

# Veritas NetBackup™ for Hadoop 管理者ガイド

UNIX、Windows および Linux

リリース 9.0

**VERITAS™**

# Veritas Hadoop 管理者ガイド

最終更新日: 2021-02-01

## 法的通知と登録商標

Copyright © 2021 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](mailto:CustomerCare@veritas.com)

日本

[CustomerCare\\_Japan@veritas.com](mailto: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](mailto: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](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# 目次

<b>第 1 章</b>	<b>概要</b> .....	6
	NetBackup を使用した Hadoop データの保護 .....	6
	Hadoop データのバックアップ .....	8
	Hadoop データのリストア .....	9
	NetBackup for Hadoop の用語 .....	10
	制限事項 .....	12
<b>第 2 章</b>	<b>NetBackup 用 Hadoop プラグインの前提条件の検証</b> .....	13
	Hadoop プラグインの配備について .....	13
	Hadoop プラグインの前提条件 .....	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 サーバーおよびクライアントの要件 .....	14
	NetBackup の Hadoop プラグインのライセンス .....	14
	Hadoop クラスタの準備 .....	14
	Hadoop プラグインを配備するためのベストプラクティス .....	15
<b>第 3 章</b>	<b>NetBackup for Hadoop の構成</b> .....	16
	NetBackup for Hadoop の構成について .....	16
	バックアップホストの管理 .....	17
	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 .....	20
	バックアップホストとしての NetBackup アプライアンスの設定 .....	21
	NetBackup での Hadoop クレデンシャルの追加 .....	21
	Hadoop 構成ファイルを使用した Hadoop プラグインの構成 .....	22
	高可用性 Hadoop クラスタ用の NetBackup の構成 .....	23
	Hadoop クラスタのカスタムポートの設定 .....	26
	バックアップホストのスレッド数の設定 .....	27
	NetBackup および Hadoop クラスタ間での SSL 対応 (HTTPS) 通 信の設定 .....	28
	Kerberos を使用する Hadoop クラスタの設定 .....	33
	Hadoop プラグインの NetBackup ポリシーの構成 .....	34
	BigData バックアップポリシーの作成 .....	34
	Hadoop クラスタのディザスタリカバリ .....	39

<b>第 4 章</b>	<b>Hadoop のバックアップとリストアの実行</b> .....	41
	Hadoop クラスタのバックアップについて .....	41
	Kerberos 認証を使用する Hadoop 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 .....	42
	Hadoop 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 .....	42
	Hadoop クラスタのバックアップ .....	43
	Hadoop クラスタのリストアについて .....	43
	Hadoop クラスタをリストアするためのベストプラクティス .....	44
	同じ Hadoop クラスタ上での Hadoop データのリストア .....	45
	代替の Hadoop クラスタ上での Hadoop データのリストア .....	48
<b>第 5 章</b>	<b>トラブルシューティング</b> .....	52
	NetBackup for Hadoop の問題のトラブルシューティングについて .....	52
	NetBackup for Hadoop のデバッグログについて .....	53
	Hadoop データのバックアップ問題のトラブルシューティング .....	53
	バックアップ操作がエラー 6609 で失敗する .....	54
	バックアップ操作がエラー 6618 で失敗した .....	54
	バックアップ操作がエラー 6647 で失敗する .....	54
	Hadoop で拡張属性 (xattrs) とアクセス制御リスト (ACL) がバックアッ プまたはリストアされない .....	55
	バックアップ操作がエラー 6654 で失敗する .....	56
	バックアップ操作が bpbrm エラー 8857 で失敗する .....	56
	バックアップ操作がエラー 6617 で失敗する .....	56
	バックアップ操作がエラー 6616 で失敗する .....	57
	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 .....	57
	バックアップイメージの選択でイメージが表示されているにもかかわらず、 リストア時に増分バックアップイメージが表示されない .....	58
	子バックアップジョブの 1 つがキューに投入された状態になる .....	58
	Hadoop データのリストア問題のトラブルシューティング .....	58
	リストアが 2850 エラーコードで失敗する .....	59
	NetBackup の Hadoop のリストアジョブが部分的に完了する .....	59
	Hadoop で拡張属性 (xattrs) とアクセス制御リスト (ACL) がバックアッ プまたはリストアされない .....	59
	Hadoop プラグインファイルがバックアップホスト上にない場合、リス トア操作が失敗する .....	59
	リストアが bpbrm エラー 54932 で失敗する .....	60
	リストア操作が bpbrm エラー 21296 で失敗する .....	60
	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 .....	60
<b>索引</b>	.....	62

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

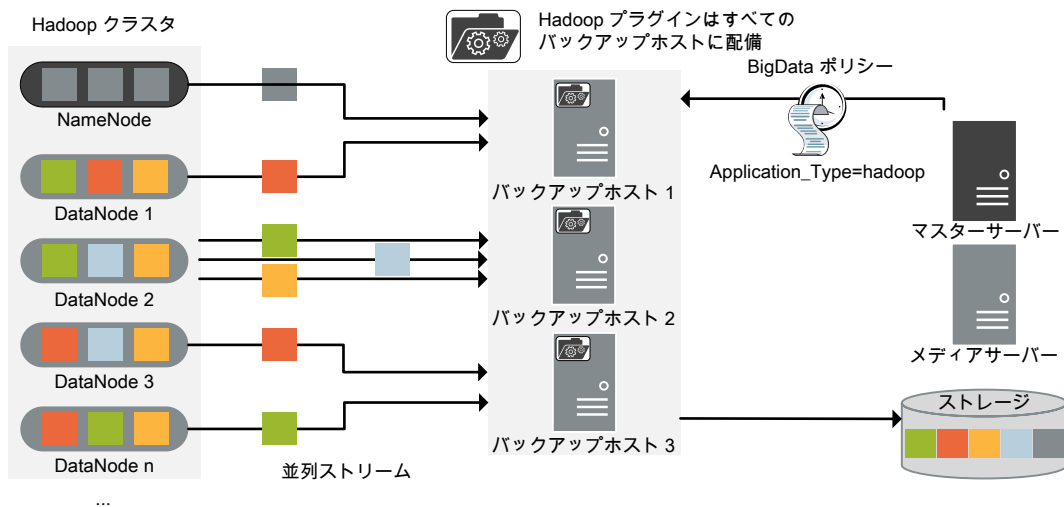
## NetBackup を使用した Hadoop データの保護

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 Hadoop 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 Hadoop 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 Hadoop 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 **DataNodes** 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。
- **Hadoop** クラスタと **NetBackup** 間の通信は、**Hadoop** 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、またはマスター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、**DataNodes** 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。
- **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 **Hadoop** 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「[Hadoop データのバックアップ](#)」を参照してください。
- p.9 の「[Hadoop データのリストア](#)」を参照してください。

