Veritas NetBackup™ Appliance アップグレードガイド

リリース 4.1

VERITAS™

Veritas NetBackup™ Appliance アップグレードガイド

最終更新日: 2021-07-19

法的通知と登録商標

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

この製品には、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入手できます。

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

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

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、この文書の供給、履行、または使用に関連して付随的または間接的に起こる損害に対して責任を負いません。本書に記載の情報は、予告なく変更される場合があります。

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートは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 でベリタスアカウント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てください。

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

マニュアル

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

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

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。

APPL.docs@veritas.com

次のベ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

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

ベリタスの 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 6

NetBackup appliance ソフトウェアバージョン 4.1 へのアップグレードについて 6
サポート対象のアップグレードパス 6
対応する NetBackup ソフトウェアのバージョンについて 7
アプライアンスインストールマネージャについて 7

第 2 章 アップグレードプラン 9

NetBackup Appliance をアップグレードするための要件およびベストプラクティス 9
NetBackup Appliance の HA 設定のアップグレードについて 13
アップグレードの推定所要時間 15

第 3 章 アップグレードの実行 16

アプライアンスのソフトウェアリリース更新をダウンロードする方法 16
NetBackup Appliance Web コンソールを使用した NetBackup Appliance へのソフトウェア更新のダウンロード 17
NetBackup Appliance へのソフトウェア更新の直接ダウンロード 18
クライアント共有を使用した NetBackup Appliance へのソフトウェア更新のダウンロード 18
NetBackup Appliance シェルメニューを使用した NetBackup appliance ソフトウェア更新のインストール 20

第 4 章 アップグレード後のタスク 26

アップグレード後のタスク 26

第 5 章 VxUpdate を使用した NetBackup クライアントのアップグレード 27

VxUpdate について 27
VxUpdate リポジトリの管理 28
配備ポリシーの管理 31
VxUpdate を使用したプライマリサーバーからのアップグレードの手動による開始 36

VxUpdate を使用したクライアントからのアップグレードの手動による開始 40
配備ジョブの状態 42

第 6 章 トラブルシューティング 44
アップグレードの問題のトラブルシューティング 44

索引 45

1

概要

この章では以下の項目について説明しています。

- NetBackup appliance ソフトウェアバージョン 4.1 へのアップグレードについて

NetBackup appliance ソフトウェアバージョン 4.1 へのアップグレードについて

SSH セッションまたは IPMI コンソールを使用して NetBackup Appliance シェルメニューにログインし、アプライアンスをアップグレードします。バージョン 3.1 以降からアップグレードする場合は、Appliance Management Console も使用できます。高可用性 (HA) 設定のノードをアップグレードするには、NetBackup Appliance シェルメニューを使用する必要があります。Appliance Management Console では、HA ノードのアップグレードはサポートされていません。

アップグレードを開始する前に、次のトピックを確認してください。

p.6 の「サポート対象のアップグレードパス」を参照してください。

p.13 の「NetBackup Appliance の HA 設定のアップグレードについて」を参照してください。

p.7 の「対応する NetBackup ソフトウェアのバージョンについて 」を参照してください。

p.7 の「アプライアンスインストールマネージャについて」を参照してください。

サポート対象のアップグレードパス

- 直接アップグレードパス
  - バージョン 3.1.1、3.1.2、3.2、3.3.0.1、4.0 のソフトウェアを搭載した 5240、5330、または 5340 Appliance
  - バージョン 3.2、3.3.0.1、および 4.0 のソフトウェアを搭載した 5250 Appliance
  - バージョン 4.0 のソフトウェアを搭載した 5350 Appliance

- 2 段階のアップグレードパス
  バージョン 31 以前のソフトウェアを搭載したアプライアンスをバージョン 4.1 にするには、2 回のアップグレードが必要です。これらのシステムは、まずバージョン 3.2 または 3.3.0.1 にアップグレードしてから、バージョン 4.1 にアップグレードすることをお勧めします。

対応する NetBackup ソフトウェアのバージョンについて

NetBackup ソフトウェアバージョン 9.1 は NetBackup appliance リリース 4.1 に付属しています。表 1-1 に、最新の NetBackup appliance のソフトウェアリリースに対応する NetBackup のバージョンを示します。

表 1-1 Appliance のソフトウェアリリースおよび対応する NetBackup ソフトウェアのバージョン

Appliance ソフトウェアのリリース	NetBackup ソフトウェアのバージョン
3.0	8.0
3.1	8.1
3.1.1	8.1.1
3.1.2	8.1.2
3.2	8.2
3.3.0.1	8.3.0.1
4.0	9.0
4.1	9.1

アプライアンスインストールマネージャについて

3.1 以降のリリースでは、[アプライアンスインストールマネージャ (Appliance Install Manager)](AIM) ウィンドウに切り替えて、アップグレードの進行状況を表示できます。このウィンドウには、推定完了時間、アップグレードの進捗バー、主なアップグレード手順、アップグレードログ、その他の便利な情報が表示されます。

アップグレード中に IPMI コンソールからシェルメニューにログオンする場合は、ソフトキーボードで Alt+F2 キーを押して[AIM]ウィンドウを開きます。

AIM ウィンドウは、アップグレードを開始するとすぐに表示され、次のビューモードを提供します。

- メイン (Main)
  このデフォルトビューには、主なアップグレード手順とタスクの結果が表示されます。

- ［詳細 (Verbose)］
  このビューには、詳細なアップグレードログが表示されます。

［メイン (Main)］ビューから［詳細 (Verbose)］ビューに切り替えるには、V キーを押します。

［詳細 (Verbose)］ビューから［メイン (Main)］ビューに切り替えるには、M キーを押します。

アップグレードを一時停止するには、P キーを押します。

AIM ウィンドウを閉じてシェルメニューに戻るには、S キーを押します。

AIM ウィンドウをもう一度表示するには、次のコマンドを入力します。

```
Main_Menu > Manage > Software >UpgradeStatus
```

2

アップグレードプラン

この章では以下の項目について説明しています。

- NetBackup Appliance をアップグレードするための要件およびベストプラクティス

NetBackup Appliance をアップグレードするための要件およびベストプラクティス

このトピックでは、アプライアンスソフトウェアのアップグレードを計画する際に参照すべき要件とベストプラクティスについて説明します。

- 現在、アプライアンス環境でソフトウェアバージョン 3.1.1、3.1.2、3.2、3.3.0.1、または 4.0 を使用していることを確認します。これらのバージョンのみがバージョン 4.1 への直接アップグレードをサポートしています。

  メモ: NetBackup RBAC ユーザーが存在するバージョン 3.1.2 または 3.2 のアプライアンスをアップグレードする場合は、アップグレード完了後、NetBackup 8.3 RBAC Roles ユーティリティをダウンロードして実行する必要があります。詳しくは、次の記事を参照してください。

  https://www.veritas.com/support/en_US/article.100047577

  https://www.veritas.com/support/en_US/article.100047660

- ソフトウェアバージョン 3.1 以降では、Appliance Management Console からアップグレードを実行できます。ソフトウェアバージョン 2.7.3 および 3.0 を使用するアプライアンスでは、コンソールを使用したアップグレードもサポートされています (アップグレード前に適切な EEB がインストールされている場合)。すべてのアップグレードガイドラインを確認して、アップグレード前に必要な操作を実行したら、『Veritas Appliance Management ガイド』のアップグレードの手順を参照してください。

