

Veritas NetBackup アップグレードガイド

リリース 8.2

Veritas NetBackup™ アップグレードガイド

最終更新日: 2019-07-22

法的通知と登録商標

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

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

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

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

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

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202、「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となります。業務用またはホスト対象サービスとしてベリタスによって提供されている場合でも同様です。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
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世界中にサポートセンターを設けています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供

されます。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の Web サイトにアクセスしてください。

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

次の URL で Veritas Account の情報を管理できます。

<https://my.veritas.com>

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

世界全域 (日本を除く)

CustomerCare@veritas.com

Japan (日本)

CustomerCare_Japan@veritas.com

マニュアル

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

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

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

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

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

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

目次

第 1 章	概要	7
	『NetBackup 8.2 アップグレードガイド』について	7
	利用可能な NetBackup アップグレード方式	8
	NetBackup 8.2 の変更について	10
	NetBackup 7.6.0.4 以前からのアップグレードの非サポート	10
	NetBackup 8.2 でサポートされる外部認証局の証明書	10
	Veritas Smart Meter について	10
	Veritas Smart Meter のベストプラクティス	11
第 2 章	アップグレード計画	13
	一般的なアップグレードの計画について	13
	NetBackup 8.2 のアップグレード計画について	13
	NetBackup 8.2 へのアップグレードの計画方法	14
	カタログバックアップの既知の制限事項	16
	NetBackup ホスト用のセキュリティ証明書について	16
	アップグレードによるファイルの自動変更について	17
	アップグレードツールについて	18
	Veritas Services and Operations Readiness Tools について	18
	SORT のアップグレードのための推奨手順	19
	SORT の新規インストールのための推奨手順	21
	NetBackup プリインストールチェッカーについて	25
	アップグレードに関する注意事項および制限事項	26
	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、	26
	NetBackup 8.2 による RHEL 7.5 でのファイバートランスポートメディア アササーバーのサポートについて	28
	NetBackup 8.1 での MSDP の変更	28
	NetApp クラスタに必要な可能性のある変更	29
	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	30
	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	30

第 3 章	マスターサーバーのアップグレード	31
	マスターサーバーのアップグレードについて	31
	NetBackup 8.2 へのアップグレードのプレインストール手順	32
	Windows システムでローカルサーバー、リモートサーバー、クラスターサーバーのアップグレードを実行する	36
	Windows システムでのサイレントアップグレードの実行	46
	NetBackup 8.2 への UNIX と Linux サーバーソフトウェアのアップグレード	50
	NetBackup 8.2 へのアップグレードのインストール後の手順	53
第 4 章	メディアサーバーのアップグレード	58
	NetBackup 8.2 への NetBackup メディアサーバーのアップグレード	58
	UNIX および 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	61
第 5 章	NetBackup の MSDP のアップグレード	67
	NetBackup 8.1 での MSDP のアップグレードの考慮事項	67
	MSDP ローリングデータ変換について	68
	MSDP 指紋アルゴリズムの変更について	69
第 6 章	クライアントのアップグレード	70
	クライアントのアップグレードについて	70
	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	71
	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	73
第 7 章	VxUpdate を使用した NetBackup 配備の管理	87
	VxUpdate について	87
	VxUpdate で使用するコマンド	88
	リポジトリの管理	89
	配備ポリシーの管理	92
	VxUpdate を使用したマスターサーバーからのアップグレードの手動による開始	97
	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	101
	配備ジョブの状態	102

付録 A	リファレンス	105
	NetBackup マスターサーバー Web サーバーのユーザーとグループの作成	106
	クラスタ化されたマスターサーバーの非アクティブノードで証明書を生成する	108
	NetBackup Java Runtime Environment について	109
	NetBackup Web ユーザーインターフェースについて	111
	NetBackup 応答ファイルについて	111
	RBAC のブートストラップについて	121
	インストール後すぐにマスターサーバー上のクラウド構成ファイルを更新するか、NetBackup 8.2 にアップグレードする	123
	NetBackup ソフトウェアの入手について	124
	NetApp クラスタのためのアップグレード前の追加手順	124
	レプリケーションディレクトリを使用した NetApp ディスクアレイの使用	126
	NetBackup のバージョン間の互換性について	130
	UNIX および Linux のインストールおよびアップグレード要件	131
	Windows および Windows クラスタのインストールおよびアップグレード要件	134
	Windows クラスタのインストールとアップグレードの要件	141
	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	142
	NetBackup OpsCenter サーバーと NetBackup マスターサーバー間の接続の無効化	143
	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	144
索引		145

概要

この章では以下の項目について説明しています。

- 『NetBackup 8.2 アップグレードガイド』について
- 利用可能な NetBackup アップグレード方式
- NetBackup 8.2 の変更について
- Veritas Smart Meter について
- Veritas Smart Meter のベストプラクティス

『NetBackup 8.2 アップグレードガイド』について

『NetBackup 8.2 アップグレードガイド』は、NetBackup 8.2 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。このマニュアルは最新情報を提供するために定期的に更新されます。このガイドの最新版は、次のリンクの NetBackup 8.2 アップグレードポータルから入手できます。

https://www.veritas.com/support/ja_JP/article.000115678

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もあります。SORT に関する詳しい情報を参照できます。

p.18 の「[Veritas Services and Operations Readiness Tools について](#)」を参照してください。

注意: NetBackup 8.2 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 8.2 へのアップグレードパスを提供しています。以前のバージョンの NetBackup に必要なアップグレード手順の情報は、NetBackup 8.1 以降のアップグレードガイドから削除されました。この変更により、NetBackup のより新しいバージョンをお持ちのカスタマのアップグレード手順を簡略化します。

NetBackup の以前のバージョンから 8.2 に直接アップグレードするには、次のことが必要です。

NetBackup への変更について理解するには、『NetBackup 8.0 リリースノート』を参照してください。

『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 8.2 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。

これらの以前のアップグレードについて詳しくは、NetBackup 8.0 だけでなく、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』も参照することを推奨します。これらの文書では、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。

https://www.veritas.com/support/ja_JP/article.DOC5332

利用可能な NetBackup アップグレード方式

次の表では、NetBackup をアップグレードするさまざまな方法について説明します。

表 1-1

アップグレード方法とオペレーティングシステム	サーバー	クライアント
UNIX および Linux の対話型	マスターサーバー p.50 の「NetBackup 8.2 への UNIX と 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。 メディアサーバー p.58 の「NetBackup 8.2 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。	サーバー情報の確認

アップグレード方法とオペレーティングシステム	サーバー	クライアント
Windows の対話型	マスターサーバー p.36 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。 メディアサーバー p.58 の「NetBackup 8.2 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。	サーバー情報の確認
UNIX および Linux のサイレント	マスターサーバーの有効なアップグレード方式ではありません。 メディアサーバー p.61 の「UNIX および 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.73 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。
Windows のサイレント	マスターサーバーとメディアサーバー p.46 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。	サーバー情報の確認
UNIX および Linux のリモート	有効なアップグレード方式ではありません。	UNIX および Linux のリモートクライアントアップグレード Chef および SCCM のテンプレート https://sortveritas.com/utility/netbackup/deployment
Windows のリモート	マスターサーバー p.36 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。 メディアサーバー p.58 の「NetBackup 8.2 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。	Chef および SCCM のテンプレート https://sortveritas.com/utility/netbackup/deployment

NetBackup 8.2 の変更について

NetBackup バージョン 8.2 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 8.2 の『NetBackup リリースノート』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 8.2 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 8.2 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/support/en_US/article.100038907

NetBackup 8.2 でサポートされる外部認証局の証明書

Veritas は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 Smart Meter について

Veritas Smart Meter 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。Smart Meter は、ライセンス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。Smart Meter には Veritas NetBackup 8.1.2 以降が必要です。

Smart Meter 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、Smart Meter 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、Smart Meter 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ベリタス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/Welcome?context=veritas_smart_meter&token=vsm_nbu_faqs

Smart Meter に接続するには、次の URL を使用します。

<https://taas.veritas.com/>

注意: Smart Meter は、Google Chrome、Mozilla Firefox、Microsoft Edge と互換性があります。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、これを使用することはお勧めしません。

p.11 の「[Veritas Smart Meter のベストプラクティス](#)」を参照してください。

Veritas Smart Meter のベストプラクティス

ベリタスでは、Smart Meter ツールに特定のベストプラクティスを推奨しています。

- Smart Meter は、Google Chrome、Mozilla Firefox、Microsoft Edge と互換性があります。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。
Smart Meter では、HTTPS を使用して関連する情報を送信します。自動アップロード機能を活用するために、マスターサーバーが、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。

Smart Meter 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、Smart Meter の Web サイトからダウンロードできる、Smart Meter 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、登録キーが集計されることがあります。この集計された登録キーには、すべてのアカウント ID が含まれます。すべてのマスターサーバーに対して、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マスター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、すべてのマスターサーバーに対して、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。
- 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/Welcome?context=veritas_smart_meter&token=vsm_nbu_faqs

カスタマ登録キーをダウンロードするには

- 1 Google Chrome、Mozilla Firefox、または Microsoft Edge を使用して Veritas Smart Meter にログインします。
<https://taas.veritas.com/>
- 2 [カスタマ登録キー (Customer Registration Keys)] ページに移動します。
- 3 マスター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。

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
- アップグレードツールについて
- アップグレードに関する注意事項および制限事項

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 8.2 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 8.2 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。
MSDP 変換	MSDP を使う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.67 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。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 8.2 での重要な変更を記述したものです。