- p.12 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。

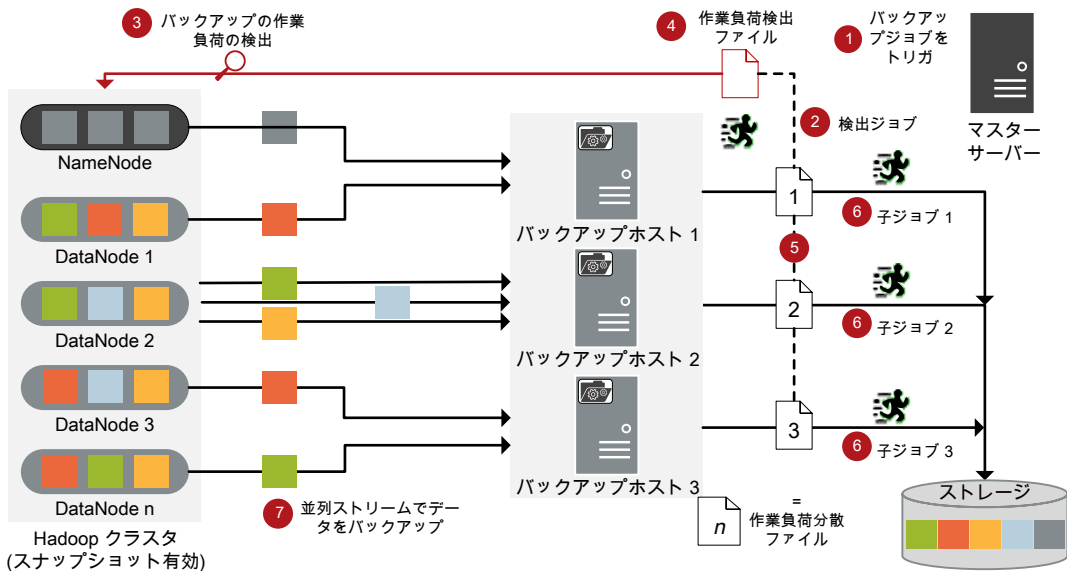
## Hadoop データのバックアップ

Hadoop 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 Hadoop DataNodes 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。

メモ: Hadoop バックアップ対象で指定されたすべてのディレクトリは、バックアップ前にスナップショット対応に設定する必要があります。

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マスターサーバーからトリガされます。
2. Hadoop 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 **NameNode** 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 **DataNodes** 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 **DataNodes** 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 **NameNode** 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のみ、複合バックアップジョブは完了します。

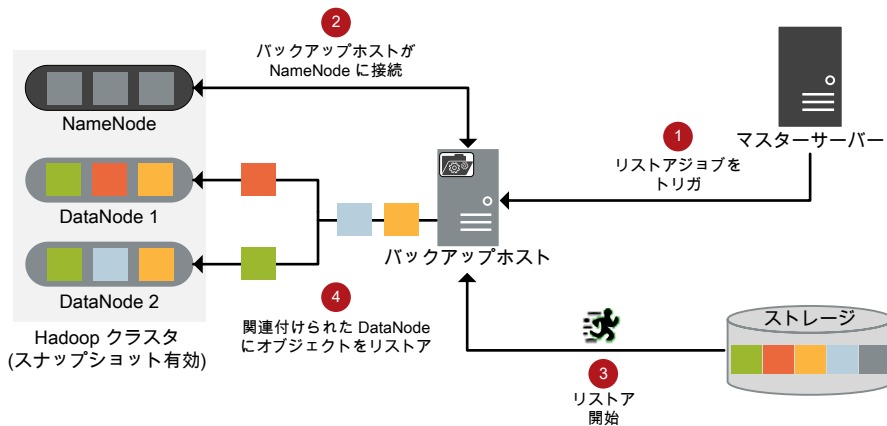
p.41 の「**Hadoop クラスタのバックアップについて**」を参照してください。

## Hadoop 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. マスター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 **NameNode** 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 **DataNodes** にリストアされます。

p.43 の「[Hadoop クラスタのリストアについて](#)」を参照してください。

## NetBackup for Hadoop の用語

次の表では、Hadoop 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><b>Hadoop</b> 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"> <li>■ 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。</li> <li>■ 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。</li> <li>■ バックアップが完了すると、ジョブは <b>NameNode</b> 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。</li> </ul>
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 <b>NameNode</b> 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 <b>DataNodes</b> 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 <b>NetBackup</b> 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 <b>DataNodes</b> 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 <b>NameNode</b> 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 <b>DataNodes</b> 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、<b>NetBackup</b> 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>

用語	定義
並列ストリーム	<b>NetBackup</b> 並列ストリーミングフレームワークにより、複数の <b>DataNodes</b> からのデータブロックを、複数のバックアップホストを同時に使用してバックアップできます。
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、またはマスターサーバーを、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。
<b>BigData</b> ポリシー	<b>BigData</b> 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"> <li>■ アプリケーションの種類を指定します。</li> <li>■ 分散マルチノード環境のバックアップを可能にします。</li> <li>■ バックアップホストを関連付けます。</li> <li>■ 作業負荷分散を実行します。</li> </ul>
アプリケーションサーバー	<b> Namenode</b> は、 <b>NetBackup</b> 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 <b>NameNode</b>	高可用性シナリオでは、1 つの <b>NameNode</b> を <b>BigData</b> ポリシーと <code>tpconfig</code> コマンドで指定する必要があります。この <b>NameNode</b> はプライマリ <b>NameNode</b> と呼ばれます。
フェールオーバー <b>NameNode</b>	高可用性シナリオでは、 <code>hadoop.conf</code> ファイル内で更新されるプライマリ <b>NameNode</b> 以外の <b>NameNode</b> は、フェールオーバー <b>NameNode</b> と呼ばれます。

**表 1-2 Hadoop の用語**

用語	定義
<b>NameNode</b>	<b>NameNode</b> は、リストア中にソースクライアントとしても使用されます。
<b>DataNode</b>	<b>DataNode</b> は、 <b>Hadoop</b> で実際のデータを格納する役割を果たします。

用語	定義
スナップショット対応ディレクトリ (スナップショット可能)	<p>スナップショットは、ディレクトリがスナップショット対応になれば、どのディレクトリでも実行できます。</p> <ul style="list-style-type: none"><li>■ 各スナップショット対応ディレクトリは、<b>65,536</b> の同時スナップショットに対応できます。スナップショット対応ディレクトリの数に制限はありません。</li><li>■ 管理者は、どのディレクトリでもスナップショット対応に設定できます。</li><li>■ スナップショット対応ディレクトリは、その中にスナップショットがあると、それらすべてのスナップショットが削除されるまでは削除したり名前を変更したりできません。</li><li>■ 親または子のいずれかがスナップショット対応ディレクトリである場合、ディレクトリはスナップショット対応にできません。</li></ul>

## 制限事項

Hadoop 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、Hadoop クラスタとバックアップホストのサポート対象です。
- 委任トークン認証方法は、Hadoop クラスタではサポートされていません。
- Hadoop 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 Hadoop 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 Hadoop 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。
- 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 Hadoop プラグインの前提条件の検証

この章では以下の項目について説明しています。

- [Hadoop プラグインの配備について](#)
- [Hadoop プラグインの前提条件](#)
- [Hadoop クラスタの準備](#)
- [Hadoop プラグインを配備するためのベストプラクティス](#)

## Hadoop プラグインの配備について

Hadoop 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 Hadoop プラグインの配備

作業	参照先
前提条件と要件	p.14 の「 <a href="#">Hadoop プラグインの前提条件</a> 」を参照してください。
Hadoop クラスタの準備	p.14 の「 <a href="#">Hadoop クラスタの準備</a> 」を参照してください。
ベストプラクティス	p.15 の「 <a href="#">Hadoop プラグインを配備するためのベストプラクティス</a> 」を参照してください。
配備の検証	
構成	p.16 の「 <a href="#">NetBackup for Hadoop の構成について</a> 」を参照してください。

## Hadoop プラグインの前提条件

Hadoop プラグインを使用する前に、次の前提条件が満たされていることを確認します。

- 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 Hadoop 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 Hadoop 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 サーバーおよびクライアントの要件

NetBackup サーバーが次の要件を満たしていることを確認します。

### NetBackup の Hadoop プラグインのライセンス

NetBackup 用 Hadoop 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。

## Hadoop クラスタの準備

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

- Hadoop ディレクトリがスナップショット対応であることを確認します。  
ディレクトリをスナップショット可能にするには、**NameNodes** で次のコマンドを実行します。

```
hdfs dfsadmin -allowSnapshot directory_name
```

