

NetBackup™ for HBase 管理者ガイド

UNIX、Windows および Linux

リリース 10.0

VERITAS™

NetBackup™ for HBase 管理者ガイド

最終更新日: 2022-05-05

法的通知と登録商標

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

テクニカルサポート

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

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

<https://www.veritas.com/support>

次の URL で **Veritas Account** の情報を管理できます。

<https://my.veritas.com>

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

世界共通 (日本を除く)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

マニュアル

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

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

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

第 1 章	概要	6
	NetBackup を使用した HBase データの保護	6
	HBase データのバックアップ	8
	HBase データのリストア	9
	NetBackup for HBase の用語	10
	制限事項	11
第 2 章	NetBackup 用 HBase プラグインの配備	13
	HBase プラグインの配備について	13
	HBase プラグインをインストールするための前提条件	14
	オペレーティングシステムとプラットフォームの互換性	14
	NetBackup の HBase プラグインのライセンス	14
	HBase クラスタの準備	14
	HBase プラグインを配備するためのベストプラクティス	15
	インストール後の手順	16
	HBase プラグインの配備の検証	16
第 3 章	NetBackup for HBase の構成	17
	NetBackup for HBase の構成について	17
	バックアップホストの管理	18
	NetBackup マスターサーバー上の NetBackup クライアントのホワイト リスト	19
	バックアップホストとしての NetBackup アプライアンスの設定	20
	NetBackup での HBase クレデンシャルの追加	20
	HBase 構成ファイルを使用した HBase プラグインの構成	22
	高可用性 HBase クラスタ用の NetBackup の構成	23
	NetBackup および HBase クラスタ間の SSL 対応 (HTTPS) 通信の 設定	25
	Kerberos を使用する HBase クラスタの設定	26
	HBase プラグイン用の NetBackup ポリシーの構成	26
	BigData バックアップポリシーの作成	26
	HBase クラスタのディザスタリカバリ	31

第 4 章	HBase のバックアップとリストアの実行	33
	HBase クラスタのバックアップについて	33
	Kerberos 認証を使用する HBase クラスタのバックアップおよびリスト ア操作実行の前提条件	34
	HBase クラスタのバックアップ	34
	HBase クラスタのバックアップを作成するためのベストプラクティス	35
	HBase クラスタのリストアについて	36
	同じ HBase クラスタへの HBase データのリストア	37
	代替 HBase クラスタへの HBase データのリストア	39
	切り捨てられたテーブルのリストア	43
	HBase クラスタをリストアするためのベストプラクティス	44
第 5 章	トラブルシューティング	45
	NetBackup for HBase のデバッグログについて	45
	バックアップがエラー 6609 で失敗する	46
	バックアップがエラー 6601 で失敗する	46
	バックアップがエラー 6623 で失敗する	47
	リストアがエラー 2850 で失敗する	47
	バックアップがエラー 20 で失敗する	47
	バックアップがエラー 112 で失敗する	47
	バックアップ操作がエラー 6654 で失敗する	48
	コンテナベースの NetBackup Appliance を再起動した後、NetBackup 構 成ファイルおよび証明書ファイルが保持されない	48
	ディザスタリカバリ後に構成ファイルがリカバリされない	49
索引	50

概要

この章では以下の項目について説明しています。

- [NetBackup を使用した HBase データの保護](#)
- [HBase データのバックアップ](#)
- [HBase データのリストア](#)
- [NetBackup for HBase の用語](#)
- [制限事項](#)

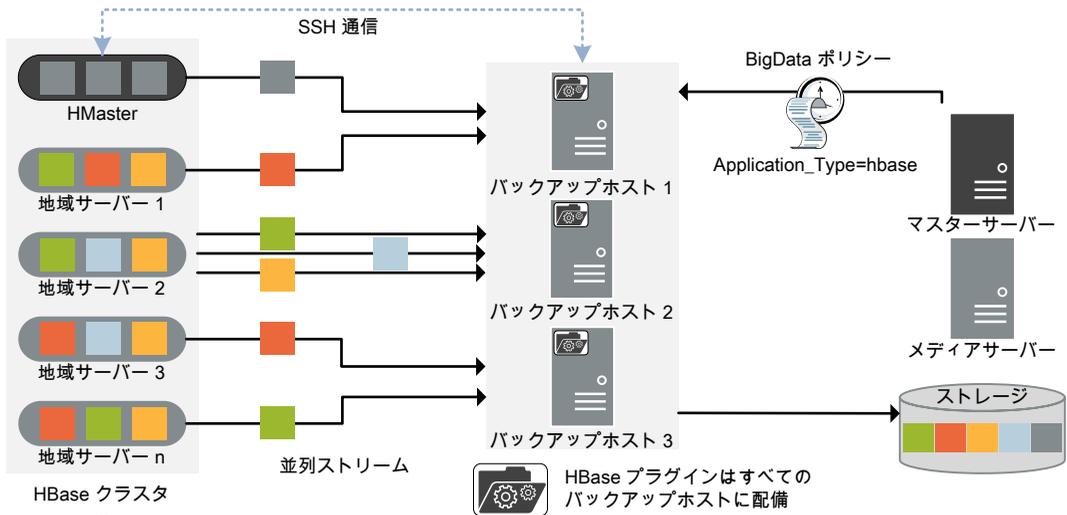
NetBackup を使用した HBase データの保護

NetBackup の並列ストリームフレームワーク (PSF) を使用した場合、NetBackup を使用して HBase データを保護できるようになりました。

次の図は、NetBackup によって HBase データを保護する方法の概要を示しています。

用語の定義も確認してください。p.10 の「[NetBackup for HBase の用語](#)」を参照してください。

図 1-1 アーキテクチャの概要



図では次の内容を説明しています。

- データは並列ストリームでバックアップされ、バックアップ時に地域サーバーはデータブロックを同時に複数のバックアップホストに対してストリームします。ジョブの処理速度が、複数のバックアップホストと並列ストリームによって向上します。
- HBase クラスタと NetBackup 間の通信は、HBase の NetBackup プラグインを使用して有効になります。
 プラグインは NetBackup のインストール時にインストールされます。
- NetBackup 通信の場合、BigData ポリシーを構成し、関連するバックアップホストを追加する必要があります。
- NetBackup のメディアサーバー、クライアント、またはプライマリサーバーをバックアップホストとして構成できます。また、地域サーバーの数によっては、バックアップホストを追加または削除できます。バックアップホストをさらに追加することで使用環境の規模を簡単に拡大できます。
- Hmaster とバックアップホスト間の通信は、SSH を介して行われます。
- NetBackup 並列ストリームフレームワークにより、エージェントレスのバックアップが可能で、バックアップとリストア操作はバックアップホストで実行します。クラスタノードには、エージェントの占有域がありません。また、NetBackup は HBase クラスタのアップグレードやメンテナンスの影響を受けません。

詳細情報:

- p.8 の「[HBase データのバックアップ](#)」を参照してください。

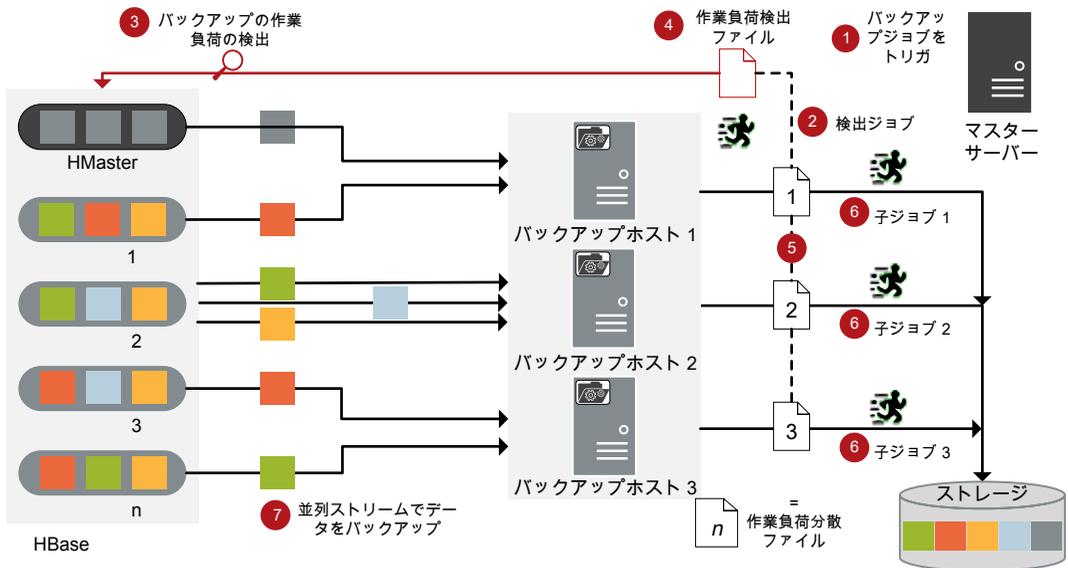
- p.9 の「[HBase データのリストア](#)」を参照してください。
- p.11 の「[制限事項](#)」を参照してください。
- NetBackup 並列ストリームフレームワーク (PSF) については、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

HBase データのバックアップ

HBase データは並列ストリームでバックアップされ、バックアップ時に HBase 地域サーバーはデータブロックを同時に複数のバックアップホストに対してストリームします。