注意: NetBackup 8.2 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:

p.18 の「[Veritas Services and Operations Readiness Tools について](#)」を参照してください。

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

NetBackup アップグレードポータル:

https://www.veritas.com/support/ja_JP/article.000115678

p.14 の「[NetBackup 8.2 へのアップグレードの計画方法](#)」を参照してください。

NetBackup 8.2 へのアップグレードの計画方法

NetBackup 8.2 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。

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.67 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.68 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.111 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 セキュリティ管理者ガイド』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 マスターサーバーには、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、各マスターサーバー（またはクラスタ化されたマスター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.106 の「NetBackup マスターサーバー 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。マスター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。

https://www.veritas.com/support/ja_JP/article.000115774

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する	p.131 の「UNIX および Linux のインストールおよびアップグレード要件」を参照してください。 p.134 の「Windows および Windows クラスタのインストールおよびアップグレード要件」を参照してください。 p.141 の「Windows クラスタのインストールと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。	詳細情報を参照できます。 p.106 の「NetBackup マスターサーバー 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.31 の「マスター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。

カタログバックアップの既知の制限事項

ベリタス社は、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atalogのバックアップを作成する場合は制限事項があります。

マスターサーバーが別のメディアサーバーにカatalogのバックアップを実行する場合に、メディアサーバーでマスターサーバーと同じバージョンの NetBackup を使う必要があります。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atalogデータが適切に保護されません。

NetBackup カatalogがマスターサーバー上に存在するため、マスターサーバーはカatalog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、マスターサーバーと同じ NetBackup バージョンを使ってカatalogバックアップを実行する必要があります。

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。

p.130 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 公開鍵インフラストラクチャ (PKI) 標準に適合しています。マスターサーバーは、NetBackup の認証局 (CA) として動作し、ホストに NetBackup の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 マスターサーバーは、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。

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

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。

セキュリティ証明書の配備、管理、使用について詳しくは、[NetBackup セキュリティ暗号化ガイド](#)』を参照してください。

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

パス	保護ファイルと保護ディレクトリ	処理
/usr/opensv/netbackup/ bin	backup_notify backup_exit_notify bpend_notify (省略可能) bpend_notify_busy (省略可能) bpstart_notify (省略可能) dbbackup_notify diskfull_notify initbpdbm initbprd restore_notify session_notify session_start_notify userreq_notify	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: backup_notify.version
/usr/opensv/msg/C /usr/opensv/netbackup/ bin/goodies /usr/opensv/netbackup/ bin/help /usr/opensv/volmgr/help	ディレクトリ全体	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/opensv/netbackup/ bin/goodies.version
/usr/opensv/volmgr/bin	drive_mount_notify (省略可能) drive_unmount_notify (省略可能) shared_drive_notify	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: shared_drive_notify.version

Windows の場合

表 2-4

パス	保護ファイルと保護ディレクトリ	処理
<code>install_path¥</code> <code>NetBackup¥bin</code>	<code>nblog.conf</code> <code>backup_exit_notify.cmd</code> <code>backup_notify.cmd</code> <code>dbbackup_notify.cmd</code> <code>diskfull_notify.cmd</code> <code>restore_notify.cmd</code> <code>session_notify.cmd</code> <code>session_start_notify.cmd</code> <code>userreq_notify.cmd</code>	ファイルは <code>install_path¥</code> <code>NetBackup¥bin.release</code> ディレクトリにコピーされます。リリース値は NetBackup の現在のバージョンです。 例 <code>install_path¥</code> <code>NetBackup¥bin.version</code>
<code>install_path¥</code> <code>NetBackup¥bin¥goodies</code>	<code>netbackup.adm</code> <code>help_script.cmd</code> <code>available_media.cmd</code> <code>check_coverage.cmd</code> <code>cleanstats.cmd</code> <code>duplicate_images.cmd</code> <code>verify_images.cmd</code> <code>bpstart_notify</code> <code>bpend_notify</code>	ファイルは <code>install_path¥</code> <code>NetBackup¥bin¥</code> <code>goodies.</code> <code>release</code> ディレクトリにコピーされます。リリース値は NetBackup の現在のバージョンです。 例 <code>install_path¥</code> <code>NetBackup¥bin.version</code>

アップグレードツールについて

SORT (Services and Operations Readiness Tools) などのツールに関するアップグレードについて詳しくは、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、ベリタス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、システムとベリタス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、今後置き換えられることなく廃止され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、他社製品の統合、ベリタス製品の統合、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

ベリタスは現在の **NetBackup** ユーザーに対して、**SORT** の最初の導入時にリストされる 3 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.21 の「SORT ページに Veritas Account を作成する方法」を参照してください。
システム固有のアップグレードレポートを作成します。	p.23 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.24 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。
今後のプラットフォームと機能の予定を確認します。	p.20 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.20 の「Hotfix と EEB の情報を確認する方法」を参照してください。

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。

SORT の新規インストールのための推奨手順

ベリタスは新規の NetBackup ユーザーに対して、SORT の最初の導入時にリストされる 3 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 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 2-6

手順	詳細
SORT Web ページに Veritas Account を作成します。	p.21 の「 SORT ページに Veritas Account を作成する方法 」を参照してください。
汎用インストールレポートを作成します。	p.22 の「 汎用インストールチェックリストを作成する方法 」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.23 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.24 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。

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。

汎用インストールチェックリストを作成する方法

1 Web ブラウザで、次の場所に移動します:

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

2 [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)] ウィジェットを見つけて選択します。

3 要求された情報を指定します

製品 (Product)	ドロップダウンメニューから適切な製品を選択してください。 NetBackup の場合は NetBackup Enterprise Server または NetBackup Server を選択してください。
インストールするまたはアップグレード後の製品バージョン (Product version you are installing or upgraded to)	NetBackup の適切なバージョンを選択してください。最新バージョンは常にリストの一番上に示されます。
プラットフォーム (Platform)	生成するチェックリストに対応するオペレーティングシステムを選択してください。
プロセッサ (Processor)	チェックリストに対して適切なプロセッサの種類を選択してください。
アップグレード前の製品バージョン (任意) (Product version you are upgrading from (optional))	新規インストールの場合は、何も選択しないでください。アップグレードの場合は、現在インストールされている NetBackup のバージョンを選択できます。

4 [チェックリストの生成 (Generate Checklist)]をクリックします。

5 選択内容に対応するチェックリストが作成されます。この画面で選択内容を変更できます。[チェックリストの生成 (Generate Checklist)]をクリックすると、新しいチェックリストが作成されます。

結果の情報は PDF として保存できます。**NetBackup** では多数のオプションを利用可能で、それらの多くは生成されたチェックリストに示されます。各セクションを十分に確認して、環境に適用するかどうかを判断してください。

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 (Data Collectors)]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 コンピュータに関する情報を収集するには、UNIX 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。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。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 (Data Collector)] 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 コンピュータに関する情報を収集するには、UNIX 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。ベリタス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。

NetBackup プリインストールチェッカーについて

UNIX/Linux プラットフォーム用と Windows プラットフォーム用のサーバーインストーラの両方にプリインストールチェッカーが含まれています。この機能を使用すると、サーバー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ないか判断しやすくなります。

この検査は、マスターまたはメディアサーバーでインストールを開始する際に自動的に実行されます。検査の結果は次のポイントで示されます。

- UNIX/Linux のアップグレードスクリプト
「このホストはマスターサーバーですか」の質問に回答した後。
- 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

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。プリインストール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。

プリインストール検査の結果は次の場所に格納されます。

- UNIX
次のパスにあるインストールトレースファイル
`/usr/opensv/tmp`
- Windows
`bpmimage` 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¥`

p.18 の「[Veritas Services and Operations Readiness Tools について](#)」を参照してください。

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 マスターサーバーには、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、各マスターサーバー (またはクラスタ化されたマスター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: UNIX および 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。

UNIX または 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/opensv/wmc
user_name

例: # useradd -g nbwebgrp -c 'NetBackup Web Services application
account' -d /usr/opensv/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 マスター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 8.2 による RHEL 7.5 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 でファイバートランスポートメディアサーバー (FTMS) の使用を計画する場合は、NetBackup を 8.1.2 以降に確実にアップグレードします。また、NetBackup 8.1.2 以降が配備された新しい RHEL 7.5 システムを使用することもできます。

RHEL を 7.5 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 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 Deduplication 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 Deduplication 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。

表 2-7 MSDP のアップグレードの詳細

動作	詳細
元の NetBackup バージョン	7.7.x および 8.0
最終的なアップグレードされた NetBackup バージョン	8.1
必要な変換	AES 暗号化と SHA2 指紋アルゴリズムへのローリング変換。NetBackup アップグレードのインストール完了後、ローリング変換が自動的に起動します。
変換の監視、制御、および時間の計算	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。
必要な停止時間は？	停止時間は必要ありません。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。

NetApp クラスタに必要なになる可能性のある変更

8.2 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。詳細情報が利用可能です。

p.124 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マスターサーバーで 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マスターサーバーは 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マスターサーバーが NetBackup 8.2 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 8.2 でターゲットドメインのマスターが 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。ベリタスでは、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。

マスター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。

- マスターサーバーのアップグレードについて
- [NetBackup 8.2 へのアップグレードのプレインストール手順](#)
- [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](#)
- [Windows システムでのサイレントアップグレードの実行](#)
- [NetBackup 8.2 への UNIX と Linux サーバーソフトウェアのアップグレード](#)
- [NetBackup 8.2 へのアップグレードのインストール後の手順](#)

マスター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、まずマスターサーバーの **NetBackup** をアップグレードします。マスター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.130 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。

メモ: **NetBackup** マスターサーバーを更新する前に、**NetBackup OpsCenter** を必ず更新してください。**OpsCenter** のデータ収集を無効にする必要もあります。詳しくは、『**NetBackup OpsCenter** 管理者ガイド』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>