---

**メモ:** 親または子のいずれかがスナップショット対応ディレクトリである場合、ディレクトリはスナップショット対応にできません。

---

詳しくは、Hadoop のマニュアルを参照してください。

- バックアップホストが Hadoop クラスタと通信できるように、ファイアウォールの設定を更新 (適切なポートが Hadoop クレデンシャルとともに追加されていることを確認) します。

- すべての **NameNodes** と **DataNodes** 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/resolv.conf` ファイルに適切な **DNS** エントリを追加します。
- **Hadoop** クラスタで `webhdfs` サービスが有効になっていることを確認します。

## Hadoop プラグインを配備するためのベストプラクティス

Hadoop プラグインを配備して、NetBackup for Hadoop 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、`hadoop.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 **NameNodes** と **DataNodes** 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/resolv.conf` ファイルに適切な **DNS** エントリを追加します。
- **NameNode** と **DataNodes** 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。
- **NameNode** のホスト名とポートは、**Hadoop** クラスタの `core-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。
- **SSL (HTTPS)** が有効になっている **Hadoop** クラスタに対して次のことを確認します。
  - **Hadoop** クラスタのすべてのノードからの公開鍵を含むバックアップホスト上に有効な証明書が存在する。
  - **CRL** を使用する **Hadoop** クラスタの場合は、**CRL** が有効で期限が切れていないことを確認する。

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

## NetBackup for Hadoop の構成について

表 3-1 NetBackup for Hadoop の構成

作業	参照先
バックアップホストの追加	p.17 の「 <a href="#">バックアップホストの管理</a> 」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.20 の「 <a href="#">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</a> 」を参照してください。



作業	参照先
NetBackup での Hadoop クレデンシャルの追加	p.21 の「 <a href="#">NetBackup での Hadoop クレデンシャルの追加</a> 」を参照してください。
Hadoop 構成ファイルを使用した Hadoop プラグインの構成	p.22 の「 <a href="#">Hadoop 構成ファイルを使用した Hadoop プラグインの構成</a> 」を参照してください。 p.23 の「 <a href="#">高可用性 Hadoop クラスタ用の NetBackup の構成</a> 」を参照してください。 p.27 の「 <a href="#">バックアップホストのスレッド数の設定</a> 」を参照してください。
Kerberos を使用する Hadoop クラスタ用のバックアップホストの構成	p.33 の「 <a href="#">Kerberos を使用する Hadoop クラスタの設定</a> 」を参照してください。
Hadoop プラグイン用の NetBackup ポリシーの構成	p.34 の「 <a href="#">Hadoop プラグインの NetBackup ポリシーの構成</a> 」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、Hadoop 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 Hadoop プラグインの場合、バックアップホストは、Hadoop 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 9.0 のリリースでは、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 Hadoop プラグインは、すべてのバックアップホストにインストールされます。

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。

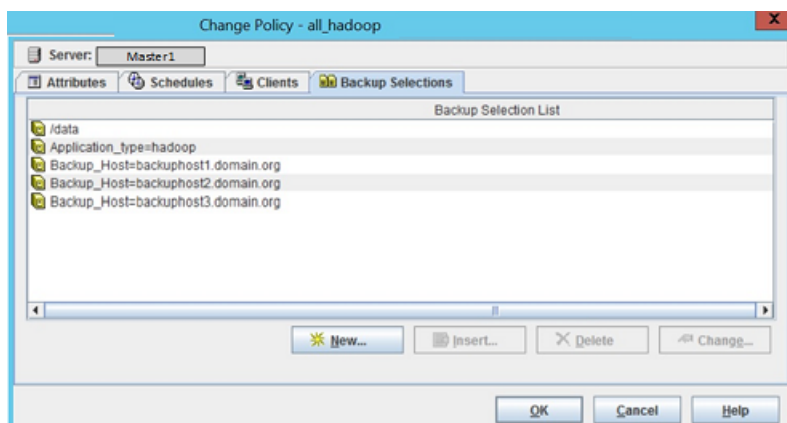
ポリシーの作成方法について詳しくは p.34 の「**BigData** バックアップポリシーの作成」を参照してください。

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=<IP アドレスまたはホスト名>**

ポリシーの作成方法について詳しくは p.34 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。

Windows の場合:

```
<Install_Path>%NetBackup%bin\admincmd\bpplinclude PolicyName -add  
"Backup_Host=IP_address or hostname"
```

UNIX の場合:

```
/usr/opensv/var/global/bin/admincmd/bpplinclude PolicyName -add  
"Backup_Host=IP_address or hostname"
```

詳しくは p.37 の「[Hadoop 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 **NameNodes** と **DataNodes** 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/resolv.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。

Windows の場合:

```
<Install_Path>%NetBackup%bin\admincmd\bpplinclude PolicyName  
-delete "Backup_Host=IP_address or hostname"
```

UNIX の場合:

```
/usr/opensv/var/global/bin/admincmd/bpplinclude PolicyName -delete  
'Backup_Host=IP_address or 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 Hadoop のバックアップホストとして使用する**  
詳しくは、ベリタスのテクニカルサポートに連絡し、担当者に 100039992 の記事を参照するよう伝えてください。
- **高可用性 Hadoop 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**  
詳しくは、ベリタスのテクニカルサポートに連絡し、担当者に 100039990 の記事を参照するよう伝えてください。

## NetBackup での Hadoop 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 Hadoop 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、Hadoop 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 Hadoop クレデンシャルを追加します。

`tpconfig` コマンドを使用してクレデンシャルの削除と更新を行うパラメータについて詳しくは

[https://www.veritas.com/content/support/ja\\_JP/DocumentBrowsing.html?product=NetBackup](https://www.veritas.com/content/support/ja_JP/DocumentBrowsing.html?product=NetBackup)  
『*NetBackup コマンドリファレンスガイド*』を参照してください。

Hadoop 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 Hadoop クラスタの場合、プライマリとフェールオーバーの NameNode 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 Hadoop クラスタの場合、「kerberos」を `application_server_user_id` 値として指定します。
- NameNode のホスト名とポートは、Hadoop クラスタの `core-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。
- パスワードについては、ランダムな値を指定します。たとえば、Hadoop です。

### NetBackup で Hadoop クレデンシヤルを追加するには

- 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。Hadoop クレデンシヤルを追加、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 application_type -requiredport IP_port_number [-password password [-key encryption_key]]` コマンドを各パラメータに適切な値を入力して実行し、Hadoop クレデンシヤルを追加します。

たとえば、`application_server_name` が `hadoop1` である Hadoop サーバーのクレデンシヤルを追加する場合、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 hadoop1 -application_type hadoop
-application_server_user_id Hadoop -requiredport 50070 -password
Hadoop
```

ここで、`-application_type` パラメータに指定された値 `hadoop` は Hadoop に対応します。

- 4 `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 Hadoop クレデンシヤルがあることを確認します。

## Hadoop 構成ファイルを使用した Hadoop プラグインの構成

バックアップホストは、Hadoop プラグインの設定を保存するために `hadoop.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。`hadoop.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。