次の図は、バックアップフローの概要を示しています。

図 1-2 バックアップフロー



次の図に示されているようになります。

1. スケジュールされたバックアップジョブはプライマリサーバーからトリガされます。
2. HBase データのバックアップジョブは複合ジョブです。バックアップジョブがトリガされると、最初に検出ジョブが実行されます。
3. 検出中に、最初のバックアップホストは Hmaster と接続し、検出を実行して、バックアップする必要があるデータの詳細を取得します。

4. 作業負荷検出ファイルは、バックアップホストに作成されます。作業負荷検出ファイルには、さまざまな地域サーバーからバックアップする必要があるデータの詳細が含まれています。
5. バックアップホストは作業負荷検出ファイルを使用し、作業負荷が複数のバックアップホスト間でどのように分散されるかを決定します。作業負荷分散ファイルは、バックアップホストごとに作成されます。
6. バックアップホストごとに個別の子ジョブが実行されます。作業負荷分散ファイルで指定されたデータがバックアップされます。
7. データブロックは、異なる地域サーバーから複数のバックアップホストに同時にストリームします。

すべての子ジョブが完了するまで、複合バックアップジョブは完了しません。子ジョブが完了すると、NetBackup は HMaster からすべてのスナップショットをクリーンアップします。クリーンアップ活動が完了した後にのみ、複合バックアップジョブは完了します。

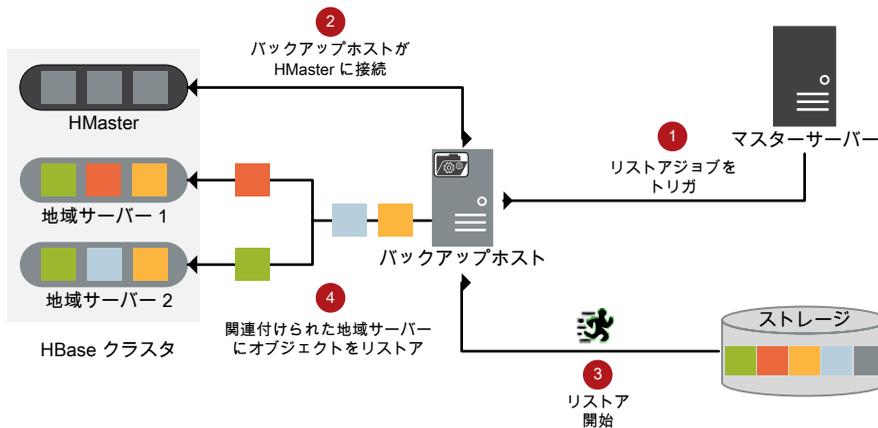
p.33 の「[HBase クラスタのバックアップについて](#)」を参照してください。

HBase データのリストア

リストアに使用されるのは、1 つのバックアップホストのみです。

次の図は、リストアフローの概要を示しています。

図 1-3 リストアフロー



図では次の内容を説明しています。

1. プライマリサーバーからのリストアジョブがトリガされます。
2. バックアップホストが HMaster と接続します。バックアップホストは宛先クライアントでもあります。

3. ストレージメディアからの実際のデータリストアが開始されます。
 4. データブロックは地域サーバーにリストアされます。
- p.36 の「[HBase クラスタのリストアについて](#)」を参照してください。

NetBackup for HBase の用語

次の表では、HBase クラスタの保護に **NetBackup** を使用するときに使われる用語を定義しています。

表 1-1 NetBackup の用語

用語	定義
複合ジョブ	<p>HBase データのバックアップジョブは複合ジョブです。</p> <ul style="list-style-type: none"> ■ バックアップジョブは、バックアップするデータの情報を取得するための検出ジョブを実行します。 ■ 子ジョブは、実際のデータ転送を実行する各バックアップホストに対して作成されます。 ■ バックアップが完了すると、ジョブは HMaster 上のスナップショットをクリーンアップし、その後ジョブ自体に完了したというマークが付けられます。
検出ジョブ	<p>バックアップジョブを実行すると、最初に検出ジョブが作成されます。検出ジョブは HMaster と通信し、バックアップする必要があるブロックの情報と、関連する地域サーバーの情報を収集します。検出の最後に、ジョブは作業負荷検出ファイルにデータを入力します。ファイルはその後 NetBackup によってバックアップホスト間で作業負荷を分散させるために使用されます。</p>
子ジョブ	<p>バックアップの場合、ストレージメディアにデータを転送するバックアップホストごとに個別の子ジョブが作成されます。子ジョブは、複数の地域サーバーからデータブロックを転送できます。</p>
作業負荷検出ファイル	<p>検出時のバックアップホストが HMaster と通信するときに、作業負荷検出ファイルが作成されます。このファイルには、バックアップするデータブロックと、関連付けられている地域サーバーについての情報が含まれています。</p>
作業負荷分散ファイル	<p>検出が完了すると、NetBackup はバックアップホストごとに作業負荷配布ファイルを作成します。これらのファイルには、それぞれのバックアップホストで転送されるデータの情報が含まれます。</p>
並列ストリーム	<p>NetBackup 並列ストリームフレームワークにより、複数のバックアップホストを同時に使用して、複数の地域サーバーからのデータブロックをバックアップできます。</p>

用語	定義
バックアップホスト	バックアップホストは、プロキシクライアントとして機能します。すべてのバックアップとリストア操作は、バックアップホストで実行されます。 メディアサーバー、クライアント、またはプライマリサーバーを、バックアップホストとして構成できます。 バックアップホストは、リストア中に宛先クライアントとしても使用されます。
BigData ポリシー	BigData ポリシーは以下を実行するために導入されました。 <ul style="list-style-type: none">■ アプリケーションの種類を指定します。■ 分散マルチノード環境のバックアップを可能にします。■ バックアップホストを関連付けます。■ 作業負荷分散を実行します。
アプリケーションサーバー	HMaster は、NetBackup ではアプリケーションサーバーと呼ばれます。
プライマリ HMaster	高可用性シナリオでは、1 つの HMaster を BigData ポリシーと tpconfig コマンドで指定する必要があります。この HMaster はプライマリ HMaster と呼ばれます。
フェールオーバー HMaster	高可用性シナリオでは、hbase.conf ファイル内で更新されるプライマリ HMaster 以外の HMaster は、フェールオーバー HMaster と呼ばれません。

制限事項

HBase プラグインを配備する前に、次の制限事項を確認します。

- RHEL および SUSE プラットフォームのみが、HBase クラスタとバックアップホストのサポート対象です。
- HBase プラグインはバックアップ中にはオブジェクトの拡張属性 (xattrs) またはアクセス制御リスト (ACL) をキャプチャしないため、それらはリストアされたファイルまたはフォルダに対しては設定されません。
- 高可用性 HBase クラスタでは、バックアップまたはリストア操作中にフェールオーバーが発生すると、ジョブは失敗します。
- バックアップ操作の検出ジョブが進行中のときにバックアップおよびリストアジョブを手動でキャンセルしても、スナップショットエントリは HBase Web グラフィカルユーザーインターフェース (GUI) から削除されません。
- 読み取り専用テーブルのバックアップはサポートされません。
- バックアップポリシーを作成するときに、バックアップ対象にテーブルを 1 つずつ追加する必要があります。

- `bp.conf`で `NB_FIPS_MODE` が有効になっている場合、**Kerberos** 認証では、バックアップおよびリストア操作はサポートされません。

メモ: Kerberos 認証でバックアップを実行するには、`NB_FIPS_MODE=0` を指定するか、無効にして、新しいバックアップホストを配備します。

- **HTTPS** ベースの **Hadoop** クラスタのバックアップ中に **CRL** の期限が切れた場合、バックアップは部分的に実行されます。
- 複数の **CRL** ベースの **Hadoop** クラスタがある場合は、クラスタごとに異なるバックアップホストを追加していることを確認します。

NetBackup 用 HBase プラグインの配備

この章では以下の項目について説明しています。

- [HBase プラグインの配備について](#)
- [HBase プラグインをインストールするための前提条件](#)
- [オペレーティングシステムとプラットフォームの互換性](#)
- [NetBackup の HBase プラグインのライセンス](#)
- [HBase クラスタの準備](#)
- [HBase プラグインを配備するためのベストプラクティス](#)
- [インストール後の手順](#)
- [HBase プラグインの配備の検証](#)

HBase プラグインの配備について

HBase プラグインは NetBackup と共にインストールされます。配備を完了するには次のトピックを確認してください。

表 2-1 HBase プラグインの配備

作業	参照先
前提条件と要件	p.14 の「 HBase プラグインをインストールするための前提条件 」を参照してください。
HBase クラスタの準備	p.14 の「 HBase クラスタの準備 」を参照してください。

作業	参照先
ベストプラクティス	p.15 の「 HBase プラグインを配備するためのベストプラクティス 」を参照してください。
配備の検証	p.16 の「 HBase プラグインの配備の検証 」を参照してください。
構成	p.17 の「 NetBackup for HBase の構成について 」を参照してください。

HBase プラグインをインストールするための前提条件

HBase プラグインをインストールする前に、次の前提条件が満たされていることを確認してください。

- p.14 の「[オペレーティングシステムとプラットフォームの互換性](#)」を参照してください。
- p.14 の「[NetBackup の HBase プラグインのライセンス](#)」を参照してください。