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ベリタスがお勧めします。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 NetBackup 管理コンソールがアンインストールされます。

p.130 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.32 の「[NetBackup 8.2 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 8.2 へのアップグレードのプレインストール手順

次の手順を使って環境を NetBackup 8.2 にアップグレードします。

Veritas ベリタスは、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ツールを開発しました。詳しくは、**Business Critical Services (BCS)** の担当者に連絡してください。

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спорт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.28 の「[NetBackup 8.2 による RHEL 7.5 でのファイバートランспорт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: NetBackup マスターサーバーをバージョン 8.2 に更新する前に NetBackup OpsCenter をバージョン 8.2 に必ず更新してください。OpsCenter のデータ収集を無効にする必要もあります。詳しくは、『NetBackup OpsCenter 管理者ガイド』を参照してください。

https://www.veritas.com/support/ja_JP/article.DOC5332

64 ビットの Windows プラットフォームで OpsCenter をアップグレードする場合には既知の問題があることに注意してください。言語パックまたは Maintenance Pack をインストールしている場合は、アップグレードに失敗する可能性があります。この問題に関する詳しい情報を参照できます。

<http://www.veritas.com/docs/TECH211070>

特定のマスターサーバーの OpsCenter データ収集を無効にすることができます。データ収集を無効にする場合は、OpsCenter サーバーの前にマスターサーバーをアップグレードできます。データ収集を無効にすると、既知の問題が発生します。データ収集の無効化とそのリスクに関して詳細情報を参照できます。

p.143 の「NetBackup OpsCenter サーバーと NetBackup マスターサーバー間の接続の無効化」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マスターサーバーを含む 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 8.2 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.19 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 Smart Meter のカスタマ登録キーをダウンロードします。Smart Meter に関する詳しい情報を参照できます。Veritas

p.10 の「Veritas Smart Meter 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。

- 3 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。
- このマスターサーバーの **OpsCenter** データ収集機能を無効にします。
- 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。
- 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 `-persist` オプションを使用して **NetBackup** 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、『**Veritas 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。

- 4 (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
```

- 5 NetBackup 8.0 より、NetBackup マスターサーバーには、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、各マスターサーバー (またはクラスタ化されたマスター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.106 の「[NetBackup マスターサーバー 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: Veritas 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。マスター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は詳しくは、次をご覧ください。

https://www.veritas.com/support/ja_JP/article.000115774

- 6 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、アップグレードする前にデータベースおよびリスナープロセスを停止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 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>

- 7 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/opensv/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.36 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.46 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.50 の「[NetBackup 8.2 への UNIX と 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 8.2 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 8.2 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、または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 8.2 をローカルホストで元の状態にリストアします。

- NetBackup 8.2 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 [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 master 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。
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、ライセンスが必要かどうか **NetBackup** によって再度確認されます。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 マスターサーバー (NetBackup Master Server)]** をクリックしてマスター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。

- 10** **[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 Smart Meter** サイトからダウンロードし、適切なマスターサーバーに配置します。**Veritas Smart Meter** に関する詳しい情報を参照できます。

p.10 の「[Veritas Smart Meter について](#)」を参照してください。

NetBackup 8.2 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。

- 11** **[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、マスター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 accounts 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です。

詳細情報を参照できます。

p.134 の「[Windows および Windows クラスターのインストールおよびアップグレード要件](#)」を参照してください。

12 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。

- [NetBackup ポート番号 (NetBackup Port Numbers)]
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。

ログオン

[ローカルシステムアカウント (Local System account)]または[アカウント(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

- [アカウント (This 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)

スタートアップの種類

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[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)]

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外します。

[安全な中止 (Safe Abort)]オプション

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。

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

マスターサーバー名 (Master Server Name)	マスター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マスター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。ベリタス社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 マスター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、または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。
OpsCenter Server Name (省略可能)	OpsCenter は、NetBackup 用の Web ベースの管理ツールです。 OpsCenter サーバーを使用しているか、またはインストールする場合は、そのサーバーのサーバー名か IP アドレスをここに入力します。 クラスタサーバーには、仮想名を使わないでください。その代わりに、クラスタノードの実際のホスト名を使います。

[次へ (Next)]をクリックします。

- 14** (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、**証明書ストア名**¥**発行者の識別名**¥**サブジェクトの識別名**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¥IssuerName¥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。

15 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、または次の方式を使ってください。

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を確認されます。

- 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、すでにマスター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を検証されます。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、クラスタ化された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。

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。
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。
16 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。変更することはできません。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。	
17 [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。 次のオプションから 1 つ選択します。	

- 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。

- 18 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。
- 19 [Installation Complete]画面で、次のオプションから選択します。

Add Licenses

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起きたかどうかが表示されます。

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。

- 20** 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、ベリタス社のテクニカルサポートにお問い合わせください。
- 21** 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.53 の「[NetBackup 8.2 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必要になります。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 2008/2012/2012 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。
 - マスターサーバーのアップグレード時: `silentmaster.cmd`
 - メディアサーバーのアップグレード時: `silentmedia.cmd`
 - NetBackup リモート管理コンソールのアップグレード時: `silentadmin.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 マスター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 SMART_METER_FILE_PATH=path`
マスターサーバーのみの場合、Veritas Smart Meter 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.10 の「[Veritas Smart Meter について](#)」を参照してください。
- `ECA_CERT_STORE`
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。
- `ECA_CERT_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。
- `ECA_TRUST_STORE_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。
- `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_CRL_CHECK_LEVEL
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。
- ECA_CRL_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。
- ECA_KEY_PASSPHRASEFILE
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。

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\
```

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.53 の「**NetBackup 8.2 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 8.2 への UNIX と 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。

UNIX と Linux サーバーソフトウェアを 8.2 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。
マスターサーバーの場合は、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マイグレーションが行われないようにするために、NetBackup グループをフリーズします。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 グループをフリーズできます。
 - 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 Solaris システムの場合はアップグレードスクリプトを実行すると、変更した可能性があるすべての NetBackup スクリプトが削除されます。

Solaris システム以外では、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.17 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: 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。

- 8 (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):
```

- 9 (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
```

- 10** (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.
```

- 11** (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 master 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):
```

- 12** (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 master 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):
```

- 13** 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.53 の「[NetBackup 8.2 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 8.2 へのアップグレードのインストール後の手順

「[「NetBackup 8.2 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 8.2 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 8.2 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 8.2 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 8.2 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。Maintenance Release 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。
UNIX および Linux の場合: `/usr/opensv/netbackup/bin/bprd`
Windows の場合: `install_path¥NetBackup¥bin¥bprd`
 - Maintenance Release 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/opensv/netbackup/bin/bp.kill_all`
Windows の場合: `install_path¥NetBackup¥bin¥bpdown -f`
 - Maintenance Release 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 システムおよび Linux システムの場合:
`/usr/opensv/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.111 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 セキュリティ管理者ガイド](#)』を参照してください。

- 4 システム上で NetBackup とやり取りするすべてのアプリケーションを起動します。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 クラスタ化されたマスター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.108 の「[クラスタ化されたマスター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) このステップはクラスタのインストールにのみ適用されます。このコンピュータがクラスタマスターサーバーのアップグレードでない場合は、次のステップに進みます。

クラスタ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マスターサーバーノードを NetBackup 8.2 に更新できます。詳しくは、『[Veritas 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。

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。

https://www.veritas.com/support/ja_JP/article.DOC5332

- 7 (該当する場合) 外部認証局 (ECA) を使用するマスターサーバーまたは 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

- 8 NetBackup 8.2 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.16 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.58 の「[NetBackup 8.2 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)。
 - このマスターサーバーの OpsCenter データ収集機能。
- 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.144 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.124 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) NetBackup 環境でクラウドストレージを使用する場合は、クラウド構成ファイルを更新する必要があります。詳細情報を参照できます。
- p.123 の「[インストール後すぐにマスターサーバー上のクラウド構成ファイルを更新するか、NetBackup 8.2 にアップグレードする](#)」を参照してください。
- 13 (該当する場合) SSL が有効なクラウドと CloudCatalyst 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。

- 14 (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 クラウド Web UI 管理者ガイド』を参照してください。

- 15 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。
- 16 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.58 の「NetBackup 8.2 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>

-
- 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。

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 8.2 への NetBackup メディアサーバーのアップグレード](#)
- [UNIX および 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](#)

NetBackup 8.2 への NetBackup メディアサーバーのアップグレード

Veritas は、メディア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、UNIX および 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。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.16 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、すべてのサポート対象バージョン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.28 の「[NetBackup 8.2 による RHEL 7.5 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マスター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。 ■ UNIX システムの場合: <code>/usr/openv/netbackup/bin/bp.kill_all</code> ■ Windows システムの場合: <code>install_path¥NetBackup¥bin¥bpdown -f</code>	
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.36 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.46 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.50 の「NetBackup 8.2 への UNIX と 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.61 の「UNIX および 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.87 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.16 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 8.2 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 8.2 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 8.2 メンテナンスリリースにアクセスする方法 1 NetBackup 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。Maintenance Release のハイパーリンクをクリックします。 4 Maintenance Release が利用可能ではない場合は手順 6 に進みます。 5 Maintenance Release 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。 UNIX および Linux の場合: <code>/usr/opensv/netbackup/bin/bp.kill_all</code> Windows の場合: <code>install_path¥NetBackup¥bin¥bpdown -f</code> 7 Maintenance Release 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。 UNIX システムおよび Linux システムの場合: <code>/usr/opensv/netbackup/bin/bp.start_all</code> Windows システムの場合: <code>install_path¥NetBackup¥bin¥bpup -f</code>	

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マスター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マスターサーバーのアップグレードに含まれる場合は、マスターサーバーのアップグレード手順を再開します。	
8	(該当する場合) メディアサーバーで MSDP を使用している場合は、アップグレードにローリングデータ変換が含まれます。 変換が正常に完了し新しいストレージ形式に問題がなければ、変換プロセスから生成されたストレージを次のようにクリーンアップします。 ■ UNIX の場合: <code>/usr/opensv/pdde/pdcr/bin/stconv --cleanup</code> ■ Windows の場合: <code>install path¥Veritas¥pdde¥stconv.exe --cleanup</code>	

UNIX および 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 UNIX および 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法のいずれかを使用できます。

- 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/opensv/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メディアサーバーを NetBackup 7.7.3 以前から NetBackup 8.2 以降にアップグレードするには、追加の手順が必要です。メディア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メディアサーバーを新しい Veritas パッケージにアップグレードすることもできます。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.74 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。

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 UNIX または 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.111 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.111 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。
- **SKIP**: 認証局の設定をスキップするために使用します。**ECA** の構成をスキップするには、必要なすべての **ECA_** 値を **SKIP** に設定します。認証局を構成せずにインストールを続行すると、バックアップとリストアが失敗することに注意してください。

■ **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 **LICENSE** エントリ
- 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.111 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 RedHat** の場合:

```
tar -xzvf NetBackup_8.2_LinuxR_x86_64.tar.gz
```

- **Linux SuSE** の場合:

```
tar -xzvf NetBackup_8.2_LinuxS_x86_64.tar.gz
```

- **Linux-s390x RedHat** の場合:

```
tar -xzvf NetBackup_8.2_zLinuxR.tar.gz
```

- **Linux-s390x SuSE** の場合:

```
tar -xzvf NetBackup_8.2_zLinuxS.tar.gz
```

- **Solaris SPARC** の場合:

```
tar -xzvf NetBackup_8.2_Solaris_Sparc64.tar.gz
```

- **Solaris x86** の場合:

```
tar -xzvf NetBackup_8.2_Solaris_x86.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 RedHat** の場合:
NetBackup_8.2_LinuxR_x86_64/linuxR_x86/anb
- **Linux SuSE** の場合:
NetBackup_8.2_LinuxS_x86_64/linuxS_x86/anb
- **Linux-s390x RedHat** の場合:
NetBackup_8.2_zLinuxR/zlinuxR/anb
- **Linux-s390x SuSE** の場合:
NetBackup_8.2_zLinuxS/zlinuxS/anb
- **Solaris SPARC** の場合:
NetBackup_8.2_Solaris_Sparc64/solaris/anb
- **Solaris x86** の場合:
NetBackup_8.2_Solaris_x86/solaris_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 および VRTSpddes.rpm
Linux-s390x には VRTSpddes.rpm が存在しないことに注意してください。
- **Solaris:** VRTSnetbp.pkg および VRTSpddes.pkg

- 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。

- **RedHat:** openv/netbackup/client/Linux/RedHat2.6.32
- **SuSE:** openv/netbackup/client/Linux/SuSE3.0.76
- **Linux-s390x RedHat:**
openv/netbackup/client/Linux-s390x/IBMzSeriesRedHat2.6.32
- **Linux-s390x SuSE:** openv/netbackup/client/Linux-s390x/SuSE3.0.76
- **SPARC:** openv/netbackup/client/Solaris/Solaris10
- **Solaris_x86:** openv/netbackup/client/Solaris/Solaris_x86

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。

Linux

```

VRTSnbpcck.rpm
VRTSspbxx.rpm
VRTSnbclt.rpm
VRTSnbjre.rpm
VRTSnbjava.rpm
VRTSpddea.rpm
VRTSnbcfg.rpm

```

Linux-s390x には VRTSpddea.rpm が存在しないことに注意してください。

Solaris

```

.pkg_defaults
VRTSnbpcck.pkg.gz
VRTSspbxx.pkg.gz
VRTSnbclt.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。

- 8 (該当する場合) Solaris では、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。

```

VRTSnbpcck.pkg
VRTSspbxx.pkg
VRTSnbclt.pkg
VRTSnbjre.pkg
VRTSnbjava.pkg
VRTSpddea.pkg
VRTSnbcfg.pkg

```

- 9 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 VRTSnbpcck.rpm
- Solaris: pkgadd -a .pkg_defaults -d VRTSnbpcck.pkg VRTSnbpcck

- 10** (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 SYMCnbc1t
rpm -e SYMCnbjre
rpm -e SYMCpddes
rpm -e SYMCnetbp
```

- 11** 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 VRTSspb.x.rpm
rpm -U VRTSnbclt.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
```

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 VRTSspb.pkg VRTSspb
pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt
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 VRTSpddes.pkg VRTSpddes
pkgadd -a .pkg_defaults -d VRTSnbcfg.pkg VRTSnbcfg
pkgadd -a .pkg_defaults -d VVRTSnetbp.pkg VRTSnetbp
```

- -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。

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](#)
- [MSDP ローリングデータ変換について](#)
- [MSDP 指紋アルゴリズムの変更について](#)

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 のフィンガープリント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。フィンガープリント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、クレデンシア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 Deduplication 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 Deduplication ガイド』

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](#)
- [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](#)
- [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](#)

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マスター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。関連付けられたマスター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.36 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.71 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ます、追加の手順も必要です。詳細情報を参照できます。

p.73 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.87 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 8.2 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 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: `ls1pp`、`installp`
- **HP-UX** の場合: `swlist`、`swinstall`
- **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/opensv/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クライアントを 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。クライアント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クライアントを新しい 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.74 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。

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 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.111 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.111 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。
 - SKIP: 認証局の設定をスキップするために使用します。ECA の構成をスキップするには、必要なすべての ECA_ 値を SKIP に設定します。認証局を構成せずにインストールを続行すると、バックアップとリストアが失敗することに注意してください。
- 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 (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 マスター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.111 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
- INSTALL_PATH

- MERGE_SERVER_LIST

各オプションに関する詳細情報を参照できます。

p.111 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	<code>gunzip NetBackup_8.2_CLIENTS1.tar.gz; tar -xvf NetBackup_8.2_CLIENTS1.tar</code>
HP-UX	<code>gunzip -dc NetBackup_8.2_CLIENTS1.tar.gz tar -xvf</code>
Linux	<code>tar -xzvf NetBackup_8.2_CLIENTS2.tar.gz</code>
Solaris	<code>tar -xzvf NetBackup_8.2_CLIENTS1.tar.gz</code>

- 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	<code>CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/RS6000/AIX6/</code>
HP-UX	<code>CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/HP-UX-IA64/HP-UX11.31/</code>
Linux	Linux RedHat の場合: <code>CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux/RedHat2.6.18/</code> Linux SuSE の場合: <code>CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux/SuSE3.0.76</code>
Linux - s390x	Linux-s390x RedHat の場合: <code>CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux-s390x/IBMzSeriesRedHat2.6.18/</code> Linux-s390x SuSE の場合: <code>CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux-s390x/IBMzSeriesSuSE3.0.76</code>

Linux -
ppc64le

Linux-ppc64le RedHat の場合:

CLIENTS2/NBClientS/anb/ClientS/usr/opensv/netbackup/client/
Linux-ppc64le/IBMpSeriesRedHat3.10.0/

Linux-ppc64le SuSE の場合:

CLIENTS2/NBClientS/anb/ClientS/usr/opensv/netbackup/client/
Linux-ppc64le/IBMpSeriesSuSE4.4.21

Solaris

Solaris SPARC の場合:

CLIENTS1/NBClientS/anb/ClientS/usr/opensv/netbackup/client/Solaris/Solaris10/

Solaris x86 の場合:

CLIENTS1/NBClientS/anb/ClientS/usr/opensv/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。

AIX

VRTSnbpcck.image
VRTSspbX.image.gz
VRTSnbclt.image.gz
VRTSnbjre.image.gz
VRTSnbjava.image.gz
VRTSpddea.image.gz
VRTSnbcfg.image.gz

HP-UX

VRTSnbpcck.depot
VRTSspbX.depot.gz
VRTSnbclt.depot.gz
VRTSnbjre.depot.gz
VRTSnbjava.depot.gz
VRTSpddea.depot.gz
VRTSnbcfg.depot.gz

Linux

VRTSnbpcck.rpm

VRTSspbxx.rpm

VRTSnbclt.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

VRTSnbpcck.pkg.gz

VRTSspbxx.pkg.gz

VRTSnbclt.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: **NetBackup Java** コンソールの **RPM** (VRTSnbjava) は省略可能です。環境内のすべてのクライアントに **NetBackup Java** コンソールをインストールする必要がないこともあります。

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、HP-UX、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。

```
VRTSnbpcck.pkg
VRTSspbxx.pkg
VRTSnbclt.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 VRTSnbpcck.image all`
- HP-UX: `swinstall -s VRTSnbpcck.depot ¥*`
- Linux: `rpm -U VRTSnbpcck.rpm`
- Solaris: `pkgadd -a .pkg_defaults -d VRTSnbpcck.pkg VRTSnbpcck`

- 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。

```
AIX      installp -ad VRTSspbxx.image all
         installp -ad VRTSnbclt.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
```

HP-UX

```
swinstall -s VRTSpxb.depot ¥*
swinstall -s VRTSnbcclt.depot ¥*
swinstall -s VRTSnbjre.depot ¥*
swinstall -s VRTSnbjjava.depot ¥*
swinstall -s VRTSpddea.depot ¥*
swinstall -s VRTSnbcfg.depot ¥*
```

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。