バックアップとリストア操作を正常に実行するために必要なすべてのパラメータを設定していることを確認します。

---

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 Hadoop クラスタ用の NetBackup の構成](#)」を参照してください。
- p.26 の「[Hadoop クラスタのカスタムポートの設定](#)」を参照してください。
- p.27 の「[バックアップホストのスレッド数の設定](#)」を参照してください。
- p.28 の「[NetBackup および Hadoop クラスタ間での SSL 対応 \(HTTPS\) 通信の設定](#)」を参照してください。

hadoop.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_namenode":
    {
      "failover_namenodes":
      [
        {
          "hostname": "hostname_of_failover_namenode",
          "port": port_of_the_failover_namenode
        }
      ],
      "port": port_of_the_primary_namenode
    }
  },
  "number_of_threads": number_of_threads
}
```

## 高可用性 Hadoop クラスタ用の NetBackup の構成

NetBackup for Hadoop クラスタの構成時に高可用性 Hadoop 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 **NameNodes** (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 **NameNode** (プライマリとフェールオーバー) を指定します。
- `hadoop.conf` ファイルを作成して、**NameNode** (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。`hadoop.conf` ファイルは **JSON** 形式です。
- **NameNode** のホスト名とポートは、**Hadoop** クラスタの `core-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 **NameNode** 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 Hadoop クラスタの `hadoop.conf` ファイルを更新するには

1 次のパラメータで `hadoop.conf` ファイルを更新します。

```
{
  "application_servers":
  {
    "hostname_of_primary_namenode1":
    {
      "failover_namenodes":
      [
        {
          "hostname": "hostname_of_failover_namenode1",
          "port": port_of_failover_namenode1
        }
      ],
      "port":port_of_primary_namenode1
    }
  }
}
```

- 2 複数の Hadoop クラスタがある場合、同じ `hadoop.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_namenode1":
    {
      "failover_namenodes":
      [
        {
          "hostname": "hostname_of_failover_namenode1",
          "port": port_of_failover_namenode1
        }
      ],
      "port": port_of_primary_namenode1
    },
    "hostname_of_primary_namenode2":
    {
      "failover_namenodes":
      [
        {
          "hostname": "hostname_of_failover_namenode2",
          "port": port_of_failover_namenode2
        }
      ],
      "port": port_of_primary_namenode2
    }
  }
}
```

- 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/
```

## Hadoop クラスタのカスタムポートの設定

Hadoop 設定ファイルを使用すると、カスタムポートを設定できます。デフォルトでは、NetBackup は 50070 番ポートを使用します。

## Hadoop クラスタのカスタムポートを設定するには

- 1 次のパラメータで `hadoop.conf` ファイルを更新します。

```
{  
  "application_servers": {  
    "hostname_of_namenode1": {  
  
      "port": port_of_namenode1  
    }  
  }  
}
```

- 2 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/
```

## バックアップホストのスレッド数の設定

バックアップのパフォーマンスを向上させるため、各バックアップホストが許容するスレッド数 (ストリーム) を設定できます。さらにバックアップホストを追加するか、バックアップホストあたりのスレッド数を増やすことで、バックアップのパフォーマンスを改善できます。

スレッド数を決定する場合、次の内容を考慮してください。

- デフォルトの値は **4** です。
- 各バックアップホストに対して最小で **1** 個、最大で **32** 個のスレッドを設定できます。
- 各バックアップホストに異なるスレッド数を設定できます。
- スレッド数を設定するときは、利用可能なコア数と使用するコア数を考慮してください。ベストプラクティスとして、**1** コアに **1** スレッド設定することをお勧めします。たとえば、**8** つのコアを利用可能で、**4** つのコアを使用する場合、**4** 個のスレッドを設定します。

### スレッド数の設定のために `hadoop.conf` ファイルを更新するには

- 1 次のパラメータで `hadoop.conf` ファイルを更新します。

```
{  
  "number_of_threads": number_of_threads  
}
```

- 2 このファイルをバックアップホストの次の場所にコピーします。

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

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

NetBackup と Hadoop クラスタ間で SSL 対応 (HTTPS) 通信を有効にするには、次の手順を実行します。

- `use_ssl` パラメータを次の形式で使用して、バックアップホストの `/usr/opensv/var/global/` ディレクトリにある `hadoop.conf` ファイルを更新します。

```
{
  "application_servers":
  {
    "hostname_of_namenode1":
    {
      "use_ssl":true
    }
  }
}
```

SSL と HA の構成ファイルの形式:

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

デフォルトでは、この値は `false` に設定されています。

複数のバックアップホストを使用する場合、`hadoop.conf` ファイルで `use_ssl` パラメータを定義したバックアップホストが通信に使用されます。

すべての **Hadoop** クラスタについて、`hadoop.conf` ファイルで `use_ssl` パラメータを定義する必要があります。

- `nbsetconfig` コマンドを使用して、アクセスホストで次の **NetBackup** 構成オプションを構成します。  
 構成オプションについては、『**NetBackup 管理者ガイド**』を参照してください。

<code>ECA_TRUST_STORE_PATH</code>	<p>信頼できるすべてのルート CA 証明書を含む証明書バンドルファイルのファイルパスを指定します。</p> <p>この外部 CA のオプションをすでに構成してある場合は、Hadoop の CA 証明書を既存の外部証明書トラストストアに追加します。</p> <p>このオプションを構成していない場合は、必要な Hadoop サーバーの CA 証明書をすべてトラストストアに追加して、このオプションを設定します。</p> <p>p.30 の「<a href="#">NetBackup サーバーとクライアントの ECA_TRUST_STORE_PATH</a>」を参照してください。</p>
<code>ECA_CRL_PATH</code>	<p>外部 CA の証明書失効リスト (CRL) が保存されているディレクトリのパスを指定します。</p> <p>この外部 CA のオプションをすでに構成してある場合は、Hadoop サーバーの CRL を CRL キャッシュに追加します。</p> <p>このオプションを構成していない場合は、必要なすべての CRL を CRL キャッシュに追加してオプションを設定します。</p> <p>p.30 の「<a href="#">NetBackup サーバーとクライアントの ECA_CRL_PATH</a>」を参照してください。</p>
<code>HADOOP_SECURE_CONNECT_ENABLED</code>	<p>このオプションは、Hadoop の安全な通信に影響します。</p> <p><code>hadoop.conf</code> ファイルで <code>use_ssl</code> を <code>true</code> に設定した場合は、この値を <code>YES</code> に設定します。<code>use_ssl</code> を <code>true</code> に設定すると、すべての Hadoop クラスタに単一の値を適用できます。</p> <p>Hadoop では、デフォルトで安全な通信が有効です。</p> <p>このオプションを使用すると、セキュリティ証明書検証をスキップできます。</p> <p>p.31 の「<a href="#">サーバーとクライアントの HADOOP_SECURE_CONNECT_ENABLED</a>」を参照してください。</p>
<code>HADOOP_CRL_CHECK</code>	<p>CRL で Hadoop サーバー証明書の失効状態を検証できます。</p> <p><code>use_ssl</code> を <code>true</code> に設定すると、すべての Hadoop クラスタに単一の値を適用できます。</p> <p>デフォルトでは、このオプションは無効になっています。</p> <p>p.32 の「<a href="#">NetBackup サーバーとクライアントの HADOOP_CRL_CHECK</a>」を参照してください。</p>

## NetBackup サーバーとクライアントの ECA\_TRUST\_STORE\_PATH

ECA\_TRUST\_STORE\_PATH オプションでは、信頼できるすべてのルート CA 証明書を含む証明書バンドルファイルへのファイルパスを指定します。

この証明書ファイルには、PEM 形式の 1 つ以上の証明書が必要です。

Windows 証明書ストアを使用する場合、ECA\_TRUST\_STORE\_PATH オプションを指定しないでください。

トラストストアは次の形式の証明書をサポートします。

- 信頼できるルート認証局の、バンドルされている証明書を持つ PKCS #7 または P7B ファイル。このファイルは、PEM または DER でエンコードされている場合があります。
- 信頼できるルート認証局の PEM エンコードされた証明書が連結されて含まれるファイル。