オペレーティングシステムとプラットフォームの互換性

このリリースでは、RHEL および SUSE プラットフォームが HBase クラスタと NetBackup バックアップホストのサポート対象です。

詳細については、[NetBackup マスター互換性リスト](#)を参照してください。

NetBackup の HBase プラグインのライセンス

NetBackup 用 HBase プラグインを使用するバックアップおよびリストア操作では、アプリケーションとデータベースパックライセンス、または NetBackup Platform Base – Big Data Workload Edition ライセンスが必要です。

ライセンスを追加する方法に関する詳細情報を参照できます。

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

HBase クラスタの準備

NetBackup の HBase クラスタを準備するには、次のタスクを実行します。

- ファイアウォールの設定 (デフォルトではポート 50070) を更新して、バックアップホストが HBase クラスタと更新できるようにします。
- すべての HMaster と地域サーバーのエントリを、すべてのバックアップホスト上の `/etc/hosts` ファイルに追加します。ホスト名は FQDN 形式で追加する必要があります。

または

`/etc/resolve.conf` ファイルに適切な DNS エントリを追加します。

- すべてのバックアップホストのエントリを、HMaster と地域サーバー上の `/etc/hosts` ファイルに追加します。
- HBase クラスタで HBase サービスが有効になっていることを確認します。
- HMaster ユーザーは SSH を実行できる必要があります。
- `jdk` パッケージがインストールされていることを確認します。また、Java パスが設定されていて、Hbase バージョンと互換性があることを確認します。
- `jps` コマンドが Hmaster で機能していることを確認します。詳しくは、HBase のマニュアルを参照してください。
- `.bashrc` ファイルで、マスターサーバーの `tpconfig` に設定されているすべてのユーザーに対して、Hmaster 用の次の環境変数を設定します。
 - `export JAVA_HOME= PATH_OF_JAVA_DIR`
 - `export HADOOP_HOME=PATH_OF_HDFS_DIR`
 - `export HADOOP_MAPRED_HOME=$HADOOP_HOME`
 - `export HADOOP_COMMON_HOME=$HADOOP_HOME`
 - `export HADOOP_HDFS_HOME=$HADOOP_HOME`
 - `export YARN_HOME=$HADOOP_HOME`
 - `export HADOOP_COMMON_LIB_NATIVE_DIR=$HADOOP_HOME/lib/native`
 - `export PATH=$PATH:$HADOOP_HOME/sbin:$HADOOP_HOME/bin`
 - `export HADOOP_INSTALL=$HADOOP_HOME`
 - `export HADOOP_OPTS="$HADOOP_OPTS
-Djava.library.path=$HADOOP_HOME/lib/native"`
 - `export HBASE_HOME=PATH OF HBASE DIR`
 - `PATH=$PATH:$HBASE_HOME/bin:$JAVA_HOME/bin`
 - `export CLASSPATH=$CLASSPATH:/usr/local/hadoop/hbase/lib/*`

HBase プラグインを配備するためのベストプラクティス

HBase プラグインを配備して、NetBackup for HBase を構成するには、次のようにします。

- バックアップホスト、メディアサーバー、マスターサーバーのホスト名に、一貫性がある表記規則を使用します。たとえば、**HBase.veritas.com** というホスト名 (FQDN 形式) を使用している場合は、他のすべての場所で同じ形式を使用します。
- すべての HMaster と地域サーバーのエントリを、すべてのバックアップホスト上の `/etc/hosts` ファイルに追加します。ホスト名は FQDN 形式で追加する必要があります。
または
`/etc/resolve.conf` ファイルに適切な DNS エントリを追加します。
- HMaster と地域サーバーを必ず FQDN 形式で指定します。
- バックアップホストから (FQDN を使用して) すべてのノードに ping を実行します。

インストール後の手順

次のインストール後の手順を完了します。

- p.16 の「[HBase プラグインの配備の検証](#)」を参照してください。
- p.26 の「[Kerberos を使用する HBase クラスタの設定](#)」を参照してください。
- p.23 の「[高可用性 HBase クラスタ用の NetBackup の構成](#)」を参照してください。

HBase プラグインの配備の検証

HBase プラグインをインストールすると、次のファイルが配備されます。

- `/usr/opensv/lib/psf-plugins/hbase/libaapipgnhbase.so`

NetBackup for HBase の構成

この章では以下の項目について説明しています。

- [NetBackup for HBase の構成について](#)
- [バックアップホストの管理](#)
- [NetBackup での HBase クレデンシャルの追加](#)
- [HBase 構成ファイルを使用した HBase プラグインの構成](#)
- [Kerberos を使用する HBase クラスタの設定](#)
- [HBase プラグイン用の NetBackup ポリシーの構成](#)
- [HBase クラスタのディザスタリカバリ](#)

NetBackup for HBase の構成について

表 3-1 NetBackup for HBase の構成

作業	参照先
バックアップホストの追加	p.18 の「 バックアップホストの管理 」を参照してください。 NetBackup クライアントをバックアップホストとして使用する場合、マスターサーバー上の NetBackup クライアントをホワイトリストに載せる必要があります。 p.19 の「 NetBackup マスターサーバー上の NetBackup クライアントのホワイトリスト 」を参照してください。

作業	参照先
NetBackup での HBase クレデンシヤルの追加	p.20 の「NetBackup での HBase クレデンシヤルの追加」を参照してください。
HBase 構成ファイルを使用した HBase プラグインの構成	p.22 の「HBase 構成ファイルを使用した HBase プラグインの構成」を参照してください。 p.23 の「高可用性 HBase クラスタ用の NetBackup の構成」を参照してください。
Kerberos を使用する HBase クラスタ用のバックアップホストの構成	p.26 の「Kerberos を使用する HBase クラスタの設定」を参照してください。
HBase プラグイン用の NetBackup ポリシーの構成	p.26 の「HBase プラグイン用の NetBackup ポリシーの構成」を参照してください。

バックアップホストの管理

バックアップホストは、HBase クラスタのすべてのバックアップとリストア操作をホストするプロキシクライアントとして機能します。NetBackup 用 HBase プラグインの場合、バックアップホストは、HBase クラスタにインストールされている独立したエージェントなしですべてのバックアップとリストア操作を実行します。

バックアップホストは、Linux コンピュータである必要があります。NetBackup は、バックアップホストとして RHEL および SUSE プラットフォームのみをサポートします。

バックアップホストとして、NetBackup クライアント、メディアサーバー、またはマスターサーバーを使用できます。メディアサーバーをバックアップホストとして設定することをお勧めします。

バックアップホストを追加する前に、次の点を考慮します。

- バックアップ操作用に、1 つまたは複数のバックアップホストを追加できます。
- リストア操作用に、バックアップホストを 1 つだけ追加できます。
- 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が、バックアップホストの役割を実行できます。
- NetBackup 用 HBase プラグインは、すべてのバックアップホストに配備されます。
- 複数のバックアップホストを使用する場合は、すべてのバックアップホストがメディアサーバーと通信していることを確認します。

NetBackup 管理コンソールまたはコマンドラインインターフェースのいずれかを使用して BigData ポリシーを構成しているときにバックアップホストを追加できます。

ポリシーの作成方法について詳しくは p.26 の「BigData バックアップポリシーの作成」を参照してください。

バックアップホストを追加するには

- 1 [バックアップ対象]タブでは、[新規]をクリックし、次の形式でバックアップホストを追加します。

Backup_Host=<hostname>

ポリシーの作成方法について詳しくは p.26 の「BigData バックアップポリシーの作成」を参照してください。

また、次のコマンドを使用して、バックアップホストを追加することもできます。

```
bpplinclude PolicyName -add "Backup_Host=hostname"
```

詳しくは p.29 の「HBase クラスタ用の BigData ポリシーを作成するための NetBackup コマンドラインインターフェース (CLI) の使用」を参照してください。

- 2 ベストプラクティスとして、すべてのバックアップホスト上の `/etc/hosts` ファイルにすべての HMaster と地域サーバーのエントリを追加します。FQDN 形式でホスト名を追加する必要があります。

または

`/etc/resolve.conf` ファイルに適切な DNS エントリを追加します。

バックアップホストを削除するには

- 1 [バックアップ対象]タブで、削除するバックアップホストを選択します。

- 2 選択したバックアップホストを右クリックし、[削除]をクリックします。

また、次のコマンドを使用して、バックアップホストを削除することもできます。

```
bpplinclude PolicyName -delete "Backup_Host=hostname"
```

NetBackup マスターサーバー上の NetBackup クライアントのホワイトリスト

NetBackup クライアントをバックアップホストとして使用するには、それをホワイトリストに載せる必要があります。NetBackup マスターサーバー上でホワイトリストへの追加手順を実行します。

ホワイトリストは、ソフトウェアまたはアプリケーションが安全な実行を承認されていないかぎり、それらを実行しないようにシステムを制限するセキュリティ手法です。

NetBackup マスターサーバー上で NetBackup クライアントをホワイトリストに載せるには

- ◆ NetBackup マスターサーバー上で次のコマンドを実行します。
 - UNIX の場合
コマンドへのディレクトリパスは
`/usr/opensv/var/global/bin/admincmd/bpsetconfig` です。

```
bpsetconfig -h masterserver
bpsetconfig> APP_PROXY_SERVER = clientname.domain.org
bpsetconfig>
UNIX systems: <ctl-D>
```
 - Windows の場合
コマンドへのディレクトリパスは
`<Install_Path>%NetBackup%\bin\admincmd\bpsetconfig` です。

```
bpsetconfig -h masterserver
bpsetconfig> APP_PROXY_SERVER = clientname1.domain.org
bpsetconfig> APP_PROXY_SERVER = clientname2.domain.org
bpsetconfig>
Windows systems: <ctl-Z>
```