```
swinstall -s ./VRTSnbpck.depot ¥*;swinstall -s
./VRTSpxb.depot ¥*;swinstall -s ./VRTSnbcclt.depot
¥*;swinstall -s ./VRTSnbjre.depot ¥*;swinstall -s
./VRTSnbjjava.depot ¥*;swinstall -s ./VRTSpddea.depot
¥*;swinstall -s ./VRTSnbcfg.depot ¥*
```

Linux

```
rpm -U VRTSpxb.rpm
rpm -U VRTSnbcclt.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjjava.rpm
rpm -U VRTSpddea.rpm
rpm -U VRTSnbcfg.rpm
```

メモ: VRTSnbjre.rpm、VRTSnbjjava.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 VRTSpxb.pkg VRTSpxb
pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt
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

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 VRTSnbpcck.image all package VRTSnbpcck.image is already installed	lsllpp -L <i>package_name</i> コマンドを使用して、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.74 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/opensv/lib/java/nbvmwaretags.jar from install of VRTSnbclt-version-platform conflicts with file from package VRTSnbclt-version-platform	lsllpp -L <i>package_name</i> コマンドを使用して、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。
HP-UX 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。	# swinstall -s ./VRTSnbpcck.depot 1 filesets have the selected revision already installed.	swlist コマンドを使用して、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。

インストール処理	エラーメッセージ	解決方法
誤った順序でバイナリをインストールしようとする。	<pre># swinstall -s ./VRTSnbcfg.depot ERROR: "hostname:/: The software dependencies for 1 products or filesets cannot be resolved.</pre>	デポ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.74 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。	<pre># swinstall -s ./VRTSnbclt.depot WARNING: "hostname:/: 1 filesets have a version with a higher revision number already installed.</pre>	swlistコマンドを使用して、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		
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。	<pre># rpm -U VRTSnbpcck.rpm package VRTSnbpcck.rpm-version-platform is already installed</pre>	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。	<pre># rpm -U VRTSnbcfg.rpm error: Failed dependencies: VRTSnbclt >= 8.1.0.0 is needed by VRTSnbcfg-version-platform</pre>	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.74 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。	<pre># rpm -U VRTSnbclt.rpm file /usr/opensv/lib/java/nbvmwaretags.jar from install of VRTSnbclt-version-platform conflicts with file from package VRTSnbclt-version-platform</pre>	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
	<pre> 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. </pre>	

インストール処理	エラーメッセージ	解決方法
	<pre>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 VRTSnbpcck was successful.</pre>	
誤った順序でバイナリをインストールしようとする。	<pre># pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt ERROR: VRTSnbpcck >=8.1.0.0 is required by VRTSnbclt.checkinstall script suspends</pre>	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.74 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。	<pre># pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt Processing package instance <VRTSnbclt> from </root/80/packages/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]</pre>	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。

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 で使用するコマンド](#)
- [リポジトリの管理](#)
- [配備ポリシーの管理](#)
- [VxUpdate を使用したマスターサーバーからのアップグレードの手動による開始](#)
- [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](#)
- [配備ジョブの状態](#)

VxUpdate について

Veritas は、LiveUpdate の代わりとして VxUpdate を導入します。VxUpdate の主要コンポーネントは、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ツールとして機能する新しい配備ポリシーです。VxUpdate のリリースに伴い、Veritas は LiveUpdate のサポートを終了します。

ポリシーをサポートするために、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、マスターサーバー上の 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。

新しい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することを可能にします。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推奨される方法は次のとおりです。Veritas

表 7-1

手順	処理 (Action)	追加情報
1	NetBackup リポジトリへの配置	p.89 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.92 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) マスターサーバー、メディアサーバー、またはクライアントからのアップグレードの手動による実行	p.97 の「 VxUpdate を使用したマスター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.101 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。このコマンドはマスター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 の導入に伴い、Veritas は LiveUpdate のサポートを終了します。その結果、Veritas NetBackup パッケージを保持するための外部リポジトリをユーザーが設定する必要がなくなりました。この機能は、**NetBackup** マスターサーバーに含まれています。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。すべてのプラットフォームについて、すべての **NetBackup 8.2** サーバーおよびクライアントパッケージをリポジトリに保存すると、マスターサーバー上に約 **20 GB** の領域が必要になります。この量には、エンジニアリングのバイナリや **Hotfix** は含まれません。このサイズは、**NetBackup** の各バージョンについて、すべてのプラットフォームのすべてのパッケージに必要な領域の概算の量であることに注意してください。

`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、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。マスターサーバーには、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、マスター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。マスター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。

クライアントパッケージは、次の命名規則に従います:

`vxupdate_nbclient_version_operatingsystem_platform.sja`

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は、次の命名規則に従います: `vxupdate_nb_version_operatingsystem_platform.sja`

- 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.90 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。

UNIX または Linux の場合: /usr/opensv/netbackup/bin/admincmd

Windows の場合:install_path¥&ProductName;¥bin¥admincmd¥

- 2 nbrepo コマンドに -a オプションを指定して実行します。

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』

- 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.91 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。

UNIX または Linux の場合: /usr/opensv/netbackup/bin/admincmd

Windows の場合:install_path¥&ProductName;¥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](#)』

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.89 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。リポジトリはマスター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マスター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マスターサーバーに設定され、変更できません。

- (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 8.2 にアップグレードすると、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。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。
precheck 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せんが、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。

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、**証明書ストア名**¥**発行者の識別名**¥**サブジェクトの識別名**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 を使用したマスター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。

ローカルでマスター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.101 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、マスター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マスター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 および Linux コンピューター、Windows コンピューターの両方の外部認証局情報の場所を指定できます。

- 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、**証明書ストア名**¥**発行者の識別名**¥**サブジェクトの識別名**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/opensv/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 -i -policy policy_name -schedule schedule
[-master_server master]
```

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、***master*** はマスターサーバーの名前です。

`-i` オプションを使用すると、スケジュールされた時間に同じポリシーとスケジュールが開始されなくなることに注意してください。この動作は、重複ジョブを防ぎます。

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

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/opensv/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 {-hosts
filename|-host_filelist 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、マスター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マスター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.97 の「[VxUpdate を使用したマスター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。