メモ: Appliance Management Console は、現在、HA 設定のアプライアンス (ノード) のアップグレードをサポートしません。これらのアプライアンスのアップグレードには NetBackup Appliance シェルメニューを使用する必要があります。

- アップグレードする前に必ず完全なディザスタリカバリ (DR) バックアップを実行します。
  - プライマリサーバー
    最新の完全な NetBackup カタログバックアップがあることを確認します。
  - MSDP の構成
    重複排除プールのカタログバックアップポリシーを構成し、バックアップを正常に実行します。詳しくは、次の記事を参照してください。
    https://www.veritas.com/support/en_US/article.100046592
- IPsec 証明書をエクスポートして再インポートします。
  アップグレードするいずれかの Appliance で IPSec 機能を設定している場合、アップグレードの完了後に IPsec 証明書が保持されない可能性があります。この問題を回避するには、アプライアンスをアップグレードする前に IPsec 証明書をエクスポートする必要があります。`Network > Security > Export` コマンドを使用してこのタスクを実行します。`Export` コマンドは、このコマンドを実行するときに指定した場所に 2 つの `.pfx` ファイル (`serialnumber.pfx` と `.serialnumber.pfx`) をコピーします。

  次のように、アップグレードする前に IPsec 証明書をエクスポートします。
  - NetBackup Appliance シェルメニューにログインして、次のビューに移動します。
    `Network > Security > Export`
  - 次のエクスポートオプションの詳細を入力します。
    `Export [EnterPasswd][PathValue]`
    [EnterPasswd] は、[パスワードを入力しますか? (Do you want to enter a password?)]という質問への回答に使うフィールドです。yes または no を入力する必要があります。
    [PathValue] は、エクスポートした証明書を保存する場所です。
  - エクスポートが完了したら、アプライアンス以外の場所に両方の `.pfx` ファイルのバックアップを作成します。
    アップグレードが完了したら、IPsec 証明書を再インポートします。
    p.26 の「アップグレード後のタスク」を参照してください。
- 以前にダウンロードしたリリースアップデート、クライアントパッケージ、クライアントアドオンを削除します。
  アップグレード中に `/inst` パーティションに十分な容量を確保するため、以前にダウンロードしたリリースの更新、クライアントパッケージ、およびクライアントアドオンのす

べてをアプライアンスから削除します。ベストプラクティスとして、すべての Appliance およびクライアントをアップグレードした後に、ダウンロードしたパッケージを必ず削除してください。

以前にダウンロードしたパッケージを削除しておらず、アプライアンスの /inst ディレクトリに十分な空き領域がない場合、プレフライトチェックと Appliance Upgrade Readiness Analyzer ツールにより、アップグレードが拒否されます。アップグレードを開始するための十分な領域があっても、古いクライアントのアドオンが削除されていないとアップグレードが失敗する場合があります。高可用性 (HA) ノードでパッケージをダウンロードした場合は、両方のノードからパッケージを削除する必要があります。

NetBackup Appliance Web コンソール

- アップグレードするアプライアンスで、[管理 (Manage)]、[ソフトウェアアップデート (Software Updates)]の順に選択します。
- [ダウンロードしたソフトウェアアップデート (Downloaded Software Updates)]表で、リスト内のリリースアップデート、クライアントパッケージ、またはクライアントのアドオンの左にあるラジオボタンをクリックし、[削除 (Delete)]をクリックします。

NetBackup Appliance シェルメニュー

- アップグレードするアプライアンスで `Manage > Software > List Downloaded` コマンドを入力して、ダウンロードしたリリースアップデートおよびクライアントパッケージのすべてを確認します。
- ダウロードした各リリースの更新およびクライアントパッケージを削除するには、コマンド `Manage > Software > Delete` *update_name* を入力します。*update_name* はリリースアップデートまたはクライアントパッケージのファイル名です。
- すべてのダウロードしたクライアントのアドオンの一覧を表示するには、コマンド `Manage > Software > List AddOns` を入力します。
- ダウロードした各クライアントのアドオンを削除するには、コマンド `Manage > Software > Rollback` *eeb_name* を入力します。*eeb_name* はクライアントのアドオンのファイル名です。

  メモ: クライアントのアドオンのファイル名を入力するときは、`.rpm` 拡張子を含める必要があります。

- アプライアンスの場合も、従来の NetBackup のアップグレードと同じアップグレードの順序に従います。NetBackup OpsCenter を使用する場合は、最初にアップグレードします。次に、アプライアンスのアップグレードをプライマリサーバーアプライアンスから始めて、その後すべてのメディアサーバーアプライアンスをアップグレードします。
- 複数のメディアサーバーをアップグレードする場合は、個別のメディアサーバーごとにアップグレードプロセスを実行する必要があります。

  HA 設定のアプライアンスメディアサーバー (ノード) は、一度に 1 台ずつ更新します。両方のノードで、同じアプライアンスソフトウェアバージョンを使用している必要があります。1 台のノードをアップグレードしたら、他方のノードをすぐにアップグレードする必要があります。

p.13 の「NetBackup Appliance の HA 設定のアップグレードについて」を参照してください。

- 従来の NetBackup プライマリサーバーがアプライアンスメディアサーバーと併用されている場合、そのプライマリサーバーにはメディアサーバーアプライアンスと同じか、それ以降のバージョンの NetBackup が必要です。たとえば、メディアサーバーアプライアンスをバージョン 4.1 にアップグレードする前に、まず NetBackup プライマリサーバーをバージョン 9.1 にアップグレードします。
  p.7 の「対応する NetBackup ソフトウェアのバージョンについて 」を参照してください。
- アプライアンスのメディアサーバーアップグレードの間、NetBackup プライマリサーバーがアクティブで動作していることを確認します。さらに、NetBackup のプロセスがプライマリサーバーとメディアサーバーの両方で開始されているか、または実行されていることを確認します。
- STIG 機能が有効になっているアプライアンスをアップグレードするか、このアプライアンスに EEB をインストールする必要がある場合、午前 4 時から午前 4 時半の間には計画しないでください。このベストプラクティスに従うと、AIDE データベースと監視対象ファイルの自動アップデートの中断を防ぐことができます。自動アップデートが中断されると、アプライアンスで複数の警告メッセージが生成される可能性があります。
- NetBackup クライアントではアプライアンスと同じか、またはそれ以前のソフトウェアバージョンを使用する必要があります。クライアントはアプライアンスよりも新しいバージョンでは動作できません。たとえば、NetBackup バージョン 9.1 のクライアントは、バージョン 4.1 以降のアプライアンスサーバーのみで使用できます。クライアントのアドオンもクライアントバージョンと同じにする必要があります。
  p.7 の「対応する NetBackup ソフトウェアのバージョンについて 」を参照してください。
- NetBackup Appliance シェルメニュー または Appliance Management Console (AMS) を使用したバージョン 3.2 以降へのアップグレードでは、ECA の配備はサポートされません。アップグレードが正常に完了したら NetBackup の ECA を有効にできます。詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。さらに、mongodb、tomcat、nginx などのアプライアンスインフラストラクチャサービスに ECA を構成できます。詳しくは、『NetBackup Appliance セキュリティガイド』を参照してください。
- アプライアンスソフトウェアバージョン 4.0 以降、ゲストユーザーと既存のローカルユーザーはユニバーサル共有または CIFS 共有にアクセスできません。バージョン 4.0 以降にアップグレードした後、次の操作により、これらの共有へのアクセス権を付与できます。
  - ゲストユーザー: 新しいローカルユーザーを作成してゲストユーザーを置き換えます。
  - 既存のローカルユーザー: これらのユーザーのパスワードを変更します。