このコマンドは `APP_PROXY_SERVER = clientname` エントリをバックアップ構成 (`bp.conf`) ファイルまたは Windows レジストリに設定します。

`APP_PROXY_SERVER = clientname` について詳しくは、『*NetBackup 管理者ガイド Vol. 1*』の *NetBackup クライアントの構成オプションのセクション*を参照してください。

[Veritas NetBackup のドキュメント](#)

バックアップホストとしての NetBackup アプライアンスの設定

NetBackup アプライアンスをバックアップホストとして使用する場合、次の記事を確認してください。

- [NetBackup アプライアンスを Kerberos 認証を使用する HBase のバックアップホストとして使用する](#)
- [高可用性 HBase クラスタによって、NetBackup アプライアンスをバックアップホストとして使用する](#)

NetBackup での HBase クレデンシャルの追加

正常なバックアップとリストア操作のために HBase クラスタと NetBackup との間でシームレスな通信を確立するには、HBase クレデンシャルを NetBackup マスターサーバーに追加して更新する必要があります。

tpconfig コマンドを使用して、NetBackup マスターサーバーでクレデンシャルを追加します。

HBase の場合、クレデンシャルを追加するときに、RSA 指紋を提供する必要があります。

tpconfig 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。

HBase クレデンシャルを追加する場合は、次の点を考慮します。

- 高可用性 HBase クラスタの場合、プライマリとフェールオーバーの HMaster のユーザーが同じであることを確認します。
- BigData ポリシーを構成するときに使用するアプリケーションサーバーのクレデンシャルを使用します。
- Kerberos を使用する HBase クラスタの場合、application_server_user_id 値として実際の Kerberos ユーザー名を指定します。
- RSA キーは、SHA-256 形式である必要があります。
- バックアップホストで RSA がサポートされていることを確認し、RSA キーを入手するために、次のコマンドを実行します。

```
ssh_host_rsa_key.pub | awk '{print $2}' | base64 -d | sha256sum  
| awk '{print $1}'
```

このユーティリティは /etc/ssh で利用可能です。

NetBackup でクレデンシャルを追加するには

- 1 次のディレクトリパスから tpconfig コマンドを実行します。

UNIX システムでは、/usr/opensv/volmgr/bin/

Windows システムでは、install_path¥Volmgr¥bin¥

- 2 tpconfig --help コマンドを実行します。HBase クレデンシャルを追加、更新、および削除するのに必要なオプションのリストが表示されます。

- 3 tpconfig -add -application_server application_server_name
-application_server_user_id user_ID -application_type hbase
-password password コマンドを各パラメータに適切な値を入力して実行し、HBase クレデンシャルを追加します。

たとえば、application_server_name が HBase1 である HBase サーバーのクレデンシャルを追加する場合、適切な <user_ID> と <password> の詳細を使用して次のコマンドを実行します。

```
tpconfig -add -application_server HBase1 -application_type hbase  
-application_server_user_id HBase -password password
```

- 4 パスワードの入力が求められます。

- 5 `tpconfig -add -application_server application_server_name -application_server_user_id user_ID -application_type application_type -requiredport IP_port_number [-password password] [-host_user_id user_ID] [-host_password password] [-host_RSA_key RSA_key_fingerprint]` を実行します。

次に例を示します。

```
tpconfig -add -application_server testserver.veritas.com
-application_server_user_id hadoop-application_type hbase
-requiredport 60010 -password hadoop -host_user_id hadoop
-host_password hadoop-host_RSA_key
b2352722053ac9f40bc1XXXXXXXXXXXXXXXXXXXXXXXXXXXX419fa241ba9431fd6b9
```

メモ: HBase ユーザーが SSH および HBase フォルダの `admin` アクセス権を持っていることを確認します。

- 6 `tpconfig -dappservers` コマンドを実行し、NetBackup マスターサーバーに追加された HBase クレデンシャルがあることを確認します。

HBase 構成ファイルを使用した HBase プラグインの構成

バックアップホストは、HBase プラグインの設定を保存するために `hbase.conf` ファイルを使用します。各バックアップホストに対して個別のファイルを作成し、`/usr/opensv/var/global/` にコピーする必要があります。`hbase.conf` ファイルは、JSON 形式で手動で作成する必要があります。デフォルトでは、インストーラはこのファイルを使用できません。

メモ: どのパラメータにも空白値は指定できません。指定するとバックアップジョブは失敗します。

このリリースでは、次のプラグインを設定できます。

- p.23 の「高可用性 HBase クラスタ用の NetBackup の構成」を参照してください。
- p.25 の「NetBackup および HBase クラスタ間の SSL 対応 (HTTPS) 通信の設定」を参照してください。

`hbase.conf` ファイルの例を次に示します。

メモ: HA 以外の環境では、フェールオーバーパラメータは必要ありません。

```
{
  "application_servers":
  {
    "hostname_of_the_primary_HMaster":
    {
      "failover_HMaster":
      [
        {
          "hostname": "hostname_of_failover_HMaster"
        }
      ]
    }
  }
}
```

高可用性 HBase クラスタ用の NetBackup の構成

NetBackup for HBase クラスタの構成時に高可用性 HBase クラスタを保護するには、次のようにします。

- **BigData** ポリシーでクライアントとしていずれかの **HMaster** (プライマリ) を指定します。
- `tpconfig` コマンドを実行するときに、アプリケーションサーバーと同じ **HMaster** (プライマリとフェールオーバー) を指定します。
- `hbase.conf` ファイルを作成して、**HMaster** (プライマリとフェールオーバー) の詳細で更新し、すべてのバックアップホストに複製します。`hbase.conf` ファイルは **JSON** 形式です。
- **HMaster** のホスト名とポートは、**HBase** クラスタの `hbase-site.xml` 内の `http` アドレスパラメータで指定したものと同じでなければなりません。
- プライマリとフェールオーバーの **HMaster** のユーザー名は同じでなければなりません。
- どのパラメータにも空白値は指定できません。指定するとバックアップジョブは失敗します。

高可用性 HBase クラスタの HBase.conf ファイルを更新するには

1 次のパラメータで hbase.conf ファイルを更新します。

```
{
  "application_servers":
  {
    "hostname_of_primary_HMaster1":
    {
      "failover_HMaster":
      [
        {
          "hostname": "hostname_of_failover_HMaster1"
        }
      ]
    }
  }
}
```

- 2 複数の HBase クラスタがある場合、同じ `hbase.conf` ファイルを使用して詳細を更新します。次に例を示します。

```
{
  "application_servers":
  {
    "hostname_of_primary_HMaster1":
    {
      "failover_HMaster":
      [
        {
          "hostname": "hostname_of_failover_HMaster1"
        }
      ],
    },
    "hostname_of_primary_HMaster2":
    {
      "failover_HMaster":
      [
        {
          "hostname": "hostname_of_failover_HMaster2",
        }
      ],
    }
  }
}
```

- 3 このファイルをすべてのバックアップホストの次の場所に複製します。

```
/usr/opensv/var/global/
```

NetBackup および HBase クラスタ間の SSL 対応 (HTTPS) 通信の設定

NetBackup と HBase 間の SSL 通信を有効にするには、『NetBackup For Hadoop 管理者ガイド』の次のトピックを参照してください。

[「NetBackup および Hadoop クラスタ間での SSL 対応 \(HTTPS\) 通信の設定」](#)

Kerberos を使用する HBase クラスタの設定

Kerberos を使用する HBase クラスタについては、すべてのバックアップホストで次のタスクを実行します。

- すべてのバックアップホストに Kerberos パッケージ (krb5-workstation パッケージ) が配布されていることを確認します。
- keytab ファイルを取得して、バックアップホストの安全な場所にコピーします。
- keytab に必要なプリンシパルがあることを確認します。
- 適切な KDC サーバーとレルムの詳細で krb5.conf ファイルを手動で更新します。

メモ: default_cache_name パラメータの値が KEYRING:persistent:%{uid} に設定されていないことを確認してください。パラメータをコメントアウトしてデフォルトを使用することもできますし、FILE:/tmp/krb_file_name:%{uid} などのファイル名を指定することもできます。

- HBase のクレデンシャルを NetBackup に追加するときに、application_server_user_id の値として「kerberos」を指定します。p.20 の「[NetBackup での HBase クレデンシャルの追加](#)」を参照してください。
- Kerberos 認証を使用する HBase クラスタのバックアップとリストア操作については、HBase クラスタを認証するため、HBase に有効な Kerberos チケット認可チケット (TGT) が必要となります。p.34 の「[Kerberos 認証を使用する HBase クラスタのバックアップおよびリストア操作実行の前提条件](#)」を参照してください。

HBase プラグイン用の NetBackup ポリシーの構成

バックアップポリシーは、NetBackup がクライアントのバックアップを作成するときに従う指示を提供します。NetBackup 用 HBase プラグインのバックアップポリシーを構成する場合は、BigData ポリシーをポリシー形式として使用します。

