NetBackup™ クラウド管理者ガイド

UNIX、Windows および Linux

リリース 11.2.0.1

COHESITY

NetBackup™ クラウド管理者ガイド

最終更新日: 2026-10-12

法的通知と登録商標

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved.Cohesity、Cohesity ロゴ、その他の Cohesity マークは、Cohesity, Inc. の米国における、および/または国際的な商標です。ここで提供される情報は、Cohesity の機密情報および専有情報であり、(a) 意図された受信者により、(b) 有効なライセンスを受けた Cohesity ソフトウェアおよびサービスと共にのみ使用することができます。Cohesity ライセンスの条項については、www.cohesity.com/agreements を参照してください。

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Cohesity 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。

Cohesity サポート

Cohesity サポートへのお問い合わせ

Cohesity サポートケースを作成するには、いくつかの方法があります。

- Cohesity サポートに移動してベリタスのナレッジベースで検索するか、電話で問い合わせます (米国およびカナダ: 1-855-9CO-HESI (926-4374)、オプション 2)。
- Cohesity サポートポータルにログインして、新しいケースを作成します。
- Cohesity UI の (?) アイコンをクリックし、[サポートポータル (Support Portal)]を選択します。

サポートおよびサービスアシスタンス

最初に、サービスおよびサポートを契約したサービスプロバイダにお問い合わせください。Cohesity と直接連携している場合や、製品の保証や資格、修理の価格設定、またはテクニカルサポートに関連する質問がある場合は、以下のオプションを参照してください。

- 製品の問題に対するソリューションや、提案およびベストプラクティスを見つけるには、Cohesity ナレッジベースを参照してください。
- Cohesity サポートポータルにログインして、新しいケースを作成します。
- オープン中のケースを監視するには、ポータルにログインし、ホームページの[ケース (Cases)]タブをクリックします。このページには、すべてのケースの状態と更新が表示されるはずです。個々のケースの状態を表示することもできます。

パートナーのハードウェアで実行されている Cohesity ソフトウェア

認定されたサードパーティ製ハードウェアで動作する Cohesity ソフトウェアの場合、次のサポートワークフローが適用されます。

1. ハードウェアの問題であると判断できない場合は、まず Cohesity サポートにお問い合わせください。

   メモ: Cohesity はパートナーのハードウェアの交換要求を処理できません。

2. Cohesity サポートは問題の優先順位を判断します。ソフトウェアの問題の場合、Cohesity サポートは引き続きこの問題に取り組みます。
3. ハードウェアまたはファームウェアの問題であるかその可能性がある場合、Cohesity は問題に関する情報をお客様に提供し、適切なパートナーに対するサポートチケットを発行するようお客様に依頼します。
4. Cohesity サポートは必要に応じて、パートナーとお客様との三者通話に参加できます。
5. お客様がパートナーのケースの進捗状況を Cohesity サポートに通知します。

目次

第 1 章 NetBackup Cloud Storage について 8

Cloud Storage の機能について 8
クラウド構成ファイルのカタログバックアップについて 11
NetBackup クラウドストレージのサポート制限事項について 12

第 2 章 クラウドストレージについて 14

NetBackup のクラウドストレージベンダーについて 14
Amazon S3 クラウドストレージの API 形式について 15
NetBackup 認定の Amazon S3 クラウドストレージベンダー 16
Amazon S3 ストレージ形式の要件 16
Amazon S3 クラウドプロバイダのユーザーに必要な権限 17
Amazon S3 のクラウドストレージプロバイダのオプション 18
Amazon S3 のクラウドストレージのオプション 21
Amazon S3 クラウドストレージサーバーの構成オプション 24
Amazon S3 クレデンシャルブローカーの詳細 26
Amazon S3 対応クラウドプロバイダのプライベートクラウドについて 27
Amazon S3 ストレージクラスについて 28
NetBackup による Amazon 仮想プライベートクラウドサポート 29
長期保持のための Amazon のデータの保護について 31
Amazon S3 Intelligent Tiering (LIFECYCLE) を使用したデータの保護 42
NetBackup での Amazon IAM ロールの使用について 46
NetBackup における Amazon S3 クラウドコネクタの文字制限について 49
Amazon Snowball および Amazon Snowball Edge を使用したデータの保護 51
Microsoft Azure クラウドストレージ API 形式について 63
NetBackup 認定の Microsoft Azure クラウドストレージベンダー 64
Microsoft Azure ストレージ形式の要件 64
Microsoft Azure クラウドストレージプロバイダのオプション 64
Microsoft Azure のサーバーの詳細な構成オプション 66
長期保持用の Microsoft Azure Archive データの保護 68

第 3 章 NetBackup のクラウドストレージの構成 71

NetBackup でクラウドストレージの構成を開始する前に 72
NetBackup のクラウドストレージの構成 73
Cloud のインストール要件 74
[拡張性のあるストレージ (Scalable Storage)]プロパティ 75
帯域幅スロットルの詳細設定 77
帯域幅スロットルの詳細設定 77
[クラウドストレージ (Cloud Storage)]プロパティ 79
クラウドストレージインスタンスの追加 80
クラウドストレージホストプロパティの変更 81
クラウドストレージホストのインスタンスの削除 82
NetBackup CloudStore Service Container について 82
NetBackup CloudStore Service Container のセキュリティ証明書 83
NetBackup CloudStore Service Container のセキュリティモード 84
NetBackup cloudstore.conf 設定ファイル 85
ホスト名ベースの証明書の配備 88
ホスト ID ベースの証明書の配備 90
クラウドバックアップ用のデータ圧縮について 91
クラウドストレージのデータ暗号化について 92
NetBackup クラウドストレージの暗号化の NetBackup KMS について 92
NetBackup クラウドストレージの暗号化の外部 KMS について 94
クラウドストレージサーバーについて 95
クラウドストレージのオブジェクトのサイズについて 95
クラウドストレージの NetBackup メディアサーバーについて 97
NetBackup クラウドのプライマリホストとしてのメディアサーバーの使用 98
クラウドストレージのストレージサーバーの構成 100
KMS データベース暗号化の設定 101
NetBackup クラウドストレージサーバーのプロパティ 102
NetBackup クラウドストレージサーバー帯域幅スロットルのプロパティ 103
NetBackup クラウドストレージサーバーの接続プロパティ 106
NetBackup クラウドストレージサーバーの暗号化プロパティ 112
クラウドストレージのディスクプールについて 113
クラウドストレージのディスクプールの構成 114
NetBackup クラウドストレージ暗号化の KMS キー名のレコードの保存 114
クラウド環境へのバックアップメディアサーバーの追加 116
クラウドストレージ用のストレージユニットの構成 117

クラウドストレージユニットのプロパティ 117
クライアントとサーバーの最適比率の構成 119
メディアサーバーへのバックアップ通信量の制御 120
NetBackup アクセラレータバックアップと NetBackup 最適化合成バックアップについて 121
クラウドストレージディスクプールのプロパティ 121
証明書失効リスト (CRL) に対する証明書の検証 123
NetBackup クラウドの認証局 (CA) の管理 124

第 4 章 監視とレポート 128

クラウドストレージジョブの詳細表示 128
圧縮率の表示 128
クラウドストレージ暗号化用の KMS キー情報の表示 129

第 5 章 操作上の注意事項 132

NetBackup bpstsinfo コマンドの操作上の注意事項 132
NetBackup アクセス制御が有効になっている場合、クラウドの構成が失敗することがある 133
クラウドストレージサーバーのアーティファクトの削除 133
csconfig reinitialize を使用した更新済みのクラウド構成設定のロード 134
プライマリサーバーとレガシークラウドストレージメディアサーバー間の通信の有効化または無効化 134

第 6 章 トラブルシューティング 137

統合ログについて 137
vxlogview コマンドを使用した統合ログの表示について 138
vxlogview を使用した統合ログの表示の例 140
レガシーログについて 141
クラウドストレージ用の NetBackup ログファイルディレクトリの作成 142
NetBackup クラウドストレージログファイル 143
libcurl ログの有効化 146
クラウドストレージの構成上の問題のトラブルシューティング 146
NetBackup の拡張性のあるストレージのホストプロパティを利用できない 147
クラウドストレージを作成できません 147
クラウドストレージサーバーへのデータ転送が、SSL モードで失敗する 148
Amazon GovCloud クラウドストレージの設定が非 SSL モードで失敗する 149

Google Nearline ストレージからのデータリストアは失敗する場合がある 149
認証バージョン V2 でのストレージリージョンのフェッチの失敗 150
スナップショットの親ジョブからのバックアップが状態コード 160 で失敗する 150
クラウドストレージの操作上の問題のトラブルシューティング 150
クラウドストレージバックアップが失敗する 151
NetBackup CloudStore Service Container の停止と起動 155
nbcssc (レガシーメディアサーバー)、nbwmc、nbsl のプロセスを再起動するとすべての cloudstore.conf 設定が元に戻される 156
NetBackup CloudStore Service Container の起動とシャットダウンのトラブルシューティング 156
GLACIER リストアジョブのキャンセル後に bptm プロセスの終了に時間がかかる 157
Amazon Glacier Vault のイメージクリーンアップエラーの処理 157
孤立したアーカイブの手動によるクリーンアップ 157
Amazon Glacier Vault からのリストアが 1 つのフラグメントで 24 時間より長くかかる 158
GLACIER_VAULT からのリストアが Oracle データベースで 24 時間より長くかかる 158
Amazon IAM アクセス権がないために発生するエラーのトラブルシューティング 160
リストアジョブの開始時刻がバックアップジョブの終了時刻と重なるとリストアジョブが失敗する 162
Azure アーカイブからのリストアの後処理が失敗する 162
Amazon Snowball および Amazon Snowball Edge の問題のトラブルシューティング 163

索引 164

1

NetBackup Cloud Storage について

この章では以下の項目について説明しています。

- Cloud Storage の機能について
- クラウド構成ファイルのカタログバックアップについて
- NetBackup クラウドストレージのサポート制限事項について

Cloud Storage の機能について

NetBackup Cloud Storage では、クラウドの STaaS (Storage as a Service) ベンダーからデータをバックアップ、リストアできます。NetBackup Cloud Storage は NetBackup OpenStorage と統合されています。

表 1-1 に、NetBackup Cloud Storage で提供される機能の概要を示します。

表 1-1　　機能

機能	詳細
クラウドストレージ構成	NetBackup Web UI では、クラウドストレージの設定とストレージプロビジョニングを簡単に行うことができます。
圧縮	NetBackup Cloud Storage Compression は、クラウドに送信する前にデータをインラインで圧縮します。圧縮機能は、LZO Pro (圧縮レベル 3) というサードパーティのライブラリを使います。

機能	詳細
暗号化	NetBackup Cloud Storage の暗号化では、データがクラウドに送信される前にデータをインラインで暗号化します。暗号化はNetBackupキーマネージメントサービス (KMS) と連動することによって暗号化キーを管理する機能を利用します。 暗号化機能では AES 256 暗号フィードバック (CFB) モードの暗号化を使用します。
スロットル	NetBackup Cloud Storage のスロットルでは、ネットワークとクラウド間のデータ転送速度を制御します。スロットル値は NetBackup メディアサーバーごとに設定されます。 特定の実装では、クラウドへのバックアップとリストアによる WAN 使用率を制限する必要があります。この制限を実装して他のネットワークの動作を制約しないようにします。スロットルは NetBackup 管理者に NetBackup Cloud Storage のトラフィックを制限する機能を提供します。クラウドの WAN トラフィックに制限を実装することで、割り当てられた以上の帯域幅を消費できないようにします。 NetBackup Cloud Storage スロットルを使用して、次の項目を構成および制御できます。 ■ 読み込み操作および書き込み操作で異なる帯域幅値。 ■ 各クラウドプロバイダで一度にサポートされる最大接続数。 ■ 総帯域幅に対するネットワーク帯域幅の割合。 ■ 時間ブロックごとのネットワーク帯域幅。
測定	NetBackup Cloud Storage の測定レポートを使用して、NetBackup Cloud Storage 内のデータ転送を監視できます。 クラウドベースのストレージは、永続的なバックアップイメージを使用する従来のテープまたはディスクメディアとは異なります。クラウドストレージベンダーは、保存されたバイトおよび転送されたバイトごとにクラウドベースのストレージのコストを計算します。 NetBackup Cloud Storage ソフトウェアでは、保存および転送されるデータを最小限に抑えるために複数の技術を使用します。これらの技術により、保護データ量に関する従来のカタログベースの情報は、保存または転送されるデータ量と一致しなくなります。測定によって、1 つ以上のクラウドベースのストレージプロバイダ間でメディアサーバーごとに転送されるデータ量をインストール時に監視できます。

機能	詳細
クラウドストレージサービス	これは、バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ該当します。 NetBackup CloudStore サービスコンテナ (nbcssc) プロセスでは、次の機能を実行します。 ■ 測定プラグインの測定情報の生成 ■ スロットルプラグインを利用したネットワーク帯域幅の使用率の制御 **メモ:** バージョン 8.1.2 以降の NetBackup メディアサーバーの場合、これらのクラウドストレージ機能は、NetBackup Service Layer (nbsl) サービスによって実行されます。 Windows では、このサービスは NetBackup によってインストールされる標準サービスです。UNIX では、このサービスは標準デーモンとして実行されます。 NetBackup CloudStore Service Container (nbcssc) は証明書ベースの認証を使います。旧リリースで使われていたこの認証方法 (レガシー認証) はデフォルトにより無効化されます。クラウドストレージサーバーとして構成しているメディアサーバーを NetBackup 8.1 以降にアップグレードすることをお勧めします。 これらのサーバーをアップグレードできない場合は、NetBackup プライマリサーバーで [8.0 以前のホストとの安全でない通信を有効にする (Enable insecure communication with 8.0 and earlier hosts)] オプションを使用します。このオプションは、Web UI の [設定 (Settings)]、[グローバルセキュリティ設定 (Global Security Settings)]、[安全な通信 (Secure Communication)] の順に選択したタブで利用できます。
NetBackup Web 管理コンソール	NetBackup Web 管理コンソール (nbwmc) プロセスは、証明書とホスト管理の要求を管理します。 このプロセスは、NetBackup Cloud Storage に関連する構成パラメータも制御するようになりました。 このプロセスは、Windows では NetBackup サービスとしてインストールされ、UNIX では標準デーモンとして実行されます。

機能	詳細
NetBackup Service Layer	NetBackup Service Layer (nbsl) サービスは、NetBackup グラフィカルユーザーインターフェース (UI) と NetBackup ロジックとの間の通信を簡易化します。 このサービスは、クラウドストレージにも必要で、現在は次の機能を実行します。 ■ 測定プラグインの測定情報の生成 ■ スロットルプラグインを利用したネットワーク帯域幅の使用率の制御 **メモ:** バージョン 7.7.x から 8.1.2 のメディアサーバーの場合、これらのクラウドストレージ機能は NetBackup Cloud Storage Service Container (nbcssc) が実行します。
ストレージプロバイダ (Storage providers)	Cohesity ベリタスでは、現在複数のクラウドストレージプロバイダをサポートしています。これらの各ベンダーについての詳細情報が利用可能です。 p.14 の「NetBackup のクラウドストレージベンダーについて」を参照してください。

クラウド構成ファイルのカタログバックアップについて

NetBackup のカタログバックアッププロセスの間に次のクラウド構成ファイルがバックアップされます。

中間測定データを含んでいる、meter ディレクトリのすべての .txt ファイル

- CloudInstance.xml
- cloudstore.conf
- libstspiencrypt.conf
- libstspimetering.conf
- libstspithrottling.conf
- libstspi*cloud_provider_name*.conf
  NetBackup がサポートするクラウドプロバイダに固有のすべての .conf ファイル

カタログバックアップのプロセス中にバックアップされるクラウド構成ファイルは次の場所にあります。

Windows の場合　*install_path*¥Veritas¥NetBackup¥var¥global¥wmc¥cloud

UNIX の場合　/usr/openv/var/global/wmc/cloud

CloudProvider.xml と cacert.pem ファイルは次の場所にあります。

Windows の場合　*<installed-path>*¥NetBackup¥var¥global¥cloud

UNIX の場合　/usr/openv/var/global/cloud/

メモ: NetBackup カタログバックアップのプロセスでは、cacert.pem ファイルのバックアップは作成されません。

この cacert.pem ファイルはクラウドプロバイダに固有のファイルです。このファイルは NetBackup インストールの一部としてインストールされます。このファイルには、NetBackup が使用する既知のパブリッククラウドベンダーの CA 証明書が含まれています。

NetBackup クラウドストレージのサポート制限事項について

以下の項目は、NetBackup クラウドストレージの制限事項の一部です。

- クラウドベンダーは最適化された複製をサポートしません。
- クラウドベンダーはテープへの直接バックアップをサポートしません (NDMP による)。
- クラウドベンダーは、バックアップイメージのディスクボリュームスパニングをサポートしません。
- NetBackup クラウドがサポートしないプラットフォームに NetBackup プライマリサーバーがインストールされている場合に、クラウドストレージサーバーの構成でこの問題が発生する場合があります。
  NetBackup がクラウドストレージでサポートするオペレーティングシステムについては、NetBackup オペレーティングシステム互換性一覧を参照してください。
  https://support.cohesity.com/s/article/article-100040093
- Hitachi クラウドストレージでは、暗号化オプションを有効にしている場合は、合成バックアップが正常に実行されません。合成バックアップを正常に実行するには、Hitachi クラウドポータルでバケット(または名前空間)のバージョニングオプションを有効にする必要があります。バージョニングオプションを有効にする方法について詳しくは、Hitachi クラウドプロバイダに問い合わせてください。
- クラウドストレージサーバーは、データを格納するために同じボリューム (バケットまたはコンテナ)を使用できません。各クラウドストレージサーバーに対して個別のボリューム (バケットまたはコンテナ) を作成する必要があります。
- NetBackup 7.7.1 以降のバージョンでは、フランクフルト地域を使ったクラウドストレージの構成をサポートしています。
- NetBackup Web UI では、以下の項目が英語でのみ表示されます。

- すべてのクラウドプロバイダ名
- クラウドプロバイダの説明
- AmazonGov では、[Certificate File Name]、[Private Key File Name]、[Private Key Passphrase]、[Agency]、[Mission Name]、および[Role] のフィールド
- OpenStack Swift では、[Tenant Type]、[Tenant Value]、[User Type]、[User Domain Type]、[User Domain Value]、[Project Domain Type]、および[Project Domain Value]のフィールド

- NetBackup は IPv6 をサポートするようになりました。IPv6 をサポートするすべてのクラウドベンダーとプロキシサーバーの種類でのみ、サポートが利用可能です。

2

クラウドストレージについて

この章では以下の項目について説明しています。

- NetBackup のクラウドストレージベンダーについて
- Amazon S3 クラウドストレージの API 形式について
- Microsoft Azure クラウドストレージ API 形式について

NetBackup のクラウドストレージベンダーについて

NetBackup では、クラウドストレージがストレージ API 形式に基づいてサポートされています。NetBackup でクラウドストレージ用にサポートされているすべてのクラウドベンダーは、サポート対象のいずれかの形式を使用しています。ストレージ API 形式およびクラウドベンダーについて詳しくは、以下を参照してください。

クラウドストレージの API 形式	p.15 の 表 2-1 を参照してください。 表では、各ストレージ API 形式の要件、およびそのストレージ API 形式を使用するクラウドベンダーの要件について説明するトピックへのリンクが提供されています。
サポート対象のクラウドベンダー	リンク「 NetBackup™ Hardware and Cloud Storage Compatibility List (HCL)」をクリックして、NetBackup Cloud Storage とそれらのストレージ API 形式で認定されているクラウドベンダーのリストを特定します。 設定のヘルプについては、ストレージ API 形式に関する情報を参照してください。

ベンダーは、Cohesity Technology Partners Program に参加して、認定を受けています。NetBackup では、これらのベンダーが提供するストレージにバックアップを送信できます。Cohesity は NetBackup リリースの間にベンダーを認定する場合があります。リリースの間で認定されたベンダーの場合、次の構成とマッピングパッケージをダウンロードしてインストールする必要があります。

NetBackup プライマリ互換性リストのランディングページに、お使いのリリースパッケージへのリンクが掲載されています。

https://support.cohesity.com/s/article/article-100040093

p.15 の 表 2-1 を参照してください。では、NetBackup Cloud Storage で認定されているクラウドストレージ API を識別します。

表 2-1 NetBackup でサポートされているクラウドストレージ API 形式

API 形式	詳細情報
Amazon S3	p.15 の「Amazon S3 クラウドストレージの API 形式について」を参照してください。
Microsoft Azure	p.63 の「Microsoft Azure クラウドストレージ API 形式について」を参照してください。

Amazon S3 クラウドストレージの API 形式について

NetBackup は、ストレージに Amazon S3 のストレージ API を使用するベンダーのクラウドストレージをサポートします。Amazon S3 のストレージ API ベンダー向けの要件と構成オプションに関する情報は、次のとおりです。

表 2-2 Amazon S3 ストレージ API 形式の情報とトピック

情報	トピック
認定されたベンダー	p.16 の「NetBackup 認定の Amazon S3 クラウドストレージベンダー」を参照してください。
要件	p.16 の「Amazon S3 ストレージ形式の要件」を参照してください。
ストレージサーバーの構成オプション	p.18 の「Amazon S3 のクラウドストレージプロバイダのオプション」を参照してください。
SSL、プロキシ、HTTP ヘッダーのオプション	p.24 の「Amazon S3 クラウドストレージサーバーの構成オプション」を参照してください。
クレデンシャルブローカーオプション	p.26 の「Amazon S3 クレデンシャルブローカーの詳細」を参照してください。
ストレージクラス	p.28 の「Amazon S3 ストレージクラスについて」を参照してください。

一部のベンダーは、Amazon S3 のストレージ形式 API を使用するプライベートクラウドをサポートしています。

p.27 の「Amazon S3 対応クラウドプロバイダのプライベートクラウドについて」を参照してください。

p.14 の「NetBackup のクラウドストレージベンダーについて」を参照してください。

NetBackup 認定の Amazon S3 クラウドストレージベンダー

「NetBackup Compatibility List for all Versions」リンクをクリックして、NetBackup クラウドストレージの認定ベンダーを特定してください。「Hardware and Cloud Storage Compatibility List (HCL)」リンクをクリックして、お使いのバージョンの NetBackup について確認してください。HCL 内で「Cloud Storage - Vendor Compatibility」を検索し、[Amazon]をクリックします。

ベンダーは Cohesity Technology Partner Program (VTPP) に参加することで認定を受けることができます。

Amazon S3 ストレージ形式の要件

次の表に、NetBackup における Amazon S3 形式のクラウドストレージの詳細と要件を示します。

表 2-3 Amazon クラウドストレージの要件

要件	詳細
ライセンス要件	クラウドストレージを許可する NetBackup ライセンスを保有している必要があります。
ベンダーアカウントの要件	お使いのベンダーが提供するストレージから作成、書き込み、読み取りを行うには、アカウントを取得する必要があります。
バケット	次に、Amazon ストレージバケットの必要条件を示します。 ■ 1 つの Amazon アカウントにつき最大 100 個のバケットを作成できます。 ■ Amazon AWS Management Console を使用して空のバケットを削除できます。ただし、NetBackup でバケットを作成するときに、削除されたバケットの名前を再利用できないことがあります。 ■ NetBackup がサポートする Amazon のストレージ領域内にバケットを作成できます。 ■ バケットが別のユーザーによって使用されている場合、そのバケットはリストに表示されません。

要件	詳細
バケット名	NetBackup で使うバケットを作成するには NetBackup を使うことをお勧めします。Amazon S3 インターフェースでは、NetBackup が許可しない文字を使用できる場合があります。したがって、NetBackup を使ってバケットを作成することにより、潜在的な問題を抑制できます。 米国標準地域でのバケット名に関する NetBackup 必要条件を以下に示します。 ■ バケット名は 3 文字から 255 文字である必要があります。 ■ 国際標準化機構 (ISO) のラテン文字アルファベットの 26 文字の小文字。これらは英語のアルファベットと同じ小文字です。 ■ 0 から 9 までの整数。 ■ 次の文字 (バケット名の最初の文字としてこれを使用することはできません): ピリオド (.)、下線 (_)、ダッシュ (-)。 ダッシュ – 例外: 通信に SSL を使用する場合は、ピリオド (.) を使用できません。デフォルトでは、NetBackup は通信に SSL を使用します。 p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。 次のシナリオでは、NetBackup でバケットを使用できません。 ■ NetBackup がサポートしていない地域でバケットを作成した場合。 ■ バケットの名前がバケットの命名規則に従っていない場合。 ■ バケットに対して指定された権限が不足している場合。p.17 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。
ディスクプールの数	最大 90 個のディスクプールを作成できます。90 個以上のディスクプールを作成しようとすると、「ディスクボリュームの作成に失敗しました、要求が無効です」というエラーメッセージが生成されます。

メモ: Amazon AWS と通信するには、SSL が有効になっている必要があります。NetBackup バックアップジョブは状態コード 87 で失敗します。

p.15 の「Amazon S3 クラウドストレージの API 形式について」を参照してください。

Amazon S3 クラウドプロバイダのユーザーに必要な権限

Amazon (S3) クラウドプロバイダを NetBackup と連携させるには、次の権限が必要です。

- s3:CreateBucket
- s3:ListAllMyBuckets

- s3:ListBucket
- s3:GetBucketLocation
- s3:GetObject
- s3:PutObject
- s3:DeleteObject
- s3:RestoreObject
- s3:GetBucketObjectLockConfiguration

Amazon S3 のクラウドストレージプロバイダのオプション

表 2-4 では、Amazon S3 のストレージサーバー構成オプションについて説明します。

表 2-4 Amazon S3 のクラウドストレージプロバイダの構成オプション

フィールド名	必要な内容
サービスホスト (Service host)	お使いのベンダーのクラウドサービスのエンドポイントの名前をドロップダウンリストから選択します。 ベンダーのクラウドサービスのエンドポイントがドロップダウンリストに表示されない場合は、クラウドストレージインスタンスを追加する必要があります。この表の[クラウドストレージの追加 (Add Cloud Storage)]の説明を参照してください。

フィールド名	必要な内容
ストレージサーバー名 (Storage server name)	ベンダーのデフォルトのストレージサーバーが表示されます。ドロップダウンリストには、使うことのできる名前のみが表示されます。複数のストレージサーバーが利用可能な場合は、デフォルト以外のストレージサーバーを選択できます。 ドロップダウンリストには、クラウドストレージの論理名を使って別のストレージサーバー名を入力できます。Amazon の同一の物理サービスホストを参照する異なる複数の名前を使って、複数のストレージサーバーを作成できます。利用できる名前がリストにない場合は、ドロップダウンリストに新しいストレージサーバー名を入力して作成できます。 **メモ:** Amazon S3 対応クラウドプロバイダを構成するときに追加するストレージサーバー名を論理名にし、物理ホスト名と一致しないようにすることをお勧めします。例: Amazon GovCloud ストレージサーバーを追加するときに、「amazongov.com」または「amazon123.com」といった名前を使わないようにします。これらのサーバーは、クラウドストレージ構成時に失敗を引き起こす可能性のある物理ホストであることがあります。代わりに、「amazongov1」または「amazonserver1」などのストレージサーバー名を使います。 **メモ:** パブリッククラウドの場合は[クラウドストレージの追加 (Add Cloud Storage)]オプションが無効になります。既存のクラウドストレージを使う必要があります。
クラウドストレージの追加 (Add Cloud Storage)	クラウドストレージの追加 (Add Cloud Storage) カスタマイズしたクラウド配備は、[サービスホスト (Service Host)]ドロップダウンリストにリストされていないクラウドインスタンスを参照します。クラウド配備の詳細を構成した後は、サービスホストが[サービスホスト (Service Host)]ドロップダウンリストに表示されます。 追加したクラウドストレージは、Web UI を使って変更または削除できません。ただし、`csconfig` コマンドを使ってストレージサーバーを変更または削除できます。 **メモ:** Amazon S3 対応クラウドプロバイダのカスタムクラウドインスタンスを作成するには、NetBackup `csconfig -a` コマンドを使うことができます。`nbdevconfig` と `tpconfig` コマンドを実行する前に `csconfig` コマンドを実行する必要があります。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。このガイドは次の URL から入手できます。 https://support.cohesity.com/s/article/article-100040135.html

フィールド名	必要な内容
メディアサーバー名 (Media server name)	NetBackup メディアサーバーをドロップダウンリストから選択します。ドロップダウンリストには、NetBackup 11.2.0.1 以降のメディアサーバーのみが表示されます。また、クラウドストレージサーバーの必要条件に適合するメディアサーバーのみがドロップダウンリストに表示されます。次のトピックでは、構成の必要条件について説明します。 p.97 の「クラウドストレージの NetBackup メディアサーバーについて」を参照してください。 選択したホストが、機能と利用可能なストレージについてストレージベンダーのネットワークに問い合わせます。メディアサーバーはバックアップおよびリストアのためのデータムーバーにもなります。 クラウドストレージをサポートするには、メディアサーバーが次の項目に適合している必要があります。 ■ クラウドストレージでオペレーティングシステムがサポートされている必要があります。NetBackup がクラウドストレージでサポートするオペレーティングシステムについては、NetBackup オペレーティングシステム互換性一覧を参照してください。 https://support.cohesity.com/s/article/article-100040093 ■ すべてのメディアサーバーで、NetBackup Service Layer (nbsl) サービスを実行している必要があります。 プライマリサーバーで、NetBackup Web 管理コンソール (nbwmc) を実行している必要があります。 ■ Amazon S3 互換クラウドプロバイダでは、メディアサーバーで NetBackup 11.2.0.1 以降のリリースを動作している必要があります。 ■ クラウドストレージに使用する NetBackup メディアサーバーは、プライマリサーバーのバージョンと同じ NetBackup バージョンにする必要があります。
クレデンシャルの入力 (Enter Credentials)	適用先: Amazon GovCloud のみ。 このオプションはデフォルトで選択されます。アクセスキー ID とシークレットアクセスキーを入力して、このウィザードパネルでクラウドストレージサーバーのクレデンシャルを設定するには、このオプションを選択します。
資格情報ブローカーの使用 (Use Credentials Broker)	適用先: Amazon GovCloud のみ。 クレデンシャルブローカーを使ってクラウドストレージサーバーを構成するには、このオプションを選択します。このオプションを選択する場合は、次に表示される[資格情報ブローカーの使用 (Use Credentials Broker)]ウィザードパネルを使って資格情報ブローカーの情報を設定します。

フィールド名	必要な内容
アクセスキー ID (Access key ID)	[資格情報ブローカーの使用 (Use Credentials Broker)]を選択する場合、Amazon GovCloud には適用されません。 ベンダーアカウントのアクセスキー ID を入力します。 アカウントがない場合は、[サービスプロバイダによるアカウントの作成 (Create an account with the service provider)]リンクをクリックします。
シークレットアクセスキー (Secret access key)	[資格情報ブローカーの使用 (Use Credentials Broker)]を選択する場合、Amazon GovCloud には適用されません。 ベンダーアカウントのシークレットアクセスキーを入力します。100 文字以下である必要があります。
IAM ロール (EC2) を使用する (Use IAM Role (EC2))	NetBackup は EC2 インスタンスに関連付けられた AWS IAM ロール名とクレデンシャルを取得します。 **メモ:** IAM ロールの場合、選択したメディアサーバーが EC2 インスタンスでホストされている必要があります。 p.46 の「NetBackup での Amazon IAM ロールの使用について」を参照してください。
詳細設定 (Advanced Settings)	クラウドストレージホストの SSL、プロキシ、HTTP ヘッダー (サーバー側の暗号化またはストレージクラス) の設定を変更するには、[詳細設定 (Advanced Settings)]をクリックします。 p.24 の「Amazon S3 クラウドストレージサーバーの構成オプション」を参照してください。

Amazon S3 のクラウドストレージのオプション

[全般設定 (General Settings)]タブ	p.22 の 表 2-5 を参照してください。
[地域の設定 (Region Settings)]タブ	p.23 の 表 2-6 を参照してください。 **メモ:** 複数の地域に対してクラウドストレージ配備を設定しない場合は、地域の設定を行う必要はありません。