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/opensv/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 master1
```

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](#)』

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。

UNIX または Linux の場合: `/usr/opensv/netbackup/bin/admincmd`

Window 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 (Hardware)
hpux	ia64
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、テクニカルノートを参照してください。

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

リファレンス

この付録では以下の項目について説明しています。

- [NetBackup マスターサーバー Web](#) サーバーのユーザーとグループの作成
- クラスタ化されたマスター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
- [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
- [RBAC](#) のブートストラップについて
- インストール後すぐにマスターサーバー上のクラウド構成ファイルを更新するか、[NetBackup 8.2](#) にアップグレードする
- [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
- レプリケーションディレクタを使用した [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](#) のインストールおよびアップグレード要件
- [Windows](#) および [Windows](#) クラスタのインストールおよびアップグレード要件
- [Windows](#) クラスタのインストールと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
- [NetBackup OpsCenter](#) サーバーと [NetBackup](#) マスターサーバー間の接続の無効化

- [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 マスターサーバー Web サーバーのユーザーとグループの作成

NetBackup 8.0 より、NetBackup マスターサーバーには、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、各マスターサーバー（またはクラスタ化されたマスター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.131 の「[UNIX および Linux のインストールおよび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。

- **UNIX および 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マスターサーバーでは、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マスターサーバーでは、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 マスター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。[『Veritas 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 および UNIX 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 および UNIX の場合: `# useradd -g nbwebgrp -c 'NetBackup Web Services account' -d /usr/opensv/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。

クラスタ化されたマスターサーバーの非アクティブノードで証明書を生成する

クラスタマスター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。

クラスタ化されたマスター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。
 UNIX の場合: `/usr/opensv/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、示されている通りに `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。『Veritas NetBackup セキュリティおよび暗号化ガイド』で、マスターサーバーノードでの証明書の配備に関するセクションを参照してください。

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、ベリタス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。

- NetBackup マスターサーバー、メディアサーバー、またはクライアントソフトウェア
- NetBackup リモート管理コンソール
- OpsCenter サーバー、エージェント、または View Builder

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。

以前は、NetBackup または OpsCenter と共にインストールされる JRE パッケージは、いずれかのソフトウェアの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 マスターサーバー、メディアサーバー、またはクライアントソフトウェア
- NetBackup リモート管理コンソール
- OpsCenter サーバー、エージェント、または View Builder

メモ: このユーティリティを使用して、VMware vCenter 用 NetBackup プラグイン用の 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	<code>install_path¥netbackup¥java¥nbcomponentupdate.exe</code>
	UNIX または Linux	<code>/usr/opensv/java/nbcomponentupdate</code>

製品	オペレーティングシステム	パス
OpsCenter Server	Windows	<code>install_path¥server¥bin¥nbcomponentupdate.exe</code>
	UNIX または Linux	<code>SYMCOpsCenterServer/bin/nbcomponentupdate</code>
OpsCenter Agent	Windows	<code>install_path¥agent¥bin¥nbcomponentupdate.exe</code>
OpsCenter View Builder	Windows	<code>install_path¥viewbuilder¥bin¥nbcomponentupdate.exe</code>
リモート管理コンソール	Windows	<code>install_path¥java¥nbcomponentupdate.exe</code>

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/ja_JP/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。

ベリタスは、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>

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、NetBackup と一緒に使用する新しい Web ユーザーインターフェースが導入されました。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 セキュリティ管理者ガイド』を参照してください。

NetBackup Web UI から NetBackup マスター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 アクセスルールを作成する必要があります。アクセスルールは、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、アクセスルールの作成、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 のセキュリティ管理者ガイド』を参照してください。

NetBackup 応答ファイルについて

NetBackup 応答ファイル (/tmp/NBInstallAnswer.conf) は、次の目的で UNIX および Linux のインストール時とアップグレード時に使用されます。

- 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。
- サポート対象のほとんどのオペレーティングシステムで UNIX および Linux クライアントの無人またはサイレントのインストールとアップグレードを実行します。

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に関連する情報とともに示します。

表 A-2 テンプレート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	アップグレードに必要かどうか
「ACCEPT_REVERSE_CONNECTION」	クライアント	NAT クライアントをサポートするように NetBackup を構成する場合のみ。
「AUTHORIZATION_TOKEN」	メディアおよびクライアント	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	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_NAME」	メディアおよびクライアント	不要
「ECA_CERT_PATH」	メディアおよびクライアント	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	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	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	不要
「ECA_PRIVATE_KEY_PATH」	メディアおよびクライアント	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	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。
「INSTALL_PATH」	メディアおよびクライアント	不要
「LICENSE」	メディア	不要
「MACHINE_ROLE」	メディアおよびクライアント	不要

オプション	NetBackup の役割	アップグレードに必要かどうか
「MEDIA_SERVER」	クライアント	不要
「MERGE_SERVERS_LIST」	クライアント	不要
「RBAC_DOMAIN_NAME」	マスター	不要
「RBAC_DOMAIN_TYPE」	マスター	不要
「RBAC_PRINCIPAL_NAME」	マスター	不要
「RBAC_PRINCIPAL_TYPE」	マスター	不要
「SERVER」	メディアおよびクライアント	不要
「SERVICES」	クライアント	不要
「WEBSVC_GROUP」	マスター	不要
「WEBSVC_USER」	マスター	不要

セキュリティ構成の注意事項について

この操作が初回インストール、または 8.0 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。

NetBackup マスターサーバーを認証局として使用するには、マスターサーバーの CA_CERTIFICATE_FINGERPRINT を指定する必要があります。マスター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マスターサーバーですでに設定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。

外部認証局を使用するには、ECA_CERT_PATH、ECA_CRL_CHECK_LEVEL、ECA_PRIVATE_KEY_PATH、および ECA_TRUST_STORE_PATH の値が必須です。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。

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、すべての必要な ECA_ オプションに SKIP を指定します。すべての ECA_ 値を SKIP に設定しない場合、インストールまたはアップグレードが失敗することに注意してください。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。

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。
- デフォルト値: FALSE
- ACCEPT_REVERSE_CONNECTION=TRUE | FALSE
- [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におけるアップグレード時には無視されることに注意してください。
 - NBCA がホストですでに構成されている
 - ECA がマスターサーバーで使用されている
- 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=ABCDEFGHJKLMNOP | 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。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。fingerprint 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。セキュリティを設定せずにインス

ツールまたはアップグレードを続行するには、`CA_CERTIFICATE_FINGERPRINT=SKIP`を指定します。

`CA_CERTIFICATE_FINGERPRINT` は、次のいずれかの条件におけるアップグレードでは無視されることに注意してください。

- **NBCA** がホストですでに構成されている
- **ECA** がマスターサーバーで使用されている
- 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 | SKIP`
- [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、単一のマスター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。

- デフォルト値: なし。
- 必要/不要: 不要
- `_NAME=client 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。認証局の設定をスキップするには、必要なすべての `ECA_` 値を `SKIP` に設定します。認証局を構成せずにインストールを続行すると、バックアップとリストアが失敗することに注意してください。

ECA がホストですでに構成されている場合、またはマスターサーバーで **NBCA** のみを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。

- 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_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。
 - **SKIP**: 認証局の設定をスキップするために使用します。**ECA** の構成をスキップするには、必要なすべての **ECA_** 値を **SKIP** に設定します。認証局を構成せずにインストールを続行すると、バックアップとリストアが失敗することに注意してください。**ECA** がホストですでに構成されている場合、またはマスターサーバーで **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。
- 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。
認証局の設定をスキップするには、必要なすべての **ECA_** 値を **SKIP** に設定します。認証局を構成せずにインストールを続行すると、バックアップとリストアが失敗することに注意してください。
ECA がホストですでに構成されている場合、またはマスターサーバーで **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。
- 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、またはマスターサーバーで 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。

- 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。
 認証局の設定をスキップするには、必要なすべての ECA_ 値を SKIP に設定します。
 認証局を構成せずにインストールを続行すると、バックアップとリストアが失敗するこ
 とに注意してください。

ECA がホストですでに構成されている場合、またはマスターサーバーで 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。

- 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。
 認証局の設定をスキップするには、必要なすべての ECA_ 値を SKIP に設定します。
 認証局を構成せずにインストールを続行すると、バックアップとリストアが失敗するこ
 とに注意してください。

ECA がホストですでに構成されている場合、またはマスターサーバーで 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。

- 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。

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。
- デフォルト値: `/usr`
- 必要/不要: 不要
- `INSTALL_PATH = path`
- [表 A-2](#)に戻ります。

LICENSE

- 説明: このオプションは、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。
- 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。

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、`MASTER`、`MEDIA`、`CLIENT` です。
- 必要/不要: 不要。
- `MACHINE_ROLE = MASTER | MEDIA | CLIENT`
- [表 A-2](#)に戻ります。

MEDIA_SERVER

- 説明: このオプションは、**NetBackup** が、指定したホストを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。クライアントとマスターサーバー上の **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` エントリが存在することがあります。それぞれが **https** 要求のトンネリ

ングの候補として使用されます。これらのエントリは、bp.conf ファイルに追加されます。

- 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。

MERGE_SERVERS_LIST

- 説明: マスター上の 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。
- 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。

RBAC_DOMAIN_NAME

- 説明: このオプションは、セキュリティ管理者とバックアップ管理者の役割に、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。
- 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、セキュリティ管理者とバックアップ管理者の役割に、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。
- 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、セキュリティ管理者とバックアップ管理者の役割に、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。
- 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、セキュリティ管理者とバックアップ管理者の役割に、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。
- 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。

SERVER

- 説明: このオプションは、このコンピュータが現在の NetBackup マスター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マスターサーバーです。これらのエントリは、`bp.conf` ファイルに追加されます。
- デフォルト値: なし。
- 必要/不要: 不要。
- `SERVER=master_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。
- デフォルト値: YES

- 必要/不要: 不要。
- SERVICES=no
- 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。
- デフォルト値: nbwebgrp
- 必要/不要: 不要。
- WEBSVC_GROUP=custom_group_account_name
- 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。
- デフォルト値: nbwebsvc
- 必要/不要: 不要。
- WEBSVC_USER=custom_user_account_name
- 表 A-2に戻ります。

RBAC のブートストラップについて

UNIX プラットフォームでの NetBackup のインストールまたはアップグレード時に、RBAC の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。UNIX 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、セキュリティ管理者およびバックアップ管理者の両方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権を提供します。たとえば、既存のユーザー **Tester1** が、いくつかのオブジェクトグループのみへのアクセス権を持つバックアップ管理者ロールに割り当てられているとします。**Tester1** に RBAC ブートストラップを指定すると、**Tester1** は、すべてのオブジェクトへのアクセス権を持つバックアップ管理者ロールとセキュリティ管理者ロールに割り当てられます。

インストールまたはアップグレード後に、Windows と UNIX 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、マスター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。

UNIX 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 のブートストラップ:

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 master.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.111 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 の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「**応答ファイルに RBAC エントリが入力されていません** (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 の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 の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。