- NetBackup 管理コンソールの互換性のあるバージョンを使用して、NetBackup サービスを管理します。
  NetBackup 管理コンソールには後方互換性があります。パッチリリース (x.x.x.x) コンソールは、1 番目と 2 番目の数字が同一の NetBackup のメジャーリリース (x.x) またはマイナーリリース (x.x.x) と互換性があります。

NetBackup Appliance の HA 設定のアップグレードについて

高可用性 (HA) 設定のノードのアップグレード要件を次に示します。

- NetBackup Appliance シェルメニュー
  このインターフェースを使用して、ノードをアップグレードします。

  メモ: Appliance Management Console では、HA ノードのアップグレードはサポートされていません。

- HA 設定の 1 つまたは 2 つのノード
  HA ノードは、HA 設定内からアップグレードする必要があります。HA 設定からノードを削除する場合、残りのノードを引き続きアップグレードできます。
- 一度に 1 台のノード
  他のノードで作業を続行できるようにするため、一度に 1 台のノードのみをアップグレードできます。
- 1 つのソフトウェアバージョン
  両方のノードで、同じアプライアンスソフトウェアバージョンを使用している必要があります。1 台のノードをアップグレードしたら、他方のノードをすぐにアップグレードする必要があります。
- ノードのアップグレード順序
  MSDP サービスと仮想 IP サービスがオフラインになっているノード (通常はパートナーノード) でアップグレードプロセスを開始します。

  最初のノードでアップグレードが完了した後、次のタスクをすぐに順序どおりに実行します。

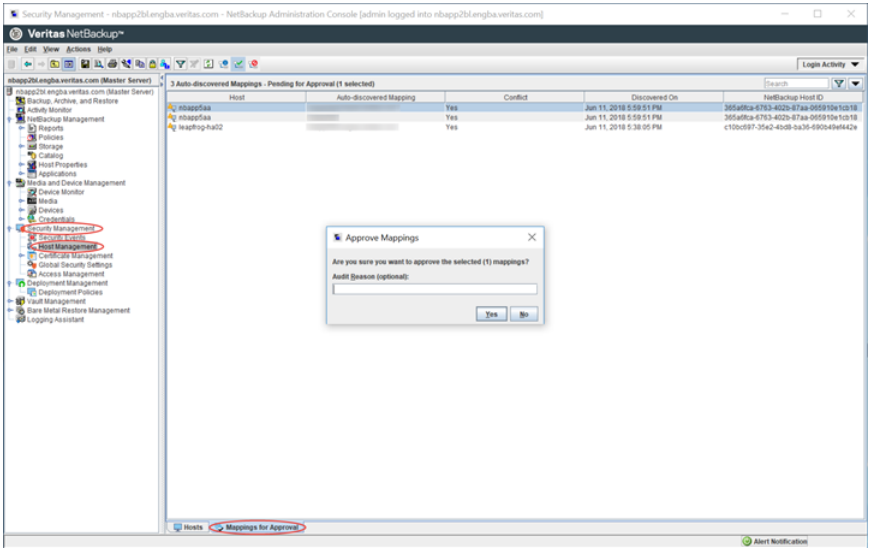
  - アップグレードされたノードで `Support > Test Software` コマンドを実行して、各種アプライアンスソフトウェアコンポーネントの状態を検証します。
  - テストに合格したら、もう一方のノードにログインし、最初のノードと同じ方法でアップグレードします。
- MSDP の構成
  リリース 4.0 以降、MSDP ストレージが構成されていなくても、HA ノードをアップグレードできます。
- NetBackup Appliance シェルメニューでのパッケージのダウンロード

rpm パッケージをダウンロードする必要があるのは 1 台のノードだけです。パッケージをダウンロードした HA ノードで `Manage > Software > List Downloaded` コマンドを実行した後、他方のノードでコマンドを実行してパッケージを利用できるようにします。

- ホスト名マッピングの承認
  ソフトウェアバージョン 3.1.1 以前からアップグレードする前に、関連付けられているプライマリサーバーの NetBackup 管理コンソールで、HA アプライアンスのホスト名マッピングを承認する必要があります。承認しなかった場合、プレフライトチェックでアップグレードを開始できません。

  ホスト名マッピングを承認するには、次の操作を行います。

  - 関連付けられているプライマリサーバーで、NetBackup 管理コンソールにログインします。
  - 左ペインで[セキュリティ管理 (Security Management)]をクリックしてプロパティを展開し、[ホスト管理 (Host Management)]をクリックします。
  - 右ペインの左下で、[承認のマッピング (Mappings for Approval)]をクリックします。
  - 右ペインの上部で、承認が保留状態となっている任意のホストマッピングをクリックします。承認を求める[マッピングの承認 (Approve Mappings)]ダイアログボックスが表示されたら、[はい (Yes)]をクリックします。承認が保留状態となっている各ホストマッピングについて、このタスクを繰り返します。



アップグレードの推定所要時間

アプライアンスのアップグレードには、ハードウェア構成と現在のソフトウェアバージョンに応じて、1.5 時間から 2.5 時間かかる場合があります。

メモ: 上記の推定時間は、すべてのサポートされている直接アップグレードパスからアップグレードする場合のラボテストの結果に基づいています。実際にアップグレードにかかる時間は構成された環境の複雑さによって異なる場合があります。

3

アップグレードの実行

この章では以下の項目について説明しています。

- アプライアンスのソフトウェアリリース更新をダウンロードする方法
- NetBackup Appliance シェルメニューを使用した NetBackup appliance ソフトウェア更新のインストール

アプライアンスのソフトウェアリリース更新をダウンロードする方法

NetBackup Appliance リリース 3.2 以降、リリース更新はベリタスダウンロードセンターの Web サイトから入手できます。

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

アプライアンスソフトウェアとクライアントパッケージは、共有から手動でダウンロードできます。アップグレードを開始する前に、最初に更新をアプライアンスにダウンロードする必要があります。

以降では、アプライアンスのソフトウェアリリース更新をダウンロードする場合に使用する方法について説明します。

- 「NetBackup Appliance Web コンソールを使用した NetBackup Appliance へのソフトウェア更新のダウンロード」
- 「NetBackup Appliance へのソフトウェア更新の直接ダウンロード」
- 「クライアント共有を使用した NetBackup Appliance へのソフトウェア更新のダウンロード」