メモ: Amazon 仮想プライベートクラウド (VPC) 環境でクラウドストレージサーバーを追加するには、考慮事項を確認してください。

p.29 の「NetBackup による Amazon 仮想プライベートクラウドサポート 」を参照してください。

表 2-5 ［全般設定 (General settings)］タブのオプション

オプション	説明
プロバイダの形式 (Provider Type)	クラウドストレージプロバイダです。このフィールドの状態は次のとおりです。 ■ ［クラウドストレージ (Cloud Storage)］ホストプロパティからクラウドストレージを追加するとアクティブになります。リストから必要なプロバイダを選択します。 ■ ［クラウドストレージサーバーの構成ウィザード (Cloud Storage Server Configuration Wizard)］からクラウドストレージを追加するか［クラウドストレージ (Cloud Storage)］ホストプロパティから設定を変更すると非アクティブになります。ウィザードまたは［クラウドストレージ (Cloud Storage)］ホストプロパティで選択したホストを示します。
サービスホスト (Service host)	クラウドサービスプロバイダのホスト名を入力します。 パブリッククラウドインスタンスを追加する場合は、クラウドストレージプロバイダからサービスホストの詳細を取得する必要があります。テキストボックスにサービスホストの詳細を入力します。 プライベートクラウド配備のクラウドストレージインスタンスを追加する場合に、クラウドプロバイダが「service.my-cloud.com/services/objectstore」という URL を使ってアクセス可能な場合は、「service.my-cloud.com」といったサービスホスト名を入力します。 カスタムインスタンスの場合、IPv6 のエンドポイントを使用するには、IPv6 対応のサービスホストを使用してインスタンスを更新するか、新しいインスタンスを作成する必要があります。 **メモ:** 「http」または「https」の接頭辞をサービスホスト名に付加しないでください。 **メモ:** デフォルト (米国東部 (北バージニア)) の AWS リージョンの VPC については、サービスホストとして external-1.amazonaws.com を使用します。jasper
サービスのエンドポイント (Service endpoint)	クラウドサービスプロバイダのエンドポイントを入力します。 ［サービスエンドポイント (Service endpoint)］- クラウドサービスプロバイダのエンドポイントを入力します。たとえば、「service.my-cloud.com/services/objectstore」URL を使ってクラウドプロバイダサービスにアクセス可能な場合、「/services/objectstorage」と入力します。 クラウドプロバイダサービスが「service.my-cloud.com」URL から直接アクセス可能な場合は、空白のままにできます。

オプション	説明
HTTP ポート (HTTP port)	非セキュアモードでクラウドプロバイダサービスにアクセスするときに使うことができる HTTP ポートを入力します。
HTTPS ポート (HTTPS port)	セキュアモードでクラウドプロバイダサービスにアクセスするときに使うことができる HTTPS ポートを入力します。
ストレージサーバー名 (Storage server name)	NetBackup を使って設定し、アクセスするクラウドストレージの論理名を入力します。 **メモ:** 同一のパブリックまたはプライベートクラウドストレージインスタンスに関連付けられた複数のストレージサーバーを設定できます。
エンドポイントのアクセススタイル (Endpoint access style)	クラウドサービスプロバイダのエンドポイントのアクセススタイルを選択します。 デフォルトのエンドポイントのアクセススタイルは[パスの形式 (Path style)]です。 クラウドサービスプロバイダが URL の仮想ホストも追加でサポートする場合は、[仮想ホステッドスタイル (Virtual hosted style)]を選択します。

メモ: 複数の地域に対してクラウドストレージ配備を設定しない場合は、地域の設定を行う必要はありません。

表 2-6 [地域の設定 (Region settings)]タブ

オプション	説明
地域名 (Region name)	クラウドストレージが配備された特定の地域を示す論理名を入力します。例: 東部
ロケーションの制約 (Location constraint)	関連付けられた地域でのデータ転送操作でクラウドプロバイダサービスが使うロケーション識別子を入力します。パブリッククラウドストレージの場合、クラウドプロバイダからロケーション制約の詳細を取得する必要があります。 **メモ:** デフォルト (米国東部 (北バージニア)) の AWS リージョンの VPC については、ロケーション識別子として US-east-1 を使用します。
サービスホスト (Service host)	地域のサービスホスト名を入力します。[全般設定 (General settings)]タブで入力したサービスエンドポイント、HTTP ポート、HTTPS ポートの情報は、任意の地域から情報にアクセスするときに使用されます。
追加 (Add)	地域を追加する場合、[追加 (Add)]をクリックします。

Amazon S3 クラウドストレージサーバーの構成オプション

メモ: これらのプロパティにアクセスするには、Web UI で[ホスト (Host)]、[ホストプロパティ(Host properties)]の順に選択します。プライマリサーバーを選択し、[プライマリサーバーの編集 (Edit primary server)]をクリックします。次に、[クラウドストレージ (Cloud Storage)]をクリックします。

次の表で、すべての Amazon S3 互換クラウドプロバイダに固有の SSL、HTTP ヘッダーの構成、プロキシサーバーオプションについて説明します。

表 2-7 [全般設定 (General settings)]タブのオプション

オプション	説明
SSL を使用する	NetBackup とクラウドストレージプロバイダ間のユーザー認証またはデータ転送に SSL (Secure Sockets Layer) プロトコルを使う場合は、[SSL を使用する (Use SSL)]を選択します。 ■ 認証のみ (Authentication only)。クラウドストレージにアクセスするときに、ユーザー認証にのみ SSL を使用する場合は、このオプションを選択します。 ■ データ転送 (Data transfer)。SSL を使用してユーザーを認証して、NetBackup からクラウドストレージにデータを転送するにはこのオプションを選択します。 **メモ:** NetBackup は、SSL モードでクラウドストレージと通信するときに、認証局 (CA) による署名付き証明書のみをサポートします。クラウドサーバー (パブリックまたはプライベート) に CA による署名付き証明書があることを確認します。CA によって署名された証明書がない場合は、SSL モードでの NetBackup とクラウドプロバイダ間のデータ転送が失敗します。 **メモ:** Amazon GovCloud クラウドプロバイダの FIPS リージョン (s3-fips-us-gov-west-1.amazonaws.com) では、セキュアモードの通信のみがサポートされます。このため、FIPS 領域を持つ Amazon GovCloud クラウドストレージを設定するときに[SSL を使用する (Use SSL)]オプションを無効にすると、設定は失敗します。 **メモ:** Amazon GovCloud クラウドプロバイダの Glacier サービスエンドポイント (glacier.us-gov-west-1.amazonaws.com) は、NetBackup GLACIER_VAULT ストレージクラスを使用したセキュアモードの通信のみをサポートします。このため、GLACIER_VAULT ストレージクラスを使用して Amazon GovCloud クラウドストレージを設定するときに、[SSL を使用する (Use SSL)]オプションを無効にすると、設定は失敗します。

オプション	説明
HTTP ヘッダー	選択した HTTP ヘッダーに適切な値を指定します。[値 (Value)]列をクリックして、ドロップダウンリストを表示して値を選択します。 ■ [x-amz-server-side-encryption] - Amazon S3 クラウドストレージのデータを保護する場合は、[値 (Value)]ドロップダウンリストから AE256 を選択します。 AE256 は 256 ビット高度暗号化標準を意味します。 ヘッダー値を AE256 に設定すると、Amazon S3 クラウドストレージが受信するすべてのオブジェクトはクラウドに保存される前に暗号化されます。Amazon S3 サーバー側の暗号化では、現在利用可能な最強のブロック暗号 AE256 を使ってデータが暗号化されます。さらに、この暗号化では、定期的に循環されるプライマリキーを使ってキー自体が暗号化されます。 **メモ:** Amazon S3 クラウドストレージサーバーを作成するときに暗号化オプションをすでに有効化している場合は、このオプションを有効にする必要はありません。NetBackup がネットワーク上でデータを送信する前に、データはすで暗号化されています。 ■ ストレージクラスは、ストレージサーバーの作成時に設定されます。ストレージクラスは、構成後に編集することはできません。

表 2-8 [プロキシ設定 (Proxy settings)]タブのオプション

オプション	説明
プロキシサーバーを使用する (Use proxy server)	プロキシサーバーを使用し、プロキシサーバーの設定を指定する場合は、[プロキシサーバーを使用する (Use proxy server)]オプションを選択します。[プロキシサーバーを使用する (Use proxy server)]オプションを選択すると、次の詳細を指定できます。 ■ プロキシホスト (Proxy host)。プロキシサーバーの IP アドレスまたは名前を指定します。 ■ プロキシポート (Proxy port)。プロキシサーバーのポート番号を指定します。 ■ プロキシの形式 (Proxy type)。次のプロキシの形式のいずれかを選択できます。 ■ HTTP **メモ:** HTTP プロキシ形式のプロキシクレデンシャルを指定する必要があります。 ■ SOCKS ■ SOCKS4 ■ SOCKS5 ■ SOCKS4A

オプション	説明
プロキシのトンネリングを使用 (Use proxy tunneling)	HTTP プロキシタイプのプロキシのトンネリングを有効にすることができます。 [プロキシのトンネリングを使用 (Use proxy tunneling)]を有効にすると、HTTP CONNECT 要求がクラウドメディアサーバーから HTTP プロキシサーバーに送信されます。TCP 接続はクラウドバックエンドストレージに直接転送されます。 データは、接続からヘッダーまたはデータを読み取ることがなくプロキシサーバーを通過します。
認証タイプ (Authentication type)	HTTP プロキシ形式を使用する場合は、次のいずれかの認証形式を選択できます。 ■ なし (None): 認証が有効になりません。ユーザー名とパスワードは要求されません。 ■ NTLM: ユーザー名とパスワードが必要です。 ■ 基本 (Basic): ユーザー名とパスワードが必要です。 ユーザー名 (Username)。プロキシサーバーのユーザー名。 パスワード (Password)。パスワードは空にできます。最大 256 文字を使用できます。

p.15 の「Amazon S3 クラウドストレージの API 形式について」を参照してください。

Amazon S3 クレデンシャルブローカーの詳細

クレデンシャルブローカーの詳細は、Amazon GovCloud のクラウドストレージサーバーの構成にも表示されます。

p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

p.81 の「クラウドストレージホストプロパティの変更」を参照してください。

表 2-9では、Amazon GovCloud のクレデンシャルブローカーのオプションについて説明します。

表 2-9　クレデンシャルブローカーの詳細

フィールド	説明
サービス URL (Service URL)	サービス URL を入力します。 例: `https://hostname:port_number/service_path`
エージェンシー (Agency)	エージェンシー名を入力します。

フィールド	説明
ミッション名 (Mission Name)	ミッション名を入力します。
役割	ロールを入力します。
証明書のファイル名 (Certificate File Name)	証明書のファイル名を入力します。
秘密鍵のファイル名 (Private Key File Name)	秘密鍵のファイル名を入力します。
秘密鍵のパスフレーズ (Private Key Passphrase)	秘密鍵のパスフレーズを指定するにはこのチェックボックスにチェックマークを付けます。100 文字以下である必要があります。 [秘密鍵のパスフレーズ (Private Key Passphrase)]は省略可能です。

メモ: 証明書ファイルと秘密鍵ファイルは次の場所に存在する必要があります。

UNIX の場合: `/usr/openv/var/global/wmc/cloud`

Windows の場合: *`install_path`*`¥Veritas¥NetBackup¥var¥global¥wmc¥cloud`

メモ: クレデンシャルブローカーのパラメータについて詳しくは、Cohesity テクニカルサポートチームにお問い合わせください。

p.15 の「Amazon S3 クラウドストレージの API 形式について」を参照してください。

Amazon S3 対応クラウドプロバイダのプライベートクラウドについて

NetBackup はプライベートクラウドまたは次の Amazon S3 対応クラウドプロバイダのクラウドインスタンスをサポートします。

- Amazon GovCloud
- Cloudian HyperStore
- Hitachi 社
- Verizon 社

プライベートクラウドを構成する前に、NetBackup を配備して利用可能にする必要があります。

［サーバーの詳細な構成 (Advanced Server Configuration)］ダイアログボックスを使用します。

メモ: NetBackup は、SSL モードでのクラウドストレージとの通信時に、認証局（CA）によって署名された証明書のみをサポートします。クラウドサーバー (パブリックまたはプライベート) に CA による署名付き証明書があることを確認します。CA によって署名された証明書がない場合は、SSL モードでの NetBackup とクラウドプロバイダ間のデータ転送が失敗します。

メモ: Amazon GovCloud クラウドプロバイダの FIPS リージョン（s3-fips-us-gov-west-1.amazonaws.com）では、セキュアモードの通信のみがサポートされます。したがって、Amazon GovCloud を FIPS リージョンで設定するときに［SSL を使用する (Use SSL)］オプションを無効にすると、設定が失敗します。

ウィザードパネルの［サービスプロバイダでアカウントを作成する (Create an account with service provider)］リンクは、アカウントを作成できるクラウドプロバイダの Web ページを開きます。プライベートクラウドを設定した場合は、構成処理の値が Web ページからなくなります。

Amazon S3 ストレージクラスについて

NetBackup は、Amazon S3 と Amazon GovCloud のストレージクラスをサポートしています。クラウドストレージを構成する際に、オブジェクトまたはデータバックアップに割り当てる特定のストレージクラスを選択できます。オブジェクトはストレージクラスに応じて格納されます。

NetBackup は、次の Amazon S3 ストレージクラスをサポートしています。

- STANDARD
- STANDARD_IA (IA は頻度が低いアクセスを表します。)
- ONEZONE_IA (Amazon S3 Intelligent Tiering なし) (IA は頻度が低いアクセスを表します。)
  単一ゾーンの耐性でアクセス頻度の低いデータをリストアするには、ONEZONE_IA (頻度が低いアクセス) ストレージクラスを選択します。
- GLACIER
  MSDP ダイレクトクラウド階層化を使用して Glacier に書き込まれたイメージは、リストア操作でのみ読み取れます。これらのイメージは、検証と複製の操作では読み取れません。
  p.32 の「Amazon Glacier でのデータの保護について」を参照してください。
- GLACIER_VAULT (MSDP ダイレクトクラウド階層化ではサポートされません)
  p.36 の「Amazon Glacier Vault でのデータの保護について」を参照してください。

- Glacier Deep Archive
  MSDP ダイレクトクラウド階層化を使用して Glacier Deep Archive に書き込まれたイメージは、リストア操作でのみ読み取れます。これらのイメージは、検証と複製の操作では読み取れません。
  p.32 の「Amazon Glacier でのデータの保護について」を参照してください。
- Amazon S3 Intelligent-Tiering (LIFECYCLE) (MSDP ダイレクトクラウド階層化ではサポートされません)
  p.42 の「Amazon S3 Intelligent Tiering (LIFECYCLE) を使用したデータの保護」を参照してください。

Amazon S3 ストレージクラスについて詳しくは、「Amazon S3 ストレージクラス」を参照してください。

次のシナリオでは、NetBackup はデフォルトの STANDARD ストレージクラスをバックアップまたはオブジェクトに割り当てます。

- Amazon S3 クラウドストレージを構成しているときに特定のストレージクラスを選択しない場合
- バックアップが以前の NetBackup バージョンで構成されたものである場合

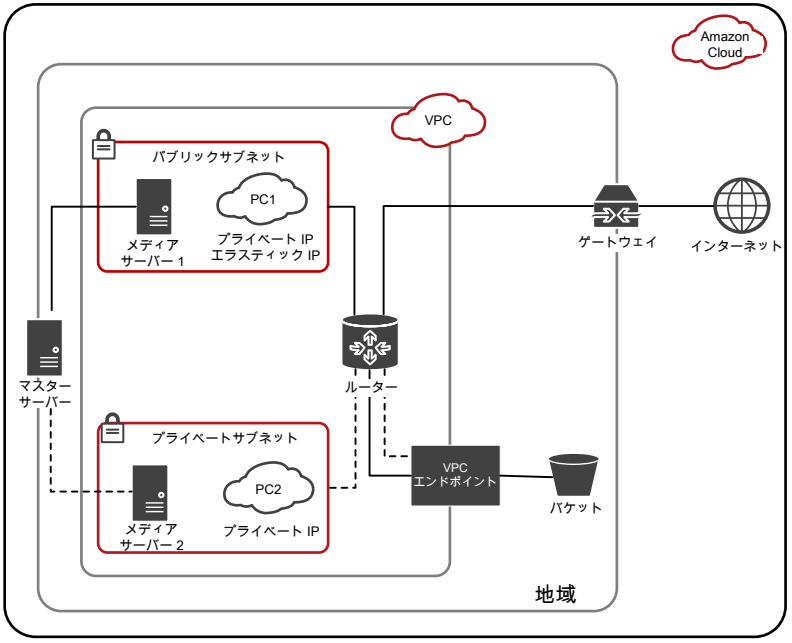
メモ: Glacier または Glacier Deep Archive からのリストアを開始すると、NetBackup でウォーム化の手順が開始されます。読み取るすべてのデータが S3 ストレージで利用可能になるまで、NetBackup によるリストアは実行されません。

Amazon を使用している場合、ウォーム化の手順は常に実行されます。Glacier と Glacier Deep Archive 以外のストレージクラスの場合、ウォーム化の手順はほぼ即座に完了するため、大きな遅延は発生しません。Glacier と Glacier Deep Archive の場合も、以前にウォーム化されたファイルが S3 Standard ストレージに残っていれば、ウォーム化の手順に時間はかからない場合があります。ただし、使用している設定に応じて、数分、数時間、数日かかる場合があります。

NetBackup による Amazon 仮想プライベートクラウドサポート

NetBackup を使用して、Amazon 仮想プライベートクラウド (VPC) 環境に新しいクラウドストレージを追加できます。

次の図では、NetBackup がどのように VPC と統合するかが示されています。



図は次の点を示しています。

- VPC 環境内にメディアサーバーを配備する必要があります。
- ローカルまたは VPC 環境にプライマリサーバーを配備できます。プライマリサーバーがメディアサーバーと通信できるように設定します。
- パブリックサブネットでは、PC1 は、プライベート IP とエラスティック IP の両方を使用して、インターネットにアクセスできます。メディアサーバー 1 もインターネットにアクセスできます。パブリックサブネットでは、インターネットまたは VPC エンドポイントを使用して、ストレージバケットを認証してアクセスできます。
- プライベートサブネットでは、PC2 は、プライベート IP のみを使用し、インターネットにアクセスできません。また、メディアサーバー 2 もインターネットにアクセスできません。プライベートサブネットでは、VPC エンドポイントを使用して、ストレージバケットを認証してアクセスできます。
- VPC は特定のリージョンに制限されます。

Amazon 仮想プライベートクラウド (VPC) 環境でクラウドストレージサーバーを設定するための考慮事項

- 特定のリージョンの新しいクラウドストレージサーバーを追加する必要があります。
- 1 つのサービスホストに複数のリージョンを設定しないでください。

- サービスホストのリージョンを設定するときは、VPC のリージョンと同じである必要があります。別のリージョンは設定できません。たとえば、シンガポールリージョンの VPC 環境のクラウドストレージを追加する場合、サービスホストリージョンをシンガポールに設定する必要があります。
- デフォルト (米国東部 (北バージニア)) の AWS リージョンの VPC については、サービスホストとして s3-external-1.amazonaws.com を、ロケーション識別子として us-east-1 を使用します。
- VPC 環境内でメディアサーバーを使用するように、NetBackup ポリシーを設定します。

長期保持のための Amazon のデータの保護について

次の Amazon クラウドストレージオプションを使用して、データの長期保持を実現できます。

- p.32 の「Amazon Glacier でのデータの保護について」を参照してください。
- p.36 の「Amazon Glacier Vault でのデータの保護について」を参照してください。

GLACIER、GLACIER_DEEP_ARCHIVE、GLACIER_VAULT ストレージクラスの違い: 用途

GLACIER と GLACIER_VAULT ストレージクラスのどちらを使用するかを決めるには、次の表を参考にしてください。

GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラス	GLACIER_VAULT ストレージクラス
GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラスは、S3 エンドポイントからのデータのアップロードと Glacier へのデータの移行に対応しています。	GLACIER_VAULT ストレージクラスは、Amazon Glacier サービスを使用した、Vault へのデータのアップロードに対応します。
GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラスの場合、メタデータは STANDARD ストレージクラスに格納されます。	GLACIER_VAULT ストレージクラスの場合、メタデータは、STANDARD ストレージクラスと GLACIER_VAULT ストレージクラスに格納されます。
GLACIER の運用コストは、GLACIER_VAULT の場合より約 2% 高くなります。	GLACIER ストレージクラスと GLACIER_VAULT ストレージクラスの運用コストはほぼ同じです。GLACIER の方が GLACIER_VAULT より約 2% 高くなります。

GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラス	GLACIER_VAULT ストレージクラス
変更不能な Vault ロック機能を使用する予定がない場合は、GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラスを使用します。	コンプライアンス目的で変更不能な Vault ロックポリシーを使用するか、ランサムウェア攻撃からデータを保護することを計画している場合は、GLACIER_VAULT ストレージクラスを使用します。
GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラスには、構成可能な取得保持期間があります。そのため、サイズや速度が原因で時間がかかるリストアに便利です。	GLACIER_VAULT ストレージクラスの取得保持期間は 24 時間 (固定値) です。p.158 の「Amazon Glacier Vault からのリストアが 1 つのフラグメントで 24 時間より長くかかる」を参照してください。
オブジェクトがアップロードされると、Amazon S3 サービスコンソールで、すべてのオブジェクトとそのストレージクラスのプロパティが可視化されます。その結果、GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラスを使用して作成された NetBackup イメージは、Amazon S3 サービスコンソールでより優れた可視性を得られます。	Amazon は、24 時間かけてアーカイブインベントリを更新します。そのため、GLACIER_VAULT ストレージクラスを使用したバックアップ中のアーカイブのアップロードは、24 時間後にならないと Amazon Glacier サービスコンソールに反映されません。ただし、バックアップ中に生成されたメタデータから、Amazon S3 サービスコンソールでバックアップを部分的に可視化できます。Amazon Glacier サービスコンソールでは、個々のアーカイブを可視化できません。
GLACIER_VAULT ストレージクラス (Amazon Glacier サービスを使用) と GLACIER および GLACIER_DEEP_ARCHIVE ストレージクラス (Amazon S3 サービスを使用) との間にはアーキテクチャ上の違いがあります。そのため、両者の間には速度の差があり、ストレージクラスを選ぶ際の判断基準になります。	GLACIER_VAULT ストレージクラス (Amazon Glacier サービスを使用) と GLACIER および GLACIER_DEEP_ARCHIVE ストレージクラス (Amazon S3 サービスを使用) との間にはアーキテクチャ上の違いがあります。そのため、両者の間には速度の差があり、ストレージクラスを選ぶ際の判断基準になります。
障害発生時のストレージクリーンアップ処理は、GLACIER と GLACIER_DEEP_ARCHIVE ストレージクラスの方が優れています。	障害発生時のストレージクリーンアップ処理は、GLACIER ストレージクラスの方が GLACIER_VAULT ストレージクラスより優れています。

Amazon Glacier でのデータの保護について

長期保持用にデータを保護するために、NetBackup を使用して Amazon (AWS) Glacier にデータをバックアップできます。NetBackup を使用して、GLACIER または GLACIER_DEEP_ARCHIVE ストレージクラスのストレージサーバーを作成できます。

Amazon GLACIER または DEEP ARCHIVE ストレージクラスのクラウドストレージサーバーを構成するには

1. Amazon GLACIER または GLACIER_DEEP_ARCHIVE クラウドストレージサーバーを構成します。

   p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

2. GLACIER または GLACIER_DEEP_ARCHIVE ストレージ用の Amazon バケットを使用して、ディスクプールを作成します。

   p.114 の「クラウドストレージのディスクプールの構成」を参照してください。

3. バックアップポリシーを作成します。

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

必要な権限が付与されていることも確認します。p.17 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。

Amazon Glacier にテープデータを複製するには

`bpduplicate` コマンドを使用して、Amazon Glacier ストレージにテープデータを複製します。

ベストプラクティス

データを Amazon Glacier に移行するようにストレージサーバーを構成する場合は、次の点を考慮してください。

- バケットが属する地域で GLACIER または GLACIER_DEEP_ARCHIVE がサポートされていることを確認してください。
- リストアは、取得保持期間を最短で 3 日に設定します。
- 時間を短縮してイメージのインポートのコストを削減するために、可能な場合には必ず True Image Recovery オプションを選択します。
  Glacier に送信されたデータを取得するために、バックアップイメージのフラグメントごとに約 4 時間の固有の時間遅延があります。イメージのインポートのフェーズ 2 の場合、この時間遅延は Glacier ストレージのイメージでは一般的です。ただし、ポリシーの True Image Recovery を有効にすると、フェーズ 2 のインポートの遅延時間は、フラグメントごとに 4 時間から数分へと大幅に短縮されます。フェーズ 1 のインポートは、True Image Recovery がポリシーに対して有効になっているかどうかに関係なく、さらに高速です。
  True Image Recovery のサポート対象の作業負荷およびファイルシステムについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。
  イメージのインポート時におけるフェーズについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。
- 並列リストアでは、リストア時間を短縮できます。この操作では、論理的な境界に複数のイメージを作成するマルチストリーミングを使用してバックアップを作成します。

- 作業負荷個別リカバリ (GRT) または VMware シングルファイルリストア (SFR) では、プライマリ、メディア、クライアントでのタイムアウトが 5 時間以上増えます。

制限事項

次の制限事項を考慮してください。

- NetBackup アクセラレータ機能は、GLACIER または GLACIER_DEEP_ARCHIVE 用に作成されたストレージユニットのポリシーではサポートされていません。[アクセラレータ]チェックボックスは選択しないでください。

Amazon Glacier からのデータのリストアについて

NetBackup イメージは、指定したストレージクラス (この場合は GLACIER または GLACIER_DEEP_ARCHIVE ストレージクラス) を持つオブジェクトのセットとして格納されます。Amazon Glacier からのリストアは 2 つの段階で行われます。

- オブジェクトは Amazon によって管理されている内部ステージング場所で最初に取得されます。
- そこから、宛先の場所にデータがリストアされます。

NetBackup は次の Amazon の取得形式をサポートします。

- Bulk 取得。5 時間から 12 時間で完了します。
- Standard 取得。3 時間から 5 時間で完了します。
- Expedited 取得。1 分から 5 分で完了します。

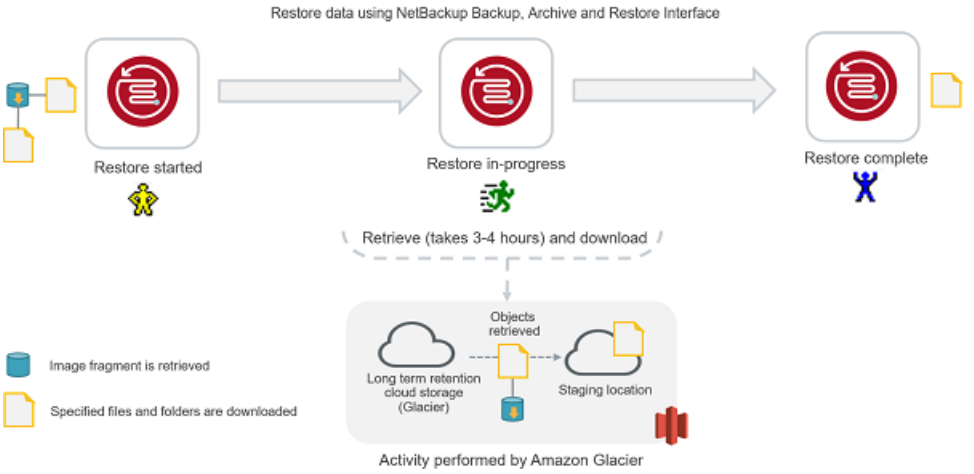
Amazon S3 ストレージクラスについて詳しくは、「Amazon S3 ストレージクラス」を参照してください。

メモ: Expedited 取得を指定すると、Amazon がリソース不足のため要求に失敗することがあります。このエラーが発生した場合は、Standard 取得または Bulk 取得を使用する必要があります。この場合、リストアジョブは失敗します (NetBackup 状態 5: リストアが完全に失敗しました)。

アクティビティモニターに、bpbrm からメッセージ「イメージのウォーム化に失敗しました 503 (Image warming failed 503)」が表示されます。MSDP ダイレクトクラウド階層化を使用すると、MSDP サーバーの ocsd_storage ログに、エラー「GlacierExpeditedRetrievalNotAvailable: Glacier Expedited 取得は現在使用できません。後でもう一度実行してください。状態コード: 503 (GlacierExpeditedRetrievalNotAvailable: Glacier expedited retrievals are currently not available, please try again later status code: 503)」が表示されます。

リストアを実行すると、選択したオブジェクトのみがダウンロードされている間に、イメージフラグメント全体がリストアされます。

図 2-1 Amazon Glacier からのリストア



メモ: MSDP ダイレクトクラウド階層化で Glacier を使用する場合、プライマリサーバーの `/usr/openv/netbackup/bin` ディレクトリで `GLACIER_RETRIEVAL` touch ファイルを作成し、`bulk`、`standard`、または `expedited` の 3 つの文字列のいずれかを含めることができます。Bulk 取得オプションを使用しない場合に、この touch ファイルを作成できます。

Glacier を使用する場合、`bulk`、`standard`、または `expedited` を使用できます。DEEP_ARCHIVE を使用する場合は、`bulk` または `standard` を使用できます。文字列が定義されておらず、touch ファイルが存在しない場合、NetBackup のデフォルトは `bulk` です。

標準の重複排除されないクラウドストレージサーバーで Glacier を使用する場合は、Amazon Standard 取得のみがサポートされます。

Amazon S3 を使用したリストアについて詳しくは、「アーカイブされたオブジェクトの復元 (Restoring Archived Objects)」を参照してください。

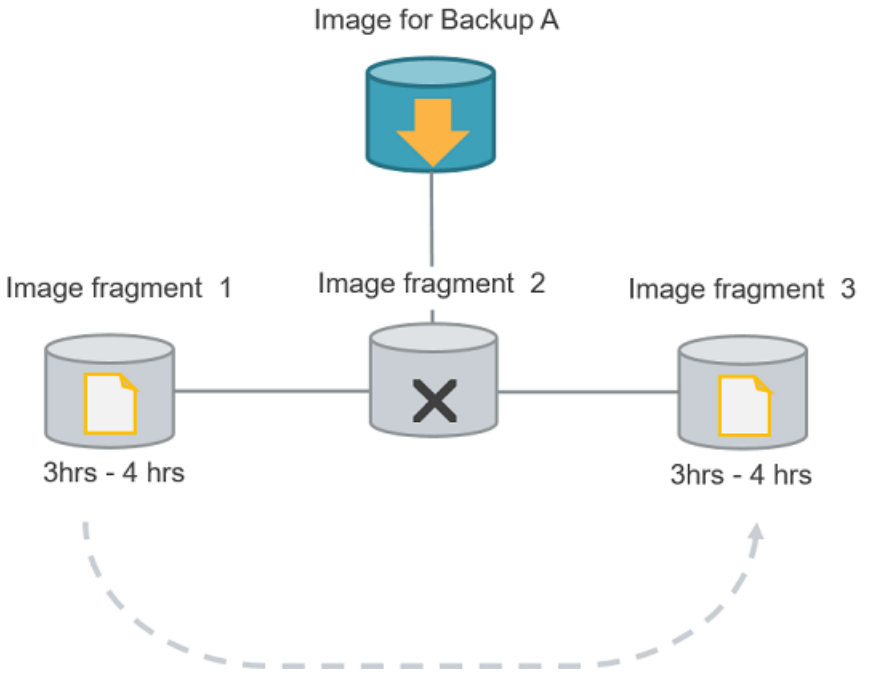
イメージフラグメントのリストアに関する考慮事項

メモ: このセクションは、MSDP ダイレクトクラウド階層化には適用されません。このセクションは、標準の重複排除されないクラウドストレージサーバーにのみ適用されます。

複数のイメージフラグメントに属するファイルとフォルダをリストアする場合は、次の点を考慮してください。

- 一度に 1 つのイメージフラグメントが取得されます。最初のイメージフラグメントの選択したファイルとフォルダがダウンロードされた後に、初めて次のイメージフラグメントが取得されます。
- リストア時間は、イメージフラグメントの数に応じて考慮する必要があります。たとえば、リストアするファイルが 2 つのフラグメントの一部である場合、さらに 6 時間から 10 時間が合計リストア時間に追加されます。

図 2-2 Amazon Glacier のイメージフラグメントのリストア



メモ: リストアの取得が開始された後にジョブをキャンセルすると、キャンセルの時点までにステージング場所で取得されたすべてのオブジェクトに対して費用が発生します。

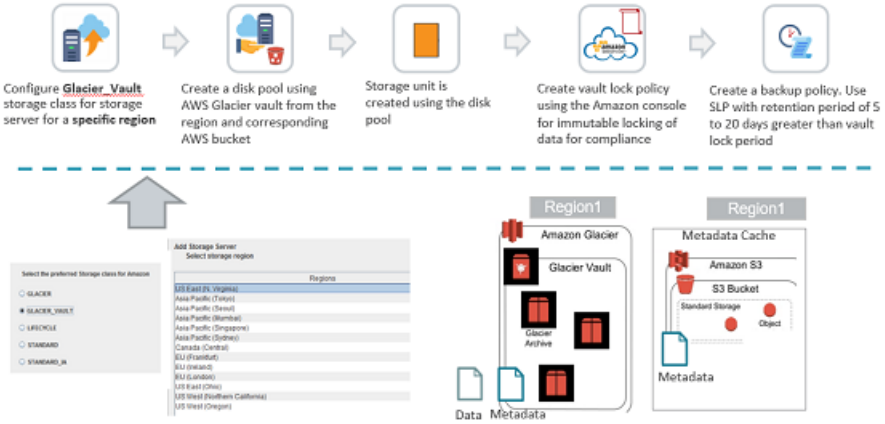
Amazon Glacier Vault でのデータの保護について

Amazon の Vault ロックポリシーを使用して長期保持用にデータを保護するため、NetBackup を使用して Amazon Glacier Vault にデータをバックアップできます。