このオプションは、ファイルベースの証明書で必須です。

表 3-2 ECA\_TRUST\_STORE\_PATH の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。
使用方法	<p>オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。</p> <p>これらのコマンドについて詳しくは、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p> <p>次の形式を使用します。</p> <p>ECA_TRUST_STORE_PATH = <i>Path to the external CA certificate</i></p> <p>例: c:\rootCA.pem</p>
同等の管理コンソールのプロパティ	NetBackup 管理コンソールのホストプロパティには、このエントリに相当するエントリは存在しません。

## NetBackup サーバーとクライアントの ECA\_CRL\_PATH

ECA\_CRL\_PATH オプションは、外部認証局 (CA) の証明書失効リスト (CRL) が保存されているディレクトリのパスを指定します。

これらの CRL は、NetBackup CRL キャッシュにコピーされます。CRL キャッシュの CRL で外部証明書の失効状態が検証されます。

CRL キャッシュ内の CRL は、ECA\_CRL\_PATH に指定されたディレクトリにある CRL に、ECA\_CRL\_PATH\_SYNC\_HOURS オプションに基づいて定期的に更新されます。

ECA\_CRL\_CHECK または HADOOP\_CRL\_CHECK オプションが DISABLE (または 0) に設定されておらず、ECA\_CRL\_PATH オプションが指定されていない場合、NetBackup は CRL 配布ポイント (CDP) で指定された URL から CRL をダウンロードし、それらを使用してピアホストの証明書の失効状態を検証します。

---

**メモ:** 仮想化サーバー証明書の失効状態の検証には、VIRTUALIZATION\_CRL\_CHECK オプションを使用します。

Hadoop サーバー証明書の失効状態の検証には、HADOOP\_CRL\_CHECK オプションを使用します。

---

**表 3-3** ECA\_CRL\_PATH の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。  VMware、RHV サーバー、Nutanix AHV、または Hadoop に対して証明書の検証が必要な場合、NetBackup がホストの通信に使用する認証局 (NetBackup CA または外部 CA) に関係なく、NetBackup マスターサーバーとそれぞれのアクセスホストまたはバックアップホストでこのオプションを設定する必要があります。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。  これらのコマンドについて詳しくは、『 <a href="#">NetBackup コマンドリファレンスガイド</a> 』を参照してください。  次の形式を使用して、CRL ディレクトリのパスを指定します。  ECA_CRL_PATH = <i>Path to the CRL directory</i>
同等の管理コンソールのプロパティ	NetBackup 管理コンソールのホストプロパティには、このエントリに相当するエントリは存在しません。

## サーバーとクライアントの **HADOOP\_SECURE\_CONNECT\_ENABLED**

HADOOP\_SECURE\_CONNECT\_ENABLED オプションを指定すると、Hadoop サーバー証明書をルートまたは中間の認証局 (CA) 証明書を使用して検証できます。

**表 3-4** HADOOP\_SECURE\_CONNECT\_ENABLED の情報

使用方法	説明
使用する場所	すべてのバックアップホスト
使用方法	<p>オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。</p> <p>これらのコマンドについて詳しくは、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p> <p>デフォルトでは、HADOOP_SECURE_CONNECT_ENABLED は YES に設定されています。</p> <p><b>Hadoop</b> の証明書検証を有効にするには、次の形式を使用します。</p> <pre>HADOOP_SECURE_CONNECT_ENABLED = YES</pre>
同等の管理コンソールのプロパティ	<b>NetBackup</b> 管理コンソールのホストプロパティには、このエントリに相当するエントリは存在しません。

## NetBackup サーバーとクライアントの HADOOP\_CRL\_CHECK

HADOOP\_CRL\_CHECK オプションを使用すると、**Hadoop** サーバーの外部証明書の失効の確認レベルを指定できます。確認に基づいて、ホストとの通信時に、証明書失効リスト (CRL) に対して **Hadoop** サーバー証明書の失効状態が検証されます。

デフォルトでは、HADOOP\_CRL\_CHECK は無効になっています。証明書失効リスト (CRL) に対して **Hadoop** サーバー証明書の失効状態を検証する場合は、オプションを別の値に設定します。

ECA\_CRL\_PATH 構成オプションまたは CRL 配布ポイント (CDP) で指定されているディレクトリの CRL を使用できます。

p.30 の「[NetBackup サーバーとクライアントの ECA\\_CRL\\_PATH](#)」を参照してください。

**表 3-5** HADOOP\_CRL\_CHECK の情報

使用方法	説明
使用する場所	すべてのバックアップホスト



使用方法	説明
使用方法	<p>オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。</p> <p>これらのコマンドについて詳しくは、『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p> <p>次の形式を使用します。</p> <pre>HADOOP_CRL_CHECK = CRL check</pre> <p>次のいずれかを指定できます。</p> <ul style="list-style-type: none"> <li>■ <b>DISABLE</b> (または <b>0</b>) - 失効の確認を無効にします。ホストとの通信時に、CRL で証明書の失効状態は検証されません。これはデフォルト値です。</li> <li>■ <b>LEAF</b> (または <b>1</b>) - CRL でリーフ証明書の失効状態が検証されます。</li> <li>■ <b>CHAIN</b> (または <b>2</b>) - CRL で証明書チェーンの証明書すべての失効状態が検証されます。</li> </ul>
同等の管理コンソールのプロパティ	<p><b>NetBackup</b> 管理コンソールのホストプロパティには、このエントリに相当するエントリは存在しません。</p>

### bp.conf ファイルのパラメータ値の例

SSL 対応 (HTTPS) CRL ベースの Hadoop クラスタの bp.conf ファイルに追加された値の例を次に示します。

```
ECA_TRUST_STORE_PATH=/tmp/cacert.pem
ECA_CRL_PATH=/tmp/backuphostdirectory
HADOOP_SECURE_CONNECT_ENABLED=YES/NO
HADOOP_CRL_CHECK=DISABLE / LEAF / CHAIN
```

## Kerberos を使用する Hadoop クラスタの設定

Kerberos を使用する Hadoop 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** パッケージが配布されていることを確認します。
  - RHEL の場合は **krb5-workstation** パッケージ
  - SUSE の場合は **krb5-client**
- 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_ccache_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。

---

- Hadoop のクレデンシヤルを 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.21 の「[NetBackup での Hadoop クレデンシヤルの追加](#)」を参照してください。
- Kerberos 認証を使用する Hadoop クラスタのバックアップとリストア操作については、Hadoop クラスタを認証するため、Hadoop 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.42 の「[Kerberos 認証を使用する Hadoop 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。
- Kerberos を使用するには、ユーザーは、HDFS のフルアクセスと所有権を持つスーパーユーザーである必要があります。バックアップホストのユーザーに有効なトークンが必要です。

## Hadoop プラグインの 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 の Hadoop 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。

---

**メモ:** NameNode のホスト名とポートは、Hadoop クラスタの `core-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。

---

BigData ポリシーの作成方法について詳しくは、p.34 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

Hadoop 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。

### Hadoop 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: Hadoop 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。

## Hadoop 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)]を展開します。
- 2 [処理 (Actions)]メニューで[新規 (New)]>[ポリシー (Policy)]をクリックします。
- 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、Hadoop 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=hadoop**  
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。
  - バックアップを作成するファイルのパスまたはディレクトリ  
複数のファイルパスを指定できます。

---

**メモ:** `BigData` ポリシーを `Application_Type=hadoop` 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ディレクトリまたはフォルダには、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。