NetBackup Appliance Web コンソールを使用した NetBackup Appliance へのソフトウェア更新のダウンロード

NetBackup Appliance Web コンソールを使用してアプライアンスにソフトウェアリリースの更新をダウンロードするには、次の手順を使用します。

NetBackup Appliance Web コンソールを使用してアプライアンスにソフトウェアリリースの更新をダウンロードするには

1. Web ブラウザを開いて、NetBackup Appliance Web コンソールでアプライアンスにログオンします。
2. [管理 (Manage)]、[ソフトウェアの更新 (Software Updates)]の順に選択します。
3. [ソフトウェアの更新 (Software Updates)]ページの[ダウンロードしたソフトウェア更新 (Downloaded Software Updates)]テーブルで、ソフトウェア更新がまだダウンロードされていないことを確認します。
   - インストールするソフトウェア更新がテーブルにある場合、次のソフトウェアのインストールに進みます。
     p.20 の「NetBackup Appliance シェルメニューを使用した NetBackup appliance ソフトウェア更新のインストール」を参照してください。
   - インストールするソフトウェア更新がテーブルにない場合、次の手順に進みます。
4. ページの[オンラインのソフトウェアアップデート (Online Software Updates)]テーブルで、ソフトウェアアップデートを選択し、[ダウンロード (Download)]をクリックします。

   [ダウンロードの進捗 (Download Progress)]列にダウンロードの状態が表示されます。ダウンロードが正常に完了すると、ソフトウェア更新が[ダウンロードしたソフトウェア更新 (Downloaded Software Updates)]テーブルの[利用可能なソフトウェア更新 (Available Software Update)]列に表示されます。

メモ: アプライアンスソフトウェアのバージョン 3.1 から、Web コンソールではアップグレードまたは EEB パッケージのインストールはサポートされていません。これらのパッケージを Web コンソールからダウンロードした後、NetBackup Appliance シェルメニューからインストールを実行する必要があります。

---

p.18 の「NetBackup Appliance へのソフトウェア更新の直接ダウンロード」を参照してください。

p.18 の「クライアント共有を使用した NetBackup Appliance へのソフトウェア更新のダウンロード」を参照してください。

NetBackup Appliance へのソフトウェア更新の直接ダウンロード

NetBackup Appliance シェルメニューを使用してアプライアンスにソフトウェアリリースの更新をダウンロードするには、次の手順を使用します。

高可用性 (HA) 設定の場合は、パッケージをダウンロードする必要があるのは 1 台のノードだけです。1 台目のノードでパッケージのダウンロードが完了したら、手順 4 を参照して他方のノードでパッケージを利用できるようにします。

ソフトウェアリリースの更新をアプライアンスに直接ダウンロードするには

1. NetBackup Appliance シェルメニューを使用し、管理者として SSH セッションを開き、アプライアンスにログオンします。
2. ソフトウェアの更新がベリタスのサポート Web サイトから利用可能かどうかを確認するには、次のコマンドを入力します。Veritas

   ```
   Main_Menu > Manage > Software > List AvailablePatch
   ```

3. 利用可能なアプライアンスのソフトウェアの更新をダウンロードするには、次のコマンドを入力します。

   ```
   Main_Menu > Manage > Software > Download
   SYMC_NBAPP_update-<release-version>.x86_64.rpm
   ```

   release はソフトウェアリリース番号、*version* はソフトウェアリリースのバージョン番号です。次に例を示します。

   ```
   Main_Menu > Manage > Software > Download
   SYMC_NBAPP_update-3.1.x86_64.rpm
   ```

4. rpm が正常にダウンロードされたことを確認するには、次のコマンドを入力します。

   ```
   Main_Menu > Manage > Software > List Downloaded
   ```

   パッケージをダウンロードした HA ノードでこのコマンドを実行した後、他方のノードでコマンドを実行してパッケージを利用できるようにします。

p.9 の「NetBackup Appliance をアップグレードするための要件およびベストプラクティス」を参照してください。

p.18 の「クライアント共有を使用した NetBackup Appliance へのソフトウェア更新のダウンロード」を参照してください。

クライアント共有を使用した NetBackup Appliance へのソフトウェア更新のダウンロード

CIFS や NFS のクライアント共有を使用してアプライアンスにソフトウェアリリースの更新またはクライアントパッケージをダウンロードするには、この手順を使用します。

高可用性 (HA) 設定の場合は、パッケージをダウンロードする必要があるのは 1 台のノードだけです。1 台目のノードでパッケージのダウンロードが完了したら、手順 7 を参照して他方のノードでパッケージを利用できるようにします。

メモ: アプライアンスに直接ソフトウェアの更新をダウンロードすることに失敗した場合は、この方法を使用して、アプライアンス上にアプライアンスソフトウェアリリースの更新またはクライアントパッケージをダウンロードできます。

アプライアンスとインターネットに接続済みであるコンピュータからこの手順を実行します。ベリタスダウンロードセンターからファイルやパッケージをダウンロードするには、インターネットにアクセスする必要があります。

CIFS または NFS のクライアント共有を使用してアプライアンスにソフトウェアリリースの更新またはクライアントパッケージをダウンロードするには:

1. NetBackup Appliance シェルメニューを使用し、管理者として SSH セッションを開き、アプライアンスにログオンします。
2. NFS または CIFS 共有を開くには、次のコマンドを入力します。

   ```
   Main_Menu > Manage > Software > Share Open
   ```

3. アプライアンス共有ディレクトリを次のようにマップまたはマウントします。
   - Windows CIFS 共有

     ```
     ¥¥<appliance-name>¥incoming_patches
     ```

   - UNIX NFS 共有

     ```
     mkdir -p /mount/<appliance-name>
     mount <appliance-name>:/inst/patch/incoming
     mount/<appliance-name>
     ```

4. このリリースの更新またはクライアントパッケージをマウント済みの共有にコピーします。

   メモ: コピー処理の間は Appliance でコマンドを実行しないでください。コマンドを実行すると、コピー操作が失敗する可能性があります。

   ---

5. リリースの更新またはクライアントパッケージをマウント済みの共有に正常にコピーした後、共有ディレクトリをマップ解除するか、マウント解除します。
6. アプライアンスで次のコマンドを入力して NFS 共有と CIFS 共有を閉じます。

   ```
   Main_Menu > Manage > Software > Share Close
   ```

   共有を閉じる前に次のいずれかのコマンドを実行すると、ダウンロードしたリリースの更新またはクライアントパッケージは共有ディレクトリの場所から適切な場所に移動

します。ここで、NFS 共有と CIFS 共有がクローズになっていることを確認するには、Share Close コマンドを実行する必要があります。

- List Version
- List Details All
- List Details Base
- Share Open
- Share Close

7 アプライアンスで利用可能なリリースの更新またはクライアントパッケージを一覧表示するには、次のコマンドを入力して、ダウンロードファイルの名前を記録します。

```
Main_Menu > Manage > Software > List Downloaded
```

このコマンドを実行すると、リリースアップデートまたはクライアントパッケージを検証し、共有ディレクトリから適切な場所に移します。この移動が行われたことは通知されません。

パッケージをダウンロードした HA ノードでこのコマンドを実行した後、他方のノードでコマンドを実行してパッケージを利用できるようにします。

p.9 の「NetBackup Appliance をアップグレードするための要件およびベストプラクティス」を参照してください。

p.18 の「NetBackup Appliance へのソフトウェア更新の直接ダウンロード」を参照してください。

NetBackup Appliance シェルメニューを使用した NetBackup appliance ソフトウェア更新のインストール

次の手順を実行して、アプライアンスのアップグレードを開始します。

メモ: STIG 機能が有効になっているアプライアンスをアップグレードするか、このアプライアンスに EEB をインストールする必要がある場合、午前 4 時から午前 4 時半の間には計画しないでください。このベストプラクティスに従うと、AIDE データベースと監視対象ファイルの自動アップデートの中断を防ぐことができます。自動アップデートが中断されると、アプライアンスで複数の警告メッセージが生成される可能性があります。