NetBackup を使用して GLACIER_VAULT ストレージクラスを作成する場合は、Vault 名と、Vault を作成する地域を指定します。

Amazon の Vault ロックポリシーを使用して、Vault でコンプライアンス制御を実行したり、Vault を WORM (Write Once Read Many) デバイスにすることができます。詳しくは、Amazon のマニュアルを参照してください。

図 2-3 Amazon Glacier Vault でのデータの保護



GLACIER_VAULT ストレージクラスのクラウドストレージサーバーを構成するには

1 Amazon GLACIER Vault クラウドストレージサーバーを構成します。

p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

メモ: 各ストレージサーバーに関連付けられる地域は 1 つのみです。

2 GLACIER ストレージ用の Amazon バケットを使用してディスクプールを作成します。

p.114 の「クラウドストレージのディスクプールの構成」を参照してください。

メモ: 目的の Vault が表示されない場合は、Vault が Vault 地域と同じ地域内に S3 バケットを持っていないか、ディスクプールを作成するストレージサーバーと対応する地域内に Vault が存在しないことを意味します。

3 Amazon コンソールを使用して Vault ロックポリシーを作成します。詳しくは、Amazon のマニュアルを参照してください。

4 バックアップポリシーを作成します。

ベストプラクティス

データを Amazon Glacier Vault にバックアップするようにストレージサーバーを構成する場合は、次の点を考慮してください。

- アーカイブの削除を禁止するために変更不可の Vault ロックポリシーを構成してある場合、Amazon Glacier Vault は、アーカイブが削除用にロック解除されるまで、アーカイブの削除を許可しません。そのため、バックアップポリシーに構成する保持期間は、Vault ロック期間より長く (2 週間以上、または環境内の GLACIER_VAULT にデータをバックアップまたは複製するときにかかる再試行を含めた最大時間) する必要があります。そうしないと、イメージの有効期限が切れるときにイメージのクリーンアップジョブが失敗します。p.157 の「Amazon Glacier Vault のイメージクリーンアップエラーの処理」を参照してください。
- Vault は、二次的なデータバックアップ先として使用することをお勧めします。
- Vault ロックポリシーを使用する予定がある場合は、Vault に使用する保持レベルごとに Vault を作成してください。
- バックアップごとに格納されるデータのサイズを縮小するには、圧縮バックアップと増分バックアップを使用します。
- 時間を短縮してイメージのインポートのコストを削減するために、可能な場合には必ず True Image Recovery オプションを選択します。
  Glacier に送信されたデータを取得するために、バックアップイメージのフラグメントごとに約 4 時間の固有の時間遅延があります。イメージのインポートのフェーズ 2 の場合、この時間遅延は Glacier ストレージのイメージでは一般的です。ただし、ポリシーの True Image Recovery を有効にすると、フェーズ 2 のインポートの遅延時間は、フラグメントごとに 4 時間から数分へと大幅に短縮されます。フェーズ 1 のインポートは、True Image Recovery がポリシーに対して有効になっているかどうかに関係なく、さらに高速です。
  True Image Recovery のサポート対象の作業負荷およびファイルシステムについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。
  イメージのインポート時におけるフェーズについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

制限事項

次の制限事項を考慮してください。

- NetBackup アクセラレータ機能は、GLACIER_VAULT 用に作成されたストレージユニットのポリシーではサポートされていません。[アクセラレータ]チェックボックスは選択しないでください。
- Amazon GovCloud クラウドプロバイダの Glacier エンドポイント (glacier.us-gov-west-1.amazonaws.com) は、NetBackup GLACIER_VAULT ストレージクラスを使用したセキュアモードの通信のみサポートします。このため、GLACIER_VAULT ストレージクラスを使用して Amazon GovCloud クラウドストレー

ジを設定するときに、[SSL を使用する (Use SSL)]オプションを無効にすると、設定は失敗します。

権限

次の権限が必要です。

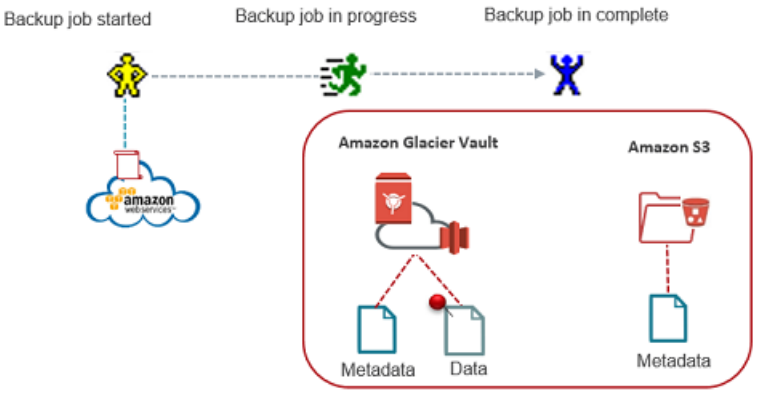
- glacier:ListVaults
- glacier:CreateVault
- glacier:DescribeVault
- glacier:UploadArchive
- glacier:DeleteArchive
- glacier:ListJobs
- glacier:Describejob
- glacier:InitiateJob
- glacier:GetJobOutput
- また、必要な S3 関連の IAM USER 権限があることも確認します。p.17 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。

権限に関連する問題について詳しくは、p.160 の「Amazon IAM アクセス権がないために発生するエラーのトラブルシューティング」を参照してください。を参照してください。

Amazon Glacier Vault へのデータのバックアップについて

NetBackup のバックアップジョブを実行して、GLACIER_VAULT ストレージクラスを使用してデータがバックアップされると、そのデータは一連のアーカイブとして Vault に格納されます。メタデータは、STANDARD ストレージクラスオブジェクトとして S3 バケットに格納されるほか、一連のアーカイブとして Amazon Glacier Vault に格納されます。

図 2-4 Amazon Glacier Vault へのバックアップ



注意事項:

- ネットワークの問題によりバックアップが失敗すると、部分的にバックアップされたデータが Vault に残り、ストレージ領域を占有します。
- 他のクラウドストレージクラスから Glacier へのデータ移動には、Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスの使用をお勧めします。p.42 の「Amazon S3 Intelligent Tiering (LIFECYCLE) を使用したデータの保護」を参照してください。ただし、他のクラウドストレージクラスから GLACIER_VAULT にデータを移動するには、クラウドメディアサーバーをホストし、それを介してデータを複製する必要があります。これは、データ損失のコストを避けるための手順です。この回避策は、GLACIER_VAULT ストレージクラスから他のクラウドストレージクラスにデータを移動する場合にも適用されます。

Amazon Glacier Vault からのデータのリストアについて

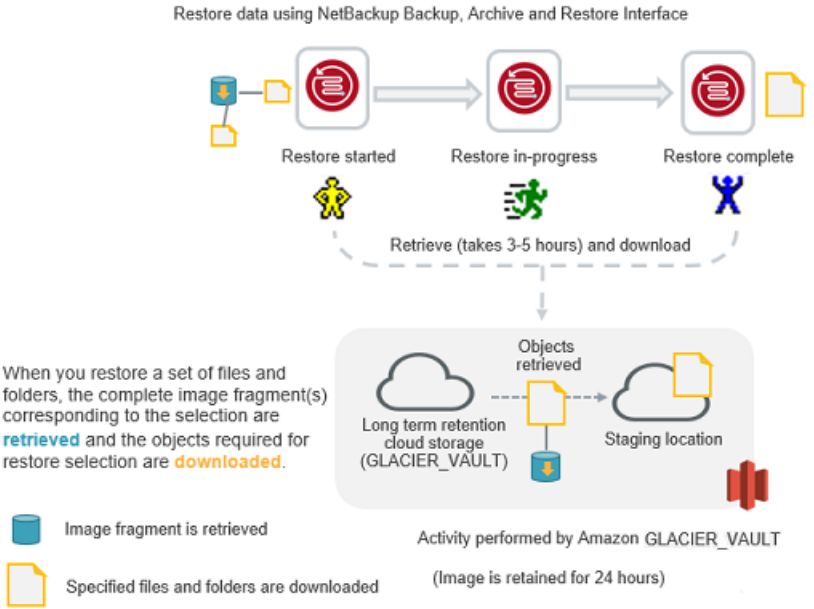
NetBackup イメージは、一連のデータアーカイブとして GLACIER_VAULT ストレージクラスに格納されます。Amazon Glacier Vault からのリストアは 2 つの段階で行われます。

- アーカイブはまず、Amazon が管理する内部ステージング場所で取得されます。
- そこから、ターゲットの場所にデータがリストアされます。

ステージングのリストア操作には最短で 3 時間から 5 時間かかります。アーカイブは Amazon ステージング場所で最大 24 時間利用できます。

メモ: NetBackup は Amazon Standard の取得をサポートしており、最短で 3 時間から 5 時間で完了します。リストアを実行すると、イメージフラグメント全体がステージング場所にリストアされ、選択したオブジェクトのみがダウンロードされます。

図 2-5 Amazon Glacier Vault からのリストア

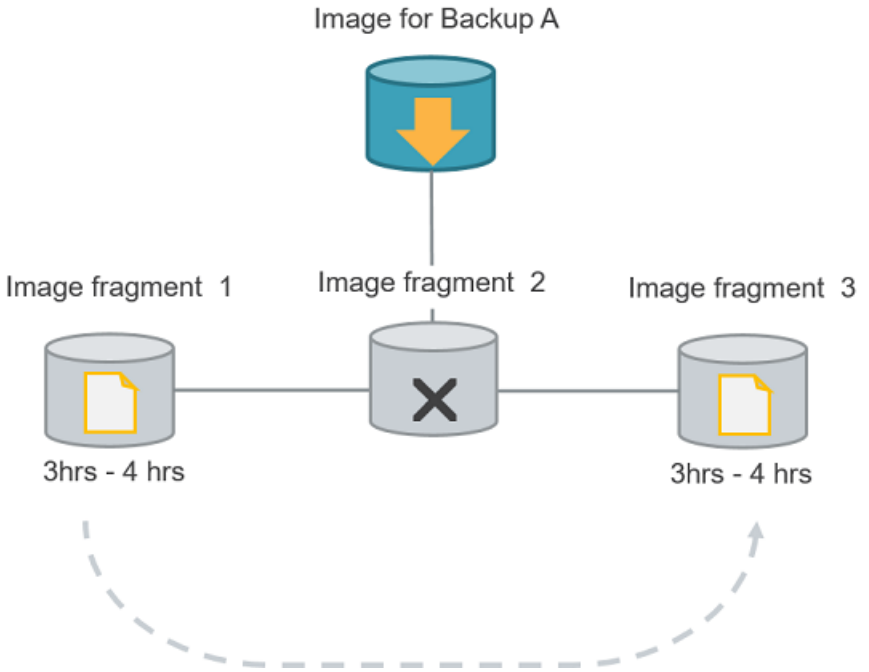


イメージフラグメントのリストアに関する考慮事項

複数のイメージフラグメントに属するファイルとフォルダをリストアする場合は、次の点を考慮してください。

- 一度に 1 つのイメージフラグメントが取得されます。最初のイメージフラグメントの選択したファイルとフォルダがダウンロードされた後に、初めて次のイメージフラグメントが取得されます。
- リストア時間は、イメージフラグメントの数に応じて考慮する必要があります。たとえば、リストアするファイルが 2 つのフラグメントの一部である場合、さらに 6 時間から 10 時間が合計リストア時間に追加されます。

図 2-6 Amazon GLACIER_VAULT のイメージフラグメントのリストア



メモ: リストアの取得が開始された後にジョブをキャンセルすると、キャンセルの時点までにステージング場所で取得されたすべてのオブジェクトに対して費用が発生します。

Amazon S3 Intelligent Tiering (LIFECYCLE) を使用したデータの保護

クラウド階層化を使用してデータを保護するには、Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスを使用します。クラウド階層化を使用すると、データを STANDARD ストレージクラスまたは STANDARD_IA ストレージクラスにバックアップしてから、STANDARD_IA ストレージクラスまたは GLACIER ストレージクラスにデータを移行できます。データが各ストレージクラスに存在する日数を決定するストレージサーバーのプロパティを構成できます。このように、短期的または長期的なデータ保護のためにストレージサーバーを構成できます。

Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスのクラウドストレージサーバーを構成する方法

1. Amazon S3 Intelligent Tiering (LIFECYCLE) クラウドストレージサーバーを構成します。

   p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

2. 次のストレージサーバーのプロパティを構成します。

   - AMZ:UPLOAD_CLASS
   - AMZ:TRANSITION_TO_STANDARD_IA_AFTER
   - AMZ:TRANSITION_TO_GLACIER_AFTER

   p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

3. Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスのディスクプールを作成します。

   p.114 の「クラウドストレージのディスクプールの構成」を参照してください。

4. バックアップポリシーを作成します。

ベストプラクティス

- 選択されたバケットに既存のライフサイクルポリシーがないことを確認します。
- データを GLACIER に移行するように設定されている場合は、次の点を考慮してください。
  - バケットが属する地域で Amazon Glacier がサポートされていることを確認してください。
  - 複数のイメージを論理的な境界で取得するには、マルチストリームを使用できます。

制限事項

次の制限事項を考慮してください。

- NetBackup アクセラレータ機能は、Amazon S3 Intelligent Tiering (LIFECYCLE) 用に作成されたストレージユニットのポリシーではサポートされていません。[アクセラレータ]チェックボックスは選択しないでください。

権限

次の権限が必要です。

- ライフサイクルポリシー関連の権限:
  - s3:PutLifecycleConfiguration

- s3:GetLifecycleConfiguration

- オブジェクトタグ付け権限
  - s3:PutObjectTagging

メモ: バケット所有者は、デフォルトでは、これらの権限を持ちます。バケットの所有者は、アクセスポリシーを作成して他のユーザーにこれらの権限を付与できます。

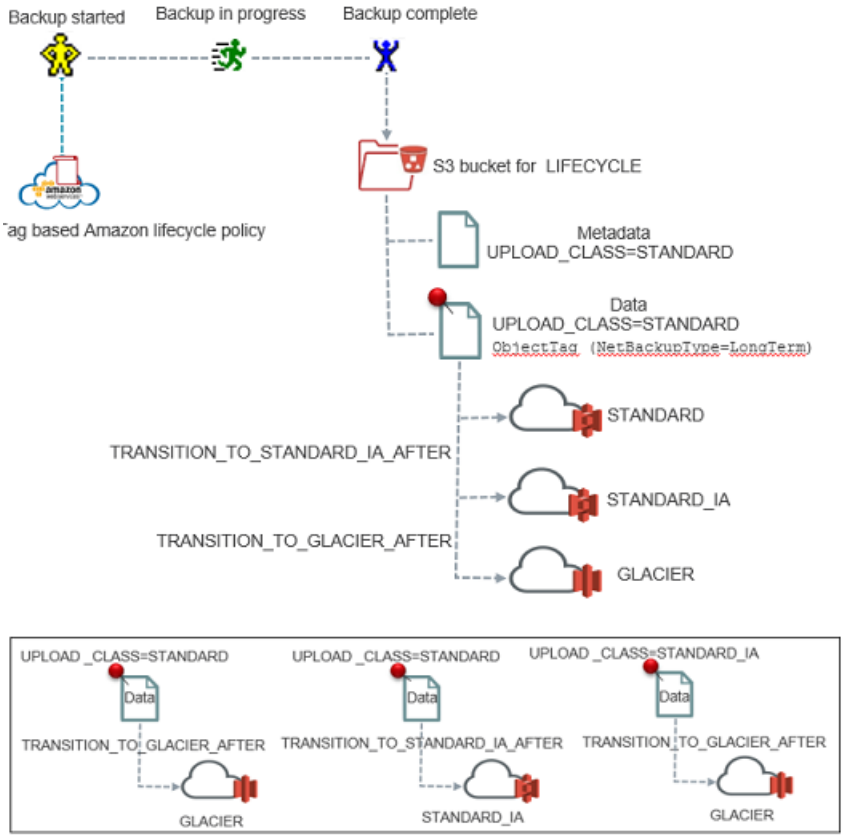
- 必要な IAM USER 権限があることも確認します。p.17 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。

Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスを使用したデータのバックアップについて

初期時には、バックアップデータはストレージサーバーのプロパティダイアログボックスの設定 AMZ:UPLOAD_CLASS によって決定されたストレージクラスに存在します (デフォルトは STANDARD です)。ただし、データが他のストレージクラスに移行するまでの期間は、次のストレージサーバーのプロパティを変更することで構成できます。

- TRANSITION_TO_STANDARD_IA_AFTER
- TRANSITION_TO_GLACIER_AFTER

図 2-7 指定可能な構成の Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスのバックアッププロセス



メモ: GLACIER または STANDARD_IA から STANDARD ストレージクラス、または GLACIER から STANDARD_IA ストレージクラスにデータを移動する場合は、クラウドメディアサーバーをホストし、それを介してデータを複製する必要があります。

ストレージサーバーのプロパティを変更した後、ストレージサーバーのディスクプールごとに新しいバックアップジョブが実行されると、新しいストレージサーバーのプロパティは、ディスクプールに関連付けられているバケットとそのバケットの古い非移行イメージに適用されます。

p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

p.32 の「Amazon Glacier でのデータの保護について」を参照してください。

Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスからのデータのリストアについて

リストアするときに、データが STANDARD または STANDARD_IA ストレージクラスにあれば、そのデータは宛先の場所にリストアされます。ただし、データが GLACIER ストレージクラスに存在していれば、データはまず Amazon によって管理されている内部ステージング場所で取得されます。それからデータは宛先の場所にリストアされます。したがって、STANDARD または STANDARD_IA ストレージクラスからデータをリストアするためにかかる時間は、GLACIER ストレージクラスからデータをリストアするためにかかる時間よりもかなり短くなります。

p.34 の「Amazon Glacier からのデータのリストアについて」を参照してください。

NetBackup での Amazon IAM ロールの使用について

AWS IAM ロールは、ID にどのタスクを実行する権限があるかを決定する権限ポリシーを伴うアマゾンウェブサービス (AWS) の ID です。ロールを使用すると、通常は AWS リソースへのアクセス権がないユーザー、アプリケーション、またはサービスにアクセス権を委任できます。ロールは、それを必要とする誰でも引き受けることができます。あるユーザーがロールを引き受けると、一時的なセキュリティクレデンシャルが動的に作成され、ユーザーに提供されます。

たとえば、AWS Elastic Compute Cloud (EC2) インスタンスで実行するアプリケーションには、S3 サービスなどの他の AWS サービスにアクセスするクレデンシャルが必要です。従来の方法では、固定のクレデンシャルのアクセスキーとシークレットアクセスキーを提供します。IAM ロールの場合は、一時的なクレデンシャルを使用して他の AWS サービスに接続します。

注意事項

NetBackup は、ストリームベースのバックアップ操作用に AWS IAM ロールをサポートしています。

1. NetBackup は、すべての S3 ストレージ通信用にメディアサーバーが構成されている AWS EC2 インスタンスに接続された AWS IAM ロールを使用します。
2. NetBackup は、AWS EC2 メタデータに接続することで、ロール名と一時的なクレデンシャルをフェッチします。
3. NetBackup プライマリサーバーは、AWS EC2 インスタンスまたはオンプレミスに配備できます。プライマリサーバーとメディアサーバー間の通信には、必須のネットワーク設定を行う必要があります。
4. IAM ロールを使用してデータをクラウドにバックアップする NetBackup メディアサーバーは、AWS EC2 インスタンスに配備する必要があります。

5. AWS EC2 インスタンスで実行している NetBackup メディアサーバーには、必須の権限を持つ AWS IAM ロールを接続する必要があります。p.17 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。
6. バックアップデータは、AWS IAM ロールが作成されたのと同じ AWS アカウントの S3 ストレージに格納されます。
7. NetBackup は、Amazon と Amazon Gov の両方のクラウドプロバイダについて、AWS IAM ロールベースの認証をサポートしています。
8. `csconfig` コマンドを使用すると、認証のみの目的で AWS IAM ロールを使用するように既存のクラウドストレージサーバー (エイリアス) を変更できます。
9. IAM ロールの割り当て、変更、無効化の操作を実行するには、AWS 管理コンソールを使用します。NetBackup は、ロール固有の情報を一切格納しません。
10. AWS EC2 IMDS (インスタンスメタデータサービス) が NetBackup メディアサーバーにアクセスできることを確認してください。これは、AWS コマンドを使用して確認できます。

    IMDSv1 または IMDSv2 を使用して、実行中のインスタンスからインスタンスのメタデータにアクセスできます。

    メモ: MSDP クラウドストレージは IMDSv2 をサポートします。Amazon S3 クラウドコネクタは IMDSv2 をサポートしません。

    IMDSv2 は、EC2 インスタンスメタデータサービスの機能強化により、オープンファイアウォール、リバースプロキシ、SSRF の脆弱性に対する防御を追加します。IMDSv2 の使用をお勧めします。詳しくは、AWS のマニュアルを参照してください。

    IMDSv2 を使用してインスタンスを構成するには、「インスタンスメタデータオプションの設定」を参照してください。

    次に例を示します。

    ロール名を取得するには、次のコマンドを実行します。

    ```
    TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H
    "X-aws-ec2-metadata-token: $TOKEN" -v
    http://169.254.169.254/latest/meta-data/iam/security-credentials/
    ```

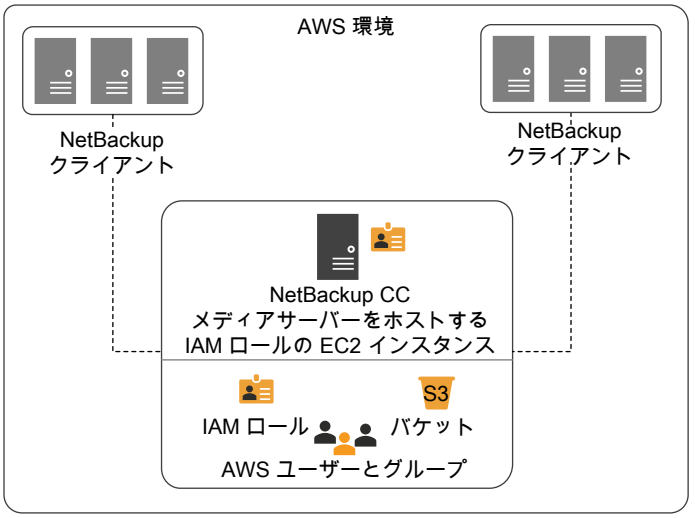
    クレデンシャルを取得するには、次のコマンドを実行します。

    ```
    TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H
    "X-aws-ec2-metadata-token: $TOKEN" -v
    http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name/role-name
    ```

11. AWS EC2 インスタンスのメタデータサービスは IPv4 のみでサポートされているため、IPv6 のみの配備では AWS IAM ロールを使用できません。
12. AWS IAM ロールは MSDP ダイレクトクラウド階層化ストレージサーバーでもサポートされます。

AWS IAM ロールの配備

次の図は、配備を示しています。



この図に示すとおり、NetBackup で AWS IAM ロールを使用する場合は次のようになります。

- NetBackup プライマリサーバーは、オンプレミスまたはクラウドに配備できます。
- バックアップデータは、AWS IAM ロールが作成されたのと同じ AWS アカウントの S3 ストレージに格納されます。
- AWS IAM ロールは、メディアサーバーを実行している AWS EC2 インスタンスに接続されます。

メモ: S3 ストレージへのアクセス権がある AWS EC2 インスタンスにロールが接続されると、NetBackup ユーザーはクレデンシャルを提供する必要がなくなります。

ヒント: NetBackup クライアントをクラウドに配備すると、パフォーマンスが向上します。

NetBackup での AWS IAM ロールの構成

AWS 管理コンソールと NetBackup Web UI を使用すると、NetBackup で AWS IAM ロールを構成できます。

NetBackup で AWS IAM ロールを構成するには

1. NetBackup で AWS IAM ロールを使用するには、AWS 管理コンソールで次の構成を実行します。
   - AWS IAM ロールを作成します。
   - NetBackup メディアサーバーとして使用する AWS EC2 インスタンスにロールを接続します。

   ガイドラインについて詳しくは、テクニカルノートを参照してください。
2. AWS IAM ロールを使用するための新しいクラウドストレージサーバーを構成します。AWS IAM ロールの使用では、クレデンシャル固有の情報は必要はありません。

   p.18 の「Amazon S3 のクラウドストレージプロバイダのオプション」を参照してください。

   p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

`csconfig` コマンドで、クレデンシャルブローカー (`-creds_broker`) に対してオプション「`CREDS_ROLE`」を使用します。

『NetBackup コマンドリファレンスガイド』を参照してください。

メモ: 認証に AWS IAM ロールを使用するように既存のクラウドストレージサーバー (エイリアス) を変更するには、`csconfig` コマンドのみを使用します。

NetBackup における Amazon S3 クラウドコネクタの文字制限について

S3 準拠のクラウドストレージの NetBackup S3 クラウドコネクタでは、仮想マシンの表示名にサポートされていない文字が含まれている場合には、VMware および Hyper-V のバックアップがサポートされません。サポートされていない文字の一覧については、Amazon S3 の「オブジェクトキーの命名のガイドライン」を参照してください。

Amazon S3 のオブジェクトキー命名ガイドラインに記載の回避する必要のある文字

仮想マシンの表示名は Amazon S3 のコンテキストのキー名に対応します。したがって、仮想マシンの表示名では以下の一連の文字を使用しないでください。

- バックスラッシュ ¥
- 左波カッコ {
- 右波カッコ }

- 出力不可の ASCII 文字 (10 進文字の 128 から 255)
- 山形記号 ^
- パーセント記号 %
- アクサングラーブまたはバッククォート `
- 右角カッコ]
- 左角カッコ [
- 二重引用符 "
- チルダ ~
- 小なり (より小さい) 記号 <
- 大なり (より大きい) 記号 <
- シャープ記号 #
- 縦棒またはパイプ |

NetBackup S3 コネクタガイドラインに記載の回避する必要のある文字

仮想マシンの表示名では以下の一連の文字を使用しないでください。

- アンパサンド &
- ドル $
- ASCII 文字の範囲: 16 進の 00 から 1F (10 進の 0 から 31) と 7F (10 進の 127)
- アットマーク @
- 等号 =
- セミコロン ;
- コロン :
- プラス +
- スペース(いくつかの用途では、意味のあるスペースのシーケンス、特に複数のスペースが無視される可能性があります)
- カンマ ,
- 疑問符 ?
- 右丸カッコ)
- 左丸カッコ (

メモ: 使用を回避する文字の最新の一覧については、Amazon S3 のマニュアルを参照してください。

Amazon Snowball および Amazon Snowball Edge を使用したデータの保護

データをクラウドにバックアップするため、NetBackup で Amazon Snowball および Amazon Snowball Edge デバイスを構成できます。

Snowball および Snowball Edge デバイスを使用してバックアップするデータは、次のように分類できます。

古いデータ	テープやディスク、またはその他のストレージメディアに格納され、長年累積されてきたバックアップイメージ。
ライブデータ	ライブデータ: オンプレミスの Amazon Snowball または Amazon Snowball Edge デバイスがある場合に、日次バックアップを使用して生成されたバックアップデータ。 このようなバックアップについては、ストレージライフサイクルポリシーを定義します。実際のバックアップはローカルストレージに保存し、セカンダリコピーは Snowball または Snowball Edge デバイスに複製します。

メモ: 標準的なストレージクラスのみがサポートされます。

ベストプラクティス

Amazon クラウドにデータをバックアップするときは、次の方針に従ってください。

- 少なくとも 1 つのコピーをオンプレミスで保存し、Snowball または Snowball Edge デバイスのデータはクラウドにインポートすることを計画します。Snowball または Snowball デバイス上のバックアップコピーが唯一のコピーである場合、`bpduplicate` コマンドを使用してコピーを作成します。
  『NetBackup コマンドリファレンスガイド』を参照してください。
- オンプレミスのバックアップコピーを破棄する (必要な場合) 前に、クラウド上のインポート済みデータを確認します。
- 最初のシード処理には、Amazon Snowball と Amazon Snowball Edge デバイスを使用します。
- データをインポートする前に、バケットを他の目的に使用しないでください。
- (ライブデータの場合) データの転送中およびクラウドへのインポート中は、複製操作を一時停止します。

- (ライブデータの場合) クラウドでデータが利用可能になったら、複製を再開してオンプレミスで生成された差分データを複製するか、別のデバイスを使用して転送します。

方法

データ転送に使用できるさまざまな方法を次に示します。

表 2-10

デバイス	方法
Amazon Snowball と NetBackup	次のトピックを参照してください。 ■ p.53 の「Amazon Snowball クライアントを使用した Amazon Snowball 用 NetBackup の構成」を参照してください。 ■ p.54 の「Amazon S3 API インターフェースを使用した Amazon Snowball 用 NetBackup の構成」を参照してください。 ■ p.61 の「Amazon Snowball および Amazon Snowball Edge の SSL の構成」を参照してください。 ■ バックアップをクラウドバケットにインポートした後、バックアップ後の手順を実行する必要があります。p.62 の「S3 API インターフェースを使用した場合のバックアップ後の手順」を参照してください。 ■ Amazon Snowball デバイスへの書き込みパフォーマンスを向上するため、複数の Amazon S3 アダプタを構成できます。複数のカスタムインスタンスが同じデバイスを指すこともできます。p.57 の「複数の Amazon S3 アダプタの使用」を参照してください。
Amazon Snowball Edge と NetBackup	次のトピックを参照してください。 ■ p.57 の「ファイルインターフェースを使用した Amazon Snowball Edge 用の NetBackup の構成」を参照してください。 ■ p.59 の「S3 API インターフェースを使用した Amazon Snowball Edge 用 NetBackup の構成」を参照してください。 ■ p.61 の「Amazon Snowball および Amazon Snowball Edge の SSL の構成」を参照してください。 ■ バックアップをクラウドバケットにインポートした後、バックアップ後の手順を実行する必要があります。p.62 の「S3 API インターフェースを使用した場合のバックアップ後の手順」を参照してください。

Amazon Snowball クライアントを使用した Amazon Snowball 用 NetBackup の構成

この方法では、データはまず NetBackup メディアサーバーにステージングされ、その後 Amazon Snowball クライアントを使用して Amazon Snowball デバイスにデータが移動されます。

ステージングに使用するファイルシステムに十分な容量があることを確認します。

Amazon Snowball クライアントを使用して Amazon Snowball にデータを転送するように NetBackup を構成するには

1 デフォルトのインスタンスで、クラウドストレージサーバーを作成します。

メモ: Amazon Snowball デバイスは、デバイスが取得される地域からデータを転送する場合のみ使用できます。したがって、ストレージサーバーのすべてのバケットが同じ地域に属することを確認します。

ディスクプールを構成する際は、Amazon Snowball 用に異なるバケットを作成します。これらのバケットは、AWS コンソールでインポートジョブを作成するために使用されます。

メモ: バケットは、NetBackup Web UI から作成することをお勧めします。AWS コンソールからバケットを作成する場合は、NetBackup でサポートされる文字のみを使用してください。

---

p.73 の「NetBackup のクラウドストレージの構成」を参照してください。

2 AWS コンソールでインポートジョブを作成します。ディスクプールの作成中に作成したバケットを選択します。詳しい手順は、AWS のマニュアルを参照してください。

3 メディアサーバーに、バックアップデータをステージングするための十分な領域があることを確認します。

4 次のストレージサーバープロパティを更新します。

- `AMZ:OFFLINE_TRANSFER_MODE: FILESYSTEM`
- `AMZ:TRANSFER_DRIVE_PATH: <absolute path where the data must be backed up>`

メモ: データを Amazon Snowball デバイスに転送した後、これらのプロパティを `NONE` に戻します。

---

p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

5 ライブデータについては、ストレージライフサイクルポリシーとバックアップポリシーを作成し、最初のシード処理のバックアップを実行します。

古いデータについては、bpduplicate コマンドを使用し、ストレージユニット上のイメージを複製します。

『NetBackup コマンドリファレンスガイド』を参照してください。

6 メディアサーバーに Amazon Snowball クライアントをインストールします。詳しい手順は、AWS のマニュアルを参照してください。

Amazon Snowball クライアントを使用して、メディアサーバーから Amazon Snowball デバイスにバックアップデータを転送します。

7 データ転送が完了したら、次を実行します。

- デバイスが移行中になるまで、バックアップポリシーを無効にするか SLP のセカンダリ操作の処理を延期します。
- 手順 4 で構成したストレージサーバープロパティを NONE に設定します。