```
principal_name の RBAC 権限を正常に構成しました。(Successfully configured the RBAC permissions for principal_name.)
```

ユーザーまたはユーザーグループに、セキュリティ管理者およびバックアップ管理者の RBAC ロール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。

警告: RBAC 権限を構成できません。`/tmp/NBInstallAnswer.conf` に 1 つ以上の必須フィールドが存在しません。(Warning: Unable to configure the RBAC permissions. One or more required fields are missing in `/tmp/NBInstallAnswer.conf`.)

RBAC の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。

インストール後すぐにマスターサーバー上のクラウド構成ファイルを更新するか、**NetBackup 8.2** にアップグレードする

警告: *principal_name* の RBAC 権限の構成に失敗しました。詳しく

は、`/usr/opensv/netbackup/logs/admin` のログを参照してください。(Warning: Failed to configure the RBAC permissions for *principal_name*. Refer to logs in `/usr/opensv/netbackup/logs/admin` for more information.)

RBAC の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/opensv/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、セキュリティ管理者およびバックアップ管理者の両方の役割と対応する 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。

インストール後すぐにマスターサーバー上のクラウド構成ファイルを更新するか、**NetBackup 8.2** にアップグレードする

NetBackup 環境でクラウドストレージを使用する場合には、NetBackup 8.2 をインストールするか、そのバージョンにアップグレードした直後に、NetBackup マスターサーバー上のクラウド構成ファイルの更新が必要になる場合があります。NetBackup 8.2 へのアップグレード後にクラウドプロバイダまたは関連の拡張機能がクラウド構成ファイルから利用できない場合、関連する操作は失敗します。

Veritas はリリース間にもクラウド構成ファイルに新しいクラウドサポートを継続的に追加します。NetBackup 8.2 の最終ビルドのクラウドストレージサポートは、クラウド構成パッケージのバージョン 2.6.0 に含まれるものと同じです。

クラウド構成ファイルの更新は、クラウド構成パッケージのバージョン 2.5.4 以降にクラウドストレージプロバイダが追加された場合にのみ必要です。バージョン 2.5.4 以降には次のクラウドサポートが追加されていますが、NetBackup 8.2 の最終ビルドには含まれていませんでした。

■ Nutanix Buckets (S3)

最新のクラウド構成パッケージについては、次の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.100033434

クラウドストレージ構成ファイルの追加方法については、次の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.100039095

NetBackup ソフトウェアの入手について

NetBackup 8.2 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-3 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-3 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	変更無し	ベリタス社と 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.125 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。
Vserver 対応モード	なし	追加手順が必要です。 p.126 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、『Veritas 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、『Veritas 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、代替読み込みみ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。

レプリケーションディレクトクを使用した NetApp ディスクアレイの使用

レプリケーションディレクトクは、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 モードは、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: クラスタ化されたデータ 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、マスターサーバー、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ポリシーをサポートします。

表 A-4 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-4 バージョンの互換性

NetBackup バージョン (NetBackup Version)	NetApp プラグイン バージョン	説明	OCUM サーバーに対するマスターサーバーの比	サポート対象のポリシー形式
7.7以降	1.1	7 モードのサポートがすべての NetBackup 7.7 レプリケーションディレクタ機能に提供されます。	1 つのマスターサーバーは多数の 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 モードのサポートがすべての NetBackup 7.7 レプリケーションディレクタ機能に提供されます。	1 つのマスターサーバーは多数の 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 つのマスターサーバーは多数の OCUM サーバーをサポートします。 プラグインは、OCUM サーバー、マスターサーバー、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。すべてのマスターサーバー、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

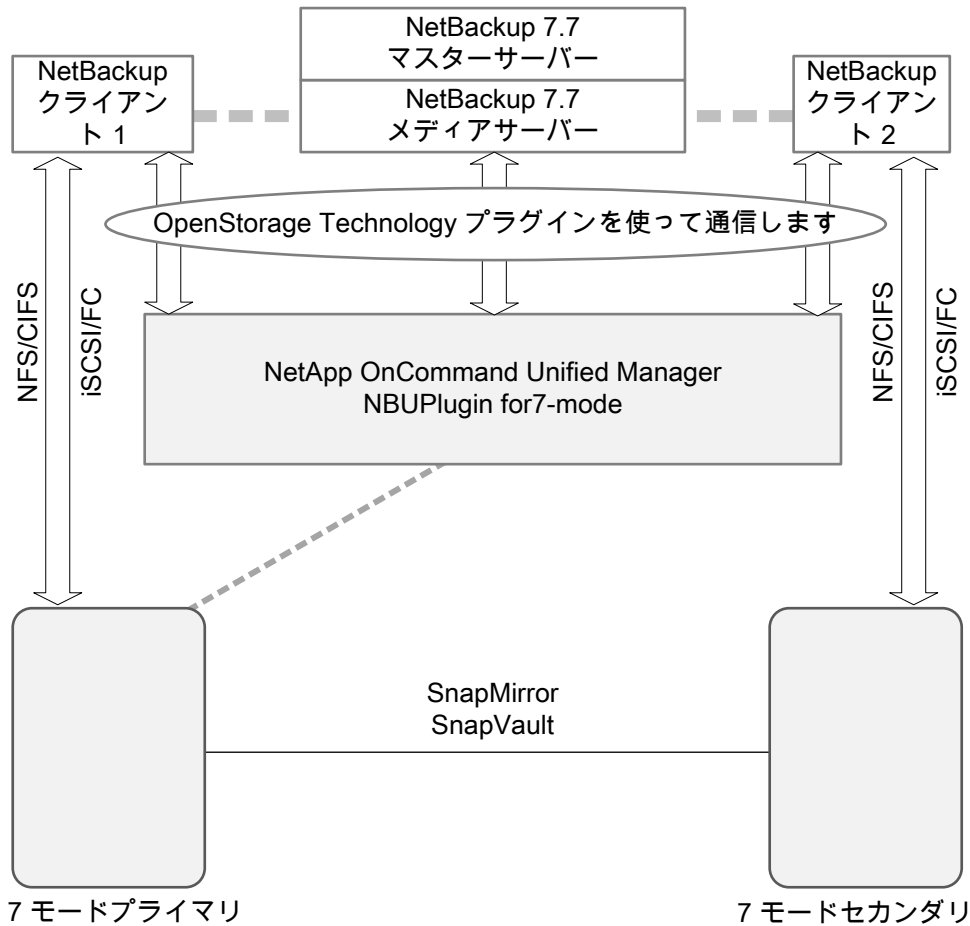
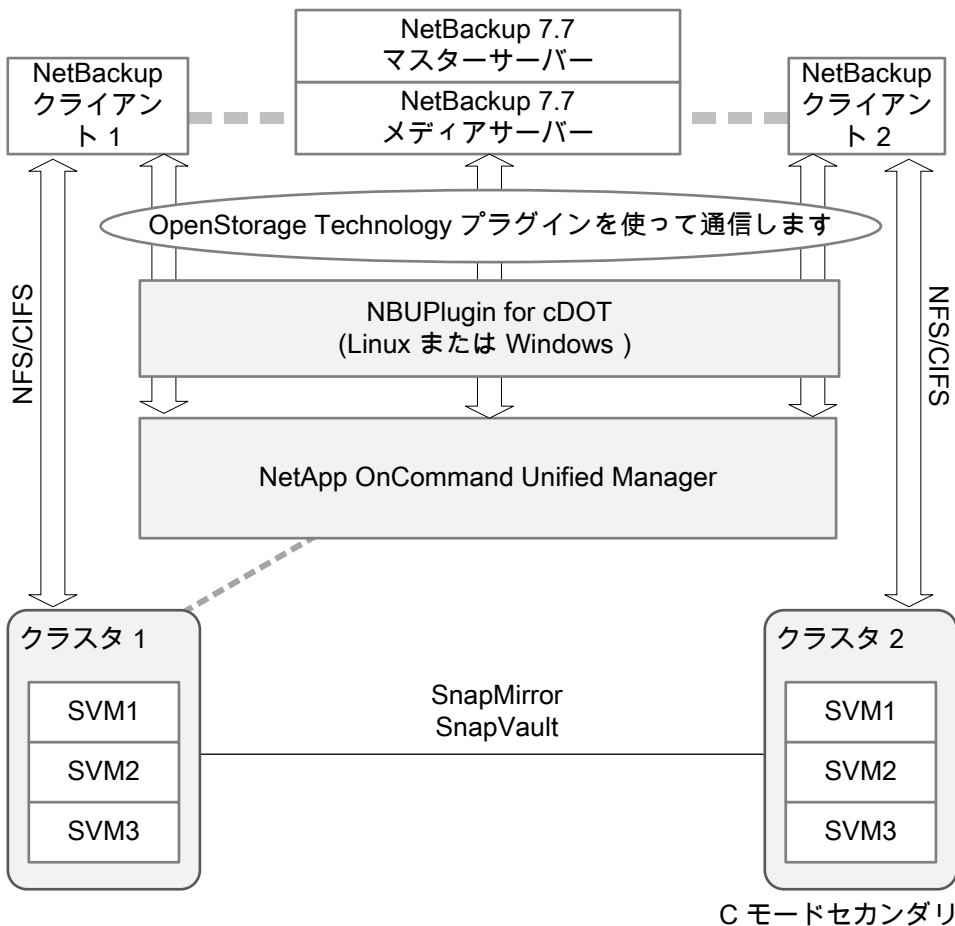


図 A-2 NetBackup と NBUPlugin for Clustered Data ONTAP 間の通信



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: `Install_path\Program Files\Netapp\NBUPlugin\version.txt`

UNIX: `/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: %NetBackup%\bin\admincmd>nbstlutil.exe stlilist -U

UNIX の場合: /usr/opensv/netbackup/bin/admincmd/nbstlutil stlilist -U

NetBackup のバージョン間の互換性について

マスターサーバー、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。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。NetBackup カタログは NetBackup マスターサーバー上に存在します。したがって、マスター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、マスターサーバーと同じ 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 8.1 でも、マスターサーバーを最初にアップグレードするという従来の必要条件に従うことが重要です。その後、8.1 クライアントをサポートするために必要なすべてのメディアサーバー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、すべてのメディアサーバーをアップグレードすることをお勧めします。すべてのマスターサーバーとすべてのメディアサーバーを NetBackup 8.1 にアップグレードしたら、クライアントを 8.1 にアップグレードします。8.1 より前のメディアサーバーは、NetBackup 8.1 クライアントをバックアップまたはリストアできません。

NetBackup バージョン間の互換性について詳しくは、ベリタスの SORT の Web サイトを参照してください。

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

ベリタスは EOSL 情報をオンラインで確認することをお勧めします。

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

p.124 の「NetBackup ソフトウェアの入手について」を参照してください。

UNIX および Linux のインストールおよびアップグレード要件

表 A-5は NetBackup のインストールのために 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 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.18 の「Veritas Services and Operations Readiness Tools について」を参照してください。

表 A-5 UNIX および Linux での NetBackup のインストールおよびアップグレード要件

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 Compatibility List (SCL)』を参照してください。 http://www.netbackup.com/compatibility https://sort.veritas.com/netbackup
	メモリ	■ 複数のデータベースエージェントが有効になっている本番環境のマスターサーバーごとに、最低 16 GB のメモリと 4 つのコアを搭載する必要があります。 NetBackup ではメモリの最小要件は適用されません。ただし、少なくとも最小限の推奨メモリを使用することをお勧めします。最小限の推奨メモリを使用しないと、許容できないほどパフォーマンスが低下する場合があります。 ■ 複数のデータベースエージェントが有効になっている本番環境のメディアサーバーごとに、最低 4 GB のメモリを搭載する必要があります。
	ディスク領域	■ 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 8.2 ■ 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 カタログはマスター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、root 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 root 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 8.2』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。root 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	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に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 ■ insserv-compat ■ 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	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 マスターサーバーには、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、各マスターサーバー（またはクラスタ化されたマスター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。詳細情報を参照できます。 p.106 の「NetBackup マスターサーバー 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。マスター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。 https://www.veritas.com/support/ja_JP/article.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 <code>nbwebsvc</code> およびグループアカウント <code>nbwebgrp</code> 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 <code>root</code> 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 <code>/tmp/NBInstallAnswer.conf</code> 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。 <pre>WEBSVC_USER=custom_user_account_name</pre> 4 次に示す行を追加して、デフォルトの Web サーバークラスタグループアカウント名を上書きします。 <pre>WEBSVC_GROUP=custom_group_account_name</pre> 5 ファイルを保存して閉じます。

チェック	要件	詳細
	Veritas Smart Meter のカスタム登録キー	NetBackup 8.1.2 以降、Veritas Smart Meter のカスタム登録キーを指定する必要があります。Veritas Smart Meter に関する詳しい情報を参照できます。 p.10 の「Veritas Smart Meter 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 <code>veritas_customer_registration_key.json</code> 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、カスタム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 クラスタのインストールおよびアップグレード要件