NetBackup Appliance シェルメニューを使用してダウンロードしたリリース更新をインストールするには

1 次の更新とアップグレード前のタスクがすでに実行されていることを確認します。

- 必要なアップグレード前の更新がすべて完了した。4.1 アップグレードより前に必要な更新の一覧全体については、次の記事を参照してください。
  https://www.veritas.com/support/en_US/article.100046066
- すべてのジョブが停止または一時停止され、SLP も一時停止されている。
- `Support > Test Software` コマンドが実行され、Pass の結果が返されている。

2 IPMI コンソールから NetBackup Appliance シェルメニューにログインします。

メモ: Veritas SSH セッションの代わりに、IPMI コンソールからシェルメニューを使用してログインすることをお勧めします。IPMI コンソールは、Veritas Remote Manager インターフェースとも呼ばれます。Veritas Remote Manager へのアクセスおよび使用方法について詳しくは、『NetBackup Appliance ハードウェア取り付けガイド』を参照してください。

---

3 Appliance Upgrade Readiness Analyzer ツールの最新版をダウンロードして実行済みであることを確認します。Analyzer ツールで `Pass` の結果が生成されてから、次の手順に進む必要があります。

4 ソフトウェアリリース更新をインストールするには、次のコマンドを実行します。

```
Main_Menu > Manage > Software > Install patch_name
```

patch_name はインストールするリリース更新の名前です。このパッチ名がインストールするパッチであることを確認します。

5 プレフライトチェックを監視し、Check failed (チェックに失敗しました) メッセージが表示されていないか確認します。

- Check failed メッセージが表示されなければ、アップグレードを開始するための次の手順に進みます。
- Check failed メッセージが表示されたら、アップグレードはできません。報告されたエラーを解決します。アップグレードスクリプトを再度実行し、エラーが解決されたかどうかをプレフライトチェックにより検証します。
- Check failed メッセージで RHEL バージョンのサードパーティプラグインが見つからないと表示された場合は、プラグインを適切なベンダーから入手する必要があります。

6 すべてのプレフライトチェック項目にパスしたら、アップグレードを開始する前に、アップグレード中にエラーが発生した場合のアップグレードプロセスの対応方法をまず選択する必要があります。次のプロンプトが表示されます。

```
If an error occurs during the upgrade, do you want to

immediately enforce an automatic rollback? [yes, no]
```

自動ロールバックをただちに適用するには、yes と入力します。

アップグレードプロセスを一時停止し、エラーを調査するには、no と入力します。

7 すべてのプレフライトチェック項目にパスした後、アップグレードプロセスを開始するために、CA 証明書とホスト ID ベースの証明書を信頼する必要がある場合があります。

CA 証明書を信頼して配備するには、次の操作を実行してください。

- 次に示すように、CA 証明書の詳細を確認して yes と入力して、CA 証明書を信頼します。

```
To continue with the upgrade, verify the following CA
certificate detail and enter "yes" to trust the CA certificate.
CA Certificate Details:
     Subject Name : /CN=nbatd/OU=root@abc.example.com/O=vx
       Start Date : Jul 14 12:59:18 2017 GMT
      Expiry Date : Jul 09 14:14:18 2037 GMT
 SHA1 Fingerprint : 31:E9:97:2E:50:11:51:7C:D6:25:7F:32:86:3D:

                    6B:D5:33:5C:11:E2

>> Do you want to trust the CA certificate? [yes, no](yes)
```

- プライマリサーバーのセキュリティレベルが[最高 (Very High)]である場合、次に示す画面で認証トークンを手動で入力して、ホスト ID ベースの証明書をアプライアンスに配備する必要があります。

```
>> Enter token:
```

メモ: 新しいバージョンへの次回のアップグレードの前にアプライアンスに有効なホスト ID 証明書が存在しない場合、次回のアップグレードには再発行トークンが必要です。

- プライマリサーバーのセキュリティレベルが[高 (High)]または[中 (Medium)]である場合、認証トークンは必要ありません。ホスト ID ベースの証明書はアプライアンスに自動的に配備されます。

セキュリティ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』の「NetBackup のセキュリティ証明書」の章を参照してください。

8 プライマリサーバーをソフトウェアバージョン 3.1.1 以前からアップグレードする場合は、Veritas Usage Insights 登録キーを入力する必要があります。登録キーを取得するには、画面の指示に従って操作します。

9 AIM ウィンドウの表示前にアップグレードの状態を確認するには、次のコマンドを入力します。

```
Main_Menu > Manage > Software >UpgradeStatus
```

アップグレードプロセス中の最初の再起動の後、SSH を使用した方法ではアプライアンスにログインできないことがあります。この問題は、アップグレードの進行中に最大 2 時間続く場合があります。この期間もアップグレードプロセスの監視を続行するには、VMware Remote Console からアプライアンスにログインします。アップグレードプロセスによってすべての更新がインストールされると、ログインプロンプトが表示されます。

10 アップグレード後のセルフテストで問題が検出された場合、[AIM]ウィンドウにアップグレードの状態が[一時停止 (Paused)]として表示されます。他の SSH セッションおよび電子メール通知にも、この状態が示されます。

[一時停止 (Paused)]の状態をクリアするには、次のタスクを実行します。

- V キーを押すと[詳細 (Verbose)]ビューに切り替わり、ログが表示されます。エラーに Unique Message Identification (UMI) コードがある場合は、そのコードをベリタスのサポート Web サイトで検索し、詳細情報を確認します。
- [AIM]ウィンドウで報告される問題の解決を試みます。
  シェルメニューを使用する必要がある場合は、SSH セッションから NetBackup Appliance シェルメニューにログオンします。AIM ウィンドウが表示されたら、S キーを押してウィンドウを閉じます。
- IPMI コンソールの AIM ウィンドウに戻ります。
  問題の解決を試みた場合、A キーを押してセルフテストを再試行してください。問題を解決できない場合、ベリタスのサポートに問い合わせるか、R キーを押してアプライアンスを以前のソフトウェアバージョンにロールバックします。

メモ: 3.1.2 リリース以降では、アップグレード後のセルフテストが失敗しても、自動ロールバックは実行されなくなりました。[再試行 (Attempt again)]を選択してもセルフテストが引き続き失敗する場合、アップグレードは再度停止し、同じオプションが表示されます。

---

11 アップグレードが完了すると、AIM ウィンドウにアップグレードの結果の概略が表示されます。

ディスクプールがオンラインに戻ると、アプライアンスは自己診断テストを実行します。テスト結果については、次のファイルを参照してください。

`/log/selftest_report_<appliance_serial>_<timedate>.txt`

SMTP が構成されている場合は、セルフテストの結果が含まれた電子メール通知が送信されます。

12 HA セットアップのみの場合:

最初のノードでアップグレードを完了したら、`Support > Test Software` コマンドを実行して、各種アプライアンスソフトウェアコンポーネントの状態を検証します。テストに合格したら、もう一方のノードにログインし、最初のノードと同じ方法でアップグレードします。