8 クラウドベンダーにデバイスを送付します。詳しい手順は、AWS のマニュアルを参照してください。

Amazon Snowball デバイスにデータを移動する Amazon クライアントコマンドの例

バックアップジョブが完了したら、バックアップデータはメディアサーバーでステージングされます。その後、Amazon Snowball クライアントのコピーコマンドを実行して、データを Amazon Snowball デバイスに転送します。次はその例です。

```
snowball cp --recursive <TransferDrivePath/MyBucket/Image>
s3://MyBucket/Logs
```

詳しい手順は、AWS のマニュアルを参照してください。

Amazon S3 API インターフェースを使用した Amazon Snowball 用 NetBackup の構成

Amazon S3 インターフェースを使用して Amazon Snowball デバイスにデータをバックアップする際、データは、ソースから Amazon Snowball デバイスに直接移動されます。この処理では Amazon S3 API を使用します。

S3 API インターフェースを使用して Amazon Snowball にデータを転送するように NetBackup を構成するには

1 一時ストレージサーバーとディスクプールを作成し、デバイスのインポートジョブに使用するバケットを作成するか、一覧表示します。

メモ: バケットは、NetBackup Web UI から作成することをお勧めします。AWS コンソールからバケットを作成する場合は、NetBackup がサポートしている文字のみを使用してください。

---

2 一時ストレージサーバーとディスクプールを削除します。

3 AWS コンソールでインポートジョブを作成します。詳しい手順は、AWS のマニュアルを参照してください。

4 別のホストに、Amazon Snowball S3 アダプタをインストールします。詳しい手順は、AWS のマニュアルを参照してください。

5 (省略可能) Amazon Snowball アダプタとの通信に SSL プロトコルを使用するには、コマンドラインで Amazon Snowball アダプタに提示される証明書をメディアサーバーの `/usr/openv/var/global/cloud/cacert.pem` ファイルに追加します。新たにコピーされた証明書の形式と長さが、`cacert.pem` 内の既存の証明書と一致することを確認します。

p.61 の「Amazon Snowball および Amazon Snowball Edge の SSL の構成」を参照してください。

6 デバイスのカスタムインスタンスを追加します。

Amazon Snowball S3 アダプタをインストールしたホストの詳細でカスタムインスタンスのクラウドストレージプロパティを設定します。

[General Settings]タブで、次の項目を設定します。

- [Provider type]: デバイスを注文したエンドポイントに応じて、Amazon または Amazon GovCloud を選択します。
- [Service host]: アダプタの IP またはホスト名
- [Service endpoint]: 空白
- [HTTP Port]: デフォルトは 8080 です。または、構成したポートを入力します。
- [HTTPS port]: デフォルトは 8443 です。または、構成したポートを入力します。
- [Endpoint access style]: パスの形式

[Region Setting]タブで、次の項目を設定します。

- [Location constraint]: デバイスを注文した領域

- ［Service host］: アダプタの IP またはホスト名

メモ: Amazon Snowball Edge デバイスは、デバイスが取得される地域からデータを転送する場合のみ使用できます。そのため、デバイスが取得される地域のロケーション制約とサービスホストを使用します。

---

p.80 の「クラウドストレージインスタンスの追加」を参照してください。

7 カスタムインスタンスを使用して、デバイスのストレージサーバーを作成します。

p.73 の「NetBackup のクラウドストレージの構成」を参照してください。

8 次のストレージサーバープロパティを更新します。

```
AMZ:OFFLINE_TRANSFER_MODE: PROVIDER_API
```

p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

9 ライブデータについては、NetBackup ストレージライフサイクルポリシーとバックアッププポリシーを作成し、最初のシード処理のバックアップを実行します。

古いデータについては、`bpduplicate` コマンドを使用し、ストレージユニット上のイメージを複製します。

『NetBackup コマンドリファレンスガイド』を参照してください。

10 データ転送が完了したら、次を実行します。

- デバイスが移行中になるまで、バックアッププポリシーを無効にするか SLP のセカンダリ操作の処理を延期します。
- 構成したストレージサーバープロパティを NONE に設定します。
- プロパティを保存します。バックアップ後の処理中に、この情報が必要になります。
  管理コンソールから、または `nbdevconfig -getconfig` コマンドを使用して、ストレージサーバーのプロパティのイメージキャプチャを作成します。『NetBackup コマンドリファレンスガイド』を参照してください。
  また、構成されているオブジェクトのサイズを書き留めます。

11 クラウドベンダーにデバイスを送付します。詳しい手順は、AWS のマニュアルを参照してください。

メモ: バックアップをクラウドバケットにインポートした後、リストアを実行する前にバックアップ後の手順を実行する必要があります。p.62 の「S3 API インターフェースを使用した場合のバックアップ後の手順」を参照してください。

複数の Amazon S3 アダプタの使用

Amazon Snowball デバイスへの書き込みパフォーマンスを向上するため、複数の Amazon S3 アダプタを構成できます。複数のカスタムインスタンスが同じデバイスを指すこともできます。

複数の Amazon S3 アダプタを使用するには

1. Amazon Snowball アダプタごとに 1 つのカスタムクラウドストレージインスタンスを作成します。
2. Amazon Snowball デバイスにデータを転送します。
3. Amazon S3 アダプタ IP をサービスホストとして使用し、カスタムインスタンスを削除します。次のコマンドを実行します。

   ```
   csconfig cldinstance -r -in <instance-name>
   ```

   『NetBackup コマンドリファレンスガイド』を参照してください。
4. Amazon Snowball デバイス用に作成されたすべてのストレージサーバーをデフォルトのクラウドインスタンス (amazon.com) に追加します。次のコマンドを実行します。

   ```
   csconfig cldinstance -as -in amazon.com -sts <storage-server-name>
   ```
5. 次のストレージサーバープロパティを更新します。

   ```
   AMZ:OFFLINE_TRANSFER_MODE: NONE
   ```

   p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
6. ストレージサーバーの SSL 設定 (実行した場合) を変更します。

ファイルインターフェースを使用した Amazon Snowball Edge 用の NetBackup の構成

ファイルインターフェースを使用して Amazon Snowball Edge デバイスにデータをバックアップする際、データは、ソースから Amazon Snowball Edge デバイスに直接移動されます。

推奨事項: バックアップのコピーは、Amazon Snowball Edge デバイスがクラウドにインポートされていないときに作成してください。

ファイルインターフェースを使用して Amazon Snowball Edge にデータを転送するように NetBackup を構成するには

1 デフォルトのインスタンスで、クラウドストレージサーバーを作成します。

メモ: Amazon Snowball Edge デバイスは、デバイスが取得される地域からデータを転送する場合のみ使用できます。したがって、ストレージサーバーのすべてのバケットが同じ地域に属することを確認します。

ディスクプールを構成する際は、Amazon Snowball Edge 用に異なるバケットを作成します。これらのバケットは、AWS コンソールでインポートジョブを作成するために使用されます。

メモ: バケットは、NetBackup Web UI から作成することをお勧めします。AWS コンソールからバケットを作成する場合は、NetBackup でサポートされる文字のみを使用してください。

---

p.73 の「NetBackup のクラウドストレージの構成」を参照してください。

2 AWS コンソールでインポートジョブを作成します。ディスクプールの作成中に作成したバケットを選択します。詳しい手順は、AWS のマニュアルを参照してください。

3 NetBackup メディアサーバーに Amazon Snowball クライアントをインストールします。

4 Amazon Snowball クライアントを使用して Amazon Snowball Edge デバイスを構成します。

5 次のストレージサーバープロパティを更新します。

- `AMZ:OFFLINE_TRANSFER_MODE: FILESYSTEM`
- `AMZ:TRANSFER_DRIVE_PATH: <absolute path of the directory where the file share of the Amazon Snowball Edge device is mounted>`
  個々のバケットではなく、ファイル共有のルートにマウントし、そのパスを `TRANSFER_DRIVE_PATH` に指定します。

  メモ: データを Amazon Snowball Edge デバイスに転送した後、プロパティを `NONE` に戻します。

  ---

p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

6 NetBackup ストレージライフサイクルポリシーとバックアップポリシーを作成します。

7 データ転送が完了したら、次を実行します。

- デバイスが移行中になるまで、バックアップポリシーを無効にするか SLP のセカンダリ操作の処理を延期します。
- 手順 5 で構成したストレージサーバープロパティを NONE に設定します。
- 手順 6 で実行した変更をロールバックします。

8 クラウドベンダーにデバイスを送付します。詳しい手順は、AWS のマニュアルを参照してください。

S3 API インターフェースを使用した Amazon Snowball Edge 用 NetBackup の構成

S3 インターフェースを使用して Amazon Snowball Edge デバイスにデータをバックアップする際、データは、ソースから Amazon Snowball Edge デバイスに直接移動されます。この処理では Amazon S3 アダプタを使用します。

S3 API インターフェースを使用して Amazon Snowball Edge にデータを転送するように NetBackup を構成するには

1 Amazon Snowball クライアントを使用して Amazon Snowball Edge デバイスを構成します。

2 一時ストレージサーバーとディスクプールを作成し、デバイスのインポートジョブに使用するバケットを作成するか、一覧表示します。

メモ: バケットは、NetBackup Web UI から作成することをお勧めします。AWS コンソールからバケットを作成する場合は、NetBackup がサポートしている文字のみを使用してください。

---

3 一時ストレージサーバーとディスクプールを削除します。

4 AWS コンソールでインポートジョブを作成します。詳しい手順は、AWS のマニュアルを参照してください。

5 Amazon Snowball クライアントを使用して Amazon Snowball Edge デバイスを構成します。

6 (省略可能) Amazon Snowball Edge との通信に SSL プロトコルを使用するには、Amazon Snowball クライアントを使用して証明書を取得し、その証明書をメディアサーバーの `/usr/openv/var/global/wmc/cloud/cacert.pem` ファイルに追加します。新たにコピーされた証明書の形式と長さが、`cacert.pem` 内の既存の証明書と一致することを確認します。

p.61 の「Amazon Snowball および Amazon Snowball Edge の SSL の構成」を参照してください。

7 デバイスのカスタムインスタンスを追加します。

p.80 の「クラウドストレージインスタンスの追加」を参照してください。

Amazon Snowball S3 アダプタをインストールしたホストの詳細でカスタムインスタンスのクラウドストレージプロパティを設定します。

［General Settings］タブで、次の項目を設定します。

- ［Provider type］: デバイスを注文したエンドポイントに応じて、Amazon または Amazon GovCloud を選択します。
- ［Service host］: IP またはホスト名
- ［Service endpoint］: 空白
- ［HTTP Port］: デフォルトは 8080 です。または、構成したポートを入力します。
- ［HTTPS port］: デフォルトは 8443 です。または、構成したポートを入力します。
- ［Endpoint access style］: パスの形式

［Region Setting］タブで、次の項目を設定します。

- ［Location constraint］: デバイスを注文した領域
- ［Service host］: IP またはホスト名

メモ: Amazon Snowball Edge デバイスは、デバイスが取得される地域からデータを転送する場合のみ使用できます。そのため、デバイスが取得される地域のロケーション制約とサービスホストを使用します。

---

8 カスタムインスタンスを使用して、デバイスのストレージサーバーを作成します。

p.73 の「NetBackup のクラウドストレージの構成」を参照してください。

9 次のストレージサーバープロパティを更新します。

```
AMZ:OFFLINE_TRANSFER_MODE: PROVIDER_API
```

p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

10 ライブデータについては、ストレージライフサイクルポリシーとバックアップポリシーを作成し、最初のシード処理のバックアップを実行します。

古いデータについては、`bpduplicate` コマンドを使用し、ストレージユニット上のイメージを複製します。

『NetBackup コマンドリファレンスガイド』を参照してください。

11 データ転送が完了したら、次を実行します。

- デバイスが移行中になるまで、バックアップポリシーを無効にするか SLP のセカンダリ操作の処理を延期します。

- 構成したストレージサーバープロパティを NONE に設定します。
- プロパティを保存します。バックアップ後の処理中に、この情報が必要になります。
  Web UI から、または nbdevconfig -getconfig コマンドを使用して、ストレージサーバーのプロパティのイメージキャプチャを作成します。『NetBackup コマンドリファレンスガイド』を参照してください。
  また、構成されているオブジェクトのサイズを書き留めます。

12 クラウドベンダーにデバイスを送付します。詳しい手順は、AWS のマニュアルを参照してください。

メモ: バックアップをクラウドバケットにインポートした後、リストアを実行する前にバックアップ後の手順を実行する必要があります。p.62 の「S3 API インターフェースを使用した場合のバックアップ後の手順」を参照してください。

Amazon Snowball および Amazon Snowball Edge の SSL の構成

Amazon Snowball の SSL を構成するには

1 /.aws/snowball/config/snowball-adapter.config ファイル内のエントリが正しいことを確認します。特に、ホスト名が設定されていることを確認します。

2 アダプタを起動します。サンプルコマンドを次に示します。

```
./snowball-adapter -i Snowball IP address -m path to manifest file -u 29 character unlock code --ssl-enabled --aws-secret-key key
```

3 自己署名された SSL 証明書とキーが /.aws/snowball/config/ ディレクトリに生成されます。

4 コマンドラインで Amazon Snowball アダプタに提示される証明書をメディアサーバーの /usr/openv/var/global/cloud/cacert.pem ファイルに追加します。新たにコピーされた証明書の形式と長さが、cacert.pem 内の既存の証明書と一致することを確認します。

Amazon Snowball Edge の SSL を構成するには

1 利用可能な証明書を一覧表示します。次の Amazon Snowball クライアントコマンドを実行します。

```
./snowballEdge list-certificates
```

2 証明書を取得します。次の Amazon Snowball クライアントコマンドを実行します。

```
./snowballEdge get-certificate --certificate-arn arn_value
```

3 コマンドラインで提示される証明書をメディアサーバーの `/usr/openv/var/global/cloud/cacert.pem` ファイルに追加します。新たにコピーされた証明書の形式と長さが、`cacert.pem` 内の既存の証明書と一致することを確認します。

メモ: `cacert.pem` ファイルのファイル権限と所有権を変更しないようにしてください。

S3 API インターフェースを使用した場合のバックアップ後の手順

バックアップをクラウドバケットにインポートした後、リストアの前に次の手順を実行します。

1. カスタムインスタンスサービスホストを実際のエンドポイントに更新します。HTTP ポートと地域の値を変更します。
2. (例外) AWS のデフォルト地域のカスタムインスタンスは、デフォルトの出荷時の NetBackup クラウドストレージインスタンスで使用されているため、更新できません。このような地域には、AWS 中国北京地域、AWS 中国寧夏地域、AWS 米国東部地域、AWS GovCloud 米国西部および米国東部地域が含まれます。このような地域の場合、次の手順を実行します。一意のホスト名でエラーが発生した場合にも、次の手順に従うことができます。
   - 保存したストレージプロパティを手元に用意してください。
   - ストレージサーバーを削除します。次のコマンドを実行します。

     ```
     csconfig cldinstance -rs -in cloud storage instance name -sts
     storage server name
     ```

     『NetBackup コマンドリファレンスガイド』を参照してください。
   - デフォルトのストレージインスタンス (amazon.com、amazon.cn、amazongov.com など) で、同じ名前の新しいストレージサーバーを追加します。次のコマンドを実行して、インスタンスを検索します。

     ```
     csconfig cldinstance -i
     ```

     次のコマンドを実行して、ストレージサーバーを追加します。

     ```
     csconfig cldinstance -as -in Cloud Storage Instance name -sts
     storage server name -obj_size size in bytes
     ```

『NetBackup コマンドリファレンスガイド』を参照してください。
オブジェクトのサイズが正確で、作成されたストレージサーバーと同じであることを確認します。
また、要件に合わせて SSL 設定を構成していることを確認します。

3. ストレージサーバーの SSL 設定が想定どおりであることを確認します。[ストレージサーバーの接続プロパティの変更 (Change Storage Server Connection Properties)]ダイアログボックスで、プロパティを確認して更新できます。

   p.81 の「関連付けられたクラウドストレージサーバーホストのプロパティを変更する方法」を参照してください。

4. [Amazon Snowball Edge デバイスのみ] Amazon アカウントのクレデンシャルで、各ストレージサーバーのクレデンシャルを更新します。次のコマンドを実行します。

   ```
   tpconfig -update -storage_server storage server name -stype
   storage server type -sts_user_id [user ID] -password password
   ```

   『NetBackup コマンドリファレンスガイド』を参照してください。

5. OFFLINE_TRANSFER_MODE ストレージサーバープロパティを確認し、NONE に更新します。
6. リストアを実行し、データを確認します。
7. ポリシーを有効にするか、SLP のセカンダリ操作の処理を有効にします。

Microsoft Azure クラウドストレージ API 形式について

NetBackup は、ストレージに Microsoft Azure ストレージ API を使うベンダーのクラウドストレージをサポートします。Microsoft Azure ストレージ API ベンダーの要件と構成オプションについての情報を次に示します。

表 2-11 Microsoft Azure ストレージ API 形式の情報とトピック

情報	トピック
認定されたベンダー	p.64 の「NetBackup 認定の Microsoft Azure クラウドストレージベンダー」を参照してください。
要件	p.64 の「Microsoft Azure ストレージ形式の要件」を参照してください。
ストレージサーバーの構成オプション	p.64 の「Microsoft Azure クラウドストレージプロバイダのオプション」を参照してください。
SSL とプロキシオプション	p.66 の「Microsoft Azure のサーバーの詳細な構成オプション」を参照してください。

NetBackup 認定の Microsoft Azure クラウドストレージベンダー

リンク (「NetBackup™ Enterprise Server and Server 9.0 - 9.x.x Hardware and Cloud Storage Compatibility List (HCL)」) をクリックして、NetBackup 11.2.0.1 リリースの時点で、Microsoft Azure ストレージ API を使用する NetBackup クラウドストレージで認定されているベンダーを特定します。

ベンダーは Cohesity Technology Partner Program (VTPP) に参加することで認定を受けることができます。

Microsoft Azure ストレージ形式の要件

表 2-12 に、NetBackup における Microsoft Azure クラウドストレージの詳細と要件を示します。

表 2-12 Microsoft Azure クラウドストレージの要件

要件	詳細
ライセンス要件	クラウドストレージの使用を可能にする NetBackup ライセンスが必要です。
Microsoft Azure アカウント要件	Microsoft Azure ストレージアカウントと、少なくとも 1 つのストレージアクセスキー (プライマリアクセスキーまたはセカンダリアクセスキー) を取得する必要があります。
コンテナ名	NetBackup を使用して、NetBackup で使用するコンテナを作成することを推奨します。 NetBackup の、コンテナ名に関する要件を次に示します。 ■ コンテナ名は 3 文字から 63 文字の長さにする必要があります。 ■ コンテナ名は文字または数値で開始する必要があり、文字、数値、およびダッシュ記号 (-) のみを含めることができます。 ■ ダッシュ記号 (-) の直前または直後に文字または数値が置かれる必要があります。また、連続するダッシュ記号をコンテナ名に含めることはできません。 ■ コンテナ名に含める文字はすべて小文字である必要があります。 次のリンクを参照できます。 https://msdn.microsoft.com/en-us/library/azure/dd135715.aspx

p.63 の「Microsoft Azure クラウドストレージ API 形式について」を参照してください。

Microsoft Azure クラウドストレージプロバイダのオプション

表 2-13 では、Microsoft Azure のストレージサーバー構成オプションについて説明します。

表 2-13 Microsoft Azure ストレージサーバーの構成オプション

フィールド名	必要な内容
サービスホスト (Service host)	サービスホストは、Microsoft Azure のクラウドサービスエンドポイントのホスト名です。 [サービスホスト (Service host)]ドロップダウンリストは、[ストレージアカウント (Storage Account)]も包含する、サービスホストの URL の一部を表示します。 サービスホストの URL の例: *storage_account*.blob.core.windows.net **メモ:** ストレージアカウントを作成した地域 (デフォルトまたは中国) に基づいて、ドロップダウンリストからサービスホストを選択する必要があります。
ストレージサーバー名 (Storage server name)	デフォルトの Azure ストレージサーバー (my-azure) を表示します。デフォルト以外のストレージサーバーも選択できます。 ドロップダウンリストには、使うことのできる名前のみが表示されます。 ドロップダウンリストには、クラウドストレージの論理名を使って別のストレージサーバー名を入力できます。Azure の同一の物理サービスホストを参照する、異なる複数の名前を使って、複数のストレージサーバーを作成できます。利用できる名前がリストにない場合は、ドロップダウンリストに新しいストレージサーバー名を入力して作成できます。 **メモ:** Azure クラウドストレージを構成するときに追加するストレージサーバー名を論理名にし、物理ホスト名と一致しないようにすることをお勧めします。例: Azure ストレージサーバーを追加するときに、「azure.com」や「azure123.com」などの名前を使わないようにします。これらのサーバーは、クラウドストレージ構成時に失敗を引き起こす可能性のある物理ホストであることがあります。その代わりに、「azure1」や「azureserver1」などのストレージサーバー名を使います。
メディアサーバー名 (Media server name)	NetBackup メディアサーバーをドロップダウンリストから選択します。 クラウドストレージサーバーの必要条件に適合するメディアサーバーのみがドロップダウンリストに表示されます。次のトピックでは、構成の必要条件について説明します。 p.97 の「クラウドストレージの NetBackup メディアサーバーについて」を参照してください。 選択したホストが、機能と利用可能なストレージについてストレージベンダーのネットワークに問い合わせます。メディアサーバーはバックアップおよびリストアのためのデータムーバーにもなります。

フィールド名	必要な内容
ストレージアカウント (Storage Account)	クラウドバックアップのために使うストレージアカウントを入力します。 Microsoft Azure ストレージサービスについて詳しくは、Microsoft Azure のドキュメントを参照してください。 http://azure.microsoft.com 次の URL を使用してストレージアカウントを作成します。 https://portal.azure.com
アクセスキー (Access key)	Azure のアクセスキーを入力します。プライマリアクセスキーまたはセカンダリアクセスキーを入力できます。100 文字以下である必要があります。 アクセスキーについては次の URL を参照してください。 https://portal.azure.com
詳細設定 (Advanced Settings)	Azure の SSL またはプロキシ設定を変更するには、[詳細設定 (Advanced Settings)]をクリックします。 p.66 の「Microsoft Azure のサーバーの詳細な構成オプション」を参照してください。
アクセス層の構成 ACCOUNT_ACCESS_TIER	Microsoft Azure アカウントのアクセス層 (ホットまたはクール) の設定を使用するには、ACCOUNT_ACCESS_TIER オプションを選択します。
アクセス層の構成 ARCHIEVE	長期間保持する場合は ARCHIVE オプションを選択します。 p.68 の「長期保持用の Microsoft Azure Archive データの保護」を参照してください。

p.63 の「Microsoft Azure クラウドストレージ API 形式について」を参照してください。

Microsoft Azure のサーバーの詳細な構成オプション

次の表で、すべての Microsoft Azure 互換クラウドプロバイダに固有の SSL とプロキシオプションについて説明します。これらのオプションは[サーバーの詳細な構成 (Advanced Server Configuration)]ダイアログボックスに表示されます。

表 2-14 ［全般 (General)］設定オプション

オプション	説明
SSL を使用する	ユーザー認証、または NetBackup とクラウドストレージプロバイダ間のデータ転送に SSL (Secure Sockets Layer) プロトコルを使う場合は、このオプションを選択します。 ■ ［認証のみ (Authentication only)］ - クラウドストレージにアクセスするときのユーザーの認証で SSL のみを使う場合は、このオプションを選択します。 ■ ［データ転送 (Data Transfer)］ - SSL を使ってユーザーを認証し、NetBackup からクラウドストレージにデータを転送するには、このオプションを選択します。 **メモ:** NetBackup は、SSL モードでのクラウドストレージとの通信時に、認証局（CA）によって署名された証明書のみをサポートします。クラウドサーバー (パブリックまたはプライベート) に CA による署名付き証明書があることを確認します。CA によって署名された証明書がない場合は、SSL モードでの NetBackup とクラウドプロバイダ間のデータ転送が失敗します。

表 2-15 ［プロキシ設定 (Proxy Settings)］タブのオプション

オプション	説明
プロキシサーバーを使用する	プロキシサーバーを使用しプロキシサーバーの設定を指定する場合は、［プロキシサーバーを使用する (Use Proxy Server)］オプションを選択します。［プロキシサーバーを使用する (Use Proxy Server)］オプションを選択すると、次の詳細を指定できます。 ■ プロキシホスト (Proxy Host): プロキシサーバーの IP アドレスまたは名前を指定します。 ■ プロキシポート (Proxy Port): プロキシサーバーのポート番号を指定します。 ■ プロキシタイプ (Proxy Type): 次のいずれか 1 つのプロキシタイプを選択できます。 ■ HTTP **メモ:** HTTP プロキシ形式のプロキシクレデンシャルを指定する必要があります。 ■ SOCKS ■ SOCKS4 ■ SOCKS5 ■ SOCKS4A

オプション	説明
プロキシのトンネリングを使用 (Use Proxy Tunneling)	HTTP プロキシタイプのプロキシのトンネリングを有効にすることができます。 [プロキシのトンネリングを使用 (Use Proxy Tunneling)]を有効にすると、HTTP CONNECT 要求がクラウドメディアサーバーから HTTP プロキシサーバーに送信され、TCP 接続がクラウドバックエンドストレージに直接転送されます。 データは、接続からヘッダーまたはデータを読み取ることがなくプロキシサーバーを通過します。
認証形式 (Authentication Type)	HTTP プロキシタイプを使用している場合は、次のいずれかの認証形式を選択できます。 ■ なし (None): 認証が有効になりません。ユーザー名とパスワードは要求されません。 ■ NTLM: ユーザー名とパスワードが必要です。 ■ 基本 (Basic): ユーザー名とパスワードが必要です。 [ユーザー名 (Username)]はプロキシサーバーのユーザー名です。 [パスワード (Password)]は空にすることができます。最大 256 文字を使用できます。

p.63 の「Microsoft Azure クラウドストレージ API 形式について」を参照してください。

長期保持用の Microsoft Azure Archive データの保護

長期保持用のデータを保護するため、NetBackup を使用して Microsoft Azure Archive Blob ストレージにデータをバックアップできます。NetBackup を使用することで、アーカイブストレージ層にストレージサーバーを作成できます。

メモ: アーカイブストレージ層は、ストレージアカウントレベルではなく、blob レベルでのみ利用可能です。

要件

次の要件を満たしていることを確認します。

- Azure Archive を使用するには、一般目的のストレージの V2 が必要です。

制限事項

次の制限事項を考慮してください。

- アクセラレータと重複排除は Azure Archive ではサポートされていません。

- リストアまたはクリーンアップが失敗した場合は、対応する blob について、アーカイブする層を手動で設定する必要があります。

高度な構成手順

1. Azure Archive クラウドストレージサーバーを構成します。

   p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

2. Microsoft Azure Container を使用してディスクプールを作成します。

   p.114 の「クラウドストレージのディスクプールの構成」を参照してください。

3. ディスクプールを使用してストレージユニットが作成されます。
4. AZR:STORAGE_TIER プロパティがストレージサーバー用に構成されているかどうかを確認します。

   メモ: ストレージサーバーを構成すると、STORAGE_TIER は変更できません。

   p.102 の「NetBackup クラウドストレージサーバーのプロパティ」を参照してください。

5. バックアップポリシーまたはサービスライフサイクルポリシーの STU を使用します。

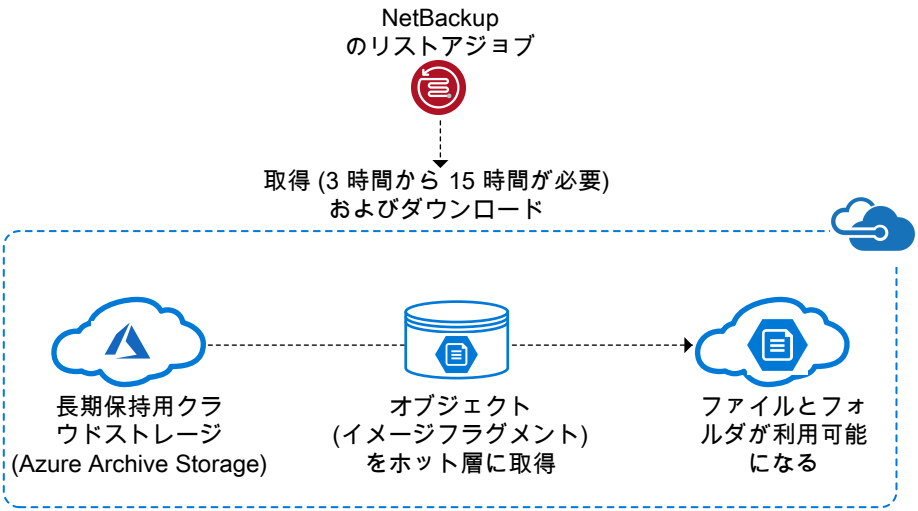
Azure Archive からのデータのバックアップとリストア

バックアップ中に、NetBackup はアーカイブ層にデータをアップロードします。

リストア中、最初に、イメージフラグメントがアーカイブ層からホット層に移動されます。イメージフラグメントの移動には約 3 時間から 15 時間かかります。イメージフラグメントがホット層で利用可能になったら、ローカルストレージにダウンロードされます。リストアが完了すると、ホット層のイメージフラグメントはアーカイブ層に戻されます。

メモ: TIR を使用した、Azure Archive ストレージからのイメージのインポートの方が高速です。

次の図に、リストアフローを示します。


NetBackup
のリストアジョブ
取得 (3 時間から 15 時間が必要)
およびダウンロード
長期保持用クラ
ウドストレージ
(Azure Archive Storage)
オブジェクト
(イメージフラグメント)
をホット層に取得
ファイルとフォ
ルダが利用可能
になる

3

NetBackup のクラウドストレージの構成

この章では以下の項目について説明しています。

- NetBackup でクラウドストレージの構成を開始する前に
- NetBackup のクラウドストレージの構成
- Cloud のインストール要件
- ［拡張性のあるストレージ (Scalable Storage)］プロパティ
- ［クラウドストレージ (Cloud Storage)］プロパティ
- NetBackup CloudStore Service Container について
- ホスト名ベースの証明書の配備
- ホスト ID ベースの証明書の配備
- クラウドバックアップ用のデータ圧縮について
- クラウドストレージのデータ暗号化について
- NetBackup クラウドストレージの暗号化の NetBackup KMS について
- NetBackup クラウドストレージの暗号化の外部 KMS について
- クラウドストレージサーバーについて
- クラウドストレージのオブジェクトのサイズについて
- クラウドストレージの NetBackup メディアサーバーについて
- クラウドストレージのストレージサーバーの構成

- NetBackup クラウドストレージサーバーのプロパティ
- クラウドストレージのディスクプールについて
- クラウドストレージのディスクプールの構成
- NetBackup クラウドストレージ暗号化の KMS キー名のレコードの保存
- クラウド環境へのバックアップメディアサーバーの追加
- クラウドストレージ用のストレージユニットの構成
- NetBackup アクセラレータバックアップと NetBackup 最適化合成バックアップについて
- クラウドストレージディスクプールのプロパティ
- 証明書失効リスト (CRL) に対する証明書の検証
- NetBackup クラウドの認証局 (CA) の管理

NetBackup でクラウドストレージの構成を開始する前に

NetBackup でクラウドストレージの構成を開始する前に次の操作を実行することを推奨します。

- お使いのクラウドストレージベンダー用の NetBackup 構成オプションを確認します。NetBackup では、ストレージ API 形式に基づいてクラウドストレージがサポートされます。Cohesity はクラウドストレージの構成に必要な情報を API 形式別に組織化しています。次の項に、API 形式、各 API 形式を使うベンダー、必要な設定情報へのリンクが記載されています。
p.14 の「NetBackup のクラウドストレージベンダーについて」を参照してください。

  メモ: Cohesity は NetBackup リリースの間にベンダーを認定する場合があります。お使いのクラウドストレージベンダーが NetBackup 製品マニュアルに記載されていない場合は、次の Web ページでサポート対象クラウドベンダーの最新のリストを参照してください。

  http://www.veritas.com/docs/000115793

  http://www.veritas.com/docs/000115793

- NetBackup でクラウドストレージを構成するために必要な情報を収集します。NetBackup 構成オプション別に組織化された必要な情報を得ることで、構成プロセスをより簡単に進めることができます。

NetBackup のクラウドストレージの構成

このトピックでは、NetBackup のクラウドストレージを構成する方法について説明します。表 3-1にクラウドストレージを構成するための作業の概要を示します。表の手順に順番に従ってください。