NetBackup 管理コンソールまたはコマンドラインインターフェースのいずれかを使用して、BigData ポリシーを作成できます。

BigData ポリシーの作成方法について詳しくは、p.26 の「[BigData バックアップポリシーの作成](#)」を参照してください。を参照してください。

BigData バックアップポリシーの作成

HBase クラスタなどのビッグデータアプリケーションをバックアップするには、BigData ポリシーを使用します。

BigData ポリシーは、他のポリシーとは次の点で異なります。

- ポリシー形式として **BigData** を指定する必要があります。
- [クライアント]タブと[バックアップ対象]で提供されるエントリは、バックアップを作成するアプリケーションに応じて異なります。
- [バックアップ対象]タブで、特定のパラメータとその適切な値を指定する必要があります。

NetBackup 管理コンソールを使用した BigData ポリシーの作成

BigData ポリシーを作成するために NetBackup 管理コンソールを使用する場合は、次のいずれかの方式を使用できます。

- ポリシーの設定ウィザードを使用した BigData ポリシーの作成
- NetBackup ポリシーユーティリティを使用した BigData ポリシーの作成

BigData ポリシーを設定する最も簡単な方法は、ポリシーの設定ウィザードを使用することです。このウィザードではセットアップ処理の手順が示され、ほとんどの構成の最適な値が自動的に選択されます。ポリシー構成オプションがすべてウィザードで表示されるわけではありません。たとえば、カレンダーを基準としたスケジュールと[データの分類]の設定がこれに当たります。ポリシーが作成された後、[ポリシー]ユーティリティのポリシーを修正して、ウィザードの一部ではないオプションを構成してください。

HBase クラスタの BigData ポリシーを作成するためのポリシーの設定ウィザードの使用

ポリシーの設定ウィザードを使用して BigData ポリシーを作成するには、次の手順を実行します。

ポリシーの設定ウィザードを使用して BigData ポリシーを作成する方法

- 1 NetBackup 管理コンソールの左ペインで、[NetBackup の管理]をクリックします。
- 2 右ペインで、[ポリシーの作成 (Create a Policy)]をクリックして、ポリシーの設定ウィザードを開始します。
- 3 作成するポリシーの種類を選択します。
 - BigData ポリシー: Hbase データをバックアップするためのポリシー
- 4 BigData ポリシーのストレージユニット形式を選択します。
- 5 [次へ (Next)]をクリックして、ウィザードを開始し、プロンプトに従います。

ウィザードの実行中にその詳細を確認するには、ウィザードパネルの [ヘルプ (Help)] をクリックします。

HBase クラスタ用の BigData ポリシーを作成するための NetBackup ポリシーユーティリティの使用

次の手順を実行して、NetBackup ポリシーユーティリティを使用し、BigData ポリシーを作成します。

NetBackup ポリシーユーティリティを使用して BigData ポリシーを作成するには

- 1 NetBackup 管理コンソールの左ペインで、[NetBackup の管理 (NetBackup Management)]、[ポリシー (Policies)]の順に展開します。
- 2 [処理 (Actions)]メニューで[新規 (New)]、[ポリシー (Policy)]の順にクリックします。
- 3 新しいポリシー用の一意の名前を[新しいポリシーの追加 (Add a New Policy)]ダイアログボックスに入力します。
[OK]をクリックします。

- 4 [属性 (Attributes)]タブで、ポリシー形式に[BigData]を選択します。
- 5 [属性 (Attributes)]タブには、BigData ポリシー形式のストレージユニットを選択します。
- 6 [スケジュール (Schedules)]タブで[新規 (New)]をクリックして、新しいスケジュールを作成します。

BigData ポリシーの完全バックアップ、差分増分バックアップ、または累積増分バックアップのスケジュールを作成できます。スケジュールを設定すると、HBase データは、ユーザーがそれ以上介入しなくても、設定されたスケジュールに従って自動的にバックアップされます。

- 7 [クライアント (Clients)]タブには、NameNode の IP アドレスまたはホスト名を入力します。
- 8 [バックアップ対象 (Backup Selections)]タブで、次のようにパラメータとその値を入力します。

- **Application_Type=hbase**
これらのパラメータ値では、大文字と小文字が区別されます。
- **Backup_Host=IP_address or hostname**
バックアップホストは、Linux コンピュータである必要があります。バックアップホストには、NetBackup クライアントまたはメディアサーバーを指定できます。複数のバックアップホストを指定できます。
- **バックアップするテーブル**
複数のテーブルを指定できます。

メモ: BigData ポリシーを `Application_Type=hbase` で定義するときにバックアップ対象に対して指定されるテーブル名には、名前にスペースまたはカンマを含めることはできません。

9 [OK]をクリックして、変更を保存します。

ビッグデータアプリケーションの場合の NetBackup の使用について詳しくは、[Veritas NetBackup のドキュメント](#)のページを参照してください。

HBase クラスタ用の BigData ポリシーを作成するための NetBackup コマンドラインインターフェース (CLI) の使用

HBase 用の BigData ポリシーを作成するには、CLI 方式を使用することもできます。

NetBackup CLI 方式を使用して BigData ポリシーを作成するには

1 管理者としてログオンします。

2 移動先:

Windows の場合: `<install_path>\NetBackup\bin\admincmd`

UNIX の場合: `/usr/opensv/var/global/bin/admincmd`

3 デフォルト設定を使用して、新しい BigData ポリシーを作成します。

`bpolicynew policyname`

4 `-L` オプションを使用して、新しいポリシーの詳細を表示します。

`bpplinfo policyname -L`

5 ポリシー形式を BigData として変更および更新します。

`bpplinfo PolicyName -modify -v -M MasterServerName -pt BigData`

6 `Application_Type` を HBase として指定します。

Windows の場合:

`bpplinclude PolicyName -add "Application_Type=hbase"`

UNIX の場合:

`bpplinclude PolicyName -add 'Application_Type=hbase`

メモ: `Application_Type=HBase` のパラメータ値では、大文字と小文字が区別されます。

- 7 HBase に対するバックアップ操作を実行するバックアップホストを指定します。

Windows の場合:

```
bpplinclude PolicyName -add "Backup_Host=hostname"
```

UNIX の場合:

```
bpplinclude PolicyName -add 'Backup_Host=hostname'
```

メモ: バックアップホストは、Linux コンピュータである必要があります。バックアップホストとして、NetBackup クライアント、メディアサーバー、またはマスターサーバーを使用できます。

- 8 バックアップする HBase ディレクトリまたはフォルダ名を指定します。

Windows の場合:

```
bpplinclude PolicyName -add "/namespace:table_name"
```

UNIX の場合:

```
bpplinclude PolicyName -add '/namespace:table_name'
```

メモ: BigData ポリシーを Application_Type=hbase で定義するときにバックアップ対象に対して指定されるテーブル名には、名前にスペースまたはカンマを含められません。

- 9 BigData ポリシーのポリシーストレージ形式を変更および更新します。

```
bpplinfo PolicyName -residence STUName -modify
```

- 10 クライアント詳細を追加するための、HMaster の IP アドレスまたはホスト名を指定します。

Windows の場合:

```
bpplclients PolicyName -M "MasterServerName" -add  
"HBaseServerHMaster" "Linux" "RedHat"
```

UNIX の場合:

```
bpplclients PolicyName -M 'MasterServerName' -add  
'HBaseServerHMaster' 'Linux' 'RedHat'
```

- 11 要件に応じて作成された **BigData** ポリシーにスケジュールを割り当てます。

```
bpplsched PolicyName -add Schedule_Name -cal 0 -rl 0 -st  
sched_type -window 0 0
```

ここで、*sched_type* 値は次のように指定できます。

スケジュール形式	説明
FULL	完全バックアップ
INCR	差分増分バックアップ
CINC	累積増分バックアップ

sched_type のデフォルト値は **FULL** です。

スケジュールを設定すると、**HBase** データは、ユーザーがそれ以上介入しなくても、設定されたスケジュールに従って自動的にバックアップされます。

- 12 別の方法として、**HBase** データの手動バックアップを実行することもできます。

手動バックアップ操作を実行するには、手順 1 から手順 11 のすべての手順を実行します。

- 13 手動バックアップ操作では、次の場所に移動します。

Windows の場合: <install_path>%NetBackup%bin

UNIX の場合: /usr/opensv/var/global/bin

次のコマンドを使用して、既存の **BigData** ポリシーの手動バックアップ操作を開始します。

```
bpbackup -i -p PolicyName -s Schedule_Name -S MasterServerName  
-t 44
```

ここで、*-p* はポリシー、*-s* はスケジュール、*-S* はマスターサーバー、および *-t 44* は **BigData** ポリシー形式を表しています。