13 バックアップ環境に SAN クライアントコンピュータが含まれる場合にのみ、このステップを完了してください。

ファイバーチャネル (FC) ポートは、SAN クライアントコンピュータがファイバートランスポート (FT) デバイスに再接続することを許可するために再スキャンする必要があります。再スキャンはアプライアンスの NetBackup CLI ビューから実行する必要があります。

FC ポートを再スキャンするには

- 次のコマンドを入力して NetBackup のユーザーアカウントの一覧を表示します。
  `Manage > NetBackupCLI > List`
- 一覧表示された NetBackup ユーザーのいずれかとしてこのアプライアンスにログオンします。
- 次のコマンドを実行して FC ポートを再スキャンします。
  `nbftconfig -rescanallclients`
- まだ動作しない SAN クライアントがある場合は、それらのクライアントのそれぞれについて、次のコマンドを示されている順序で実行します。
  UNIX クライアントの場合:
  `/usr/openv/netbackup/bin/bp.kill_all`
  `/usr/openv/netbackup/bin/bp.start_all`
  Windows クライアントの場合、
  `<install_path>¥NetBackup¥bin¥bpdown`
  `<install_path>¥NetBackup¥bin¥bpup`
- まだ動作しない SAN クライアントがある場合、OS レベルで SCSI デバイスの更新を手動で開始する必要があります。更新方法はクライアントのオペレーティン

グシステムによって決まります。更新が完了したら、再度 `nbftconfig -rescanallclients` コマンドの実行を試みます。

- まだ動作しない SAN クライアントがある場合は、それらのクライアントを再ブートします。

メモ: まだ動作しない SLES 10 または SLES 11 SAN クライアントがある場合、ベリタスはそれらのクライアントの QLogic ドライバをアップグレードすることをお勧めします。VeritasSLES 10 クライアントの場合は、バージョン 8.04.00.06.10.3-K にアップグレードします。SLES 11 クライアントの場合は、バージョン 8.04.00.06.11.1 にアップグレードします。

4

アップグレード後のタスク

この章では以下の項目について説明しています。

- アップグレード後のタスク

アップグレード後のタスク

アップグレードプロセスが正常に完了したら、以下を参照して、実行する必要がある必須または推奨されるタスクを確認してください。

- NetBackup RBAC ユーザーが使用するバージョン 3.1.2 または 3.2 のアプライアンスをアップグレードした場合は、NetBackup 8.3 RBAC Roles ユーティリティをダウンロードして実行する必要があります。詳しくは、次の記事を参照してください。
  https://www.veritas.com/support/en_US/article.100047577
  https://www.veritas.com/support/en_US/article.100047660
- バージョン 4.1 以降へのアップグレードでは、既存の NetBackup CLI ユーザーに対するデフォルトの NetBackup RBAC 権限はなくなりました。これは、アップグレード後に新しく追加された NetBackup CLI ユーザーにも適用されます。これらのユーザーが NetBackup Web UI または REST API へのアクセスを必要とする場合は、適切な NetBackup RBAC の役割を手動で付与する必要があります。詳しくは『NetBackup Web UI 管理者ガイド』を参照してください。

5

VxUpdate を使用した NetBackup 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。

- VxUpdate について
- VxUpdate リポジトリの管理
- 配備ポリシーの管理
- VxUpdate を使用したプライマリサーバーからのアップグレードの手動による開始
- VxUpdate を使用した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、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 はクライアントアップグレード用の簡略化されたツールを提供します。追加の外部ツールを必要とせず、バックアップポリシーに類似した、使い慣れたポリシーベース形式の構成になっています。署名済みパッケージが検証され、プライマリサーバー上の VxUpdate リポジトリにインストールされます。パッケージがインストールされると、配備ポリシーで利用可能になります。さらに、配備ポリシーを使用して、Veritas から提供される緊急エンジニアリングバイナリのインストールを自動化できます。

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、[配備の管理 (Deployment Management)]> [配備ポリシー (Deployment Policies)]のNetBackup 管理コンソールにあります。

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

表 5-1

手順	処理	追加情報
1	NetBackup リポジトリへの配置	p.28 の「VxUpdate 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.31 の「配備ポリシーの管理」を参照してください。
3	(オプション) プライマリサーバー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.36 の「VxUpdate を使用したプライマリサーバーからのアップグレードの手動による開始」を参照してください。 p.40 の「VxUpdate を使用した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 リポジトリの管理

アプライアンスの `VxUpdate` コマンドが VxUpdate パッケージリポジトリのコンテンツを制御します。`VxUpdate` 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、すべてのクライアントパッケージをリポジトリに配置すると、アプライアンスプライマリサーバー上に約 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。これは、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す。

`AddPkg` オプションは、リポジトリとサポート対象の VxUpdate クライアントを検証し、NetBackup EEB 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パッケージをリポジトリに配置しようとすると、失敗します。これらのパッケージは、ターゲットホストに NetBackup をインストールする配備ポリシーで参照されます。`AddPkg` オプションを使用してリポジトリに配置する場合は、必要なディスク容量に注意してください。プライマリサーバーには、配備ポリシーで指定された NetBackup のバージョンとプラットフォーム向けパッケージを格納するために十分なディスク容量が確保されている必要があります。

リポジトリにロードできるパッケージには、次の種類があります。

- VxUpdate クライアントパッケージ
  VxUpdate を使用して、NetBackup 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 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。NetBackup 8.1.2 以降のリリース向けにVeritasが作成したすべてのクライアント Hotfix には、VxUpdate 形式の修正が含まれています。

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

Veritasの承認済み NetBackup クライアントパッケージのダウンロード

1. ベリタスのサポートのライセンスポータルにアクセスします。
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の命名規則は次のとおりです。

    `vxupdate_nbclient_`*`version_operatingsystem_platform`*`.sja`

11 ファイルをローカルマシンにダウンロードして、アプライアンスの /inst/patch/incoming にファイルをアップロードします。続いて、次の手順に従って、アプライアンスにファイルをアップロードします。

- ダウンロードしたファイルが存在するマシンで NetBackup Appliance Web コンソールにログインし、[管理 (Manage)]、[ソフトウェアアップデート (Software updates)]の順に移動します。
- ダウンロードしたファイルを選択し、アプライアンスにアップロードします。

12 次のコマンドを実行して、すべてのパッケージがダウンロードおよび抽出されたことを確認します。

```
Main > Manage > Software > List Downloaded
```

13 ダウンロードおよび抽出されたすべてのパッケージが一覧表示されていることを確認したら、パッケージを NetBackup パッケージリポジトリに追加します。

p.30 の「VxUpdate 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。

VxUpdate パッケージリポジトリへのパッケージの追加

VxUpdate では、VxUpdate 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。VxUpdate の AddPkg オプションを使用して、リポジトリにパッケージを追加します。また、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。Listpkgs オプションを使用して、パッケージリポジトリの内容を一覧表示し、パッケージが追加されたことを確認できます。

パッケージをリポジトリに追加するには

1 アプライアンスプライマリサーバーで、管理者として NetBackup Appliance シェルメニューにログインし、次のメニューに移動します。

```
Main > Manage > Software > VxUpdate
```