『NetBackup 管理者ガイド Vol. I』では、基本の NetBackup 環境を構成する方法を説明しています。『NetBackup 管理者ガイド Vol. I』は、次の URL で利用可能です。

https://support.cohesity.com/s/article/article-100040135.html.html

表 3-1 NetBackup のクラウド構成プロセスの概要

手順	作業	詳細情報
手順 1	プライマリサーバーとメディアサーバーでの NetBackup ログファイルディレクトリの作成	p.143 の「NetBackup クラウドストレージログファイル」を参照してください。 p.142 の「クラウドストレージ用の NetBackup ログファイルディレクトリの作成」を参照してください。
手順 2	クラウドのインストール要件を確認します	p.74 の「Cloud のインストール要件」を参照してください。
手順 3	NetBackup のクラウドストレージプロバイダのプロビジョニングと構成の要件を決定します	p.14 の「NetBackup のクラウドストレージベンダーについて」を参照してください。
手順 4	必要に応じてクラウドストレージホスト全体のプロパティを構成します	p.75 の「[拡張性のあるストレージ (Scalable Storage)]プロパティ」を参照してください。
手順 5	クラウドストレージのプロパティを設定します	必要に応じて、NetBackup ホストプロパティを使用してクラウドストレージサービスのホストを追加します。 p.79 の「[クラウドストレージ (Cloud Storage)]プロパティ」を参照してください。
手順 6	CloudStore サービスコンテナのロールの理解 バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ適用。	p.82 の「NetBackup CloudStore Service Container について」を参照してください。
手順 7	メディアサーバーでの認証用のセキュリティ証明書のプロビジョニング	p.83 の「NetBackup CloudStore Service Container のセキュリティ証明書」を参照してください。 p.88 の「ホスト名ベースの証明書の配備」を参照してください。

手順	作業	詳細情報
手順 8	暗号化のキー管理について理解しておきます	暗号化は、必要に応じて行います。 p.92 の「クラウドストレージのデータ暗号化について」を参照してください。 p.92 の「NetBackup クラウドストレージの暗号化の NetBackup KMS について」を参照してください。 p.94 の「NetBackup クラウドストレージの暗号化の外部 KMS について」を参照してください。
手順 9	ストレージサーバーを構成します	p.95 の「クラウドストレージサーバーについて」を参照してください。 p.80 の「クラウドストレージインスタンスの追加」を参照してください。 p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。 p.95 の「クラウドストレージのオブジェクトのサイズについて」を参照してください。
手順 10	ディスクプールを構成します	p.113 の「クラウドストレージのディスクプールについて」を参照してください。 p.114 の「クラウドストレージのディスクプールの構成」を参照してください。
手順 11	ストレージサーバーの追加のプロパティを構成します	p.102 の「NetBackup クラウドストレージサーバーのプロパティ」を参照してください。
手順 12	追加のメディアサーバーを追加します	追加メディアサーバーの追加はオプションです。 p.97 の「クラウドストレージの NetBackup メディアサーバーについて」を参照してください。 p.116 の「クラウド環境へのバックアップメディアサーバーの追加」を参照してください。
手順 13	ストレージユニットを構成します	p.117 の「クラウドストレージ用のストレージユニットの構成」を参照してください。

Cloud のインストール要件

NetBackup Cloud ソリューションの実装計画を作成する際には、表 3-2 を使用して計画に役立ててください。

表 3-2 Cloud のインストール要件

要件	詳細
NetBackup メディアサーバープラットフォームのサポート	NetBackup がクラウドストレージでサポートするオペレーティングシステムについては、NetBackup オペレーティングシステム互換性一覧を参照してください。 https://support.cohesity.com/s/article/article-100040093 NetBackup メディアサーバーソフトウェアをホストにインストールするときに、必ず NetBackup サーバー名の完全修飾ドメインを指定してください。
クラウドストレージプロバイダのアカウント	NetBackup Cloud Storage を構成する前に、希望するクラウドストレージプロバイダにアカウントを作成する必要があります。利用可能な NetBackup のクラウドストレージプロバイダのリストを参照してください。 このアカウントはクラウドストレージ構成ウィザードで作成できます。 p.14 の「NetBackup のクラウドストレージベンダーについて」を参照してください。
NetBackup Cloud Storage のライセンス	NetBackup クラウドストレージは、基本の NetBackup とは別ライセンスです。 ライセンスによって NetBackup ポリシーの［属性 (Attributes)］タブの［アクセラレータを使用する (Use accelerator)］機能も有効になります。アクセラレータはファイルシステムの完全バックアップの速度を増加させます。

［拡張性のあるストレージ (Scalable Storage)］プロパティ

この設定にアクセスするには、Web UI で［ホスト (Host)］、［ホストプロパティ (Host properties)］の順に選択します。［メディアサーバー (Media Server)］を選択します。必要に応じて［接続 (Connect)］をクリックし、［メディアサーバーの編集 (Edit media server)］をクリックします。［拡張性のあるストレージ (Scalable storage)］をクリックします。

［拡張性のあるストレージ (Scalable Storage)］プロパティには、暗号化、測定、帯域幅の調整、NetBackup ホストとクラウドストレージプロバイダの間のネットワーク接続に関する情報が含まれます。これらのプロパティは、ホストがクラウドストレージでサポートされている場合にのみ表示されます。該当リリースの『NetBackup Enterprise Server and Server - Hardware and Cloud Storage Compatibility List』については、次の URL を参照してください。

https://support.cohesity.com/s/article/article-100040093

［拡張性のあるストレージ (Scalable storage)］プロパティは、現在選択されているメディアサーバーに適用されます。

［拡張性のあるストレージ (Scalable storage)］ホストプロパティには、次の設定が含まれます。

表 3-3　［拡張性のあるストレージ (Scalable storage)］ホストプロパティ

プロパティ	説明
Key Management Server (KMS) 名 (Key Management Server (KMS) name)	キーマネージメントサービス (KMS) サーバーを設定した場合は、KMS サーバーに要求を送信するプライマリサーバーの名前がここに表示されます。
測定間隔 (Metering interval)	NetBackup がレポート用に接続情報を収集する頻度を決めます。値は秒単位で設定されます。デフォルト設定は 300 秒 (5 分) です。この値を 0 に設定すると、測定は無効になります。
合計利用可能帯域幅 (Total available bandwidth)	この値は、クラウドへの接続の速度を指定するために使用します。値は、KB/秒で指定されます。デフォルト値は 102,400 KB/秒です。
サンプリング間隔 (Sampling interval)	帯域幅使用状況の測定間隔 (秒)。この値を大きくするほど、NetBackup が使用帯域幅を調べる頻度が少なくなります。 この値が 0 (ゼロ) の場合は、スロットル調整は無効です。
詳細設定 (Advanced settings)	［詳細設定 (Advanced settings)］を展開して、スロットル調整の追加設定を構成します。 p.77 の「帯域幅スロットルの詳細設定」を参照してください。 p.77 の「帯域幅スロットルの詳細設定」を参照してください。
最大並列実行ジョブ数 (Maximum concurrent jobs)	メディアサーバーがクラウドストレージサーバーで実行できるデフォルトの最大並行実行ジョブ数。 この値は、クラウドストレージサーバーではなくメディアサーバーに適用されます。クラウドストレージサーバーに接続できるメディアサーバーが複数ある場合、各メディアサーバーで異なる値を持つ場合があります。したがって、クラウドストレージサーバーへの接続の合計数を判断するには、各メディアサーバーからの値を追加してください。 NetBackup が接続数よりも多いジョブ数を許可するように設定されている場合、NetBackup は接続の最大数に達した後で開始されたジョブでは失敗します。ジョブにはバックアップジョブとリストアジョブの両方が含まれています。 ジョブ数の制限は、バックアップポリシーごと、ストレージユニットごとに設定できます。 **メモ:** NetBackup はジョブを開始するときに、同時並行ジョブの数、メディアサーバーごとの接続の数、メディアサーバーの数、ジョブの負荷分散ロジックなどの多くの要因を明らかにする必要があります。したがって、NetBackup は正確な最大接続数でジョブを失敗しない場合もあります。NetBackup は、接続数が最大数よりもわずかに少ない場合、正確に最大数の場合、最大数よりわずかに多い場合にジョブを失敗することがあります。 値 100 は通常は不要です。

帯域幅スロットルの詳細設定

帯域幅スロットルの詳細設定では、NetBackup のホストとクラウドストレージプロバイダ間の接続のさまざまな面を制御できます。

p.75 の「［拡張性のあるストレージ (Scalable Storage)］プロパティ」を参照してください。

帯域幅スロットルの詳細設定を行うには

1. NetBackup Web UI を開きます。
2. 左側で、［ホスト (Hosts)］、［ホストプロパティ (Host properties)］の順に選択します。
3. ［メディアサーバー (Media Server)］を選択します。
4. 必要に応じて、［接続 (Connect)］をクリックします。次に、［メディアサーバーの編集 (Edit media server)］をクリックします。
5. ［拡張性のあるストレージ (Scalable storage)］をクリックします。
6. ［詳細設定 (Advanced settings)］を展開します。
7. 設定を構成し、［保存 (Save)］をクリックします。

p.77 の「帯域幅スロットルの詳細設定」を参照してください。

帯域幅スロットルの詳細設定

次の表で、帯域幅スロットルの詳細設定を説明します。

表 3-4　スロットルの詳細設定

プロパティ	説明
読み取り帯域幅 (Read bandwidth)	このフィールドを使用して、読み取り操作が使用できる総帯域幅の割合を指定します。0 から 100 までの値を指定します。不正な値を入力すると、エラーが生成されます。 数分内に指定された量のデータを伝送するために帯域幅が不足する場合、タイムアウトによりリストアエラーまたはレプリケーションエラーが発生することがあります。 必要な帯域幅を計算する際は、複数のメディアサーバーでの同時実行ジョブの合計負荷を考慮してください。 デフォルト値: 100 指定可能な値: 0 - 100

プロパティ	説明
書き込み帯域幅 (Write bandwidth)	このフィールドを使用して、書き込み操作が使用できる総帯域幅の割合を指定します。0 から 100 までの値を指定します。不正な値を入力すると、エラーが生成されます。 数分内に指定された量のデータを伝送するために帯域幅が不足する場合、タイムアウトによりバックアップエラーが発生することがあります。 必要な帯域幅を計算する際は、複数のメディアサーバーでの同時実行ジョブの合計負荷を考慮してください。 デフォルト値: 100 指定可能な値: 0 - 100
作業時間 (Work time)	クラウド接続の作業時間とみなされる時間間隔を指定します。 開始時刻と終了時刻を指定します。 クラウド接続で使用できる帯域幅を［割り当て帯域幅 (Allocated bandwidth)］フィールドに示します。この値によって、利用可能な帯域幅のうちどのくらいがこの時間帯のクラウド操作に使用されるかが決まります。値はパーセントまたは KB/秒で表示されます。
オフ時間 (Off time)	このフィールドを使用して、クラウド接続のオフ時間とみなされる時間間隔を指定します。 開始時刻と終了時刻を指定します。 クラウド接続で使用できる帯域幅を［割り当て帯域幅 (Allocated bandwidth)］フィールドに示します。この値によって、利用可能な帯域幅のうちどのくらいがこの時間帯のクラウド操作に使用されるかが決まります。値はパーセントまたは KB/秒で表示されます。
週末 (Weekend)	週末の開始時間と終了時間を指定します。 クラウド接続で使用できる帯域幅を［割り当て帯域幅 (Allocated bandwidth)］フィールドに示します。この値によって、利用可能な帯域幅のうちどのくらいがこの時間帯のクラウド操作に使用されるかが決まります。値はパーセントまたは KB/秒で表示されます。
読み取り帯域幅 (KB/秒) (Read Bandwidth (KB/s))	このフィールドには、それぞれのリストアジョブでクラウドのストレージサーバーから NetBackup のメディアサーバーに転送するのに、どのくらいの帯域幅が利用可能かが示されます。値は、KB/秒で表示されます。
書き込み帯域幅 (KB/秒) (Write Bandwidth (KB/s))	このフィールドには、それぞれのバックアップジョブで NetBackup のメディアサーバーからクラウドのストレージサーバーに転送するのに、どのくらいの帯域幅が利用可能かが示されます。値は、KB/秒で表示されます。

[クラウドストレージ (Cloud Storage)]プロパティ

メモ: これらのプロパティにアクセスするには、Web UI で[ホスト (Host)]、[ホストプロパティ(Host properties)]の順に選択します。プライマリサーバーを選択し、[プライマリサーバーの編集 (Edit primary server)]をクリックします。次に、[クラウドストレージ (Cloud Storage)]をクリックします。

NetBackup の[クラウドストレージ (Cloud Storage)]プロパティは、現在選択されているプライマリサーバーに適用されます。

この[クラウドストレージ (Cloud Storage)]リストに表示されるホストは、ストレージサーバーを構成するときに選択できます。[サービスプロバイダ (Service provider)]タイプのクラウドベンダーは、サービスホストが利用可能または必要かどうかを判断します。

NetBackup は、一部のクラウドストレージプロバイダのサービスホストを備えています。[サービスプロバイダ (Service provider)]のタイプで可能であれば、新規ホストを[クラウドストレージ (Cloud Storage)]リストに追加できます。ホストを追加する場合は、ホストのプロパティを変更するかまたはホストを[クラウドストレージ (Cloud Storage)]リストから削除できます(NetBackup に含まれている情報を削除することはできません)。

この[クラウドストレージ (Cloud Storage)]リストにサービスホストを追加しない場合は、ストレージサーバーを構成するときにサービスホストを追加できます。クラウドベンダーの[サービスプロバイダ (Service provider)]タイプによって、[サービスのホスト名 (Service host name)]が利用可能または必要かどうかが決まります。

[クラウドストレージ (Cloud Storage)]ホストのプロパティには以下のプロパティが含まれます。

表 3-5 クラウドストレージ

プロパティ	説明
クラウドストレージ	NetBackup がサポートするさまざまなクラウドサービスプロバイダに対応するクラウドストレージが、ここに一覧表示されます。 p.80 の「クラウドストレージインスタンスの追加」を参照してください。 p.81 の「クラウドストレージホストプロパティの変更」を参照してください。 p.82 の「クラウドストレージホストのインスタンスの削除」を参照してください。
次の関連付けられたクラウドストレージサーバー: (Associated cloud storage servers for <host>)	選択したクラウドストレージに対応するクラウドストレージサーバーが表示されます。 p.81 の「クラウドストレージホストプロパティの変更」を参照してください。

クラウドストレージインスタンスの追加

NetBackup クラウドストレージサーバーを構成する前にカスタムクラウドストレージインスタンスを追加する必要がある場合があります。カスタムクラウドストレージでは、別のサービスホストや別のプロパティを使ったカスタマイズが可能です。

クラウドストレージプロバイダの種類により、カスタムクラウドストレージインスタンスを追加する必要があるかが決まります。

p.14 の「NetBackup のクラウドストレージベンダーについて」を参照してください。

次のようにして、カスタムクラウドストレージインスタンスを追加できます。

プライマリサーバーのホストプロパティ	この方法では、NetBackup でストレージサーバーを構成する前にクラウドストレージインスタンスを追加します。インスタンスを追加すると、ストレージを構成するウィザードに、インスタンスの詳細が自動的に入力されます。ストレージサーバーを構成するときにインスタンスを選択します。 p.80 の「ホストプロパティでクラウドストレージインスタンスを追加するには」を参照してください。
NetBackup Web UI を使用する	この方法では、NetBackup でストレージサーバーを構成すると同時にインスタンスを同時に追加します。構成したストレージに、インスタンスの詳細はユーザー自身で追加するまで入力されません。 p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

ホストプロパティでクラウドストレージインスタンスを追加するには

1. NetBackup Web UI を開きます。
2. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。
3. クラウドストレージインスタンスを追加するプライマリサーバーを選択します。
4. 必要に応じて、[接続 (Connect)]をクリックします。次に、[プライマリサーバーの編集 (Edit primary server)]をクリックします。
5. [クラウドストレージ (Cloud Storage)]をクリックします。
6. [追加 (Add)]をクリックします。
7. 設定を構成します。

   メモ: 詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

8. 設定を構成した後、[保存 (Save)]をクリックします。

クラウドストレージホストプロパティの変更

[クラウドストレージ (Cloud Storage)]プロパティでは、次の設定を変更できます。

[クラウドストレージ (Cloud Storage)]プロパティ	追加するホストのプロパティを変更できます。(NetBackup に含まれているクラウドストレージプロバイダのプロパティを変更または削除することはできません。) p.81 の「クラウドストレージホストのプロパティを変更するには」を参照してください。
関連付けられたクラウドストレージサーバーのプロパティ	p.81 の「関連付けられたクラウドストレージサーバーホストのプロパティを変更する方法」を参照してください。

クラウドストレージサーバーのプロパティを変更する方法は、別の項で説明します。

クラウドストレージホストのプロパティを変更するには

1. NetBackup Web UI を開きます。
2. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。
3. クラウドストレージインスタンスを追加するプライマリサーバーを選択します。
4. 必要に応じて、[接続 (Connect)]をクリックします。次に、[プライマリサーバーの編集 (Edit primary server)]をクリックします。
5. [クラウドストレージ (Cloud Storage)]をクリックします。
6. [クラウドストレージ (Cloud Storage)]リストで、編集するクラウドストレージを見つけます。
7. [処理 (Actions)]、[編集 (Edit)]の順にクリックします。
8. プロパティを変更します。
9. [保存 (Save)]、[保存 (Save)]の順にクリックします。

関連付けられたクラウドストレージサーバーホストのプロパティを変更する方法

1. NetBackup Web UI を開きます。
2. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。
3. クラウドストレージインスタンスを追加するプライマリサーバーを選択します。
4. 必要に応じて、[接続 (Connect)]をクリックします。次に、[プライマリサーバーの編集 (Edit primary server)]をクリックします。
5. [クラウドストレージ (Cloud Storage)]をクリックします。
6. [次の関連付けられたクラウドストレージサーバー: <サーバー>(Associated cloud storage servers for *server*)] リストと、編集するストレージサーバーを見つけます。

7 [編集 (Edit)]をクリックします。

8 プロパティを変更します。

p.24 の「Amazon S3 クラウドストレージサーバーの構成オプション」を参照してください。

p.26 の「Amazon S3 クレデンシャルブローカーの詳細」を参照してください。

9 [保存 (Save)]、[保存 (Save)]の順にクリックします。

クラウドストレージホストのインスタンスの削除

プライマリサーバーの[クラウドストレージ (Cloud Storage)]ホストプロパティで、カスタムクラウドストレージ (クラウドインスタンス) を削除できます。NetBackup で提供されたクラウドストレージインスタンスを削除できません。

p.79 の「[クラウドストレージ (Cloud Storage)]プロパティ」を参照してください。

クラウドストレージホストのインスタンスを削除する方法

1 NetBackup Web UI を開きます。

2 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。

3 クラウドストレージを削除するプライマリサーバーを選択します。

4 必要に応じて、[接続 (Connect)]をクリックします。次に、[プライマリサーバーの編集 (Edit primary server)]をクリックします。

5 [クラウドストレージ (Cloud Storage)]をクリックします。

6 削除するクラウドストレージを見つけます。

7 [処理 (Actions)]、[削除 (Delete)]、[削除 (Delete)]の順にクリックします。

8 [保存 (Save)]をクリックします。

NetBackup CloudStore Service Container について

この情報は、バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ該当します。

NetBackup CloudStore Service Container (`nbcssc`) は、クラウドストレージ用に構成された古いメディアサーバーで実行する Web ベースのサービスコンテナです。

このコンテナは、スロットルサービスと測定データコレクタサービスをホストします。

[拡張性のあるストレージ (Scalable Storage)]ホストプロパティで、NetBackup CloudStore Service Container の動作を構成できます。

p.75 の「[拡張性のあるストレージ (Scalable Storage)]プロパティ」を参照してください。

NetBackup CloudStore Service Container サービスのポート番号は 5637 です。クラウドストレージ用に構成されている古いメディアサーバーでは、このポートを使用する必要があります。古いメディアサーバーが別のポートを使用している場合、プライマリサーバーとの通信が失敗します。NetBackup で使用するポートについて詳しくは、『NetBackup ネットワークポートリファレンスガイド』を参照してください。

NetBackup は、NetBackup CloudStore サービスコンテナの複数のセキュリティの方法を次のように使います。

セキュリティ証明書	NetBackup CloudStore Service Container を実行する NetBackup ホストは、セキュリティ証明書または証明書を使用してプロビジョニングする必要があります。 p.83 の「NetBackup CloudStore Service Container のセキュリティ証明書」を参照してください。 **メモ:** クラウドストレージを構成する前にすでに生成済みの場合は、セキュリティ証明書を生成する必要はありません。
セキュリティモード	NetBackup CloudStore サービスコンテナはさまざまなセキュリティモードで実行できます。 p.84 の「NetBackup CloudStore Service Container のセキュリティモード」を参照してください。

p.97 の「クラウドストレージの NetBackup メディアサーバーについて」を参照してください。

メモ: NetBackup 8.1.2 以降のリリースでは、`nbcssc` サービスは配備されません。NetBackup Web 管理コンソール (`nbwmc`) サービスは、クラウドストレージの構成操作を処理し、NetBackup Service Layer (`nbsl`) サービスは、スロットルサービスおよび測定データコレクタサービスの機能を処理します。バージョン 8.1.2 より後のメディアサーバーでは、ホスト ID ベースの証明書を使用して認証を行います。

これらのサービスについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

NetBackup CloudStore Service Container のセキュリティ証明書

NetBackup CloudStore Service Container を開始して実行するためには、デジタルセキュリティ証明書が必要です。セキュリティ証明書がどのようにプロビジョニングされるかは、次に示すように、NetBackup のリリースレベルによって決まります。

NetBackup 8.2 以降

CloudStore Service Container を実行する NetBackup ホストには、ID ベースの証明書が必要です。これらのホストには、証明書のインストールが必要になる場合があります。

p.90 の「ホスト ID ベースの証明書の配備」を参照してください。

NetBackup プライマリサーバーがクラスタ化されている場合は、アクティブノードとパッシブノードにホスト ID ベースの証明書があることを確認する必要があります。詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup 8.0 から 8.1.2

CloudStore Service Container を実行する NetBackup ホストには、ホスト ID ベースの証明書とホスト名ベースの証明書の両方が必要です。それらのホストに証明書をインストールする必要がある場合があります。

p.88 の「ホスト名ベースの証明書の配備」を参照してください。

p.90 の「ホスト ID ベースの証明書の配備」を参照してください。

NetBackup プライマリサーバーがクラスタ化されている場合、アクティブノードとパッシブノードにホスト名ベースの証明書とホスト ID ベースの証明書の両方があることを確認する必要があります。詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

メディアサーバーのセキュリティ証明書がどこに配置されるかは、次のように NetBackup のリリースレベルによって決まります。

NetBackup 7.7 から 8.1.2

証明書名は、ホストで NetBackup メディアサーバーソフトウェアを設定したときに使ったホスト名です。証明書のパスは、オペレーティングシステムに応じて、次のようになります。

- UNIX/Linux の場合: `/usr/openv/var/vxss/credentials`
- Windows: *`install_dir`*`¥Veritas¥NetBackup¥var¥VxSS¥credentials`

p.82 の「NetBackup CloudStore Service Container について」を参照してください。

NetBackup CloudStore Service Container のセキュリティモード

これは、バージョン 8.1.2 までの NetBackup にのみ適用されます。

NetBackup CloudStore Service Container は、2 つの異なるモードのいずれかで実行できます。次に示すように、セキュリティモードによってクライアントとサービスの通信方法が決定します。

セキュアモード

デフォルトのセキュアモードでは、クライアントコンポーネントを CloudStore Service Container で認証する必要があります。認証の後で、セキュリティ保護された HTTPS チャネルを介して通信が行われます。

非セキュアモード　CloudStore Service Container では、非セキュア通信を使います。クライアントは認証を必要とせずに HTTP 経由でサーバーと通信します。

セキュリティモードの設定に、CSSC_IS_SECURE ファイルの CSSC_IS_SECURE 属性を使うことができます。デフォルト値は 64 (セキュリティ保護された通信) です。

p.85 の「NetBackup cloudstore.conf 設定ファイル」を参照してください。

p.82 の「NetBackup CloudStore Service Container について」を参照してください。

NetBackup cloudstore.conf 設定ファイル

表 3-6で、cloudstore.conf 設定ファイルのパラメータについて説明しています。

cloudstore.conf ファイルは、NetBackup クラウドがサポートするプラットフォームにインストールされるプライマリサーバーとすべてのメディアサーバーで利用可能です。

メモ: cloudstore.conf ファイルでいずれかのパラメータを変更する場合は、変更前に nbcssc サービス (バージョン 7.7.x から 8.1.2 のメディアサーバーのみ) と nbwmc サービス (プライマリサーバー) を停止する必要があります。パラメータを変更したら、これらのサービスを再起動して、変更を有効にします。

---

cloudstore.conf ファイルは、次のディレクトリに存在します。

- UNIX: /usr/openv/var/global/cloud
  メディアサーバーバージョン 7.7.x から 8.1.2 では、パスは次のとおりです。
  /usr/openv/netbackup/db/cloud
- Windows: *install_path*¥NetBackup¥var¥global¥cloud
  メディアサーバーバージョン 7.7.x から 8.1.2 では、パスは次のとおりです。
  install_path¥Veritas¥NetBackup¥db¥cloud

表 3-6　cloudstore.conf 設定ファイルのパラメータと説明

パラメータ	説明
CSSC_VERSION	この値は変更しないことをお勧めします。 cloudstore.conf ファイルのバージョンを指定します。デフォルト値は 2 です。

パラメータ	説明
CSSC_PLUGIN_PATH	この値は変更しないことをお勧めします。 NetBackup クラウドストレージプラグインのインストールパスを指定します。デフォルトのパスは次のとおりです。 Windows の場合: *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins UNIX の場合: /usr/openv/lib/ost-plugins
CSSC_PORT	この設定は、バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ該当します。 CloudStore Service Container (nbcssc) のポート番号を指定します。値として 5637 を指定します。 このポートは、クラウドストレージ用に構成された古いメディアサーバー用に、旧バージョンのメディアサーバーをサポートするために使用されます。古いメディアサーバーがこのポートを使用していることを確認してください。古いメディアサーバーが別のポートを使用している場合、プライマリサーバーとの通信が失敗します。
CSSC_LOG_DIR	csconfig、nbcldutil、およびクラウドプラグインがログファイルを生成するディレクトリのパスを指定します。 デフォルトのパスは次のとおりです。 Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥nbcssc UNIX の場合: /usr/openv/netbackup/logs/nbcssc **メモ:** バージョン 7.7.x から 8.1.2 のメディアサーバーの場合、nbcssc サービスはログファイル用にこのパスを使用します。
CSSC_LOG_FILE	この設定は、NetBackup リリース 8.1.2 までのバージョンにのみ該当します。 nbcssc サービスがログに書き込むのに使うファイル名を指定します。デフォルト値は空です。これは、NetBackup のログ記録機構によってログのファイル名が決められることを意味します。
CSCONFIG_LOG_FILE	csconfig ユーティリティがログへ書き込む際に使用するファイル名を指定します。デフォルト値は空です。これは、NetBackup のログ記録機構によってログのファイル名が決められることを意味します。

パラメータ	説明
CSSC_IS_SECURE	nbcssc サービスを、セキュアモード (値 64) または非セキュアモード (値 0) のどちらで実行するかを指定します。デフォルトの値は 64 です。
CSSC_CIPHER_LIST	NetBackup が次の目的で使用する暗号リストを指定します。 ■ クラウドプライマリホストの暗号は、クラウドサービスプロバイダとの通信に使用されます。 ■ メディアサーバーの暗号は、クラウドプライマリホストの nbwmc サービスやクラウドサービスプロバイダと通信するために使用されます。 この値は変更しないことをお勧めします。暗号リストをカスタマイズする目的に応じて、プライマリサーバーとメディアサーバーの cloudstore.conf の暗号リストを変更する必要があります。 **メモ:** 暗号リストが無効な場合、カスタマイズされた暗号リストはデフォルトの暗号リストに置き換えられます。 デフォルト値は AES:!aNULL:@STRENGTH です。
CSSC_LOG_LEVEL	CLI ユーティリティの csconfig と nbcldutil のログ記録のログレベルを指定します。値 0 はログ記録が無効になることを、0 以外の値はログ記録が有効になることをそれぞれ示します。 デフォルトの値は 0 です。
CSSC_MASTER_PORT	この設定は、バージョン 7.7.x から 8.1.2 のメディアサーバーについてのみ該当します。NetBackup のバージョン 8.2 以降のプライマリサーバーとメディアサーバーには該当しません。 このパラメータ値は、5637 に設定する必要があります。 このポートは、クラウドストレージ用に構成された古いメディアサーバー用に、旧バージョンをサポートするために使用されます。古いメディアサーバーがこのポートを使用していることを確認してください。古いメディアサーバーが別のポートを使用している場合、プライマリサーバーとの通信が失敗します。
CSSC_MASTER_NAME	NetBackup プライマリサーバーの名前を指定します。このエントリは nbwmc サービスがこのホストで動作することを示します。ここでは、CloudProvider.xml ファイルと CloudInstance.xml ファイルに基づいて、クラウドプロバイダ固有のすべての要求が処理されます。

パラメータ	説明
CSSC_ALLOW_LEGACY_AUTH	プライマリサーバーが、クラウドストレージ用に構成されているレガシーメディアサーバーと通信できるかどうかを指定します。サポートされるのは、バージョン 7.7.x から 8.1.2 のメディアサーバーのみです。 値 1 (デフォルト値) は通信が有効であることを示し、値 0 は通信が無効であることを示します。 このパラメータは、NetBackup Web UI の[8.0 以前のホストとの安全でない通信を有効にする (Enable insecure communication with 8.0 and earlier hosts)]オプション ([設定 (Settings)]、[グローバルセキュリティ (Global security)]、[安全な通信 (Secure communication)]) と共に使用します。 この GUI オプションを使用すると、すべての旧バージョンのレガシーメディアサーバーとプライマリサーバーの通信を有効または無効にできます。これは「すべて」または「なし」として動作する設定で、クラウドストレージメディアサーバーに固有の設定ではありません。このパラメータは、クラウドに対する追加レベルの制御を提供します。この設定を使用して、プライマリサーバーと旧バージョンのクラウドストレージメディアサーバーの通信を明示的に有効または無効にできます。 たとえば、GUI オプションが有効になっており (デフォルト値)、このパラメータ値が 0 に設定されている場合、NetBackup プライマリサーバーは、他のストレージサーバーと同様に、サポートされている旧バージョンのメディアサーバーと引き続き通信します。ただし、ハードコードされたクレデンシャルを使用して古い通信方式を使用しているレガシークラウドストレージメディアサーバーはすべて遮断されるため、NetBackup 環境のセキュリティは強化されます。 **メモ:** GUI オプションが無効になっている場合、このパラメータ値は影響を与えません。このパラメータ値を変更した場合は、NetBackup Web 管理コンソール (nbwmc) サービスを再起動して、変更を有効にする必要があります。

ホスト名ベースの証明書の配備

この手順は、メディアサーバーのバージョンが 7.7.x から 8.1.2 の場合にのみ適用可能です。

クラウドストレージに使用する NetBackup メディアサーバーに、必要なホスト名ベースのセキュリティ証明書を配備できます。クラウドストレージのために使用する各メディアサーバーは、NetBackup CloudStore Service Container を実行します。

p.82 の「NetBackup CloudStore Service Container について」を参照してください。

証明書を個別のメディアサーバーまたはすべてのメディアサーバーに対して配備できます。クラウドストレージのために使用するメディアサーバーには、ホスト名ベースのセキュリティ証明書が必要です。

メモ: ホスト名ベースの証明書の配備は 1 つのホストごとに行う 1 回のみの操作です。ホスト名ベースの証明書が以前のリリースまたは修正プログラムで配備された場合は、再び配備を行う必要はありません。

ホスト名ベースの証明書を配備する前に、次のことを確認します。

- クラスタのすべてのノードにホスト ID ベースの証明書がある
- クラスタノードのすべての完全修飾ドメイン名 (FQHN) と短縮名は、それぞれのホスト ID にマッピングされます。

メディアサーバーにホスト名ベースの証明書を配備する

この手順は、同時に多数のホストにホスト名ベースのセキュリティ証明書を配備する場合に適しています。NetBackup 配備と同様に通常、この方法はネットワークが安全であることを前提とします。

メディアサーバーのホスト名ベースのセキュリティ証明書を配備する方法

1. 環境に応じて、プライマリサーバーで次のコマンドを実行します。個別のメディアサーバーの名前を指定または `-AllMediaServers` を指定します。

   Windows の場合: *`install_path`*`¥NetBackup¥bin¥admincmd¥bpnbaz -ProvisionCert` *`host_name`*`|-AllMediaServers`

   UNIX の場合: `/usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert` *`host_name`*`|-AllMediaServers`

   NetBackup Appliance (`NetBackupCLI` ユーザーとして) : `bpnbaz -ProvisionCert` *`Media_server_name`*

2. メディアサーバーで NetBackup Service Layer (`nbsl`) サービスを再起動します。

メモ: ホスト上で動的 IP を使用する場合 (DHCP) は、ホスト名と IP アドレスがプライマリサーバーで正しく一覧表示されていることを確認します。これを行うには、プライマリサーバーで次の NetBackup `bpclient` コマンドを実行します。