HBase クラスタのディザスタリカバリ

HBase クラスタをディザスタリカバリする場合、次のタスクを実行します。

表 3-2 **ディザスタリカバリの実行**

タスク	説明
<p>HBase クラスタとノードが起動した後、クラスタで NetBackup による操作の準備をします。</p>	<p>次のタスクを実行します。</p> <p>ファイアウォールの設定を更新して、バックアップホストが HBase クラスタと通信できるようにします。</p> <p>HBase クラスタで webhbase サービスが有効になっていることを確認します。</p> <p>p.14 の「HBase クラスタの準備」を参照してください。</p>
<p>正常なバックアップとリストア操作のために HBase クラスタと NetBackup の間のシームレスな通信を確立するには、HBase のクレデンシヤルを NetBackup マスターサーバーに追加して更新する必要があります。</p>	<p>tpconfig コマンドを使用して、NetBackup マスターサーバーに HBase のクレデンシヤルを追加します。</p> <p>p.20 の「NetBackup での HBase クレデンシヤルの追加」を参照してください。</p>
<p>バックアップホストは、HBase プラグインの構成設定を保存するために HBase.conf ファイルを使用します。各バックアップホストに個別のファイルを作成して、/usr/opensv/var/global/ にコピーする必要があります。HBase.conf ファイルは JSON 形式で作成する必要があります。</p>	<p>このリリースでは、次のプラグインを設定できません。</p> <ul style="list-style-type: none"> ■ p.23 の「高可用性 HBase クラスタ用の NetBackup の構成」を参照してください。
<p>元の HMaster 名で BigData ポリシーを更新します。</p>	<p>p.26 の「HBase プラグイン用の NetBackup ポリシーの構成」を参照してください。</p>

HBase のバックアップとリストアの実行

この章では以下の項目について説明しています。

- [HBase クラスタのバックアップについて](#)
- [HBase クラスタのリストアについて](#)
- [代替 HBase クラスタへの HBase データのリストア](#)
- [切り捨てられたテーブルのリストア](#)
- [HBase クラスタをリストアするためのベストプラクティス](#)

HBase クラスタのバックアップについて

NetBackup のバックアップ、アーカイブおよびリストアコンソールを使用して、バックアップ操作を管理します。

表 4-1 HBase データのバックアップ

タスク	参照先
プロセスの理解	p.8 の「 HBase データのバックアップ 」を参照してください。
(オプション) Kerberos の前提条件をすべて満たす	p.34 の「 Kerberos 認証を使用する HBase クラスタのバックアップおよびリストア操作実行の前提条件 」を参照してください。
HBase クラスタのバックアップ	p.34 の「 HBase クラスタのバックアップ 」を参照してください。

タスク	参照先
ベストプラクティス	p.35 の「 HBase クラスタのバックアップを作成するためのベストプラクティス 」を参照してください。
トラブルシューティングのヒント	検出とクリーンアップの関連ログについては、検出をトリガした最初のバックアップホスト上の次のログファイルを確認します。 <code>/usr/opensv/var/global/logs/nbaapidiscv</code> データ転送関連ログについては、マスターサーバー上のログファイルから、対応するバックアップホストを (ホスト名を使用して) 検索します。 p.45 の「 NetBackup for HBase のデバッグログについて 」を参照してください。

Kerberos 認証を使用する HBase クラスタのバックアップおよびリストア操作実行の前提条件

Kerberos 認証を使用する HBase クラスタのバックアップとリストア操作については、HBase クラスタを認証するため、HBase に有効な Kerberos チケット認可チケット (TGT) が必要となります。

メモ: バックアップ操作中とリストア操作中は、TGT を有効にする必要があります。このため、適切な形で TGT の有効期間を指定するか、操作中に必要なときに更新する必要があります。

次のコマンドを実行して TGT を生成します。

```
kinit -k -t /keytab_file_location/keytab_filename principal_name
```

次に例を示します。

```
kinit -k -t /usr/opensv/var/global/nbusers/hbase_mykeytabfile.keytab  
hbase@MYCOMPANY.COM
```

設定に関連する情報も確認してください。p.26 の「[Kerberos を使用する HBase クラスタの設定](#)」を参照してください。

HBase クラスタのバックアップ

バックアップジョブはスケジュール設定して実行することもできれば、手動で実行することもできます。『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

バックアップ処理の概要については、p.8 の「[HBase データのバックアップ](#)」を参照してください。を参照してください。

バックアッププロセスは、次のステージで構成されます。

1. 事前処理: 事前処理のステージでは、**BigData** ポリシーで構成した最初のバックアップホストが検出をトリガします。このステージでは、バックアップ対象全体のスナップショットが生成されます。スナップショットの詳細は、地域サーバーの **Web** インターフェースに表示されます。
2. データ転送: データ転送処理中には、バックアップホストごとに 1 つの子ジョブが作成されます。
3. 事後処理: 事後処理の一部として、**NetBackup** は地域サーバー上のスナップショットをクリーンアップします。

注意事項

- **Hmaster** の `/etc/ssh/sshd_config` ファイルで、`PasswordAuthentication` フィールドを **Yes** に設定します。ファイルを更新したら **sshd** を再起動します。
すべてのクラスタサーバーで、同じハッシュキーアルゴリズム (**RSA**) がサポートされることを確認します。
- 手動でジョブをキャンセルすると、スナップショットはクリーンアップされません。ジョブをキャンセルしたら、**HBase** シェルから手動でスナップショットを削除する必要があります。
- 空のテーブルのバックアップを作成する場合は、**HBase** シェルから手動でスナップショットをクリーンアップする必要があります。
- p.35 の「[HBase クラスタのバックアップを作成するためのベストプラクティス](#)」を参照してください。

HBase クラスタのバックアップを作成するためのベストプラクティス

HBase クラスタのバックアップを作成する前に、次の点を考慮します。

- バックアップジョブを実行する前に、すべてのノードでバックアップホストからホスト名 (FQDN) への正常な **ping** のレスポンスが返ることを確認します。
- ファイアウォールの設定を更新して、バックアップホストが **HBase** クラスタと通信できるようにします。
- 保護する **HBase** テーブルがスナップショット作成可能であることを確認します。
- このテーブルでスナップショットを作成した場合は、**HBase** テーブルフォルダを **hdfs** から削除しないようにします。削除すると、スナップショットは参照を失い、そのスナップショットからデータのリストアやリカバリを実行できなくなります。
- 切り捨てられたテーブルや空のテーブルはバックアップしないでください。バックアップジョブが失敗します。
- 名前空間とテーブルの名前は、同じにしないでください。バックアップジョブが失敗します。

- バックアップ対象に指定したテーブルの名前には、スペースやカンマを含めないでください。
選択したテーブルは、コロンで区切る必要があります。たとえば、`namespace:tablename` のようにします。
- バックアップ対象に指定したテーブルは空にできません。
- HBase ノードとバックアップホストのローカル時刻が NTP サーバーと同期していることを確認します。

HBase クラスタのリストアについて

NetBackup のバックアップ、アーカイブおよびリストアコンソールを使用して、リストア操作を管理します。

表 4-2 HBase データのリストア

作業	参照先
プロセスの理解	p.9 の「 HBase データのリストア 」を参照してください。
Kerberos の前提条件をすべて満たす	p.34 の「 Kerberos 認証を使用する HBase クラスタのバックアップおよびリストア操作実行の前提条件 」を参照してください。
同じ HMaster または HBase クラスタへの HBase データのリストア	<ul style="list-style-type: none">■ p.37 の「同じクラスタに HBase データをリストアするためのリストアウィザードの使用」を参照してください。■ p.38 の「同じ HBase クラスタに HBase データをリストアするための bprestore コマンドの使用」を参照してください。
代替 HMaster または HBase クラスタへの HBase データのリストア このタスクは bprestore コマンドを使用してのみ実行できます。	p.39 の「 代替 HBase クラスタへの HBase データのリストア 」を参照してください。
HBase には、切り捨てられたテーブルのリストアに制限があります。回避策として、アーカイブパスにリストアする必要があります。	p.43 の「 切り捨てられたテーブルのリストア 」を参照してください。

作業	参照先
ベストプラクティス	p.44 の「HBase クラスタをリストアするためのベストプラクティス」を参照してください。
トラブルシューティングのヒント	p.45 の「NetBackup for HBase のデバッグログについて」を参照してください。

注意事項

無効化されたテーブルをリストアする場合、リストアが成功した後にテーブルが有効になります。

同じ HBase クラスタへの HBase データのリストア

同じ HBase クラスタ上で HBase データをリストアするには、次の点を考慮してください。

- HBase データリストア操作を開始するには、バックアップ、アーカイブおよびリストアコンソールを使用します。このインターフェースでは、リストアするオブジェクトが存在する NetBackup サーバー、およびバックアップイメージを表示するクライアントを選択できます。これらの選択に基づいて、バックアップイメージの履歴の表示、個々の項目の選択およびリストアの開始を行うことができます。
- リストアブラウザを使用すると、HBase ディレクトリオブジェクトを表示できます。オブジェクトは階層表示され、リストアに使用するオブジェクトを選択できます。HBase クラスタを構成するオブジェクト (HBase ディレクトリまたはファイル) は、個々のディレクトリを展開すると表示されます。
- 管理者は、HBase ディレクトリおよび個々の項目を参照してリストアできます。ユーザーがリストアできるオブジェクトには、HBase ファイルとフォルダが含まれます。

同じクラスタに HBase データをリストアするためのリストアウィザードの使用

このトピックでは、同じ HBase クラスタに HBase データをリストアするためのリストアウィザードの使用方法について説明します。

リストアウィザードを使用してリストアを実行するには

- 1 バックアップ、アーカイブおよびリストアインターフェースを開きます。
- 2 データセット全体をリストアする適切な日付範囲を選択します。
- 3 [ディレクトリの参照]で、参照するパスとしてルートディレクトリ (/) を指定します。
- 4 [ファイル]メニュー (Windows の場合) または [処理]メニュー (UNIX の場合) から、[NetBackup マシンおよびポリシー形式の指定]を選択します。
- 5 [NetBackup マシンおよびポリシー形式の指定]ウィザードで、リストアのソースと宛先の詳細を入力します。