2 AddPkg *package_name* オプションを実行します。ここで、*package_name* はクライアントパッケージ名です。

例: AddPkg vxupdate_nbclient_8.2_suse_ppc64le.sja

3 リポジトリを表示して、パッケージが追加されたことを確認するには、ListPkgs オプションを実行します。

4 パッケージの詳細を表示するには、ShowPkgDetails n オプションを実行します。ここで、*n* はパッケージ ID 番号です。

VxUpdate 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。パッケージを削除するには、DelPkg オプションを使用します。パッケージが削除されたことを確認するには、ListPkgs オプションを使用して既存のすべてのパッケージを一覧表示します。

パッケージをリポジトリから削除するには

1. アプライアンスプライマリサーバーで、管理者として NetBackup Appliance シェルメニューにログインし、次のメニューに移動します。

   ```
   Main > Manage > Software > VxUpdate
   ```

2. リポジトリ内のパッケージのリストを表示するには、ListPkgs オプションを実行し、各パッケージを識別する ID 番号を書き留めます。

3. DelPkg *ID* オプションを実行して、すべての使用されていないパッケージを削除します。

   例: DelPkg 1

VxUpdate コマンドのオプションについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

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。

---

1. NetBackup 管理コンソールの左ペインで、[配備の管理 (Deployment Management)]、[配備ポリシー (Deployment Policies)]の順に選択します。
2. [処理 (Actions)]メニューで[新しい配備ポリシー (New Deployment Policy)]を選択します。
3. 新しいポリシー用の一意の名前を[新しい配備ポリシーの追加 (Add a New Deployment Policy)]ダイアログボックスに入力します。
4. [OK]をクリックします。
5. [配備ポリシーの変更 (Change Deployment Policy)]ウィンドウの[属性 (Attributes)]タブに表示されている情報を指定します。
   - [パッケージ (Package)]: 配備するパッケージをドロップダウンメニューから選択します。

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

- [メディアサーバー (Media server)]: メディアサーバーをドロップダウンメニューから指定します。指定したメディアサーバーは、ポリシーに含まれている NetBackup ホストに接続してファイルを転送するために使用します。メディアサーバーは NetBackup リポジトリからファイルのキャッシュも行います。メディアサーバーは、NetBackup 8.1.2 以降のバージョンでなければなりません。リポジトリはプライマリサーバーに存在するため、メディアサーバーフィールドのデフォルト値はプライマリサーバーになります。
- Java GUI および JRE: ターゲットシステムで Java GUI と JRE をアップグレードするかどうかを指定します。3 つのオプションがあります。
  - [インクルード (INCLUDE)]: 指定したコンピュータで Java GUI と JRE コンポーネントをインストールまたはアップグレードします。
  - [除外 (EXCLUDE)]: 指定したコンピュータから Java GUI と JRE コンポーネントを除外します。既存の NetBackup Java GUI および JRE パッケージがすべて削除されます。
  - [一致 (Match)]: Java GUI と JRE コンポーネントの現在の状態を保持します。アップグレード前のシステムにコンポーネントが存在する場合、コンポーネントはアップグレードされます。アップグレード前のシステムにコンポーネントが存在しない場合、コンポーネントはインストールされません。
- (該当する場合): [同時ジョブ数の制限 (Limit simultaneous jobs)]オプションを選択し、[ジョブ (Jobs)]の値を指定して、一度に実行できる同時ジョブの合計数を制限します。最小値は 1 で、最大値は 999 です。
  チェックボックスにチェックマークが付いている場合、デフォルト値は 3 です。
  チェックボックスのチェックマークをはずした場合は、アップグレードの同時ジョブに制限は適用されません。
  コマンドラインインターフェースで値を 0 に設定すると、同時アップグレードジョブを無制限に設定できます。
- [ホストを選択 (Select hosts)]: [利用できるホスト (Available hosts)]リストからホストを選択し、[追加 (Add)]を選択して配備ポリシーにホストを追加します。リストは、ホストデータベースとバックアップポリシーのホストから生成されます。[追加 (Add)]を選択すると、[選択したホスト (Selected hosts)]にホストが表示されます。

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

そのポリシー内の、すべてのスケジュールの概略を確認できます。

7 ［新規 (New)］を選択します。

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

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

  スケジュール形式:

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

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

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

- ［追加 (Add)］または［OK］を選択すると、スケジュールが作成されます。［OK］を選択して、ポリシーを保存して作成します。

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

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

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

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

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

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

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

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

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

- ［CRL は使用しない (Do not use a CRL)］: 追加の情報は不要です。
- ［証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)］: 追加の情報は不要です。

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

11 ［証明書ファイルパスから (ファイルベースの証明書の場合)］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。

配備ポリシーを変更するには

1 配備ポリシーを右クリックして、［変更 (Change)］を選択します。

2 配備ポリシーの各タブを参照して、ポリシーに必要な変更を加えます。

3 ［OK］を選択すると、ポリシーが更新されます。

配備ポリシーの削除

1 配備ポリシーを右クリックして、［削除 (Delete)］を選択します。

2 ［OK］を選択します。

3 ポリシーの削除を確認します。

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

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

ローカルでプライマリサーバーにログインし、即時に更新を強制実行する必要がある場合は、配備ポリシーを手動で開始します。または、緊急バイナリ用に、即時のアップグレードを開始できます。VxUpdate では、コマンドラインを使用してクライアント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.40 の「VxUpdate を使用した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クライアントのアップグレードを手動で開始するには

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

管理コンソールからポリシー内の特定の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[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。
- アップグレードするホストが［選択したホスト (Selected hosts)］にあることを確認します。

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

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

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

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

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

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

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

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

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

- ［CRL は使用しない (Do not use a CRL)］: 追加の情報は不要です。
- ［証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)］: 追加の情報は不要です。

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

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

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

8 ［OK］を選択して、アップグレードを起動します。

メモ: NetBackup 管理コンソールの［ポリシー (Policies)］セクションから、アップグレードジョブを起動することもできます。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。

ポリシー内のすべての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クライアントのアップグレードを開始します。選択したクライアントで、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クライアントに対してコマンドラインからアップグレードを手動で開始するには」

1 コマンドプロンプトを開いて、次のディレクトリに移動します。

Windows の場合: *install_path*¥netbackup¥bin

UNIX または Linux の場合: /usr/openv/netbackup/bin

2 次に示すように、nbinstallcmd コマンドを使用してポリシーを起動します。

```
nbinstallcmd -policy policy_name -schedule schedule
[-master_server primary]
```

ここで、*policy_name* は配置ポリシーの名前、*schedule* はスケジュールの名前、*primary* はプライマリサーバーの名前です。

ポリシー内の選択した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

ポリシー内の選択した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選択した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クライアントに対してコマンドラインからアップグレードを手動で開始するには」

1 コマンドプロンプトを開いて、次のディレクトリに移動します。

Windows の場合: *install_path*¥netbackup¥bin

UNIX または Linux の場合: /usr/openv/netbackup/bin

2 次に示すように、nbinstallcmd コマンドを使用します。

```
nbinstallcmd -policy policy_name -schedule schedule
{-host_filelist filename|-hosts client1, client2, clientN}
```

以下はその説明です。

- *policy_name* は配備ポリシーの名前です。
- *schedule* はスケジュールの名前です。

- *filename* は、アップグレードする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、ローカルクライアントでのみ起動できます。クライアントで nbinstallcmd コマンドを使用し、他のクライアント上でジョブを起動することはできません。他のクライアントで更新を起動するには、プライマリサーバーからそれらを開始する必要があります。