Windows の場合: *`Install_path`*`¥NetBackup¥bin¥admincmd¥bpclient -L -All`

UNIX の場合: `/usr/openv/netbackup/bin/admincmd/bpclient -L -All`

ホスト ID ベースの証明書の配備

証明書配備のセキュリティレベルに応じて、プライマリ以外のホストは、認証局 (プライマリサーバー) からホスト ID ベースの証明書を取得できるようになるために、認証トークンが必要になる場合があります。証明書が自動的に配備されない場合は、管理者が NetBackup コマンドを使って nbcertcmd ホストに手動で証明書を配備する必要があります。

次の項で、配備レベルと、各レベルで認証トークンが必要かどうかについて説明します。

トークンが不要の場合の配備

ホスト管理者が、認証トークンを必要とせずに、証明書をプライマリ以外のホストに配備できるセキュリティレベルでは、次の手順を実行します。

トークンが不要の場合にホスト ID ベースの証明書を生成して配備する方法

1. ホスト管理者が、プライマリサーバーが信頼できる状態を確立するためにプライマリ以外のホストで次のコマンドを実行します。

   ```
   nbcertcmd -getCACertificate
   ```

2. プライマリ以外のホストで次のコマンドを実行します。

   ```
   nbcertcmd -getCertificate
   ```

   メモ: 複数の NetBackup ドメインと通信するには、そのホストの管理者が -server オプションを使って各プライマリサーバーから証明書を要求する必要があります。

   特定のプライマリサーバーから証明書を取得するには、次のコマンドを実行します。

   ```
   nbcertcmd -getCertificate -server primary_server_name
   ```

3. 証明書がホストに配備されていることを検証するには、次のコマンドを実行します。

   ```
   nbcertcmd -listCertDetails
   ```

トークンが必要な場合の配備

CA からホスト ID ベースの証明書を配備するために認証トークンがホストで必要となるセキュリティレベルでは、次の手順を実行します。

トークンが必要な場合にホスト ID ベースの証明書を生成して配備するには

1. 操作を続行する前に、ホスト管理者が認証トークン値を CA から取得している必要があります。トークンは各環境のさまざまなセキュリティガイドラインに応じて、電子メール、ファイル、または口頭で管理者に伝えられます。
2. プライマリサーバーが信頼できる状態を確立するためにプライマリ以外のホストで次のコマンドを実行します。

   ```
   nbcertcmd -getCACertificate
   ```

3. プライマリ以外のホストで次のコマンドを実行して、メッセージが表示されたらトークンを入力します。

   ```
   nbcertcmd -getCertificate -token
   ```

   メモ: 複数の NetBackup ドメインと通信するには、そのホストの管理者が `-server` オプションを使って各プライマリサーバーから証明書を要求する必要があります。

   管理者がトークンをファイルで取得した場合、次を入力します。

   ```
   nbcertcmd -getCertificate -file authorization_token_file
   ```

4. 証明書がホストに配備されていることを検証するには、次のコマンドを実行します。

   ```
   nbcertcmd -listCertDetails
   ```

   クラスタの証明書を表示するには、`-cluster` オプションを使用します。

クラウドバックアップ用のデータ圧縮について

NetBackup では、クラウドストレージサーバーに送信する前にデータを圧縮できます。

クラウドストレージサーバーを構成する際に、NetBackup メディアサーバーにおけるデータ圧縮を有効にできます。NetBackup

p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

メモ: クラウドストレージ構成中にデータ圧縮を有効化した後に、データ圧縮を無効化することはできません。

NetBackup でのデータ圧縮に関する注意

- NetBackup は、圧縮レベル 3 で、LZO Pro というサードパーティ製ライブラリを使用します。`bptm` ログには、クラウドストレージでバックアップを作成した後のデータ圧縮率の情報が含まれています。
  p.128 の「圧縮率の表示」を参照してください。

- NetBackup は、256 KB のチャンクでデータを圧縮します。
- NetBackup アクセラレータおよび移動検出機能を備えた True Image Restore (TIR) は、圧縮でサポートされます。
- バックアップデータは、クラウドストレージサーバーへの転送前に圧縮されます。圧縮オプションと暗号化オプションの両方が選択された場合、データは暗号化前に圧縮されます。
- データ圧縮では、圧縮可能なデータの量に応じてバックアップ時間が短縮されデータサイズが削減されます。しかしながら、圧縮しない場合のデータと比較すると、帯域幅使用率が削減されていることが分かります。
- 圧縮できないデータの場合は、データ圧縮のパフォーマンスが低下します。そのため、ポリシーデータなどの圧縮不能なデータのバックアップに対して圧縮を有効化しないことを推奨します。
- 別の種類のストレージサーバーで同じバケットを使用しないことを推奨します。
- ストレージサーバー側の圧縮と一緒にクライアント側の圧縮を使用しないでください。
- ストレージサーバーの作成後に、圧縮構成の設定 (有効または無効) を変更することはできません。

クラウドストレージのデータ暗号化について

クラウドに送信する前にデータを暗号化できます。ストレージの構成時に暗号化を構成できます。

NetBackup はクラウドディスクストレージの場合にデータの暗号化を管理するために NetBackup キーマネージメントサービス (NetBackup KMS) と外部キーマネージメントサービスを使用します。

p.92 の「NetBackup クラウドストレージの暗号化の NetBackup KMS について」を参照してください。

p.94 の「NetBackup クラウドストレージの暗号化の外部 KMS について」を参照してください。

NetBackup KMS と外部 KMS に関する詳細情報を参照できます。

詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup クラウドストレージの暗号化の NetBackup KMS について

NetBackup は、NetBackup キーマネージメントサービス (NetBackup KMS) を使用して、ディスクストレージのデータ暗号化用のキーを管理します。NetBackup KMS は

NetBackupプライマリサーバーベースの対称キーマネージメントサービスです。このサービスは、NetBackup プライマリサーバーで実行されます。NetBackup KMS 機能を使用するために追加のライセンスは必要ありません。NetBackup は、クラウドストレージの暗号化キーを管理するのに NetBackup KMS を使用します。

p.92 の「クラウドストレージのデータ暗号化について」を参照してください。

Cloud Storage サーバーの構成ウィザードを使用した暗号化を有効にし、ディスクプールの構成ウィザードを使用してディスクプールを構成する場合は、KMS とキー固有の情報を指定する必要があります。キー固有の情報は、KMS サーバーの構成に基づいています。KMS サーバーが設定されていない場合、クラウドストレージサーバーの暗号化設定の一部として、NetBackup KMS サーバーはデフォルトで KMS サーバーとして構成されます。

NetBackup KMS データベースに必要となるキーを次の表で説明します。[クラウドストレージサーバーの構成ウィザード (Cloud Storage Server Configuration Wizard)]を使うときに、これらのキーのパスフレーズを入力できます。

表 3-7　　KMS データベースに必要な暗号化キー

キー	説明
ホストマスターキー (Host Master Key)	ホストマスターキーはキーデータベースを保護します。ホストマスターキーはパスフレーズと ID を必要とします。NetBackup KMS はキーを生成するのにパスフレーズを使用します。
キーの保護キー (Key Protection Key)	キーの保護キーは、キーデータベースの個別のレコードを保護します。キーの保護キーはパスフレーズと ID を必要とします。NetBackup KMS はキーを生成するのにパスフレーズを使用します。

ストレージサーバーとボリューム組み合わせのそれぞれに必要となる暗号化キーを次の表で説明します。クラウドストレージサーバーを構成したときに暗号化を指定すると、ストレージボリュームのキーグループに対してパスフレーズを設定する必要があります。[ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)]を使うときに、これらのキーのパスフレーズを入力します。

表 3-8 ストレージサーバーとボリュームの各組み合わせの暗号化キーとキーレコード

項目	説明
キーグループのキー	キーグループのキーはそのキーグループを保護します。ストレージサーバーとボリュームの組み合わせごとにキーグループが必要になり、各キーグループのキーにはパスフレーズが必要です。キーグループ名は、次のとおりに記述されるストレージ形式を使用する必要があります。 クラウドストレージの場合の形式は次のとおりです。 *storage_server_name*:*volume_name* 次の項目では、クラウドストレージに関するキーグループ名のコンポーネントの必要条件について説明します。 ■ *storage_server_name*: ストレージサーバーに使った名前と同じ名前を使う必要があります。名前は完全修飾ドメイン名か省略名にできますが、ストレージサーバーと同じものにする必要があります。 ■ コロン (:) は *storage_server_name* の後に必要です。 ■ *volume_name*: ストレージベンダーが NetBackup に公開している LSU 名を指定する必要があります。 [ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)]は、キーグループを作成するときにこの形式に準拠します。
キーレコード (Key record)	作成する各キーグループはキーレコードを必要とします。キーレコードはストレージサーバーとボリュームのデータを保護する実際のキーを格納します。 キーレコードの名前はオプションです。キー名を使う場合は、どんな名前でも使えます。ボリューム名と同じ名前を使うことを推奨します。[ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)]ではキーレコードのキーは要求されません。このウィザードでは、ボリューム名がキー名として使われます。

NetBackup KMS と外部 KMS について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup クラウドストレージの暗号化の外部 KMS について

クラウドストレージの場合は、NetBackup は外部キーマネージメントサービス (外部 KMS) サーバーのキーをサポートします。

ストレージサーバーおよびボリュームの各組み合わせに必要な Symmetric 暗号化キー外部 KMS サーバーでは、ストレージサーバーおよびボリュームの各組み合わせに対して Symmetric 暗号化キーは作成されません。'storage_server_name:volume_name'

形式のキーグループ名の値を持つカスタム属性が設定されている Symmetric 暗号化キーが、外部 KMS サーバーにすでに存在することを確認する必要があります。

外部 KMS について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

クラウドストレージサーバーについて

ストレージサーバーは、ストレージに対してデータの書き込みと読み込みを実行するエンティティです。クラウドストレージサーバーの場合、NetBackup メディアサーバーを使用してバックアップ操作を実行するためにクラウドベンダーが公開したホストまたはエンドポイントです。NetBackup でクラウドストレージサーバーを構成するときに、クラウドストレージを識別するために任意の論理名を使用できます。

クラウドストレージサーバーを構成するとき、NetBackup の［拡張性のあるストレージ (Scalable Storage)］プロパティが継承されます。

p.75 の「［拡張性のあるストレージ (Scalable Storage)］プロパティ」を参照してください。

ストレージサーバーを構成した後、ストレージサーバーのプロパティを変更できます。

NetBackup メディアサーバーは、クライアントをバックアップし、ストレージサーバーにデータを送信します。

p.97 の「クラウドストレージの NetBackup メディアサーバーについて」を参照してください。

クラウドストレージのオブジェクトのサイズについて

バックアップ中、NetBackup はバックアップイメージデータを「オブジェクト」と呼ばれるチャンクに分割します。各オブジェクトをクラウドストレージに移動するために、オブジェクトごとに PUT 要求が実行されます。

カスタムのオブジェクトサイズを設定すると、クラウドストレージとの間で送受信される PUT 要求と GET 要求の量を制御できます。PUT 要求と GET 要求の数を少なくすると、要求に対して課金されるコストを減らすことができます。

オブジェクトサイズのカスタム値は、クラウドストレージサーバーの作成時に指定できます。クラウドストレージプロバイダ、ハードウェア、インフラストラクチャ、期待するパフォーマンス、およびその他の要因を考慮して値を決定してください。クラウドストレージサーバーのオブジェクトサイズは、一度設定すると変更できません。別のオブジェクトサイズを設定するには、クラウドストレージサーバーを再作成する必要があります。

p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

オブジェクトのサイズを選択するためのガイドライン

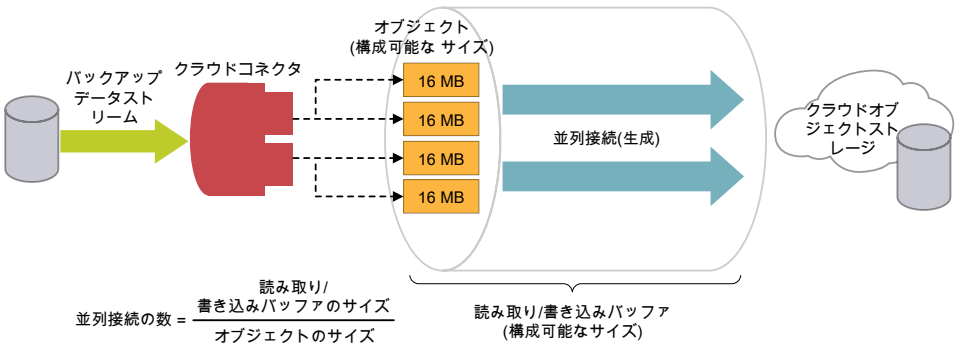
クラウドでの NetBackup のパフォーマンスは、オブジェクトのサイズ、並列接続の数、読み取りまたは書き込みバッファのサイズの組み合わせによって決まります。

バックアップ操作とリストア操作のパフォーマンスを向上するため、NetBackup はクラウドストレージへの複数の並列接続を使用します。NetBackup のパフォーマンスは並列接続数によって異なります。並列接続数は読み取りまたは書き込みバッファのサイズとオブジェクトのサイズから算出されます。

読み取りまたは書き込みバッファのサイズ (ユーザー設定) ÷ オブジェクトのサイズ (ユーザー設定) = 並列接続の数 (算出)。これらの決定要因の関連を次の図に示します。

これらの決定要因の関連を次の図に示します。

図 3-1 オブジェクトのサイズ



- 並列接続数を決定する際は、以下の要因を考慮します。
  - クラウドストレージプロバイダによって許可される並列接続の最大数
  - NetBackup とクラウドストレージ環境の間のネットワークで利用可能な帯域幅
  - NetBackup ホストで利用可能なシステムメモリ
- オブジェクトのサイズを大きくすると、並列接続の数は減ります。並列接続の数は、アップロードやダウンロードの速度に影響します。
- 読み取りまたは書き込みバッファのサイズを大きくすると、並列接続数が増加します。同様に、並列接続数を少なくしたい場合は、読み取りまたは書き込みバッファのサイズを小さくします。ただし、ネットワーク帯域幅と利用可能なシステムメモリを考慮する必要があります。
- クラウドプロバイダは、バックアップまたはリストアの処理中に開始した PUT 要求と GET 要求の数に対して課金します。オブジェクトのサイズが小さいほど、PUT 要求または GET 要求の数は多くなり、結果的にコストが高くなります。

- データ転送で一時的なエラーが発生した場合、NetBackup は、再試行を何度か実行して、失敗したオブジェクトを転送しようとします。エラーが続くと、完全なオブジェクトが再び転送されます。また、レイテンシとパケット損失が大きい場合は、パフォーマンスが低下することがあります。レイテンシとパケット損失の問題は並列接続数を大きくすると解決することがあります。
- NetBackup では、クライアント側でいくつかのタイムアウトが設定されています。アップロード操作が算出された最低の NetBackup データ転送速度より (オブジェクトのサイズが大きいために) 遅くなる場合は、NetBackup でエラーが発生している可能性があります。
- 重複排除がサポートされていないレガシー環境では、接続数が少ないと、並列で行われるダウンロードの数は以前の接続数の場合より少なくなります。
  たとえば、旧バージョン (8.0 以前) のイメージからリストアする場合にオブジェクトのサイズが 1 MB のときは、(1 つの接続につき) 16 MB のバッファは完全には使用されず、メモリは消費されます。オブジェクトのサイズを大きくしても、利用可能な読み取りまたは書き込みバッファサイズのメモリのため、接続数には制限があります。

現在のデフォルト設定

デフォルト設定は以下のとおりです。

表 3-9　現在のデフォルト設定

クラウドストレージプロバイダ	オブジェクトのサイズ	デフォルトの読み取りまたは書き込みバッファのサイズ
Amazon S3 と Amazon GovCloud	16 MB (固定)	400 MB (16 MB から 1 GB に設定可能)
Azure	4 MB (固定)	400 MB (4 MB から 1 GB に設定可能)

クラウドストレージの NetBackup メディアサーバーについて

クラウドストレージで使う NetBackup メディアサーバーは、NetBackup クライアントをバックアップしてバックアップデータをクラウドストレージサーバーに送信します。その後、データはストレージサーバーからストレージに書き込まれます。

p.95 の「クラウドストレージサーバーについて」を参照してください。

また、NetBackup メディアサーバーはリストア時にプライマリストレージ (クライアント) にデータを移動し、複製時にセカンダリストレージから三次ストレージにデータを移動することもできます。メディアサーバーはデータムーバーとしても知られています。これらは、ストレージの実装時にストレージとの通信に使うソフトウェアプラグインをホストします。

クラウドストレージサーバーを構成するときに、ウィザードまたはコマンドラインで指定するメディアサーバーがクラウドストレージのデータムーバーになります。

p.100 の「クラウドストレージのストレージサーバーの構成」を参照してください。

クライアントのバックアップのために追加のメディアサーバーを追加できます。メディアサーバーは、クラウドストレージに送信するバックアップの負荷を分散するのに役立ちます。

p.116 の「クラウド環境へのバックアップメディアサーバーの追加」を参照してください。

NetBackup ストレージユニットを構成するときに、バックアップと複製に使うデータムーバーを制御できます。

p.117 の「クラウドストレージ用のストレージユニットの構成」を参照してください。

クラウドメディアサーバーをクラウドプライマリホストとして構成できます。

p.98 の「NetBackup クラウドのプライマリホストとしてのメディアサーバーの使用」を参照してください。

クラウドストレージをサポートするには、メディアサーバーが次の項目に適合している必要があります。

- クラウドストレージでオペレーティングシステムがサポートされている必要があります。NetBackup がクラウドストレージでサポートするオペレーティングシステムについては、NetBackup オペレーティングシステム互換性一覧を参照してください。
  https://support.cohesity.com/s/article/article-100040093
  https://support.cohesity.com/s/article/article-100040093
- バージョン 7.7.x から 8.1.2 のメディアサーバーで、NetBackup Cloud Storage Service Container (`nbcssc`) を実行している必要があります。
  p.82 の「NetBackup CloudStore Service Container について」を参照してください。
- クラウドストレージに使用する NetBackup メディアサーバーは、プライマリサーバーのバージョンと同じ NetBackup バージョンにする必要があります。

NetBackup クラウドのプライマリホストとしてのメディアサーバーの使用

これらの手順は、バージョン 8.1.2 までのメディアサーバーに適用されます。

NetBackup クラウドでサポートされていないすべてのオペレーティングシステムでこの手順を実行する必要があります。

該当リリースの NetBackup ハードウェア互換性リストについては、次の URL を参照してください。

https://support.cohesity.com/s/article/article-100040093

ディザスタリカバリの場合は、NetBackup クラウドのプライマリホストとして構成したメディアサーバーから、次のファイルを手動でバックアップする必要があります。

- CloudProvider
- CloudInstance .xml

NetBackup クラウドのプライマリホストとしてメディアサーバーを使用するには

1 いずれかの NetBackup クラウドのメディアサーバーを、クラウドのプライマリホストとして指定します。

NetBackup プライマリサーバーとバージョンが同一のメディアサーバーを選択します。バージョンの異なるメディアサーバーは使用しないでください。

メモ: クラウドストレージの構成や、バックアップやリストアなどの操作を行うときにすべてのメディアサーバーで必要となる CloudProvider.xml ファイルのプライマリコピーは、メディアサーバーに保持されません。

---

2 クラウドのプライマリホストとして選択されているサーバーを含む、すべての NetBackup クラウドのメディアサーバーで次のコマンドを実行します。

```
nbcssc -t -a Netbackup
```

```
nbcssc -s -a Netbackup -m cloud_master_host -f
```

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。

3 クラウドのプライマリホストの cloudstore.conf ファイルで述べられているように、CSSC_PORT と CSSC_IS_SECURE の値が CSSC_MASTER_PORT と CSSC_MASTER_IS_SECURE として、他のすべての NetBackup クラウドのメディアサーバーの cloudstore.conf ファイルにコピーされていることを確認します。

クラウドのプライマリホストを選択した後は、別のメディアサーバーを指すように名前を再度変更しないでください。変更する必要が生じた場合は、Cohesity のテクニカルサポートにお問い合わせください。

ディザスタリカバリ後の追加タスク

プロキシサーバーを使用するクラウドストレージサーバーの場合は、プロキシのクレデンシャルを更新する必要があります。

- NetBackup 管理者コンソールを使用してこのタスクを実行するには、p.81 の「クラウドストレージホストプロパティの変更」を参照してください。を参照してください。
- コマンドを使用してこのタスクを実行するには、次のコマンドを実行します。

```
csconfig cldinstance -us -in instance_name -sts storage_server_name
-pxtype proxy_type -pxhost proxy_host -pxport proxy_port
-pxautth_type proxy_auth_type -pxtunnel proxytunnel_usage
```

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。

プライマリサーバーのアップグレード後の追加タスク

これは、Solaris x86 や Windows Server 2008 などのサポート対象外のオペレーティングシステムでプライマリサーバーが実行されており、メディアサーバーがクラウドプライマリホストとして昇格している NetBackup 環境に適用されます。

プライマリサーバーをアップグレードした後、メディアサーバーでのローリングアップグレードの実行を予定している場合は、メディアサーバーのアップグレード後もクラウドストレージサーバーがシームレスに動作するように、アップグレード後の追加手順を実行する必要があります。

詳しくは、次のテクニカルノートを参照してください。

https://support.cohesity.com/s/article/article-100044766

クラウドストレージのストレージサーバーの構成

このコンテキストでの構成とは、クラウドストレージに対して読み書きできるストレージサーバーとしてホストを構成することをいいます。

p.95 の「クラウドストレージサーバーについて」を参照してください。

また、KMS サーバーが構成されていない場合、NetBackup UI では暗号化を有効にして、NetBackup キーマネージメントサービス (NetBackup KMS) サーバーの対応するパラメータを構成できます。

p.92 の「クラウドストレージのデータ暗号化について」を参照してください。

データの暗号化と NetBackup KMS が構成されている場合、キー名のレコードを保存することをお勧めします。

p.114 の「NetBackup クラウドストレージ暗号化の KMS キー名のレコードの保存」を参照してください。

CLI を使用してストレージサーバーを構成する場合、`nbdevconfig` および `tpconfig` コマンドを実行する前に `csconfig` コマンドを実行する必要があります。

『NetBackup コマンドリファレンスガイド』を参照してください。

構成プロセス中に選択した NetBackup メディアサーバーは、クラウドストレージの必要条件に適合している必要があります。

p.97 の「クラウドストレージの NetBackup メディアサーバーについて」を参照してください。

クラウドストレージサーバーの構成について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

KMS データベース暗号化の設定

このセクションでは、NetBackup キーマネージメントサービスデータベースとクラウドストレージの暗号化キーを構成するための設定について説明します。この情報は、NetBackup でデータの暗号化に使用するキーを含むデータベースを保護します。キーグループおよびキーレコードも暗号化に必要です。

詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

表 3-10　　暗号化データベースに必要な情報

フィールド名	必要な情報
KMS サーバー名 (KMS Server Name)	このフィールドは NetBackup プライマリサーバーの名前を表示します。プライマリサーバーでは KMS のみを構成できます。このフィールドは変更できません。 KMS が構成されていない場合は、このフィールドは <kms_server_name> を表示します。
ホストマスターキー (HMK) のパスフレーズ (Host Master Key (HMK) Passphrase)	データベースを保護するキーを入力します。KMS の用語では、キーはパスフレーズと呼ばれています。
HMK パスフレーズの再入力 (Re-enter HMK Passphrase)	ホストのマスターキーを再入力します。
ホストマスターキー ID (Host Master Key ID)	ID はマスターキーに割り当てるラベルです。特定のホストのマスターキーを ID で識別できるようにします。このフィールドは 255 文字に制限されています。 キーストアファイルの内容を復号するためには、正しいキーの保護キーとホストのマスターキーを識別する必要があります。これらの ID はキーストアファイルヘッダーに暗号化されずに保存されています。キーストアファイルへのアクセスしかなくても正しい ID を選択できます。ディザスタリカバリを実行するには、ファイルと関連付けられる正しい ID とパスフレーズを覚える必要があります。
キーの保護キー (KPK) パスフレーズ (Key Protection Key (KPK) Passphrase)	KMS データベース内の個別のレコードを保護するパスワードを入力します。KMS の用語では、キーはパスフレーズと呼ばれています。
KPK パスフレーズの再入力 (Re-enter KPK Passphrase)	キーの保護パスワードを再入力します。
キーの保護キー ID (Key Protection Key ID)	ID はキーに割り当てるラベルです。特定のキーの保護キーを ID で識別できるようにします。このフィールドは 255 文字に制限されています。 キーストアファイルの内容を復号するためには、正しいキーの保護キーとホストのマスターキーを識別する必要があります。これらの ID はキーストアファイルヘッダーに暗号化されずに保存されています。キーストアファイルへのアクセスしかなくても正しい ID を選択できます。ディザスタリカバリを実行するには、ファイルと関連付けられる正しい ID とパスフレーズを覚える必要があります。

ストレージサーバーとディスクプールを設定した後にキー名のレコードを保存することをお勧めします。

p.114 の「NetBackup クラウドストレージ暗号化の KMS キー名のレコードの保存」を参照してください。

NetBackup クラウドストレージサーバーのプロパティ

[ストレージサーバーの変更 (Change Storage Server)]ダイアログボックスの[プロパティ (Properties)]タブを使用すると、NetBackup とクラウドストレージの対話に影響するいくつかのプロパティを変更できます。次の表は、NetBackup がプロパティを分類するために使用する接頭辞について説明しています。

すべてのプロパティがすべてのストレージベンダーに適用されるわけではありません。

表 3-11　　接頭辞の定義

接頭辞	定義	詳細情報
AMZ	Amazon	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
AMZGOV	Amazon GovCloud	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
AZR	Microsoft Azure	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
CLD	Cloudian Hyperstore	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
CRYPT	暗号化	p.112 の「NetBackup クラウドストレージサーバーの暗号化プロパティ」を参照してください。
GOOG	Google Nearline	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
HT	Hitachi	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
HTTP	HTTP ヘッダー	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。 **メモ:** このフィールドは、Amazon S3 対応クラウドプロバイダに適用されます。
METER	測定 (Metering)	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

接頭辞	定義	詳細情報
ORAC	Oracle クラウド	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
SWSTK-SWIFT	SwiftStack (Swift)	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
THR	スロットル (Throttling)	p.103 の「NetBackup クラウドストレージサーバー帯域幅スロットルのプロパティ」を参照してください。
VER	Verizon	p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

NetBackup クラウドストレージサーバー帯域幅スロットルのプロパティ

次のストレージサーバーのプロパティは、帯域幅スロットルに適用されます。THR の接頭辞はスロットル調整のプロパティを指定します。目的のクラウドベンダーに対して適切なクラウドプロバイダの URL を使用します。

p.75 の「[拡張性のあるストレージ (Scalable Storage)]プロパティ」を参照してください。

表 3-12　クラウドストレージサーバー帯域幅スロットルのプロパティ

プロパティ	説明
THR:*storage_server*	特定のクラウドストレージサーバーで実行可能な同時並行ジョブの最大数を示します。 クラウドストレージサーバーであるメディアサーバーのスロットル調整を設定する場合: ■ この値を 160 以上に変更します。 ■ この値は、[拡張性のあるストレージ (Scalable Storage)]のホストプロパティ内の[最大並列実行ジョブ数 (Maximum concurrent jobs)]メディアサーバープロパティと同じである必要があります。 p.75 の「[拡張性のあるストレージ (Scalable Storage)]プロパティ」を参照してください。 デフォルト値: なし 指定可能な値: [説明 (Description)] 列を参照

プロパティ	説明
THR:AVAIL_BANDWIDTH	この読み取り専用フィールドには、クラウド機能で利用可能な帯域幅の合計値が表示されます。値はバイト / 秒の単位で表示されます。0 (ゼロ) より大きい数字を指定する必要があります。ゼロを入力すると、エラーが生成されます。 デフォルト値: 104857600 有効値: 正の整数
	メディアサーバーがクラウドストレージサーバーのために実行可能な同時並行ジョブのデフォルトの最大数。 THR:*storage_server* が設定されている場合は、NetBackup は THR:DEFAULT_MAX_CONNECTIONS の代わりに THR:*storage_server* を使います。 これは読み取り専用フィールドです。 この値は、クラウドストレージサーバーではなくメディアサーバーに適用されます。クラウドストレージサーバーに接続できるメディアサーバーが複数ある場合、各メディアサーバーで異なる値を持つ場合があります。したがって、クラウドストレージサーバーで実行可能なジョブの合計数を判断するには、各メディアサーバーからの値を追加してください。 NetBackup が THR:DEFAULT_MAX_CONNECTIONS よりも多いジョブ数を許可するように設定されている場合は、NetBackup では最大ジョブ数に達した後に開始されたジョブがすべて失敗します。ジョブにはバックアップジョブとリストアジョブの両方が含まれています。 ジョブ数の制限は、バックアップポリシーごと、ストレージユニットごとに設定できます。 『NetBackup 管理者ガイド Vol. 1』を参照してください。 **メモ:** NetBackup はジョブを開始するときに、並列実行ジョブの数、メディアサーバーごとの THR:DEFAULT_MAX_CONNECTIONS の数、メディアサーバーの数、ジョブの負荷分散ロジックなどの多くの要素を把握する必要があります。したがって、NetBackup は正確な最大接続数でジョブを失敗しない場合もあります。NetBackup は、接続数が最大数よりもわずかに少ない場合、正確に最大数の場合、最大数よりわずかに多い場合にジョブを失敗することがあります。 実際には、この値を 100 より大きく設定する必要はありません。 デフォルト値: 10 指定可能な値: 1 - 2147483647

プロパティ	説明
THR:OFF_TIME_BANDWIDTH_PERCENT	この読み取り専用フィールドには、業務外時間に使用される帯域幅の割合が表示されます。 デフォルト値: 100 指定可能な値: 0 - 100
THR:OFF_TIME_END	この読み取り専用フィールドには、業務外時間の終了時刻が表示されます。24 時間形式で時間を指定します。たとえば、午前 8 時は 8、午後 6 時 30 分は 1830 です。 デフォルト値: 8 指定可能な値: 0 - 2359
THR:OFF_TIME_START	この読み取り専用フィールドには、業務外時間の開始時刻が表示されます。24 時間形式で時間を指定します。たとえば、午前 8 時は 8、午後 6 時 30 分は 1830 です。 デフォルト値: 18 指定可能な値: 0 - 2359
THR:READ_BANDWIDTH_PERCENT	この読み取り専用フィールドには、クラウド機能が使う読み取り帯域幅の割合が表示されます。0 から 100 までの値を指定します。不正な値を入力すると、エラーが生成されます。 デフォルト値: 100 指定可能な値: 0 - 100
THR:SAMPLE_INTERVAL	この読み取り専用フィールドには、バックアップストリームが利用率をサンプリングし、帯域幅の使用を調整する頻度が表示されます。値は、秒単位で指定されます。この値を 0 に設定すると、スロットル調整は無効になります。 デフォルト値: 0 指定可能な値: 1 - 2147483647
THR:WEEKEND_BANDWIDTH_PERCENT	この読み取り専用フィールドには、週末に使用される帯域幅の割合が表示されます。 デフォルト値: 100 指定可能な値: 0 - 100
THR:WEEKEND_END	この読み取り専用フィールドには、週末の終了時刻が表示されます。曜日の値は、月曜日は 1、火曜日は 2、のように番号で指定されます。 デフォルト値: 7 指定可能な値: 1 - 7

プロパティ	説明
THR:WEEKEND_START	この読み取り専用フィールドには、週末の開始時刻が表示されます。曜日の値は、月曜日は 1、火曜日は 2、のように番号で指定されます。 デフォルト値: 6 指定可能な値: 1 - 7
THR:WORK_TIME_BANDWIDTH_PERCENT	この読み取り専用フィールドには、作業時間に使用される帯域幅の割合が表示されます。 デフォルト値: 100 指定可能な値: 0 - 100
THR:WORK_TIME_END	この読み取り専用フィールドには、作業時間の終了時刻が表示されます。24 時間形式で時間を指定します。たとえば、午前 8 時は 8、午後 6 時 30 分は 1830 です。 デフォルト値: 18 指定可能な値: 0 - 2359
THR:WORK_TIME_START	この読み取り専用フィールドには、作業時間の開始時刻が表示されます。24 時間形式で時間を指定します。たとえば、午前 8 時は 8、午後 6 時 30 分は 1830 です。 デフォルト値: 8 指定可能な値: 0 - 2359
THR:WRITE_BANDWIDTH_PERCENT	この読み取り専用フィールドには、クラウド機能が使う書き込み帯域幅の割合が表示されます。0 から 100 までの値を指定します。不正な値を入力すると、エラーが生成されます。 デフォルト値: 100 指定可能な値: 0 - 100

NetBackup クラウドストレージサーバーの接続プロパティ

クラウドストレージサーバーのすべてまたはほとんどは、表 3-13のストレージサーバーのプロパティを使います。現在サポートされるクラウドベンダーの接頭辞を以下に示します。

- Amazon: AMZ
- Amazon GovCloud: AMZGOV
- Cloudian: CLD
- Google Nearline: GOOG
- 日立: HT

