります。

```
Solaris Solaris9 curry
```

- (オプション) `file` を編集します。
  `file` の内容を変更するには、この手順を実行します。NetBackup クライアントソフトウェアで更新するクライアントだけが含まれるように `file` を編集します。クライアントのホスト名は、クライアントの各ノード名である必要があります。仮想名は指定できません。`hostname` コマンドと `domainname` コマンドは個々のノード名の正しい値を戻します。形式は、`hostname` または `hostname.domainname` です。

7 update_clients スクリプトを実行すると、プライマリサーバー情報の入力が要求されます。

```
Starting update_clients script.
There are N clients to upgrade.
Do you want the bp.conf file on the clients updated to list this

server as the primary server? (y/n) [y]
```

y または n のどちらかを入力します。

Enter キーを押します。

8 同時に実行する更新の数を入力します。

```
Enter the number of simultaneous updates you wish to take
place. [1 - 30] (default: 15):
```

9 インストーラは認証局の証明書の詳細を取得しようとします。

```
Getting CA certificate details.
Depending on the network, this action may take a few minutes. To
continue without setting up secure communication, press Ctrl+C.
```

Ctrl+C を押す場合は、インストールを再実行するか、必要なセキュリティコンポーネントを使用せずにインストールを続行する必要があります。必要なセキュリティコンポーネントが存在しない場合はバックアップとリストアが失敗します。

認証局の証明書が見つかった場合、次のメッセージが表示されます。

```
Using CA Certificate fingerprint from primary server:
01:23:45:67:89:AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23:45:67
If clients need an authorization token for installation, please
specify one here. Token (leave blank for no authorization token):
```

認証トークンを空白のままにした場合、次のメッセージが表示されます。

```
WARNING: Authorization Token was not specified.
Manual steps may be required before backups and restores can
occur.
```

10 質問に対して、y または n のどちらかを入力します。

```
The upgrade will likely take Y to Z minutes.
Do you want to upgrade clients now? (y/n) [y]
```

11 すべてのサーバーおよびクライアントが更新されたら、プライマリサーバー上で root ユーザーとして次のコマンドを入力して、bprd デーモンを起動します。

```
/usr/openv/netbackup/bin/initbprd
```

アップグレードエラーのロールバック手順

NetBackup 10.1 へのアップグレードが成功すると、レガシーログディレクトリの権限の制限が厳しくなります。NetBackup 10.1 へのアップグレードが失敗した場合は、アップグレードに伴う権限の変更をロールバックする必要があります。そうしないと、NetBackup が正常に動作しない可能性があります。

Linux で権限をロールバックするには:

1 /usr/openv/tmp ディレクトリに移動します。

2 次のコマンドを実行します。

```
. recoverPermissions.txt
```

Windows で権限をロールバックするには:

1 *install_path*¥NetBackup¥logs¥ ディレクトリに移動します。

2 次のコマンドを実行します。

```
icacls install_path¥NetBackup¥logs¥ /restore
install_path¥NetBackup¥Temp¥recoverPermissions.txt /C
```

/C スイッチは、使用するとエラーが発生しても処理を続行できるため、重要です。このスイッチを使用しないと、エラーが発生した場合に処理が停止します。

NetBackup プライマリサーバーとドメインのサイズについてのガイダンス

NetBackup プライマリサーバーのサイズ決定は、全体的な NetBackup ソリューション設計の一環として重要なアクティビティです。Veritas は、NetBackup プライマリサーバーと NetBackup ドメイン用に最適な構成を判断するために、データ保護を包括的に評価することをお勧めします。

次の情報はガイドラインを示すものです:

- NetBackup では、カタログサイズにハード制限はありません。ただし、Veritas はカタログバックアップとリカバリのパフォーマンスを良好にするために、カタログサイズを 4 TB 未満に保つことをベストプラクティスとして推奨します。
  NetBackup カタログのサイズと、NetBackup カタログからのデータの読み取りに関連するパフォーマンスは、I/O パフォーマンス、つまりディスク速度によって決定されます。Veritas では、可能な場合はカタログに SSD (ソリッドステートドライブ) を使用することをお勧めします。ディスクには優れた読み取りおよび書き込みパフォーマンスが必要です。これは、大規模環境ではさらに重要です。
  長期保持 (LTR) を使用したイメージでは、圧縮とカタログアーカイブを使用したカタログサイズの管理をお勧めします。
  圧縮とカタログアーカイブによるカタログサイズの管理について詳しくは、『NetBackup バックアップ計画とパフォーマンスチューニングガイド』を参照してください。
- EMM データベース内のデバイス数は 1,500 を超えないようにしてください。
  デバイスには、テープドライブ、テープライブラリ、ディスクプールなどがあります。
- メディアサーバーの数は 50 を超えないようにしてください。
  各 NetBackup ドメイン内で管理可能な数のメディアサーバーとストレージターゲットを維持することが重要です。配備されるメディアサーバーとストレージターゲットは管理および保守が必要で、最終的にパッチの適用とアップグレードが必要になります。これらの各メディアサーバーにも、保守が必要な構成が含まれています。したがって、管理性、操作性、管理の影響を考慮することが重要です。Veritas では、バックアップの作業負荷をサポートするために、必要な CPU、メモリ、ネットワーク帯域幅、およびディスク I/O で適切にサイズが設定されたメディアサーバーとストレージターゲットの配備をお勧めします。同じ作業負荷で DR の場所への複製またはレプリケーションが必要かどうかを考慮することも重要です。それらの二次的なオプションに対応するように、メディアサーバーとストレージターゲットのサイズを決定することは不可欠です。まとめると、ドメインごとに 50 未満の数を維持しながら、適切なサイズのメディアサーバーとストレージターゲットを配備することを Veritas はお勧めします。
- ジョブの数は、1 クライアントあたり 1 秒に 1 つを超えないようにする必要がありますが、別々のクライアントから各ジョブを送信することで、1 秒に複数のジョブを送信できます。各バックアップクライアントには「1 クライアントあたり 1 秒に 1 つのジョブ」の制限があるため、複数のクライアントで並列して実行される場合があります。
- CPU やメモリなどのコンピュータリソースは、プライマリサーバーがどこまで拡張できるかに影響します。

メディアサーバーからのメタデータストリームの処理に対応するには、必須の量のシステムリソースがプライマリサーバーに存在する必要があります。メディアサーバーは、バックアップしたファイルに関するメタデータをプライマリサーバーに送信します。このメタデータは定期的にバッチ処理され、送信されます。調整パラメータ MAX_ENTRIES_PER_ADD によって決定されるバッチサイズは、プライマリサーバーのパフォーマンス、特に多数の小さいファイルを含むバックアップイメージの場合に大きな影響を与えます。

NetBackup カタログにメタデータを送信するためのバッチサイズについて詳しくは、『NetBackup バックアップ計画とパフォーマンスチューニングガイドガイド』を参照してください。

プライマリサーバーは、これらのメタデータメッセージのペイロードをそれぞれ処理する必要があります。各ペイロードにはオペレーティングシステムプロセスが必要で、それぞれのプロセスがシステムリソースを消費します。消費されるシステムリソースは、ディスク容量、CPU サイクル、メモリ容量、ネットワーク帯域幅、ディスク I/O です。

表 A-10 に、詳細を示します。

表 A-10　　サイズの決定に関するガイドライン

プロセッサの数	推奨メモリ要件	プライマリサーバーごとのメディアサーバーの最大数 *
8	128 GB	20
16	256 GB	100

* Veritas では、メディアサーバーの数をドメインごとに 50 未満に制限することをお勧めします。

プロセッサとメモリの要件について、追加の推奨事項が利用可能です。

p.166 の「UNIX および Linux の場合のアップグレード要件」を参照してください。

p.169 の「Windows および Windows クラスタのアップグレード要件」を参照してください。