表 A-6 は 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 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.18 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でない場合、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、マスター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-6 Windows および Windows クラスタでの NetBackup のインストールおよびアップグレード要件

チェック	要件	詳細
	オペレーティングシステム	■ 最新のオペレーティングシステムパッチと更新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	■ 本番環境では、マスターサーバーにも最低 16 GB のメモリと 4 つ のコアを搭載する必要があります。 NetBackup ではメモリの最小要件は適用されません。ただし、少なくとも最小限の推奨メモリを使用することをお勧めします。最小限の推奨メモリを使用しないと、許容できないほどパフォーマンスが低下する場合があります。 ■ 複数のデータベースエージェントが有効になっている本番環境のメディアサーバーごとに、最低 4 GB のメモリを搭載する必要があります。
	ディスク領域	■ NTFS パーティション。 ■ サーバ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 8.2 ■ アップグレードの場合は、Windows がインストールされているドライブに、さらに 500 MB のディスク領域が必要になります。アップグレードの完了後は、この領域は不要です。 ■ 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。 ■ 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 カタログはマスター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 2008 Server、Windows 2008 R2 Server、Windows 2012 R2、Windows 2012 (UAC 有効化)、Windows Server 2016 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 2008/2008 R2 Server/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。 Windows 2008 R2 の場合、クラスタは Enterprise と Data Center エディションでのみサポートされ、Standard エディションではサポートされません。 ■ 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 2008/2008 R2/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

チェック	要件	詳細
		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。 『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	マスター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る場合、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。 ■ 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、すべてのマスターサーバー、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	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に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.130 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 2008/2008 R2 Server Core、2012/2012 R2 Server Core でのインストール/Windows 2016	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.46 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。

チェック	要件	詳細
	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。
	Web サービス	NetBackup 8.0 より、NetBackup マスターサーバーには、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、各マスターサーバー（またはクラスタ化されたマスター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.106 の「NetBackup マスターサーバー 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: ペリタスは、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。マスター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は詳しくは、次をご覧ください。 https://www.veritas.com/support/ja_JP/article.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、インストール時にマスターサーバーの 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

チェック	要件	詳細
	外部認証局	マスターサーバー (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
	Veritas Smart Meter のカスタム登録キー	NetBackup 8.1.2 以降、Veritas Smart Meter のカスタム登録キーを指定する必要があります。Veritas Smart Meter に関する詳しい情報を参照できます。 p.10 の「Veritas Smart Meter 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 <code>veritas_customer_registration_key.json</code> 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、カスタム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.131 の「[UNIX および Linux のインストールおよびアップグレード要件](#)」を参照してください。

Windows クラスタのインストールとアップグレードの要件

通常のサーバー要件に加えて、NetBackup のクラスタインストールは特別な配慮を必要とします。

次に、Windows システムで NetBackup のクラスタインストールおよびアップグレードを行う場合のガイドラインを記述します。

表 A-7 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	
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。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)	
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。

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、『**NetBackup 管理者ガイド Vol. 1**』で詳しく説明しています。『**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。

NetBackup OpsCenter サーバーと NetBackup マスターサーバー間の接続の無効化

NetBackup OpsCenter サーバーをアップグレードする前に NetBackup マスターサーバーをアップグレードする必要がある場合、マスターサーバーと OpsCenter サーバー間の関係を無効にすることができます。

制限事項とデータ収集の無効化に関連する潜在的なデータ損失の懸念事項に注意してください。

- Veritas では、OpsCenter より上位のバージョンの NetBackup マスターサーバーとの OpsCenter のデータ収集はサポートしません。OpsCenter は、NetBackup マスターサーバーより上位または同じバージョンである必要があります。
- マスターサーバーの OpsCenter データ収集が無効化されると、OpsCenter はアラートまたは OpsCenter レポートの新しいデータを受信しません。データ収集が無効化される前に収集されたデータは、その後も OpsCenter レポートで利用可能です。
- OpsCenter をアップグレードし、データ収集を有効にすると、OpsCenter はマスターサーバーの新しいアラートやレポートの新しいデータを受信します。OpsCenter では、データがまだマスターサーバー上で利用可能な場合にのみ、データ収集が無効になった時のデータを収集します。マスターサーバーのジョブ保持レベルがデータ収集が無効になっている時間より短い場合は、データのレポートとアラートが失われます。

マスターサーバーと OpsCenter サーバー間の接続を無効にするには

- 1 OpsCenter でのデータ収集を無効にします。

[設定 (Settings)] > [構成 (Configuration)] > [NetBackup] > [アップグレードする NetBackup マスターサーバー (NetBackup Master Server)] > [データ収集の無効化 (Disable Data Collection)]

- 2 NetBackup マスターサーバーをアップグレードします。

これで NetBackup および OpsCenter のどちらも動作できますが、OpsCenter には完全なデータがありません。

マスターサーバーと OpsCenter サーバー間の接続を有効にするには

- 1 OpsCenter をアップグレードします。

- 2 OpsCenter のアップグレードが正常に完了したら OpsCenter でのデータ収集を有効にします。

[設定 (Settings)] > [構成 (Configuration)] > [NetBackup] > [アップグレードする NetBackup マスターサーバー (NetBackup Master Server)] > [データ収集の有効化 (Enable Data Collection)]

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。マスターサーバーで 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、『Veritas 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)]、[クレデンシヤル (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`

記号

アップグレード

マスターサーバー 31

メディアサーバー 58

自動ファイル変更 17

計画 13~14

アップグレード方式 32、53

インストール要件

UNIX システムおよび Linux システム 131

Windows システム 134

カタログバックアップ

制限事項 16

クラスタ

プライベートネットワーク 44

クラスタのインストールおよびアップグレード

要件 141

サーバー

Windows でのサイレントアップグレード 46

サーバーのインストール

Linux の要件 132

Red Hat Linux の要件 132

サーバーのインストール要件

Linux 132

Red Hat Linux 132

サーバーソフトウェアのアップグレード

サーバーソフトウェア 50

セキュリティ証明書

NetBackup ホスト用 16

ドメインネームサービス (DNS) 132

ネットワーク情報サービス (NIS) 132

バージョン、NetApp NBUPugin の判断 127

バージョンの混在のサポート

NetBackup 8.x 130

プライベートネットワーク

クラスタ 44

プラグイン

NetApp 127

NetApp からのアップグレード 130

プリインストールチェッカー

概要 25

マスターサーバー

アップグレード 31

メディアサーバー

アップグレード 58

ユーザーアカウント

Web サーバー 26

ローカル、リモート、クラスタ化されたアップグレード

Windows システム 36

制限事項

カタログバックアップ 16

変更

NetBackup 8.2 10

推奨アップグレード手順

Veritas Operations Readiness Tools 19

概要

UNIX と Linux のインストール要件 131

プリインストールチェッカー 25

自動イメージレプリケーション

Bare Metal Restore

エラー 30

自動ファイル変更

アップグレード後 17

要件

クラスタのインストールおよびアップグレード 141

証明書。「セキュリティ証明書」を参照

認証証明書。「セキュリティ証明書」を参照

B

Bare Metal Restore

自動イメージレプリケーション

エラー 30

H

hosts ファイル 132

N

NBUPugin

アップグレード 130

バージョンの判別 129

NetBackup 8.2

変更 10

NetBackup 8.x

バージョンの混在のサポート 130

NetBackup 電子ソフトウェア配布 (ESD) イメージ 124

S

SORT

Veritas Operations Readiness Tools 19

Veritas Operations Readiness Tools 21

Veritas Services and Operations Readiness
Tools 18

U

UNIX と Linux のインストール要件

概要 131

UNIX システムおよび Linux システム

インストール要件 131

V

Veritas Operations Readiness Tools (SORT)

推奨アップグレード手順 19

Veritas Operations Readiness Tools (SORT)

推奨インストール手順 21

Veritas Services and Operations Readiness Tools
(SORT)

概要 18

W

Web サーバー

ユーザーアカウント 26

Windows でのサイレントアップグレード

サーバー 46

Windows システム

インストール要件 134

クラスターのインストールおよびアップグレード要件 141

ローカル、リモート、クラスタ化されたアップグレー
ド 36

か

概要

Veritas Services and Operations Readiness
Tools 18

さ

推奨インストール手順

Veritas Operations Readiness Tools 21