## Hadoop 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

Hadoop 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。

`bppolicynew 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 **Hadoop** として指定します。

**Windows** の場合:

`bpplinclude PolicyName -add "Application_Type=hadoop"`

**UNIX** の場合:

`bpplinclude PolicyName -add 'Application_Type=hadoop'`

---

**メモ:** `Application_Type=hadoop` のパラメータ値は大文字と小文字が区別されません。

---

- 7 Hadoop 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=IP_address or hostname"
```

UNIX の場合:

```
bpplinclude PolicyName -add 'Backup_Host=IP_address or 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 Hadoop 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 "/hdfsfoldername"
```

UNIX の場合:

```
bpplinclude PolicyName -add '/hdfsfoldername'
```

---

**メモ:** BigData ポリシーを Application\_Type=hadoop で定義するときにバックアップ対象に使用されるディレクトリまたはフォルダには、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 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、NameNode 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  
"HadoopServerNameNode" "Linux" "RedHat"
```

UNIX の場合:

```
bpplclients PolicyName -M 'MasterServerName' -add  
'HadoopServerNameNode' '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、**Hadoop** 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、**Hadoop** 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、`/usr/opensv/var/global/bin` に移動します。

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。

## Hadoop クラスタのディザスタリカバリ

Hadoop 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 3-6**                    **ディザスタリカバリの実行**

タスク	説明
<p>Hadoop 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 Hadoop クラスタと通信できるようにします。</p> <p>Hadoop クラスタで webhdfs 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「<a href="#">Hadoop クラスタの準備</a>」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 Hadoop クラスタと NetBackup の間のシームレスな通信を確立するには、Hadoop のクレデンシャルを 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。</p>	<p>tpconfig コマンドを使用して、NetBackup マスターサーバーに Hadoop のクレデンシャルを追加します。</p> <p>p.21 の「<a href="#">NetBackup での Hadoop クレデンシャルの追加</a>」を参照してください。</p>
<p>バックアップホストは、Hadoop プラグインの設定を保存するために hadoop.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。hadoop.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"> <li>■ p.23 の「<a href="#">高可用性 Hadoop クラスタ用の NetBackup の構成</a>」を参照してください。</li> <li>■ p.27 の「<a href="#">バックアップホストのスレッド数の設定</a>」を参照してください。</li> </ul>
<p>元の NameNode 名で BigData ポリシーを更新します。</p>	<p>p.34 の「<a href="#">Hadoop プラグインの NetBackup ポリシーの構成</a>」を参照してください。</p>



# Hadoop 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。

- [Hadoop クラスタのバックアップについて](#)
- [Hadoop クラスタのリストアについて](#)

## Hadoop 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 Hadoop 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「 <a href="#">Hadoop データのバックアップ</a> 」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.42 の「 <a href="#">Kerberos 認証を使用する Hadoop 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</a> 」を参照してください。
Hadoop クラスタのバックアップ	p.43 の「 <a href="#">Hadoop クラスタのバックアップ</a> 」を参照してください。
ベストプラクティス	p.42 の「 <a href="#">Hadoop 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</a> 」を参照してください。

タスク	参照先
トラブルシューティングのヒント	<p>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。</p> <pre>/usr/opencv/var/global/logs/nbaapidiscv</pre> <p>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> <p>p.53 の「<a href="#">Hadoop データのバックアップ問題のトラブルシューティング</a>」を参照してください。</p>

## Kerberos 認証を使用する Hadoop 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 Hadoop クラスタのバックアップとリストア操作については、Hadoop クラスタを認証するため、Hadoop 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/opencv/var/global/nbusers/hdfs_mykeytabfile.keytab
hdfs@MYCOMPANY.COM
```

設定に関連する情報も確認してください。p.33 の「[Kerberos を使用する Hadoop クラスタの設定](#)」を参照してください。

## Hadoop 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

Hadoop 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。

- Hadoop ファイルシステム全体のバックアップを作成する前に、バックアップ対象として「/」を指定し、「/」でスナップショットが有効になっていることを確認します。
- 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 Hadoop クラスタと通信できるようにします。

- HDFS 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。
- SSL (HTTPS) が有効になっている Hadoop クラスタに、有効な証明書があることを確認します。

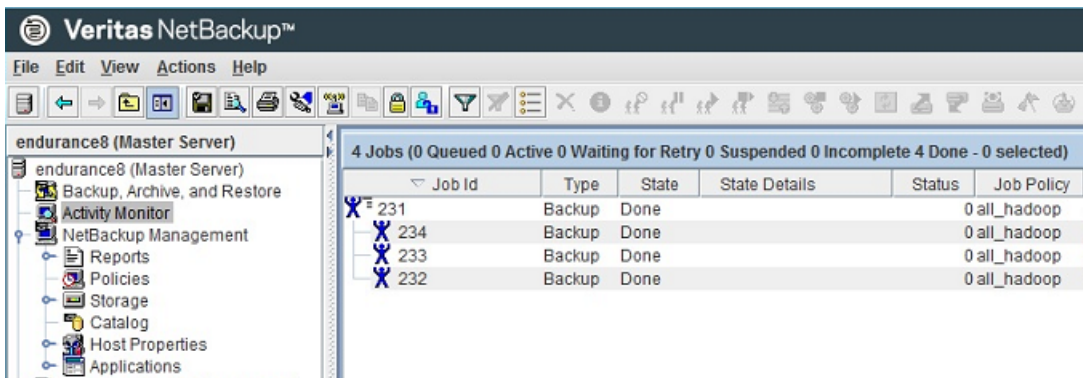
## Hadoop クラスタのバックアップ

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「[Hadoop 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、NameNode 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 NameNode 上のスナップショットをクリーンアップします。

## Hadoop 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 Hadoop データのリストア

作業	参照先
プロセスの理解	p.9 の「 <a href="#">Hadoop データのリストア</a> 」を参照してください。
Kerberos の前提条件をすべて満たす	p.42 の「 <a href="#">Kerberos 認証を使用する Hadoop 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</a> 」を参照してください。
同じ NameNode または Hadoop クラスタへの Hadoop データのリストア	<ul style="list-style-type: none"> <li>■ p.45 の「<a href="#">同じ Hadoop クラスタに Hadoop 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</a>」を参照してください。</li> <li>■ p.46 の「<a href="#">同じ Hadoop クラスタに Hadoop データをリストアするための bprestore コマンドの使用</a>」を参照してください。</li> </ul>
代替 NameNode または Hadoop クラスタへの Hadoop 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.48 の「 <a href="#">代替の Hadoop クラスタ上での Hadoop データのリストア</a> 」を参照してください。
ベストプラクティス	p.44 の「 <a href="#">Hadoop クラスタをリストアするためのベストプラクティス</a> 」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.58 の「 <a href="#">Hadoop データのリストア問題のトラブルシューティング</a> 」を参照してください。

## Hadoop クラスタをリストアするためのベストプラクティス

Hadoop 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 Hadoop クラスタと通信できるようにします。
- SSL (HTTPS) が有効になっている Hadoop クラスタのすべてのクラスタノードに、有効な証明書があることを確認します。
- バックアップホストに有効な PEM 証明書ファイルがあることを確認します。
- HTTP または HTTPS ベースのクラスタ用に、適切なパラメータが `hadoop.conf` ファイルに追加されていることを確認します。

- バックアップホストに期限が切れていない有効な CRL が含まれていることを確認します。
- アプリケーションレベルまたはファイルシステムレベルの暗号化は Hadoop ではサポートされません。リストアが正しく動作するには、Hadoop のスーパーユーザーである必要があります。