- Microsoft Azure: AZR
- Verizon: VER

表 3-13　ストレージサーバーのクラウド接続プロパティ

プロパティ	説明
METER:DIRECTORY	この読み取り専用フィールドには、データストリームの測定情報を格納するためディレクトリが表示されます。 デフォルト値: UNIX の場合: /usr/openv/var/global/wmc/cloud または /usr/openv/netbackup/db/cloud (メディアサーバーのバージョンが 7.7.x から 8.1.2 の場合のみ) Windows の場合: *install_path*¥Veritas¥NetBackup¥var¥global¥wmc¥cloud または *install_path*¥Veritas¥NetBackup¥db¥cloud¥ (メディアサーバーのバージョンが 7.7.x から 8.1.2 の場合のみ)
METER:INTERVAL	NetBackup がレポート用に接続情報を収集する間隔です。 値は秒単位で設定されます。デフォルト設定は 300 秒 (5 分) です。この値を 0 に設定すると、測定は無効になります。 このプロパティを変更するには、[拡張性のあるストレージ (Scalable Storage)]ホストプロパティの[測定 (Metering)]間隔を構成します。 p.75 の「[拡張性のあるストレージ (Scalable Storage)]プロパティ」を参照してください。 デフォルト値: 300 指定可能な値: 1 - 10000
PREFIX:CURL_CONNECT_TIMEOUT	クラウドストレージサーバーに接続するためにメディアサーバーに割り当てられている時間。この値は秒単位で指定されます。デフォルトは 300 秒 (5 分) です。 この設定は接続時間のみを制限し、セッション時間は制限しません。指定された時間内にメディアサーバーがクラウドストレージサーバーに接続できなければ、ジョブは失敗します。 この値は無効にできません。無効な番号が入力されると、CURL_CONNECT_TIMEOUT はデフォルト値の 300 に戻ります。 デフォルト値: 300 指定可能な値: 1 - 10000

プロパティ	説明
PREFIX:CURL_TIMEOUT	データ操作の完了までに許容される最大時間 (秒単位)。この値は秒単位で指定されます。操作が指定された時間内に完了しない場合、操作は失敗します。デフォルトは 900 秒 (15 分) です。この設定を無効にするには、値を 0 (ゼロ) に設定します。 デフォルト値: 900 指定可能な値: 1 - 10000
PREFIX:LOG_CURL	cURL アクティビティがログに記録されるかどうかを判断します。デフォルトは NO です。この場合、ログアクティビティは無効になります。 デフォルト値: NO 有効値: NO (無効) および YES (有効)
PREFIX:READ_BUFFER_SIZE	読み込み操作に使用するバッファのサイズ。READ_BUFFER_SIZE はバイト単位で指定されます。 バッファの使用を有効にするには、この値を 0 (ゼロ) 以外の数字に設定します。 READ_BUFFER_SIZE は、各リストアジョブ中にストレージサーバーから送信されるデータパケットのサイズを決定します。値を増加すると、大量の連続的なデータにアクセスされる際のパフォーマンスが向上する場合があります。数分内に指定された量のデータを伝送するために帯域幅が不足する場合、タイムアウトによりリストアエラーが発生することがあります。必要な帯域幅を計算する際には、複数のメディアサーバーで同時にバックアップジョブとリストアジョブを行う総負荷を考慮してください。 p.95 の「クラウドストレージのオブジェクトのサイズについて」を参照してください。
PREFIX:USE_SSL	制御 API に Secure Sockets Layer による暗号化を使用するかどうかを判断します。デフォルト値は YES です。この場合、SSL は有効になります。 デフォルト値: YES 有効値: YES または NO
PREFIX:USE_SSL_RW	読み込み操作および書き込み操作に Secure Sockets Layer による暗号化を使用するかどうかを判断します。デフォルト値は YES です。この場合、SSL は有効になります。 デフォルト値: YES 有効値: YES または NO

プロパティ	説明
Provider Suffix: USE_CRL	SSL を有効にして CRL オプションを有効にすると、CRL で自己署名以外の各 SSL 証明書が検証されます。
PREFIX: OBJECT_SIZE	NetBackup が HTTP PUT 要求や GET 要求を使用してクラウドストレージサーバーに送信するデータオブジェクトのサイズ。 オブジェクトのサイズはバイト単位で指定します。一度値を設定すると、[オブジェクトのサイズ (Object Size)] は編集できません。 p.95 の「クラウドストレージのオブジェクトのサイズについて」を参照してください。
PREFIX: WRITE_BUFFER_NUM	このパラメータは Amazon S3 と互換性のあるクラウドプロバイダに適用されません。 この読み取り専用フィールドには、プラグインによって使用される書き込みバッファの合計数が表示されます。 WRITE_BUFFER_SIZE 値はバッファのサイズを定義します。 値は 1 に設定され、変更できません。 デフォルト値: 1 有効値: 1
PREFIX:WRITE_BUFFER_SIZE	書き込み操作に使用するバッファのサイズ。 WRITE_BUFFER_SIZE はバイト単位で指定されます。 バッファの使用を無効にするには、この値を 0 (ゼロ) に設定します。 WRITE_BUFFER_SIZE の値は、バックアップ中にデータムーバーからストレージサーバーに送信されるデータパックのサイズを決定します。値を増加すると、大量の連続的なデータにアクセスされる際のパフォーマンスが向上する場合があります。数分内に指定された量のデータを伝送するために帯域幅が不足する場合、タイムアウトによりバックアップエラーが発生することがあります。必要な帯域幅を計算する際には、複数のメディアサーバーで同時にバックアップジョブとリストアジョブを行う総負荷を考慮してください。 p.95 の「クラウドストレージのオブジェクトのサイズについて」を参照してください。
HTTP:User-Agent	このプロパティは、Amazon S3 と互換性のあるクラウドプロバイダに対してのみ適用可能です。 このプロパティは内部的に設定され、ユーザーは変更できません。

プロパティ	説明
HTTP:x-amz-server-side-encryption	このプロパティが適用可能なクラウドプロバイダは、Amazon S3 と Amazon GovCloud のみです クラウドストレージに転送する必要があるデータについてサーバー側の暗号化を有効にするにはこのプロパティを使います。 AES-256 はサーバー側の暗号化標準です。 クラウドプロバイダのサーバー側の暗号化を無効にするにはこのプロパティを NONE に設定します。 **メモ:** クラウドストレージサーバーを構成したときにすでにメディアサーバー側の暗号化オプションを有効にした場合は、このプロパティを有効にしないでください。
AMZ:REGION_NAME	このプロパティは、Amazon GLACIER_VAULT ストレージクラスに対してのみ適用可能です。 ストレージサーバーの構成中に設定された領域を表示します。 このプロパティは、ストレージサーバーの構成中に設定され、ユーザーが変更することはできません。
AMZ:UPLOAD_CLASS	このプロパティは、Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスに対してのみ適用可能です。 データをバックアップするためのストレージクラスを指定するには、このプロパティを使用します。 デフォルト値: STANDARD 有効値: STANDARD または STANDARD_IA
AMZ:RETRIEVAL RETENTION PERIOD	このプロパティは、Amazon Glacier に対してのみ適用可能です。 取得保持期間を日数で指定するには、このプロパティを使用します。
AMZ:TRANSITION_TO_STANDARD_IA_AFTER	このプロパティは、Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスに対してのみ適用可能です。 STANDARD として UPLOAD_CLASS を設定した場合、TRANSITION_TO_STANDARD_IA_AFTER は NONE または 30 ～ 2147483617 の範囲のいずれかに設定する必要があります。 STANDARD_IA として UPLOAD_CLASS を設定した場合、TRANSITION_TO_STANDARD_IA_AFTER を NONE に設定する必要があります。

プロパティ	説明
AMZ:TRANSITION_TO_GLACIER_AFTER	このプロパティは、Amazon S3 Intelligent Tiering (LIFECYCLE) ストレージクラスに対してのみ適用可能です。 STANDARD として UPLOAD_CLASS を設定した場合および TRANSITION_TO_STANDARD_IA_AFTER が 30 ～ 2147483617 の範囲に設定されている場合、TRANSITION_TO_GLACIER_AFTER を NONE または 60 ～ 2147483647 の範囲に設定する必要があります。STANDARD_IA ストレージクラスのデータの場合、この値には最低 30 日の保持期間が含まれます。 STANDARD として UPLOAD_CLASS を設定した場合および TRANSITION_TO_STANDARD_IA_AFTER が NONE に設定されている場合、TRANSITION_TO_GLACIER_AFTER を 1 ～ 2147483647 の範囲に設定する必要があります。 STANDARD_IA として UPLOAD_CLASS を設定した場合および TRANSITION_TO_STANDARD_IA_AFTER が NONE に設定されている場合、TRANSITION_TO_GLACIER_AFTER を 30 ～ 2147483647 の範囲に設定する必要があります。
AMZ:STORAGE_CLASS	このプロパティは、Amazon S3 クラウドプロバイダにのみ適用可能です。 クラウドストレージサーバーによって使用されるストレージクラスが表示されます。 このプロパティは内部的に設定され、ユーザーは変更できません。
AZR:STORAGE_TIER	このプロパティは、Microsoft Azure アーカイブに対してのみ適用可能です。 クラウドストレージサーバーによって使用されるストレージ層が表示されます。

プロパティ	説明
AMZ:OFFLINE_TRANSFER_MODE	このプロパティは、Amazon S3 クラウドプロバイダにのみ適用可能です。 Amazon Snowball のストレージの宛先を設定するには、このプロパティを使用します。 デフォルト値: NONE **メモ:** Snowball モードを使用した処理が完了したら、プロパティを NONE に設定します。このモードでは、エンドポイントが Amazon パブリックエンドポイントを参照する必要があります。 指定可能な値: FILESYSTEM: ファイルインターフェースを使用して Amazon Snowball にデータを転送する場合は、このプロパティを設定します。 ストレージサーバーのエンドポイントは、Amazon パブリックエンドポイントを参照する必要があります。 PROVIDER_API: Amazon 社が提供する S3 インターフェースを使用して Amazon Snowball にデータを転送する場合は、このプロパティを設定します。 ストレージサーバーのエンドポイントは、Snowball エンドポイントを参照する必要があります。
AMZ:TRANSFER_DRIVE_PATH	このプロパティは、Amazon S3 クラウドプロバイダを使用する場合と AMZ:OFFLINE_TRANSFER_MODE プロパティが FILESYSTEM に設定されている場合にのみ適用可能です。 Amazon Snowball のデータのバックアップを作成する必要がある絶対マウントポイントを設定するには、このプロパティを使用します。 デフォルト値: NONE

NetBackup クラウドストレージサーバーの暗号化プロパティ

次の暗号化固有のストレージサーバープロパティは、ストレージベンダーの全員またはほとんどの人が使っています。CRYPT 接頭辞は、暗号化のプロパティを指定します。これらの値は表示専用であり、変更できません。

表 3-14 暗号化クラウドストレージサーバーのプロパティ

プロパティ	説明
CRYPT:KMS_SERVER	この読み取り専用フィールドには、KMS サービスをホストする NetBackup サーバーが表示されます。ストレージサーバーのプロパティを設定する際には、KMS サーバーホストの名前を入力します。デフォルトでは、このフィールドには NetBackup プライマリサーバーの名前が含まれています。この値は変更できません。 デフォルト値: NetBackup プライマリサーバー名 有効値: 適用なし
CRYPT:KMS_VERSION	この読み取り専用フィールドには、NetBackup のキーマネージメントサービスのバージョンが表示されます。この値は変更できません。 デフォルト値: 16 有効値: 適用なし
CRYPT:LOG_VERBOSE	この読み取り専用フィールドには、暗号化アクティビティのログが有効かどうかが表示されます。値は、ログを有効にする場合は YES、無効にする場合は NO のいずれかを指定します。 デフォルト値: NO 有効値: YES および NO
CRYPT:VERSION	この読み取り専用フィールドには、暗号化のバージョンが表示されます。この値は変更できません。 デフォルト値: 13107 有効値: 適用なし

クラウドストレージのディスクプールについて

ディスクプールは、基礎となるディスクストレージ上のディスクボリュームを表します。ディスクプールは、NetBackup ストレージユニットの宛先ストレージです。クラウドストレージでは、1 つのディスクプールに対してボリュームを 1 つだけ指定してください。

ディスクプールとディスクボリュームの名前は、クラウドストレージプロバイダの環境内で一意である必要があります。

クラウドストレージのディスクプールがストレージライフサイクルポリシーのストレージ先である場合、NetBackup 容量管理が適用されます。

ディスクプールを作成する手順については、『NetBackup™ Web UI 管理者ガイド』を参照してください。

クラウドストレージのディスクプールの構成

Web UI を使用して、クラウドストレージのディスクプールを作成します。暗号化されたストレージを作成して NetBackup KMS が構成されている場合は、暗号化を使用する選択した各ボリュームのパスフレーズを入力する必要があります。パスフレーズによって、そのボリュームの暗号化キーが作成されます。暗号化されたストレージを作成して外部 KMS が構成されている場合は、選択した各ボリュームのパスフレーズを入力する必要はありません。

ディスクプールを作成する手順については、『NetBackup™ Web UI 管理者ガイド』を参照してください。

NetBackup クラウドストレージ暗号化の KMS キー名のレコードの保存

暗号化キー名とキータグのレコードを保存することをお勧めします。キーをリカバリしたり再作成する必要がある場合は、キータグが必要です。

NetBackup KMS サーバーキー名のレコードの保存

クラウドストレージのストレージサーバー構成中に暗号化設定を有効にしたときに NetBackup KMS サーバーが設定されている場合は、次の手順を実行してキー名のレコードを保存します。

p.92 の「クラウドストレージのデータ暗号化について」を参照してください。

キー名のレコードを保存する方法

1 キーグループ名を特定するには、プライマリサーバー上で次のコマンドを使用します。

UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkgs`

Windows の場合: *install_path*¥Program Files¥Veritas¥NetBackup¥bin¥admincmd¥nbkmsutil.exe -listkgs

次に出力例を示します。

```
Key Group Name         : CloudVendor.com:symc_backups_gold
Supported Cypher       : AES_256
Number of Keys         : 1
Has Active Key         : Yes
Creation Time          : Tues Oct 01 01:00:00 2013
Last Modification Time: Tues Oct 01 01:00:00 2013
Description            : CloudVendor.com:symc_backups_gold
```

2 キーグループごとに、グループに属するすべてのキーをファイルに書き込みます。プライマリサーバーでコマンドを実行します。コマンドの構文は次のとおりです。

UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkeys -kgname key_group_name > filename.txt`

Windows の場合: `install_path¥Program Files¥Veritas¥NetBackup¥bin¥admincmd¥nbkmsutil.exe -listkeys -kgname key_group_name > filename.txt`

次に出力例を示します。

```
nbkmsutil.exe -listkeys -kgname CloudVendor.com:symc_backups_gold
> encrypt_keys_CloudVendor.com_symc_backups_gold.txt

Key Group Name        : CloudVendor.com:symc_backups_gold
Supported Cypher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description           : Key group to protect cloud volume
FIPS Approved Key     : Yes

Key Tag               : 532cf41cc8b3513a13c1c26b5128731e
                          5ca0b9b01e0689cc38ac2b7596bbae3c
Key Name              : Encrypt_Key_April
Current State         : Active
Creation Time         : Tues Jan 01 01:02:00 2013
Last Modification Time: Tues Jan 01 01:02:00 2013
Description           : -

Number of Keys: 1
```

3 キーレコードの作成に使ったパスフレーズをファイルに含めます。

4 安全な場所にファイルを格納します。

外部 KMS サーバーキー名のレコードの保存

キーのリカバリ手順については、KMS サーバーのマニュアルを参照してください。

クラウド環境へのバックアップメディアサーバーの追加

クラウド環境に追加のメディアサーバーを追加できます。追加のメディアサーバーによってバックアップのパフォーマンスの改善が助長されます。このようなサーバーはデータムー

バーとして知られています。追加するメディアサーバーには、ストレージサーバーのクレデンシャルが割り当てられます。このクレデンシャルによって、データムーバーはストレージサーバーと通信します。

NetBackup メディアサーバーは、クラウドストレージの必要条件に適合する必要があります。

p.97 の「クラウドストレージの NetBackup メディアサーバーについて」を参照してください。

クラウド環境にバックアップメディアサーバーを追加するには

1. 左側で[ストレージ (Storage)]、[ディスクストレージ (Disk storage)]の順に選択します。
2. クラウドストレージサーバーを選択します。
3. [処理 (Actions)]メニューで[編集 (Edit)]を選択します。
4. [メディアサーバー (Media servers)]で、[追加 (Add)]をクリックします。
5. [保存 (Save)]をクリックします。
6. 必要に応じて、ディスクプール、ストレージユニット、およびポリシーを変更します。

クラウドストレージ用のストレージユニットの構成

ディスクプールを参照するストレージユニットを 1 つ以上作成します。

ディスクプールにストレージユニットが存在するかを判断するには、[ストレージ (Storage)]、[ストレージユニット (Storage units)]の順に選択します。

ストレージユニットはディスクプールのプロパティを継承します。ストレージユニットがレプリケーションプロパティを継承する場合、プロパティによって、NetBackup ストレージライフサイクルポリシーに、ストレージユニットとディスクプールの意図されていた目的が通知されます。自動イメージレプリケーションはストレージライフサイクルポリシーを必要とします。

ストレージユニットの構成について詳しくは、『NetBackup™ Web UI 管理者ガイド』を参照してください。

ストレージユニットのプロパティを使用して、バックアップトラフィックを制御できます。

p.119 の「クライアントとサーバーの最適比率の構成」を参照してください。

p.120 の「メディアサーバーへのバックアップ通信量の制御」を参照してください。

p.117 の「クラウドストレージユニットのプロパティ」を参照してください。

クラウドストレージユニットのプロパティ

クラウドディスクプールのストレージユニットの構成オプションは、次のとおりです。

表 3-15 クラウドストレージユニットのプロパティ

プロパティ	説明
ストレージユニット名 (Storage unit name)	新しいストレージユニットの一意の名前。名前でストレージ形式を示すことができます。ストレージユニット名は、ポリシーおよびスケジュールでストレージユニットを指定する際に使用される名前です。ストレージユニット名は、作成後に変更できません。
ストレージユニット形式 (Storage unit type)	ストレージユニット形式として[ディスク (Disk)]を選択します。
ディスク形式 (Disk Type)	そのディスクタイプのクラウドストレージ (*type*) を選択します。*type*は、ストレージベンダー、暗号化などに基づくディスクプールの種類を表します。
ディスクプール (Disk Pool)	このストレージユニットのストレージが含まれているディスクプールを選択します。 指定された[ディスク形式 (Disk type)]のすべてのディスクプールが[ディスクプール (Disk Pool)]リストに表示されます。ディスクプールが構成されていない場合、ディスクプールはリストに表示されません。
メディアサーバー (Media server)	[メディアサーバー(Media server)]の設定で、クライアントのバックアップを作成してデータをクラウドストレージサーバーに移動できる NetBackup メディアサーバーを指定します。メディアサーバーはデータをリストアまたは複製操作用に移動できます。 次のようにメディアサーバーを指定します。 ■ メディアサーバーリスト内の任意のサーバーでデータを重複排除できるようにするには、[任意のメディアサーバーを使用 (Use any available media server)]を選択します。 ■ データを重複排除するのに特定のメディアサーバーを使うには、[次のメディアサーバーのみを使用 (Only use the following media servers)]を選択します。その後、許可するメディアサーバーを選択します。 ポリシーの実行時に、使用するメディアサーバーが NetBackup によって選択されます。

プロパティ	説明
最大並列実行ジョブ数 (Maximum concurrent jobs)	[最大並列実行ジョブ数 (Maximum concurrent jobs)]設定によって、NetBackup がディスクストレージユニットに一度に送信できるジョブの最大数が指定されます。(デフォルトは 1 つのジョブです。ジョブ数は 0 から 256 の範囲で指定できます)。この設定は、Media Manager ストレージユニットでの[最大並列書き込みドライブ数 (Maximum concurrent write drives)]に対応するものです。 ジョブは、ストレージユニットが利用可能になるまで NetBackup によってキューに投入します。3 つのバックアップジョブがスケジュールされている場合、[最大並列実行ジョブ数 (Maximum concurrent jobs)]が 2 に設定されていると、NetBackup は最初の 2 つのジョブを開始し、3 つ目のジョブをキューに投入します。ジョブに複数のコピーが含まれる場合、各コピーが[最大並列実行ジョブ数 (Maximum concurrent jobs)]の数にカウントされます。 [最大並列実行ジョブ数 (Maximum concurrent jobs)]は、バックアップジョブと複製ジョブの通信を制御しますが、リストアジョブの通信は制御しません。カウントは、サーバーごとにではなく、ストレージユニットのすべてのサーバーに適用されます。ストレージユニットの複数のメディアサーバーを選択し、[最大並列実行ジョブ数 (Maximum concurrent jobs)]で 1 を選択すると、一度に 1 つのジョブのみが実行されます。 ここで設定する数は、利用可能なディスク領域、および複数のバックアップ処理を実行するサーバーの性能によって異なります。 **警告:** [最大並列実行ジョブ数 (Maximum concurrent jobs)]設定に 0 (ゼロ) を指定すると、ストレージユニットは無効になります。
最大フラグメントサイズ (Maximum fragment size)	通常のバックアップの場合、各バックアップイメージは、ファイルシステムが許容する最大ファイルサイズを超過しないように NetBackup によってフラグメントに分割されます。20 MB から 51200 MB までの値を入力できます。 FlashBackup ポリシーの場合、最適な複製パフォーマンスを実現するために、デフォルトの最大フラグメントサイズを使用することを推奨します。

クライアントとサーバーの最適比率の構成

ストレージユニット設定を使って、クライアントとサーバーの最適比率を構成できます。1 つのディスクプールを使って、複数のストレージユニットでバックアップ通信量を分割するように構成できます。すべてのストレージユニットが同じディスクプールを使うので、ストレージをパーティション化する必要はありません。

たとえば、100 個の重要なクライアント、500 個の通常のクライアント、4 つのメディアサーバーが存在すると想定します。最も重要なクライアントをバックアップするために 2 つのメディアサーバーを使って、通常のクライアントをバックアップするのに 2 つのメディアサーバーを使うことができます。

次の例では、クライアントとサーバーの比率を最適に構成する方法について記述します。

- NetBackup の重複排除のメディアサーバーを構成し、ストレージを構成します。
- ディスクプールを構成します。
- 最も重要なクライアントのストレージユニット (STU-GOLD など) を構成します。ディスクプールを選択します。[次のメディアサーバーのみを使用 (Only use the following media servers)]を選択します。重要なバックアップに使うメディアサーバーを 2 つ選択します。
- 100 個の重要なクライアント用のバックアップポリシーを作成し、STU-GOLD ストレージユニットを選択します。ストレージユニットで指定したメディアサーバーは、クライアントデータを重複排除ストレージサーバーに移動します。
- 別のストレージユニット (STU-SILVER など) を構成します。同じディスクプールを選択します。[次のメディアサーバーのみを使用 (Only use the following media servers)]を選択します。他の 2 つのメディアサーバーを選択します。
- 500 個の通常のクライアント用にバックアップポリシーを構成し、STU-SILVER ストレージユニットを選択します。ストレージユニットで指定したメディアサーバーは、クライアントデータを重複排除ストレージサーバーに移動します。

バックアップ通信は、ストレージユニット設定によって目的のデータムーバーにルーティングされます。

メモ: NetBackup は、書き込み動作 (バックアップと複製) でのメディアサーバーの選択に対してのみストレージユニットを使います。リストアの場合、NetBackup はディスクプールにアクセスできるすべてのメディアサーバーから選択します。

メディアサーバーへのバックアップ通信量の制御

ディスクプールのストレージユニットで[最大並列実行ジョブ数 (Maximum concurrent jobs)]の設定を使用し、メディアサーバーへのバックアップ通信量を制御できます。同じディスクプールで複数のストレージユニットを使う場合、この設定によって、より高い負荷には特定のメディアサーバーが効率的に指定されます。並列実行ジョブの数が多いほど、数が少ない場合に比べて、ディスクはビジー状態になりやすくなります。

たとえば、2 つのストレージユニットが同じセットのメディアサーバーを使用しているとします。一方のストレージユニット (STU-GOLD) の[最大並列実行ジョブ数 (Maximum concurrent jobs)]に、もう一方 (STU-SILVER) よりも大きい値が設定されています。[最大並列実行ジョブ数 (Maximum concurrent jobs)]に大きい値が設定されているストレージユニットでは、より多くのクライアントバックアップを実行できます。

NetBackup アクセラレータバックアップと NetBackup 最適化合成バックアップについて

NetBackup クラウドストレージは NetBackup アクセラレータと NetBackup 最適化合成をサポートしています。NetBackup アクセラレータバックアップまたは NetBackup 最適化合成バックアップを有効にしたとき、暗号化、測定、スロットル調整は機能し、サポートされます。非クラウドバックアップと同様に NetBackup アクセラレータバックアップと NetBackup最適化合成バックアップの両方を有効にします。NetBackup アクセラレータバックアップと NetBackup 最適化合成バックアップに関する詳細情報が利用可能です。

- 『NetBackup Deduplication ガイド』を参照してください。
- 『NetBackup 管理者ガイド Vol. 1』を参照してください。

クラウドストレージディスクプールのプロパティ

ディスクプールのプロパティはディスクプールの目的によって変更できます。

メモ: 利用可能な合計領域 (Total available space)、合計最大物理容量 (Total raw size)、使用可能サイズ (Usable Size)、低水準点 (Low water mark)、高水準点 (High water mark) の各プロパティは、クラウドストレージディスクプールには適用されません。

これらすべての値はストレージ容量から導出され、クラウドプロバイダから取得することはできません。

次の表に、使用可能なプロパティを示します。

表 3-16 クラウドストレージディスクプールのプロパティ

プロパティ	説明
名前	ディスクプールの名前。
ストレージサーバー	ストレージサーバーの名前。
ディスクボリューム (Disk volumes)	ディスクプールを構成するディスクボリューム。
合計最大物理容量 (Total raw size)	ディスクプールのストレージの raw (未フォーマット) サイズの合計。 ストレージのホストはストレージの最大物理容量を表示する場合としない場合があります。 **メモ:** [合計最大物理容量 (Total raw size)]はクラウドストレージディスクプールには適用されません。

プロパティ	説明
利用可能な合計領域 (Total available space)	ディスクプールで使用できる空き領域の合計。 **メモ:** ［利用可能な合計領域 (Total available space)］はクラウドストレージディスクプールには適用されません。
コメント (Comments)	ディスクプールに関連付けられているコメント。
高水準点 (High Water Mark)	［高水準点 (High water mark)］は、ボリュームまたはディスクプールが空きがないと見なされるしきい値です。 **メモ:** ［高水準点 (High water mark)］は、クラウドストレージディスクプールには適用されません。
低水準点 (Low Water Mark)	［低水準点 (Low water mark)］は がイメージのクリーンアップを停止するしきい値です。Ashwini - ET 3864623 - 16th Feb 06NetBackup ［低水準点 (Low water mark)］は、クラウドストレージディスクプールには適用されません。
I/O ストリーム数を制限 (Limit I/O streams)	ディスクプールの各ボリュームの読み書きストリーム (つまり、ジョブ) の数を制限するために選択します。ジョブはバックアップイメージを読み書きすることがあります。デフォルトでは、制限はありません。 制限に達すると、NetBackup は書き込み操作に別のボリュームを (利用可能であれば) 選択します。ボリュームが利用不能な場合、利用可能になるまで NetBackup はジョブをキューに登録します。 ストリームが多すぎると、ディスクスラッシングのためにパフォーマンスが低下することがあります。ディスクスラッシングとは、RAM とハードディスクドライブ間でデータが過度にスワップすることです。ストリームを少なくするとスループットを改善でき、一定の期間に完了するジョブ数を増やすことができます。 開始点で、ディスクプールのボリューム数別にすべてのストレージユニットの最大並列実行ジョブ数を分割します。[NetBackup 7.6 Best Practices white paper from Alex Davies.]

プロパティ	説明
ボリュームごと (per volume)	ボリュームあたりの許可する読み書きストリームの数を選択または入力します。 多くの要因が最適なストリーム数に影響します。要因はディスク速度、CPU の速度、メモリ容量などです。 [スナップショット (Snapshot)]用に構成され、[レプリケーションソース (Replication source)]プロパティがあるディスクプールの場合: ■ この設定を変更する場合は、常に増分 2 を使用します。単一のレプリケーションジョブは 2 つの I/O ストリームを使います。 ■ ストリームより多くのレプリケーションジョブがある場合は、ストリームが利用可能になるまで NetBackup はジョブをキューに登録します。 ■ バッチ処理は、単一の NetBackup ジョブ内で多数のレプリケーションを引き起こす可能性があります。スナップショットレプリケーションジョブのバッチ処理に影響する設定もあります。

証明書失効リスト (CRL) に対する証明書の検証

すべてのクラウドプロバイダに対し、NetBackup は証明書失効リスト (CRL) に対して SSL 証明書を検証するための機能を提供します。SSL を有効にして CRL オプションを有効にすると、CRL で自己署名以外の各 SSL 証明書が検証されます。証明書が無効である場合、NetBackup はクラウドプロバイダに接続しません。

次のいずれかの方法を使用して、CRL に対する検証を有効にできます。

- SSL パラメータに `csconfig` CLI: `crl` パラメータを追加します。このオプションは、ストレージサーバーを追加または更新するときに利用できます。CRL 値は、エイリアスを作成する前に `csconfig` CLI を介してのみ変更できます。
- [ストレージサーバーのプロパティ (Storage Server Properties)]ダイアログ: このダイアログで USE_CRL プロパティを更新します。GUI では、構成後に CRL オプションの無効化のみを行えます。
  p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
- `getconfig` オプションと `setconfig` オプションを指定して `nbdevconfig` CLI を使用し、CRL に対する検証を有効または無効にすることもできます。

メモ: アップグレード後、SSL が有効なクラウドストレージサーバーについては、CRL の検証はデフォルトで有効になっています。

証明書失効リスト (CRL) に対する証明書検証を有効にするための要件

- CRL 配布エンドポイントは HTTP なので、外部ネットワークへの HTTP (ポート 80) 接続をブロックするファイアウォールルールはすべてオフにします。たとえば、http://crl3.provider.com/server-g2.crl などです。
- CRL のダウンロード URL は証明書から動的にフェッチされるため、不明な URL をブロックするファイアウォールルールはすべて無効にします。
- 通常、CRL URL (配布エンドポイント) は IPV4 をサポートします。IPV6 環境では、CRL オプションを無効にします。
- プライベートクラウドには通常、自己署名証明書があります。そのため、プライベートクラウドでは CRL の確認は必要ありません。CRL オプションが有効になっていても、この確認はスキップされます。
- x.509 証明書に、CRL 配布ポイントが示されている必要があります。配布ポイントの種類は、HTTP である必要があります。

NetBackup クラウドの認証局 (CA) の管理

NetBackup クラウドは、.PEM (Privacy-enhanced Electronic Mail) 形式の X.509 証明書のみをサポートしています。

`cacert.pem` バンドルの認証局 (CA) の詳細は、次の場所にあります。

- Windows の場合:
  - メディアサーバーバージョン 10.0 以降では、パスは次のとおりです。
    <installation-path>¥NetBackup¥var¥global¥cloud
  - メディアサーバーバージョン 8.2 から 9.1 では、パスは次のとおりです。
    *<installation-path>*NetBackup¥var¥global¥wmc¥cloud¥cacert.pem
  - メディアサーバーバージョン 7.7.x から 8.1.2 では、パスは次のとおりです。
    install_path¥Veritas¥NetBackup¥db¥cloud¥cacert.pem
- UNIX の場合:
  - メディアサーバーバージョン 10.0 以降では、パスは次のとおりです。
    /usr/openv/var/global/cloud/
  - メディアサーバーバージョン 8.2 から 9.1 では、パスは次のとおりです。
    /usr/openv/var/global/wmc/cloud/cacert.pem
  - メディアサーバーバージョン 7.7.x から 8.1.2 では、パスは次のとおりです。
    /usr/openv/netbackup/db/cloud/cacert.pem

メモ: クラスタ配備では、NetBackup データベースパスは、アクティブノードからアクセス可能な共有ディスクを指します。

cacert.pem バンドルの CA を追加または削除できます。

変更を完了した後に、新しいバージョンの NetBackup にアップグレードすると、cacert.pem バンドルが新しいバンドルによって上書きされます。追加または削除したすべてのエントリが失われます。ベストプラクティスとして、編集した cacert.pem ファイルのローカルコピーを保管します。アップグレードされたファイルをローカルコピーを使用して上書きすることで、変更をリストアできます。

メモ: cacert.pem ファイルのファイル権限と所有権を変更しないようにしてください。

CA を追加するには

必要なクラウドプロバイダから CA 証明書を取得し、cacert.pem ファイルで CA 証明書を更新する必要があります。証明書は .PEM 形式である必要があります。