- リストア操作を実行するソースとして **HBase HMaster** を指定します。
[リストアのソースクライアント (Source client for restores)]リストから、必要な **HMaster** を選択します。
 - バックアップホストを宛先クライアントとして指定します。
[リストアの宛先クライアント]リストから、必要なバックアップホストを選択します。
 - [NetBackup マシンおよびポリシー形式の指定]ウィザードで、リストアのポリシー形式の詳細を入力します。
[リストアのポリシー形式]リストから、リストアのポリシー形式として **BigData** を選択します。
[OK]をクリックします。
- 6 [バックアップ履歴]に移動し、リストアするバックアップイメージを選択します。
 - 7 [ディレクトリ構造]ペインで、[ディレクトリ]を展開します。
そのディレクトリの下にある後続のすべてのファイルとフォルダが、[選択されたディレクトリの内容]ペインに表示されます。
 - 8 [選択されたディレクトリの内容 (Contents of Selected Directory)]ペインで、リストアする **HBase** ファイルにチェックマークを付けます。
 - 9 [リストア]をクリックします。
 - 10 [マークされたファイルのリストア]ダイアログボックスで、要件に応じてリストアの宛先を選択します。
 - バックアップを実行したのと同じ場所にファイルをリストアする場合は、[元の位置にすべてをリストア]を選択します。
 - バックアップの場所とは異なる場所にファイルをリストアする場合は、[すべてを異なる位置にリストア]を選択します。
 - 11 [リストアの開始]をクリックします。
 - 12 リストアされたファイルを確認します。

同じ HBase クラスタに HBase データをリストアするための bprestore コマンドの使用

bprestore コマンドを実行すると、1 つのバックアップ済みまたはアーカイブ済みファイル、またはリストで指定した複数のファイルをリストアできます。リストア先のディレクトリを指定することもできます。ディレクトリ名を含める場合、bprestore を実行すると、そのディレクトリのすべてのファイルおよびサブディレクトリのリストアが行われます。感嘆符 (!) をファイルパスまたはディレクトリパスの前に付けることによって、すでにリストアに含まれているファイルまたはディレクトリのパスをエクスクルードできます (**NDMP** リストアには適用されません)。たとえば、エクスクルード機能はディレクトリの一部をリストアからエクスクルードする場合に有効です。

UNIX システムでのこのコマンドへのディレクトリパスは `/usr/opencv/var/global/bin/` です。

Windows システムでのこのコマンドへのディレクトリパスは `install_path¥NetBackup¥bin¥` です。

バックアップの場所と同じ場所に HBase データをリストアするには

- 1 Windows または UNIX システムのどちらかを使用しているかに応じて、管理者または root ユーザーとしてログインします。
- 2 NetBackup マスターサーバー上で、適切な値を指定して、次のコマンドを実行します。

```
bprestore -S master_server -D backup_host -C client -t 44 -L  
progress_log -f listfile
```

手順の詳細:

```
-S master_server
```

このオプションでは、NetBackup マスターサーバー名を指定します。

```
-D backup_host
```

バックアップホストの名前を指定します。

```
-C client
```

このオプションでは、ファイルのリストア元のバックアップまたはアーカイブの検索に使用するソースとして HMaster を指定します。この名前は、NetBackup カタログに表示される名前と一致する必要があります。

```
-f listfile
```

このオプションでは、リストアするファイルのリストを含むファイル (**listfile**) を指定します。このオプションは、ファイル名オプションの代わりに使用できます。listfile では、各ファイルパスを個別の行に指定する必要があります。

```
-L progress_log
```

このオプションでは、進捗情報を書き込むホワイトリストファイルパスの名前を指定します。

```
-t 44
```

ポリシー形式として **BigData** を指定します。

代替 HBase クラスタへの HBase データのリストア

NetBackup では、HBase データを別の HMaster または HBase クラスタにリストアできます。この種類のリストア方法は、リダイレクトリストアと呼ばれます。

代替リストアを実行する場合、次のことを考慮します。

- 別のクラスタに HBase テーブルをリストアするには、両方のクラスタに同じバージョンの HBase が配備されている必要があります。
- NetBackup では、コマンドラインインターフェース (CLI) を使用してのみ、リダイレクトリストアをサポートします。
- NetBackup マスターサーバーで、代替の HMaster または HBase クラスタのクレデンシアルを追加したことを確認します。

HBase のリダイレクトリストアを実行するには

- 1 *rename_file* および *listfile* の値を次のように変更します。

パラメータ	値
<i>rename_file</i>	/<namespace:source_table_name> を /<namespace:destination_table_name> ALT_APPLICATION_SERVER=<alternate name node> に変更します。
<i>listfile</i>	リストアするすべての HBase ファイルのリスト

メモ: /<namespace:source_table_name> と
 /<namespace:destination_table_name> は異なる値にする必要があります。

- 2 手順 1 で説明したパラメータに、変更した値を使用して、**NetBackup** マスターサーバーで `bprestore -S master_server -D backup_host -C client -R rename_file -t 44 -L progress_log -f listfile` コマンドを実行します。

手順の詳細:

`-S master_server`

このオプションでは、**NetBackup** マスターサーバー名を指定します。

`-D backup_host`

バックアップホストの名前を指定します。

`-C client`

このオプションでは、ファイルのリストア元のバックアップまたはアーカイブの検索に使用するソースとして **HMaster** を指定します。この名前は、**NetBackup** カタログに表示される名前と一致している必要があります。

`-f listfile`

このオプションでは、リストアするファイルのリストを含むファイル (**listfile**) を指定します。このオプションは、ファイル名オプションの代わりに使用できます。**listfile** では、各ファイルパスを個別の行に指定する必要があります。

`-L progress_log`

このオプションでは、進捗情報を書き込むホワイトリストファイルパスの名前を指定します。

`-t 44`

ポリシー形式として **BigData** を指定します。

`-R rename_file`

このオプションでは、代替パスへのリストアのために名前を変更するファイル名を指定します。

ファイル名の変更を記述するファイルのエントリには、次の形式を使用します。

`change backup_tablename to restore_tablename`

`ALT_APPLICATION_SERVER=<Application Server Name>`

ファイルパスは / (スラッシュ) で始まる必要があります。

メモ: **NetBackup** インストールパスの一部としてまだ組み込まれていない、`<rename_file_path>`、`<progress_log_path>` などのすべてのファイルパスをホワイトリストに載せたことを確認します。

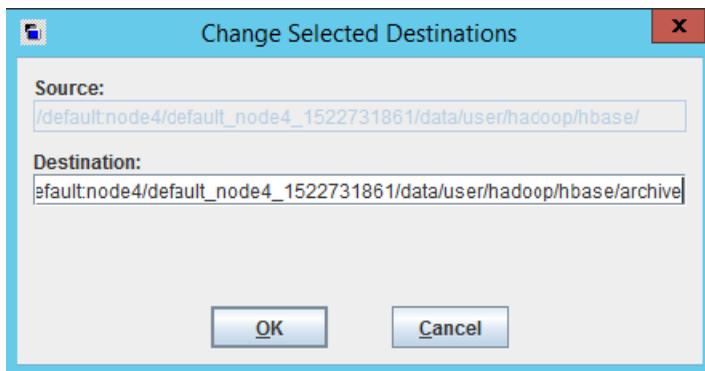
切り捨てられたテーブルのリストア

HBase には、切り捨てられたテーブルのリストアに制限があります。回避策として、次の手順に従います。

切り捨てられたテーブルをリストアするには

- 1 バックアップ、アーカイブおよびリストアインターフェースを開きます。
- 2 データセット全体をリストアする適切な日付範囲を選択します。
- 3 [ディレクトリの参照]で、参照するパスとしてルートディレクトリ ("/") を指定します。
- 4 [ファイル]メニュー (Windows の場合) または [処理]メニュー (UNIX の場合) から、[NetBackup マシンおよびポリシー形式の指定]を選択します。
- 5 [NetBackup マシンおよびポリシー形式の指定]ウィザードで、リストアのソースと宛先の詳細を入力します。
 - リストア操作を実行するソースとして HBase HMaster を指定します。
[リストアのソースクライアント (Source client for restores)]リストから、必要な HMaster を選択します。
 - バックアップホストを宛先クライアントとして指定します。
[リストアの宛先クライアント]リストから、必要なバックアップホストを選択します。
 - [NetBackup マシンおよびポリシー形式の指定]ウィザードで、リストアのポリシー形式の詳細を入力します。
[リストアのポリシー形式]リストから、リストアのポリシー形式として **BigData** を選択します。
[OK]をクリックします。
- 6 [バックアップ履歴]に移動し、リストアするバックアップイメージを選択します。
- 7 [ディレクトリ構造]ペインで、[ディレクトリ]を展開します。
そのディレクトリの下にある後続のすべてのファイルとフォルダが、[選択されたディレクトリの内容]ペインに表示されます。
- 8 [選択されたディレクトリの内容 (Contents of Selected Directory)]ペインで、リストアする HBase ファイルにチェックマークを付けます。
- 9 [リストア]をクリックします。
- 10 [マークされたファイルのリストア (Restore Marked Files)]ダイアログボックスで[個々のディレクトリやファイルを異なる位置にリストア (Restore individual directories and files to different locations)]を選択します。
- 11 ソース HBase ディレクトリを選択します。