## 同じ Hadoop クラスタ上での Hadoop データのリストア

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

- Hadoop 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、Hadoop ディレクトリオブジェクトを表示することができます。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。Hadoop クラスタを構成するオブジェクト (Hadoop 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、Hadoop ディレクトリおよび個々の項目を参照し、リストアすることができます。ユーザーがリストアできるオブジェクトには、Hadoop ファイルとフォルダが含まれます。

## 同じ Hadoop クラスタに Hadoop 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 Hadoop クラスタに Hadoop 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 Hadoop NameNode を指定します。  
[リストアのソースクライアント]リストから、必要な NameNode 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]ペインで、リストアする **Hadoop** ファイルのチェックボックスを選択します。
  - 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 Hadoop クラスタに Hadoop 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。

バックアップの場所と同じ場所に **Hadoop** 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 **NameNode** 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。

## 代替場所で Hadoop データをリストアするには

- 1 管理者としてログオンします。
- 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 -R rename_file -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 **NameNode** 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。

/<source\_folder\_path> を /<destination\_folder\_path> に変更します。

## 代替の Hadoop クラスタ上での Hadoop データのリストア

**NetBackup** では、別の **NameNode** または **Hadoop** クラスタに **Hadoop** データをリストアできます。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。



---

**メモ:** 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。

---

---

**メモ:** NetBackup マスターサーバーに代替 NameNode または Hadoop クラスタのクレデンシャルが追加されており、NetBackup マスターサーバーでホワイトリストへの追加タスクが完了していることを確認してください。NetBackup で Hadoop クレデンシャルを追加する方法とホワイトリストへの追加手順の詳細については: p.21 の「[NetBackup での Hadoop クレデンシャルの追加](#)」を参照してください。p.20 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。

---

**Hadoop 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>	<code>/&lt;source_folder_path&gt;</code> を <code>/&lt;destination_folder_path&gt;</code> <code>ALT_APPLICATION_SERVER=&lt;alternate name node&gt;</code> に変更します。
<i>listfile</i>	リストアするすべての Hadoop ファイルのリス ト

- 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 **NameNode** 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_filepath to restore_filepath`

`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。

---

# 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 Hadoop の問題のトラブルシューティング](#)について
- [NetBackup for Hadoop のデバッグログ](#)について
- [Hadoop データのバックアップ問題のトラブルシューティング](#)
- [Hadoop データのリストア問題のトラブルシューティング](#)

## NetBackup for Hadoop の問題のトラブルシューティングについて

表 5-1 NetBackup for Hadoop の問題のトラブルシューティング

領域	参照
一般的なログとデバッグ	p.53 の「 <a href="#">NetBackup for Hadoop のデバッグログ</a> について」を参照してください。
バックアップの問題	p.53 の「 <a href="#">Hadoop データのバックアップ問題のトラブルシューティング</a> 」を参照してください。
リストアの問題	p.58 の「 <a href="#">Hadoop データのリストア問題のトラブルシューティング</a> 」を参照してください。
問題を避けるために、ベストプラクティスも確認	p.15 の「 <a href="#">Hadoop プラグインを配備するためのベストプラクティス</a> 」を参照してください。 p.42 の「 <a href="#">Hadoop 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</a> 」を参照してください。 p.44 の「 <a href="#">Hadoop クラスタをリストアするためのベストプラクティス</a> 」を参照してください。

# NetBackup for Hadoop 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 5-2 Hadoop 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
<code>install_path/NetBackup/logs/bpVMutil</code>	ポリシーの構成	マスターサーバー
<code>install_path/NetBackup/logs/nbaapidisvcv</code>	BigData フレームワーク、検出、および Hadoop 構成ファイルのログ	バックアップホスト
<code>install_path/NetBackup/logs/bpbbrm</code>	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
<code>install_path/NetBackup/logs/bpbkar</code>	バックアップ	バックアップホスト
<code>install_path/NetBackup/logs/tar</code>	リストアおよび Hadoop 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。

## Hadoop データのバックアップ問題のトラブルシューティング

次の項を参照してください。

- p.53 の「[NetBackup for Hadoop のデバッグログについて](#)」を参照してください。
- p.54 の「[バックアップ操作がエラー 6609 で失敗する](#)」を参照してください。
- p.54 の「[バックアップ操作がエラー 6618 で失敗した](#)」を参照してください。
- p.54 の「[バックアップ操作がエラー 6647 で失敗する](#)」を参照してください。

- p.55 の「**Hadoop** で拡張属性 (**xattrs**) とアクセス制御リスト (**ACL**) がバックアップまたはリストアされない」を参照してください。
- p.56 の「バックアップ操作がエラー **6654** で失敗する」を参照してください。
- p.56 の「バックアップ操作が **bpbrm** エラー **8857** で失敗する」を参照してください。
- p.56 の「バックアップ操作がエラー **6617** で失敗する」を参照してください。
- p.57 の「バックアップ操作がエラー **6616** で失敗する」を参照してください。

## バックアップ操作がエラー 6609 で失敗する

このエラーは、次のシナリオ中に発生します。

1. **Hadoop** プラグインファイルが、バックアップホスト (1 つまたは複数) から削除されているか失われています。

回避方法:

**Hadoop** プラグインをダウンロードしてインストールします。

2. `Application_Type` の詳細が不正です。

回避方法:

**Hadoop** の代わりに `hadoop` を使用して、`Application_Type` を指定します。

## バックアップ操作がエラー 6618 で失敗した

バックアップ操作がエラー **6618** で失敗し、次のエラーが表示されます。

```
NetBackup cannot find the file to complete the operation.(6618)
```

このエラーは、バックアップ選択として無効なディレクトリを指定した場合に発生します。

回避方法:

**BigData** ポリシーのバックアップ選択として有効なディレクトリを指定します。

## バックアップ操作がエラー 6647 で失敗する

バックアップ操作がエラー **6647** で失敗し、次のエラーが表示されます。

```
Unable to create or access a directory or a path. (6647)
```

このエラーは、次の状況のいずれかで発生します。

- ディレクトリでスナップショットが有効になっていない

- ポリシーではバックアップ選択としてルートフォルダのスナップショットを作成するように設定されているが、子フォルダの 1 つですでにスナップショットが有効になっている
- ポリシーではバックアップ選択として子フォルダのスナップショットを作成するように設定されているが、親フォルダの 1 つですでにスナップショットが有効になっている
- ポリシーでバックアップ選択としてファイルのスナップショットを作成するように設定されている

回避方法:

Hadoop では、入れ子になったディレクトリでスナップショットを有効にすることは許可されていません。親ディレクトリですでにスナップショットが有効である場合、親ディレクトリの下の子ディレクトリではスナップショットを有効にできません。Bigdata ポリシー形式でのバックアップ選択については、バックアップに対してスナップショットが有効なディレクトリのみを選択する必要があります。その他の子ディレクトリを選択してはいけません。

## Hadoop で拡張属性 (xattrs) とアクセス制御リスト (ACL) がバックアップまたはリストアされない

拡張属性によって、ユーザーアプリケーションは、追加のメタデータを Hadoop のファイルまたはディレクトリに関連付けることができます。これは、デフォルトでは、Hadoop 分散ファイルシステム (HDFS) で有効になっています。

アクセス制御リストによって、特定の名前付きユーザーや名前付きグループに対して、標準のアクセス許可も含めて、アクセス許可を個別に設定できます。これは、デフォルトでは、HDFS で無効になっています。

Hadoop プラグインは、バックアップ中に、オブジェクトの拡張属性またはアクセス制御リスト (ACL) をキャプチャしないため、リストアされるファイルやフォルダにはこれらは設定されません。