VxUpdate を使用すると、コマンドラインを使用してプライマリサーバーからアップグレードを起動することもできます。詳細情報を参照できます。

p.36 の「VxUpdate を使用したプライマリサーバーからのアップグレードの手動による開始」を参照してください。

ターゲットクライアントまたはメディアサーバーで非ポリシーベースのアップグレードを直接開始した場合、旧バージョンのホストの nbinstallcmd バージョンは現在の nbinstallcmd バージョンではありません。nbinstallcmd コマンドの正確な形式については、現在インストールされているバージョンの NetBackup についての『NetBackup コマンドリファレンスガイド』を参照してください。

この古いバージョンの nbinstallcmd により、通常の VxUpdate 動作で次のような例外が発生します。

- プライマリサーバーで NetBackup 証明書と外部証明書の両方を使用しており、ターゲットメディアサーバーまたはクライアントが NetBackup 8.1.2 にある場合、ターゲッ

トホストで非ポリシーベースのアップグレードを直接実行することはサポートされていません。次に示すオプションのいずれかを使用してアップグレードする必要があります。

- VxUpdate を使用して、プライマリサーバーからクライアントまたはメディアサーバーをアップグレードします。
- プライマリサーバー上でポリシーを作成します。次に、ターゲットクライアントまたはメディアサーバーでポリシーベースの nbinstallcmd を実行します。
- ターゲットホストで非ポリシーベースのアップグレードを開始する前に、プライマリサーバーの外部証明書を無効にします。外部証明書は、アップグレードが正常に完了した後で有効にできます。

- クライアントまたはメディアサーバーが NetBackup 8.2 以前のバージョンにある場合、-components フラグは利用できません。このフラグは、NetBackup Java GUI と JRE のオプションインストールを有効にするために NetBackup 8.3 で導入されました。NetBackup 8.2 以前のクライアントまたはメディアサーバーでアドホックの nbinstallcmd を実行すると、-components javagui_jre オプションはデフォルト値の MATCH に設定されます。この値を指定すると、アップグレード前のホストの Java GUI と JRE の状態と一致するようにアップグレードされます。アップグレード前のホストに Java GUI と JRE がインストールされている場合、アップグレード後もインストールされたままになります。アップグレード前のホストに Java GUI と JRE がインストールされていない場合、アップグレード後もインストールされません。

既存のポリシーに基づいてクライアントが開始した配備ジョブを開始するには

1. コマンドプロンプトからバイナリのディレクトリに移動します。

   UNIX または Linux の場合: /usr/openv/netbackup/bin

   Windows の場合: *install_path*¥netbackup¥bin

2. nbinstallcmd を次のように使用します。

   nbinstallcmd -policy *policy* -schedule *schedule* -master_server *name*

   例: nbinstallcmd -policy all_clients -schedule install812 -master_server primary1

   ジョブが正常に開始された場合は、エラーメッセージは表示されずにコマンドプロンプトに戻ります。

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/openv/netbackup/bin/admincmd`

Windows の場合: *`install_path`*`¥netbackup¥bin¥admincmd`

次の構文を使用します。

`bpplclients` *`deployment_policy_name`* `-modify` *`client_to_update`* `-hardware` *`new_hardware_value`* `-os` *`new_os_value`*

配備ポリシーは、オペレーティングシステムとハードウェアの値に、簡素化した命名スキームを使用します。bpplclients コマンドに示すように値を使用します。

表 5-2　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
hpux	ia64
debian	x64
redhat	x64
suse	x64
redhat	ppc64le
suse	ppc64le
redhat	zseries

オペレーティングシステム	ハードウェア
suse	zseries
aix	rs6000
solaris	sparc
solaris	x64
windows	x64

[証明書配備のセキュリティレベル (Security Level for certificate deployment)]が[最高 (Very High)]に設定されている場合、セキュリティ証明書は VxUpdate アップグレードの一環としては配置されません。この設定は、NetBackup 管理コンソールの NetBackup の[グローバルセキュリティ設定 (Global Security Settings)]にあります。

クライアントのアップグレードに VxUpdate を使用した後で、クライアントと通信できなくなった場合は、アップグレード中に適切なセキュリティ証明書が発行されたことを確認してください。証明書の手動配備が必要な場合があります。詳しくは、次の記事を参照してください。

https://www.veritas.com/content/support/en_US/article.100039650

配備ジョブの状態コードが 7207 になる場合もあります。このエラーは、NetBackup 事前チェックまたはアップグレードのプロセスが完了するまでに予想より長い時間がかかる、または完了しない場合に発生する可能性があります。プライマリサーバーの NetBackup 構成で次の値を定義すると、ジョブが状態 7207 で終了するまでに VxUpdate が待機する時間を構成できます。

VXUPDATE_CLIENT_READ_TIMEOUT_SECONDS

この値は、事前チェック操作とクライアントのアップグレード操作に許容される時間 (秒) を制御します。デフォルト値は 1800 (30 分) です。最短 600 (10 分)、または最長 3600 (60 分) まで設定できます。

VXUPDATE_SERVER_READ_TIMEOUT_SECONDS

この値は、サーバーのアップグレード操作に許容される時間 (秒) を制御します。デフォルト値は 2700 (45 分) です。最短 600 (10 分)、または最長 5400 (90 分) まで設定できます。

bpsetconfig コマンドを使用してプライマリサーバーの NetBackup 構成に値を追加する方法について詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

6

トラブルシューティング

この章では以下の項目について説明しています。

- アップグレードの問題のトラブルシューティング

アップグレードの問題のトラブルシューティング

アップグレードが失敗した場合、または他のアップグレードの問題が発生した場合、次の情報にアクセスして問題を解決します。

- NetBackup appliance のアップグレード失敗後のロールバックにより、メディアサーバーが無効になる
- プレフライトチェックポイント作成エラーにより、NetBackup appliance アップグレードを開始できない
- NetBackup appliance のアップグレードまたはロールバックを中断した後も古いチェックポイントが残る
- NetBackup appliance のアップグレードの初期段階でアップグレードプロセスが失敗すると AIM ウィンドウがハングアップする

索引

N

NetBackup Appliance シェルメニューから更新をインストール
　バージョン 4.1 20

あ

アップグレード
　サポートされているアップグレードパス 6
　バージョン 4.1 および RHEL オペレーティングシステム 6
アップグレードの推定所要時間 15
アップグレードの問題のトラブルシューティング 44
アプライアンスインストールマネージャ (AIM) 7
アプライアンスのアップグレード
　要件およびベストプラクティス 9
アプライアンスのサーバーまたはクライアントパッケージ
　直接ダウンロード 18

か

クライアント共有
　ソフトウェア更新のダウンロード 18

さ

ソフトウェア更新
　NetBackup Appliance Web コンソールからのダウンロード 17
ソフトウェア更新のダウンロード
　NetBackup Appliance Web コンソールから 17
　クライアント共有の使用 18

た

ダウンロード方法
　リリース更新 16
直接ダウンロード
　アプライアンスのサーバーまたはクライアントパッケージ 18

は

バージョン 4.1
　NetBackup Appliance シェルメニューから更新をインストール 20
バージョン 4.1 へのアップグレード
　RHEL オペレーティングシステム 6

や

要件およびベストプラクティス
　アプライアンスのアップグレード 9