- 12 [選択された宛先の変更 (Change Selected Destinations)]をクリックします。
[選択された宛先の変更 (Change Selected Destinations)]ダイアログボックスが表示されます。
- 13 [宛先 (Destination)]フィールドで、宛先ディレクトリの最後にアーカイブを追加します。



- 14 [OK]をクリックします。
- 15 [リストアの開始]をクリックします。
- 16 リストアされたファイルを確認します。

HBase クラスタをリストアするためのベストプラクティス

HBase クラスタをリストアするときは、次の内容を考慮してください。

- リストアジョブを実行する前に、クラスタにリストアジョブを完了する十分な領域があることを確認します。
- ファイアウォールの設定を更新して、バックアップホストが HBase クラスタと通信できるようにします。
- サイズの大きいテーブルをリストアする場合は、バックアップホストで大きい値にタイムアウト値が設定されていることを確認します。

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。

- [NetBackup for HBase のデバッグログについて](#)
- [バックアップがエラー 6609 で失敗する](#)
- [バックアップがエラー 6601 で失敗する](#)
- [バックアップがエラー 6623 で失敗する](#)
- [リストアがエラー 2850 で失敗する](#)
- [バックアップがエラー 20 で失敗する](#)
- [バックアップがエラー 112 で失敗する](#)
- [バックアップ操作がエラー 6654 で失敗する](#)
- [コンテナベースの NetBackup Appliance を再起動した後、NetBackup 構成ファイルおよび証明書ファイルが保持されない](#)
- [ディザスタリカバリ後に構成ファイルがリカバリされない](#)

NetBackup for HBase のデバッグログについて

NetBackup は、バックアップ操作とリストア操作に関連するさまざまなプロセスのプロセス固有のログを保持します。これらのログを調べて、問題の根本原因を見つけることができます。

これらのログフォルダは、ログの記録用にあらかじめ存在している必要があります。これらのフォルダが存在しない場合は作成する必要があります。

次のディレクトリにあるログフォルダ

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

- UNIX または Linux の場合: /usr/opensv/var/global/logs

表 5-1 HBase に関連する NetBackup ログ

ログフォルダ	メッセージの内容	ログの場所
install_path/NetBackup/logs/bpVutil	ポリシーの構成	マスターサーバー
install_path/NetBackup/logs/nbaapidiscv	BigData フレームワーク、検出、および HBase 構成ファイルのログ	バックアップホスト
install_path/NetBackup/logs/bpbrm	ポリシー検証、バックアップ、およびリストア操作	メディアサーバー
install_path/NetBackup/logs/bpbkar	バックアップ	バックアップホスト
install_path/NetBackup/logs/tar	リストアおよび HBase 構成ファイル	バックアップホスト

詳しくは、『[NetBackup ログリファレンスガイド](#)』を参照してください。

バックアップがエラー 6609 で失敗する

バックアップが次のエラーで失敗します。

```
(6609) The NetBackup plug-in cannot complete the operation because the object is invalid.
```

回避方法:

HBase プラグインをダウンロードしてインストールします。

バックアップがエラー 6601 で失敗する

バックアップが次のエラーで失敗します。

```
(6601) One or more of the input parameters or arguments are invalid.
```

回避方法:

存在しないテーブルをバックアップ対象から削除します。

バックアップがエラー 6623 で失敗する

バックアップが次のエラーで失敗します。

```
(6623) Failed to connect to the application server or the backup host. The server is either shut down or not reachable.
```

回避方法:

HMaster またはデータノードがオフラインです。HMaster またはデータノードを確実にオンラインにします。

リストアがエラー 2850 で失敗する

リストアが次のエラーで失敗します。

```
(2850) Restore error.
```

回避方法:

宛先クライアントがバックアップホストであることを確認します。

バックアップがエラー 20 で失敗する

バックアップが次のエラーで失敗します。

```
(20) invalid command parameter.
```

回避方法:

バックアップホストをオンラインにし、HMaster に確実に接続するようにします。

バックアップがエラー 112 で失敗する

バックアップが次のエラーで失敗します。

```
(112) no files specified in the file list.
```

回避策

HBase クレデンシヤルが NetBackup マスターサーバーに追加されていないか、追加されたクレデンシヤルが無効です。

HBase クレデンシヤルを NetBackup マスターサーバーに確実に追加します。

NetBackup tpconfig コマンドを使用してクレデンシヤルを追加できます。p.20 の「[NetBackup での HBase クレデンシヤルの追加](#)」を参照してください。

バックアップ操作がエラー 6654 で失敗する

このエラーは、次のシナリオ中に発生します。

- HBase のクレデンシヤルが NetBackup マスターサーバーに追加されていない場合
回避方法:
HBase のクレデンシヤルが NetBackup マスターサーバーに追加されていることを確認します。tpconfig コマンドを使用します。詳しくは、p.20 の「[NetBackup での HBase クレデンシヤルの追加](#)」を参照してください。を参照してください。
- バックアップホストに HBase プラグインがインストールされていない場合
回避方法:
バックアップ操作を開始する前に、すべてのバックアップホストに確実に HBase プラグインファイルをインストールします。
- バックアップホストとして使用されている NetBackup クライアントが許可リストに載っていない場合
回避方法:
バックアップ操作を開始する前に、バックアップホストとして使用されている NetBackup クライアントが許可リストに載っていることを確認します。
p.19 の「[NetBackup マスターサーバー上の NetBackup クライアントのホワイトリスト](#)」を参照してください。

コンテナベースの NetBackup Appliance を再起動した後、NetBackup 構成ファイルおよび証明書ファイルが保持されない

コンテナベースの NetBackup Appliance を何らかの理由で再起動した後、hadoop.conf または hbase.conf などの NetBackup 構成ファイル、または SSL 証明書や CRL パスが保持されません。この問題は、バックアップホストとしてコンテナベースの NetBackup Appliance を使用して Hadoop または HBase の作業負荷を保護する場合に該当します。

理由:

NetBackup Appliance 環境では、Docker ホストの永続的な場所で利用可能なファイルは再起動操作後も保持されます。hadoop.conf と hbase.conf ファイルはカスタム構成ファイルであり、永続的な場所に一覧表示されません。

構成ファイルは、フェールオーバー中の HA (高可用性) ノードやバックアップのスレッド数などの値を定義するために使用されます。これらのファイルが削除された場合、バックアップでは、HA とスレッド数の両方にデフォルト値 (それぞれ、プライマリ名ノードと 4) が使用されます。このようなケースでは、プライマリノードが停止した場合のみ、プラグインがセカンダリサーバーの検出に失敗するためバックアップは失敗します。

SSL 証明書と CRL パスのファイルが永続的ではない場所に格納されている場合、アプリケーションを再起動するとバックアップとリストア操作は失敗します。

回避方法:

Hadoop と HBase のカスタム構成ファイルが再起動後に削除された場合は、次の場所にファイルを手動で作成できます。

- Hadoop: /usr/opensv/var/global/hadoop.conf
- HBase: /usr/opensv/var/global/hbase.conf

Hadoop または HBase の SSL 証明書と CRL に署名した CA 証明書は、次の場所に格納できます。

/usr/opensv/var/global/

ディザスタリカバリ後に構成ファイルがリカバリされない

SSL 対応 (HTTPS) の HBase クラスタまたは HBase クラスタで高可用性のために NetBackup マスターサーバーをバックアップホストとして使用する場合、完全なカタログリカバリを実行すると、hbase.conf 構成ファイルがリカバリされません。

構成ファイルは手動で作成してください。構成ファイルには、次の形式を使用してください。

```
{
  "application_servers":
  {
    "primary.host.com":
    {
      "use_ssl":true
      "failover_namenodes":
      [
        {
          "hostname":"secondary.host.com",
          "use_ssl":true
          "port":11111
        }
      ],
      "port":11111
    }
  },
  "number_of_threads":5
}
```

記号

- インストール
 - 検証 16
- ディザスタリカバリ 31
- バックアップ 8、33～34
- ホワイトリスト
 - バックアップホスト 19
- ポリシー
 - 構成 26
- ライセンス 14
- リストア 9、37
 - bprestore コマンド 38
 - 代替 HMaster 39
- リストア (Restore) 36
- 並列ストリームフレームワーク 6
- 互換性
 - サポート対象のオペレーティングシステム 14
- 作成
 - BigData バックアップポリシー 26
- 制限事項 11
- 削除
 - バックアップホスト 18
- 概要
 - インストール 6
 - バックアップ 6
 - リストア 6
 - 構成 6
 - 配備 6
- 準備 14
- 用語 10
- 追加
 - バックアップホスト 18

B

- BigData ポリシー
 - NetBackup 管理コンソール 27
 - コマンドラインインターフェース 29
 - ポリシーの設定ウィザード 27
 - ポリシーユーティリティ 28

H

- HBase クレデンシヤル追加 20

K

- Kerberos
 - インストール後 26
- kerberos
 - バックアップ 34
 - リストア 34

N

- NetBackup
 - デバッグログ 45
- NetBackup アブライアンス
 - バックアップホスト 20