回避方法:

Application\_Type = hadoop の BigData ポリシーを使用してバックアップが作成されるファイルまたはディレクトリのいずれかに拡張属性が設定されている場合、リストアされるデータに拡張属性を明示的に設定する必要があります。

拡張属性は、fs -getfattr や hadoop fs -setfattr など、Hadoop シェルコマンドを使用して設定できます。

Application\_Type = hadoop の BigData ポリシーを使用してバックアップが作成されるファイルまたはディレクトリのいずれかでアクセス制御リスト (ACL) が有効で、設定されている場合、リストアされるデータに ACL を明示的に設定する必要があります。

ACL は、hadoop fs -getfacl や hadoop fs -setfacl など、Hadoop シェルコマンドを使用して設定できます。

## 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。

- Hadoop 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:  
Hadoop 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.21 の「[NetBackup での Hadoop 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 Hadoop 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 Hadoop 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 クライアントがホワイト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 クライアントがホワイトリストに載っていることを確認します。  
p.20 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。

## バックアップ操作が bpbrm エラー 8857 で失敗する

このエラーは、NetBackup マスターサーバーで NetBackup クライアントがホワイトリストに追加されていない場合に発生します。

回避方法:

バックアップホストとして NetBackup クライアントを使用する場合は、NetBackup マスターサーバーでホワイトリストに追加する手順を実行する必要があります。詳しくは、p.20 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。を参照してください。

## バックアップ操作がエラー 6617 で失敗する

バックアップ操作がエラー 6617 で失敗し、次のエラーが表示されます。

システムコールに失敗しました。

Kerberos 対応 Hadoop クラスタの場合には、バックアップホストに有効なチケット認可チケット (TGT) があることを確認します。

回避方法:

TGT を更新します。



## バックアップ操作がエラー 6616 で失敗する

バックアップ操作がエラー 6616 で失敗し、次のエラーがログに記録されます。

hadoopOpenConfig: 構成ファイルから JSON オブジェクトを作成するのに失敗しました。

回避方法:

hadoop.conf ファイルを検証して、パラメータ値に空白の値または不正な構文が使用されていないことを確認します。

## 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、アプライアンス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/

## バックアップイメージの選択でイメージが表示されているにもかかわらず、リストア時に増分バックアップイメージが表示されない

この問題は、増分バックアップイメージをリストアしようとしたときに、バックアップポリシーのバックアップ対象リストに、/ のサブフォルダ内のバックアップ対象が含まれている場合に発生します。

次に例を示します。

```
/data/1  
/data/2
```

回避方法

増分バックアップイメージからリストアできる利用可能なデータを表示するには、増分バックアップイメージとともに関連する完全バックアップイメージを選択します。

## 子バックアップジョブの 1 つがキューに投入された状態になる

複数のバックアップホストがあるシナリオで、子バックアップジョブの 1 つがキューに投入された状態になり、メディアサーバーを待機し続けます。

理由:

この問題は、複数のバックアップホストが使用されていて、メディアサーバーが非アクティブな状態になっている NetBackup Appliance 環境で確認できます。

回避方法:

NetBackup 管理コンソールの [メディアおよびデバイスの管理 (Media and Device Management)]、[デバイス (Devices)]、[メディアサーバー (Media servers)] メニューから、状態が [無効 (Deactivated)] なメディアサーバーを右クリックし、[有効化 (Activate)] を選択します。

## Hadoop データのリストア問題のトラブルシューティング

- p.59 の「リストアが 2850 エラーコードで失敗する」を参照してください。
- p.59 の「NetBackup の Hadoop のリストアジョブが部分的に完了する」を参照してください。
- p.55 の「Hadoop で拡張属性 (xattrs) とアクセス制御リスト (ACL) がバックアップまたはリストアされない」を参照してください。
- p.59 の「Hadoop プラグインファイルがバックアップホスト上にない場合、リストア操作が失敗する」を参照してください。
- p.60 の「リストアが bpbrm エラー 54932 で失敗する」を参照してください。

- p.60 の「リストア操作が `bpbrm` エラー 21296 で失敗する」を参照してください。

## リストアが 2850 エラーコードで失敗する

このエラーは、次のシナリオで発生する場合があります。

- `Error:2850 "errno = 62 - Timer expired"`  
回避方法:  
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 Hadoop クラスタと通信できるようにします。
- 要求されたファイルはリカバリされません。  
回避方法:  
Kerberos 対応 Hadoop クラスタの場合には、バックアップホストに有効なチケット認可チケット (TGT) があることを確認します。  
TGT を更新します。
- アプリケーションサーバーの値が不正で、クレデンシャルが無効です。  
回避方法:  
リストア中に宛先 Hadoop クラスタのホスト名を正しく入力したことを確認してください。  
これは `tpconfig` コマンドで提供されたものと同じである必要があります。

## NetBackup の Hadoop のリストアジョブが部分的に完了する

リストアデータの容量が Hadoop クラスタで使用できる領域を超えている場合、リストアジョブが部分的に完了します。

回避方法:

Hadoop クラスタの領域をクリーンアップします。

## Hadoop で拡張属性 (xattrs) とアクセス制御リスト (ACL) がバックアップまたはリストアされない

この問題について詳しくは、p.55 の「Hadoop で拡張属性 (xattrs) とアクセス制御リスト (ACL) がバックアップまたはリストアされない」を参照してください。を参照してください。

## Hadoop プラグインファイルがバックアップホスト上にない場合、リストア操作が失敗する

Hadoop プラグインファイルがインストールされていないバックアップホストでリストアジョブがトリガされると、リストア操作が次のエラーで失敗します。

```
client restore EXIT STATUS 50: client process aborted
```

回避策: Hadoop プラグインをダウンロードしてインストールします。

## リストアが bpbrm エラー 54932 で失敗する

このエラーは、リストアするファイルのバックアップが正常に作成されていない場合に発生します。

回避方法:

リストア操作を開始する前に、バックアップ作成が正常に完了していることを確認します。

あるいは、アクティビティモニターメニューで[ジョブ状態]タブをクリックして、特定のジョブ ID を探し、エラーメッセージの詳細を確認します。

## リストア操作が bpbrm エラー 21296 で失敗する

<application\_server\_name> に不正な値を指定し、Hadoop クレデンシャルを NetBackup マスターサーバーに追加した場合に、このエラーが発生します。

回避方法:

<application\_server\_name> で指定される詳細が正しいかどうかを確認します。

## 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 Hadoop クラスタまたは Hadoop 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、hadoop.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

ディザスタリカバリ 39  
トラブルシューティング  
    バックアップ 53  
    リストア 59  
バックアップ 8、43  
    Hadoop 41  
ホワイトリスト  
    バックアップホスト 20  
ポリシー  
    構成 34  
ライセンス  
    Hadoop 14  
リストア 9  
    bprestore コマンド 46  
    Hadoop 43  
    Hadoop クラスタ 45  
    代替 NameNode 48  
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 34  
制限事項 12  
削除  
    バックアップホスト 17  
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  
    Hadoop 14  
用語 10  
追加  
    バックアップホスト 17

## B

BigData ポリシー  
    NetBackup 管理コンソール 35

コマンドラインインターフェース 37  
ポリシーの設定ウィザード 35  
ポリシーユーティリティ 36

## H

Hadoop クレデンシヤル  
追加 21

## K

Kerberos  
    インストール後 33  
kerberos  
    バックアップ 42  
    リストア 42

## N

NetBackup  
    サーバーおよびクライアントの要件 14  
    デバッグログ 53  
NetBackup アプライアンス  
    バックアップホスト 21