1. cacert.pem ファイルを開きます。
2. 自己署名 CA 証明書を、cacert.pem ファイルの先頭または末尾の新しい行に追加します。

   次の情報ブロックを追加します。

   ```
   Certificate Authority Name

   ==========================

   -----BEGIN CERTIFICATE-----

   <Certificate content>

   -----END CERTIFICATE-----
   ```

3. ファイルを保存します。

CA を削除するには

cacert.pem ファイルから CA を削除する前に、関連する証明書を使用しているクラウドジョブがないことを確認します。

1 cacert.pem ファイルを開きます。

2 目的の CA を削除します。次の情報ブロックを削除します。

```
Certificate Authority Name

==========================

-----BEGIN CERTIFICATE-----

<Certificate content>

-----END CERTIFICATE-----
```

3 ファイルを保存します。

NetBackup によって承認されている CA のリスト

- AddTrust External Root
- Baltimore CyberTrust Root
- Cybertrust Global Root
- DigiCert Assured ID Root CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Global CA G2
- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert High Assurance EV Root CA
- DigiCert Trusted Root G4
- D-Trust Root Class 3 CA 2 2009
- GeoTrust Global CA
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority - G2
- GeoTrust Primary Certification Authority - G3
- GeoTrust Universal CA
- GeoTrust Universal CA 2
- RSA Security 2048 v3

- Starfield Services Root Certificate Authority - G2
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- Verisign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Universal Root Certification Authority

4

監視とレポート

この章では以下の項目について説明しています。

- クラウドストレージジョブの詳細表示
- 圧縮率の表示
- クラウドストレージ暗号化用の KMS キー情報の表示

クラウドストレージジョブの詳細表示

ジョブの詳細を表示するには、NetBackup のアクティビティモニターを使用します。

クラウドストレージジョブの詳細を表示する方法

1. 左側で、[アクティビティモニター (Activity Monitor)]をクリックします。
2. [ジョブ (Jobs)]タブをクリックします。
3. 特定のジョブの詳細を表示するには、[ジョブ (Jobs)]テーブルに表示されているジョブをクリックします。

圧縮率の表示

bptm ログには、クラウドストレージでバックアップを作成した後のデータ圧縮率の情報が含まれています。圧縮率は元々のサイズを圧縮後のサイズで除算して算出されます。たとえば、元々のサイズが 15302918144 バイトで、圧縮後が 7651459072 である場合、圧縮率は 2.00 になります。

圧縮率を表示するには

1 バックアップジョブの bptm PID をメモします。

p.128 の「クラウドストレージジョブの詳細表示」を参照してください。

2 bptm.log ファイルを開きます。ログファイルは次のディレクトリにあります。

UNIX の場合 /usr/openv/netbackup/logs/

Windows の場合 *install_path*¥NetBackup¥logs¥

3 bptm PID インスタンスを検索します。

次の行に、イメージ形式に基づいた圧縮率情報が示されます。

```
date:time <PID> <4> 35:bptm:<PID>:
media_server_IP: compress: image image_name_C1_F1 compressed from
 data in bytes to data in bytes bytes, compression ratio
ratio_value
```

```
date:time <PID> <4> 35:bptm:<PID>:
media_server_IP: compress: image image_name_C1_HDR compressed
from data in bytes to data in bytes bytes, compression ratio
ratio_value
```

クラウドストレージ暗号化用の KMS キー情報の表示

キーグループとキーレコードについての以下の情報をリストするために nbkmsutil コマンドを使うことができます。

キーグループ	「KMS キーグループ情報を表示する方法」を参照してください。
キー	「KMS キー情報を表示する方法」を参照してください。

メモ: レコードキー情報を保管することを推奨します。キーをリカバリする必要がある場合、出力に表示されるキータグが必要です。

KMS キーグループ情報を表示する方法

- すべてのキーグループをリストするには、-listkgs オプションを指定して nbkmsutil を使います。コマンド形式は次のとおりです。

  UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkgs`

  Windows の場合:
  install_path¥Veritas¥NetBackup¥bin¥admincmd¥nbkmsutil -listkgs

  UNIX ホストストレージ上の出力の例は次のとおりです。Windows では、ボリューム名は使用されません。

```
nbkmsutil -listkgs

Key Group Name         : CloudStorageVendor.com:symc_volume_for_backups
Supported Cypher       : AES_256
Number of Keys         : 1
Has Active Key         : Yes
Creation Time          : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description            : -
```

KMS キー情報を表示する方法

- キーグループ名に属するすべてのキーをリストするには、-listkgs と -kgname オプションを指定して nbkmsutil を使います。コマンド形式は次のとおりです。

  UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkeys -kgname AdvDiskServer1.example.com:AdvDisk_Volume`

  Windows の場合: *install_path*¥Veritas¥NetBackup¥bin¥admincmd¥nbkmsutil -listkeys -kgname AdvDiskServer1.example.com:

  UNIX ホストストレージ上の出力の例は次のとおりです。Windows では、ボリューム名は使用されません。

```
nbkmsutil -listkeys -kgname CloudStorageVendor.com:symc_volume_for_backup

Key Group Name        : CloudStorageVendor.com:symc_volume_for_backups
Supported Cypher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description           : -

Key Tag             : 532cf41cc8b3513a13c1c26b5128731e5ca0b9b01e0689cc38ac2b7596bbae3c
Key Name              : Encrypt_Key_April
Current State         : Active
Creation Time         : Tues Jan 01 01:02:00 2013
Last Modification Time: Tues Jan 01 01:02:00 2013
Description           : -
```

nbkmscmd コマンドを使用して、NetBackup KMS と外部 KMS サーバーのキーを一覧表示することもできます。'storage_server_name:volume_name' 形式のキーグループ名の値を持つカスタム属性が設定されている Symmetric 暗号化キーが、外部 KMS サーバーにすでに存在することを確認する必要があります。

NetBackup KMS と外部 KMS のキー情報を表示するには

1. 次のコマンドを実行して KMS サーバーの構成名を取得します。

   `nbkmscmd -listkmsconfig`

2. 次のコマンドを実行して KMS サーバーからキーグループのキー情報を取得します。

   `nbkmscmd -listkeys -name KMS_server_name -keyGroupName key_group_name -jsonRaw`

5

操作上の注意事項

この章では以下の項目について説明しています。

- NetBackup bpstsinfo コマンドの操作上の注意事項
- NetBackup アクセス制御が有効になっている場合、クラウドの構成が失敗することがある
- クラウドストレージサーバーのアーティファクトの削除
- csconfig reinitialize を使用した更新済みのクラウド構成設定のロード
- プライマリサーバーとレガシークラウドストレージメディアサーバー間の通信の有効化または無効化

NetBackup bpstsinfo コマンドの操作上の注意事項

次の表に、NetBackup クラウドストレージで bpstsinfo コマンドを使用するための操作上の注意事項を示します。

表 5-1 bpstsinfo コマンドの操作上の注意事項

備考	説明
-stype オプションか -storageserverprefix のいずれかを使用する	ストレージサーバー情報のリストを表示するには、bpstsinfo コマンドを制約する -stype オプションか -storageserverprefix オプションを使ってください。これらのオプションを使用しない場合、すべてのプロバイダが検索されるので、時間がかかり、タイムアウトになる場合もあります。
正しい -stype を指定する	情報を要求するプラグインは、戻される情報に影響します。従って、bpstsinfo コマンドで正しい -stype を使用する必要があります。-stype を確認するには、次のコマンドを使用します。 nbdevquery -liststs -storage_server *fq_host_name* ストレージが暗号化されている場合、-stype には _crypt 接尾辞が含まれます。

備考	説明
bpstsinfo コマンド出力に表示される暗号化されたストレージユニットと暗号化されていないストレージユニット	暗号化された論理ストレージユニット (LSU) の情報を表示する際に bpstsinfo コマンドを使用すると、出力には暗号化された LSU と暗号化されていない LSU の両方が表示されます (両タイプが存在する場合)。この出力が予測どおりの結果です。bpstsinfo コマンドはストレージのプラグインレベルで動作し、暗号化などの高レベルの詳細は考慮しません。 暗号化されたストレージを指定するコマンドの例を次に示します。 `bpstsinfo -lsuinfo -storage_server amazon.com -stype amazon_crypt`

NetBackup アクセス制御が有効になっている場合、クラウドの構成が失敗することがある

NetBackup アクセス制御を使う環境でクラウドストレージサーバーを構成しようとすると、次のようなエラーメッセージを受け取る場合があります。

```
Error creating Key Group and Keys cannot connect on socket
```

NetBackup がこのエラーメッセージを生成するのは、NetBackup アクセス制御内でユーザーに十分な権限がないからです。クラウドストレージサーバーを構成するアカウントは、NBU_KMS 管理グループのメンバーでなければなりません。

NetBackup のアクセス制御とアカウントの設定について詳しくは、NetBackup『セキュリティおよび暗号化ガイド』を参照してください。

クラウドストレージサーバーのアーティファクトの削除

ストレージサーバーを誤って削除すると、構成ファイルは孤立した状態でコンピュータに残ります。新しいストレージサーバーを作成しようとすると、ログインエラーを示すエラーメッセージが表示されて失敗します。ストレージサーバーを正しく削除するには、次の手順を実行します。

ストレージサーバーの削除

1. ストレージサーバーのすべてのイメージを期限切れにします。
2. ストレージユニットを削除します。
3. ディスクプールを削除します。
4. ストレージサーバーを削除します。
5. .pref ファイルを db/cloud ディレクトリから削除します。

csconfig reinitialize を使用した更新済みのクラウド構成設定のロード

通常、NetBackup プライマリサーバーをアップグレードした場合や新しいバージョンの NetBackup クラウド構成パッケージ (CloudProvider.xml 構成ファイル) をダウンロードした場合に、NetBackup クラウドストレージの構成設定を更新します。更新済みのパッケージをインストールしたり、既存のクラウドストレージの構成設定を更新したときに、構成の変更を有効にするには、NetBackup リリースのバージョンに応じて NetBackup CloudStore Service Container (nbcssc) または NetBackup Web 管理コンソール (nbwmc) サービスを再起動する必要があります。

場合によっては、nbcssc または nbwmc サービスがハングアップしたり、サービスの再起動に失敗したりすることがあります。このエラーは、CloudProvider.xml ファイルが無効であるか、xml ファイルと構成済みの CloudStore のバージョンが不一致であるために発生します。サービスの再起動に失敗すると、NetBackup バックアップジョブでのエラーの発生につながる可能性があります。

NetBackup 8.2 リリース以降では、csconfig ユーティリティを使用すれば、サービスを再起動することなく更新済みのクラウド構成設定を再ロードできます。

構成を更新したら、NetBackup プライマリサーバーまたはメディアサーバーで次のコマンドを実行します。

UNIX の場合は、/usr/openv/netbackup/bin/admincmd/ ディレクトリから次のコマンドを実行します。

```
# sudo ./csconfig reinitialize
```

Windows の場合は、*<install_path>*¥NetBackup¥bin¥admincmd¥ ディレクトリから次のコマンドを実行します。

```
csconfig reinitialize
```

csconfig reinitialize コマンドオプションを実行すると、nbwmcサービスで Cloudstore.conf、CloudProvider.xml、CloudInstance.xml ファイルから構成設定が再ロードされます。nbwmc サービスを再起動する必要はありません。

プライマリサーバーとレガシークラウドストレージメディアサーバー間の通信の有効化または無効化

これは、バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ該当します。

古いクラウドストレージメディアサーバーで実行されている NetBackup CloudStore Service Container (nbcssc) サービスは、プライマリサーバーとの通信にポート 5637 を使用します。リリース 8.2 以降、nbcssc サービスは配備されなくなりました。NetBackup Web 管

理コンソール (nbwmc) と NetBackup Service Layer (nbsl) サービスがこの機能を処理するようになりました。

プライマリサーバーを 8.2 以降にアップグレードする場合でも、レガシークラウドストレージメディアサーバーはプライマリサーバーとの通信にレガシークラウドサービスを使用し続けます。ただし、NetBackup 8.2 プライマリサーバーは、レガシークラウドストレージメディアサーバーをサポートしています。8.2 プライマリサーバーと古いメディアサーバー間の通信を許可するには、プライマリサーバーでポート 5637 を開く必要があります。

ポート 5637 で nbwmc サービスの通信を有効にするには

1. プライマリサーバーで次のコマンドを実行します。

   UNIX の場合:

   ```
   # usr/openv/wmc/bin/install/configurePorts -addLegacyCloudService
   ```

   Windows の場合:

   ```
   <install_path>¥NetBackup¥wmc¥bin¥install¥configurePorts
   -addLegacyCloudService
   ```

2. nbwmc サービスを再起動して変更を反映します。

3. 次のコマンドを実行して、メディアサーバーのホスト名ベースの証明書をプロビジョニングします。

   UNIX の場合:

   ```
   # usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert
   <media_server>
   ```

   Windows の場合:

   ```
   <install_path>¥NetBackup¥bin¥admincmd¥bpnbaz -ProvisionCert
   <media_server>
   ```

   アプライアンスの場合は、代わりに次のコマンドを実行します。

   UNIX の場合:

   ```
   # usr/openv/netbackup/bin/bpnbat -AddMachine <appliance_hostname>
   ```

   Windows の場合:

   ```
   <install_path>¥NetBackup¥bin¥bpnbat -AddMachine
   <appliance_hostname>
   ```

4. メディアサーバーでクラウドストレージサービスを再起動します。

古いバージョンのメディアサーバーがサポートされている場合でも、このようなメディアサーバーを 8.2 以降のバージョンにアップグレードすることをお勧めします。すべてのレガシーメディアサーバーをアップグレードした後、ポート 5637 での nbwmc サービスの使用を無効にすることができます。

ポート 5637 で nbwmc サービスの通信を無効にするには

1. プライマリサーバーで次のコマンドを実行します。

   UNIX の場合:

   ```
   # usr/openv/wmc/bin/install/configurePorts
   -removeLegacyCloudService
   ```

   Windows の場合:

   ```
   <install_path>¥NetBackup¥wmc¥bin¥install¥configurePorts
   -removeLegacyCloudService
   ```

2. nbwmc サービスを再起動して変更を反映します。

6

トラブルシューティング

この章では以下の項目について説明しています。

- 統合ログについて
- レガシーログについて
- NetBackup クラウドストレージログファイル
- libcurl ログの有効化
- クラウドストレージの構成上の問題のトラブルシューティング
- クラウドストレージの操作上の問題のトラブルシューティング
- Amazon Snowball および Amazon Snowball Edge の問題のトラブルシューティング

統合ログについて

統合ログ機能では、すべての Cohesity 製品に共通の形式で、ログファイル名およびメッセージが作成されます。`vxlogview` コマンドを使用した場合だけ、ログの情報を正しく収集して表示することができます。サーバープロセスとクライアントプロセスは統合ログを使用します。

オリジネータ ID のログファイルはログの構成ファイルで指定した名前のサブディレクトリに書き込まれます。すべての統合ログは次のディレクトリのサブディレクトリに書き込まれます。

Windows の場合　*install_path*¥NetBackup¥logs

UNIX の場合　/usr/openv/logs

メモ: ログにアクセスできるのは、Linux システムの場合は root ユーザーと service ユーザー、Windows システムの場合は administrators グループに属するユーザーのみです。

ログコントロールには、[ログ (Logging)]ホストプロパティでアクセスできます。また、次のコマンドで統合ログを管理できます。

`vxlogcfg`	統合ログ機能の構成設定を変更します。
`vxlogmgr`	統合ログをサポートする製品が生成するログファイルを管理します。
`vxlogview`	統合ログによって生成されたログを表示します。 p.140 の「vxlogview を使用した統合ログの表示の例」を参照してください。

vxlogview コマンドを使用した統合ログの表示について

vxlogview コマンドを使用した場合だけ、統合ログの情報を正しく収集して表示することができます。統合ログファイルは、バイナリ形式のファイルで、一部の情報は関連するリソースファイルに含まれています。これらのログは次のディレクトリに保存されます。特定プロセスのファイルに検索を制限することによって vxlogview の結果をより速く表示することができます。

UNIX の場合	`/usr/openv/logs`
Windows の場合	*install_path*¥NetBackup¥logs

表 6-1 vxlogview 問い合わせ文字列のフィールド

フィールド名	形式	説明	例
PRODID	整数または文字列	プロダクト ID または製品の略称を指定します。	PRODID = 51216 PRODID = 'NBU'
ORGID	整数または文字列	オリジネータ ID またはコンポーネントの略称を指定します。	ORGID = 116 ORGID = 'nbpem'
PID	long 型の整数	プロセス ID を指定します。	PID = 1234567
TID	long 型の整数	スレッド ID を指定します。	TID = 2874950

フィールド名	形式	説明	例
STDATE	long 型の整数または文字列	秒単位またはロケール固有の短い形式の日時で開始日付を指定します。たとえば、「mm/dd/yy hh:mm:ss AM/PM」の形式を使用しているロケールなどがあります。	STDATE = 98736352 STDATE = '4/26/11 11:01:00 AM'
ENDATE	long 型の整数または文字列	秒単位またはロケール固有の短い形式の日時で終了日付を指定します。たとえば、「mm/dd/yy hh:mm:ss AM/PM」の形式を使用しているロケールなどがあります。	ENDATE = 99736352 ENDATE = '04/27/11 10:01:00 AM'
PREVTIME	文字列	hh:mm:ss の形式で、時間を指定します。このフィールドには、=、<、>、>= および <= の演算子だけを使用できます。	PREVTIME = '2:34:00'
SEV	整数	次の使用可能な重大度の種類のうちのいずれかを指定します。 0 = INFO 1 = WARNING 2 = ERR 3 = CRIT 4 = EMERG	SEV = 0 SEV = INFO
MSGTYPE	整数	次の使用可能なメッセージの種類のうちのいずれかを指定します。 0 = DEBUG (デバッグメッセージ) 1 = DIAG (診断メッセージ) 2 = APP (アプリケーションメッセージ) 3 = CTX (コンテキストメッセージ) 4 = AUDIT (監査メッセージ)	MSGTYPE = 1 MSGTYPE = DIAG
CTX	整数または文字列	識別子の文字列としてコンテキストトークンを指定するか、'ALL' を指定してすべてのコンテキストインスタンスを取得して表示します。このフィールドには、= および != の演算子だけを使用できます。	CTX = 78 CTX = 'ALL'

表 6-2　日付を含む問い合わせ文字列の例

例	説明
`(PRODID == 51216) && ((PID == 178964)|| ((STDATE == '2/5/15 09:00:00 AM') && (ENDATE == '2/5/15 12:00:00 PM'))`	2015 年 2 月 5 日 の午前 9 時から正午までを対象に NetBackup プロダクト ID 51216 のログファイルメッセージを取り込みます。
`((prodid = 'NBU') && ((stdate >= '11/18/14 00:00:00 AM') && (endate <= '12/13/14 12:00:00 PM'))) || ((prodid = 'BENT') && ((stdate >= '12/12/14 00:00:00 AM') && (endate <= '12/25/14 12:00:00 PM')))`	2014 年 11 月 18 日から 2014 年 12 月 13 日までを対象に NetBackup プロダクト NBU のログメッセージを取り込み、2014 年 12 月 12 日から 2014 年 12 月 25 日までを対象に NetBackup プロダクト BENT のログメッセージを取り込みます。
`(STDATE <= '04/05/15 0:0:0 AM')`	2015 年 4 月 5 日、またはその前に記録されたすべてのインストール済み Cohesity 製品のログメッセージを取得します。

vxlogview を使用した統合ログの表示の例

次の例は、vxlogview コマンドを使って統合ログを表示する方法を示します。

メモ: ログにアクセスできるのは、Linux システムの場合は root ユーザーと service ユーザー、Windows システムの場合は administrators グループに属するユーザーのみです。

表 6-3　vxlogview コマンドの使用例

項目	例
ログメッセージの全属性の表示	`vxlogview -p 51216 -d all`
ログメッセージの特定の属性の表示	NetBackup (51216) のログメッセージの日付、時間、メッセージの種類およびメッセージテキストだけを表示します。 `vxlogview --prodid 51216 --display D,T,m,x`
最新のログメッセージの表示	オリジネータ 116 (nbpem) によって 20 分以内に作成されたログメッセージを表示します。-o 116 の代わりに、-o nbpem を指定することもできます。 `# vxlogview -o 116 -t 00:20:00`

項目	例

特定の期間からのログメッセージの表示	指定した期間内に nbpem で作成されたログメッセージを表示します。
	
	`# vxlogview -o nbpem -b "05/03/15 06:51:48 AM"`
	`-e "05/03/15 06:52:48 AM"`

より速い結果の表示	プロセスのオリジネータを指定するのに -i オプションを使うことができます。 `# vxlogview -i nbpem` vxlogview -i オプションは、指定したプロセス (nbpem) が作成するログファイルのみを検索します。検索するログファイルを制限することで、vxlogview の結果が速く戻されます。一方、vxlogview -o オプションでは、指定したプロセスによって記録されたメッセージのすべての統合ログファイルが検索されます。 **メモ:** サービスではないプロセスに -i オプションを使用すると、vxlogview によってメッセージ [ログファイルが見つかりません。(No log files found)]が戻されます。サービスではないプロセスには、ファイル名にオリジネータ ID がありません。この場合、-i オプションの代わりに -o オプションを使用します。 -i オプションはライブラリ (137、156、309 など) を含むそのプロセスの一部であるすべての OID のエントリを表示します。
ジョブ ID の検索	特定のジョブ ID のログを検索できます。 `# vxlogview -i nbpem | grep "jobid=`*`job_ID`*`"` jobid=という検索キーは、スペースを含めず、すべて小文字で入力します。 ジョブ ID の検索には、任意の vxlogview コマンドオプションを指定できます。この例では、-i オプションを使用してプロセスの名前 (nbpem) を指定しています。このコマンドはジョブ ID を含むログエントリのみを返します。jobid=*job_ID* を明示的に含まないジョブの関連エントリは欠落します。

レガシーログについて

NetBackup レガシーデバッグログの場合、プロセスが個別のログディレクトリにデバッグアクティビティのログファイルを作成します。デフォルトでは、NetBackup は次の場所にログディレクトリのサブセットのみを作成します。

Windows
install_path¥NetBackup¥logs
install_path¥Volmgr¥debug

UNIX
/usr/openv/netbackup/logs
/usr/openv/volmgr/debug

レガシーログを使用するには、プロセスのログファイルディレクトリが存在している必要があります。ディレクトリがデフォルトで作成されていない場合は、mklogdir ユーティリティを使用してディレクトリを作成できます。または、手動でディレクトリを作成することもできます。プロセスのログ記録を有効にすると、プロセスの開始時にログファイルが作成されます。ログファイルがあるサイズに達すると、NetBackup プロセスはそのファイルを閉じて新しいログファイルを作成します。

メモ: レガシーログディレクトリに適切な権限を付与するために、Windows と Linux に存在する mklogdir ユーティリティを常に使用して各プラットフォームのレガシーログディレクトリを作成します。

次のユーティリティを使用して、すべてのログディレクトリを作成できます。

- Windows の場合: *install_path*¥NetBackup¥Logs¥mklogdir.bat
- UNIX の場合: /usr/openv/netbackup/logs/mklogdir

レガシーログフォルダを作成して使用する場合は、次の推奨事項に従います。

- レガシーログフォルダ内でシンボリックリンクまたはハードリンクを使用しないでください。
- root 以外のユーザーまたは管理者以外のユーザーに対してプロセスが実行された場合、レガシーログフォルダにログが記録されない場合があります。その場合は、mklogdir コマンドを使用して、必要なユーザーのフォルダを作成します。
- root 以外のユーザーまたは管理者以外のユーザー用にコマンドラインを実行するには (NetBackup サービスが実行されていない場合のトラブルシューティング)、特定のコマンドライン用のユーザーフォルダを作成します。フォルダは、mklogdir コマンドを使用して、または root 以外のユーザーや管理者以外のユーザー権限で手動で作成します。

クラウドストレージ用の NetBackup ログファイルディレクトリの作成

NetBackup の機能を構成する前に、NetBackup のコマンドがログファイルを書き込むディレクトリを作成します。プライマリサーバーとご利用の機能で使う各メディアサーバーにディレクトリを作成します。ログファイルは次のディレクトリに存在します。

- UNIX の場合: /usr/openv/netbackup/logs/
- Windows の場合: *install_path*¥NetBackup¥logs¥

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

NetBackup のコマンドのログディレクトリを作成する方法

- オペレーティングシステムに応じて、次のスクリプトの 1 つを実行します。

  UNIX の場合: `/usr/openv/netbackup/logs/mklogdir`

  Windows の場合: *install_path*¥NetBackup¥logs¥mklogdir.bat

tpconfig コマンドのログディレクトリを作成する方法

- オペレーティングシステムに応じて、debug ディレクトリと tpcommand ディレクトリを作成します (デフォルトでは、debug ディレクトリと tpcommand ディレクトリは存在しません)。ディレクトリのパス名は次のとおりです。

  UNIX の場合: `/usr/openv/volmgr/debug/tpcommand`

  Windows の場合: *install_path*¥Veritas¥Volmgr¥debug¥tpcommand

NetBackup クラウドストレージログファイル

NetBackup クラウドストレージは Cohesity OpenStorage フレームワーク内に存在します。したがって、クラウドのアクティビティについては、OpenStorage と同じログファイルといくつかの追加のログファイルが使われます。

NetBackup の一部のコマンドまたは処理では、メッセージがそれぞれ固有のログファイルに書き込まれます。それらのコマンドやプロセス用に、ユーティリティがログメッセージを書き込むことができるようにログディレクトリが存在する必要があります。

他の処理では、Veritas Unified Logging (VxUL) が使用されます。各プロセスに VxUL オリジネータ ID が付けられます。VxUL のログファイルには、標準化された名前およびファイル形式が使用されます。VxUL のログファイルを表示するためには、NetBackup の `vxlogview` のコマンドを使ってください。

ログファイルの表示方法と管理方法についての詳細情報が利用可能です。『NetBackup ログリファレンスガイド』を参照してください。

次に、ログメッセージのコンポーネント識別子を示します。

- `sts_` 接頭辞はストレージの読み書きを行うプラグインとの通信に関連しています。
- クラウドストレージサーバーのプレフィックスはそのクラウドベンダーのストレージネットワークとの相互作用に関連しています。
- `encrypt` 接頭辞は暗号化プラグインとの通信に関連しています。
- `KMSCLIB` 接頭辞は NetBackup キーマネージメントサービスとの通信に関連しています。

ほとんどの通信は NetBackup メディアサーバーで発生します。したがって、ディスク操作に使うメディアサーバーのログファイルを最も参照することになります。

警告: ログレベルが高いほど、NetBackup のパフォーマンスに対する影響が大きくなります。ログレベル 5 (最も高い) を使うのは、Cohesity の担当者から指示された場合だけにしてください。ログレベル 5 はトラブルシューティングにのみ使います。

NetBackup のログレベルは、NetBackup プライマリサーバーの[ログ (Logging)]ホストプロパティで指定します。特定のオプションに固有の一部のプロセスについては、表 6-4 に示すように構成ファイルでログレベルを設定します。

ログの説明を表 6-4に示します。

表 6-4 NetBackup のログクラウドストレージの場合

動作	OIDw	プロセス (Processes)
バックアップおよびリストア	該当なし	次の処理のメッセージがログファイルに表示されます。 ■ bpbrm(Backup Restore Manager)。 ■ bpdbm(Database Manager)。 ■ bpdm(Disk Manager)。 ■ bptm (Tape Manager) の I/O 処理。 ログファイルは次のディレクトリに存在します。 ■ UNIX の場合: /usr/openv/netbackup/logs/ ■ Windows の場合: *install_path*¥NetBackup¥logs¥
バックアップおよびリストア	117	nbjm (Job Manager)。
イメージのクリーンアップ、検証、インポートおよび複製	該当なし	bpdbm Database Manager のログファイル。 ログファイルは次のディレクトリに存在します。 ■ UNIX の場合: /usr/openv/netbackup/logs/bpdbm ■ Windows の場合: *install_path*¥NetBackup¥logs¥bpdbm
クラウドの接続操作	該当なし	bpstsinfo ユーティリティはクラウドストレージサーバーへの接続についての情報をログファイルに書き込みます。
クラウドのアカウントの構成	222	クラウドストレージのアカウントを作成するプロセスは Remote Manager and Monitor Service です。RMMS はメディアサーバー上で動作します。

動作	OIDw	プロセス (Processes)
Cloud Storage Service Container	該当なし	このデーモンは、メディアサーバーのバージョンが 7.7.x から 8.1.2 の場合にのみ適用可能です。 NetBackup Cloud Storage Service Container (nbcssc) では、次のディレクトリにログファイルが書き込まれます。 ■ Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥nbcssc ■ UNIX の場合: /usr/openv/netbackup/logs/nbcssc
NetBackup Web 管理コンソール	495	NetBackup Web 管理コンソール (nbwmc) サービスは、次のディレクトリにログを書き込みます。 ■ Windows の場合: *install_path*¥Veritas¥netbackup¥logs¥nbwebservice ■ UNIX の場合: /usr/openv/logs/nbwebservice
NetBackup Service Layer	該当なし	NetBackup Service Layer (nbsl) サービスは、次のディレクトリにログを書き込みます。 ■ Windows の場合: *install_path*¥Veritas¥netbackup¥logs¥nbsl ■ UNIX の場合: /usr/openv/logs/nbsl
csconfig ユーティリティ	該当なし	NetBackup csconfig コマンドラインユーティリティは、次のディレクトリにログを書き込みます。 ■ Windows の場合: *install_path*¥Veritas¥netbackup¥logs¥nbcssc ■ UNIX の場合: /usr/openv/netbackup/logs/nbcssc
クレデンシャルの構成	該当なし	tpconfig ユーティリティ。tpconfig コマンドは tpcommand ディレクトリにログファイルを書き込みます。
デバイスの構成	111	nbemm の処理。
デバイスの構成	178	Enterprise Media Manager (EMM) プロセスで実行される Disk Service Manager プロセス。
デバイスの構成	202	Remote Manager and Monitor Service で動作するストレージサーバーインターフェースの処理。RMMS はメディアサーバー上で動作します。
デバイスの構成	230	Remote Manager and Monitor Service で動作する Remote Disk Service Manager (RDSM) インターフェース。RMMS はメディアサーバー上で動作します。

p.150 の「クラウドストレージの操作上の問題のトラブルシューティング」を参照してください。

libcurl ログの有効化

cURL ログを有効にするには、ストレージサーバーのプロパティ *CLOUD_PREFIX*:LOG_CURL を YES に設定します。CLOUD_PREFIX の値は各ストレージプロバイダの接頭辞の値です。指定可能な値は、次のとおりです。

AMZ	Amazon
AMZGOV	Amazon GovCloud
AZR	Microsoft Azure
CLD	Cloudian HyperStore
GOOG	Google Nearline
HT	Hitachi
ORAC	Oracle クラウド
SWSTK-SWIFT	SwiftStack (Swift)
VER	Verizon

たとえば、Amazon の LOG_CURL を有効にするには、AMZ:LOG_CURL を YES に設定します。

クラウドストレージの構成上の問題のトラブルシューティング

構成の問題のトラブルシューティングでは、次の項の情報が役に立つ場合があります。

p.147 の「NetBackup の拡張性のあるストレージのホストプロパティを利用できない」を参照してください。

p.147 の「クラウドストレージを作成できません」を参照してください。

p.148 の「クラウドストレージサーバーへのデータ転送が、SSL モードで失敗する」を参照してください。

p.149 の「Amazon GovCloud クラウドストレージの設定が非 SSL モードで失敗する」を参照してください。

p.149 の「Google Nearline ストレージからのデータリストアは失敗する場合がある」を参照してください。

p.150 の「認証バージョン V2 でのストレージリージョンのフェッチの失敗」を参照してください。

NetBackup の拡張性のあるストレージのホストプロパティを利用できない

NetBackup CloudStore Service Container がアクティブでない場合は、[拡張性のあるストレージ (Scalable Storage)]のホストプロパティが利用不能になります。次の 2 つの現象のいずれかが起こる可能性があります。

- メディアサーバーの[拡張性のあるストレージ (Scalable Storage)]プロパティが利用不能です。
- ポップアップのボックスに、[拡張性のあるストレージの設定を取得できません (Unable to fetch Scalable Storage settings)]のメッセージが表示される場合があります。

NetBackup CloudStore Service Container が非アクティブになっている原因を判断して、問題を解決し、次にサービスコンテナを開始します。

p.156 の「NetBackup CloudStore Service Container の起動とシャットダウンのトラブルシューティング」を参照してください。

p.155 の「NetBackup CloudStore Service Container の停止と起動」を参照してください。

クラウドストレージを作成できません

NetBackup でクラウドストレージを作成できない場合は、次の点を確認してください。

- NetBackup `cacert.pem` ファイルが、NetBackup のプライマリサーバーとメディアサーバーの両方で次の場所に存在します。
  - UNIX/Linux の場合: `/usr/openv/var/webtruststore`
  - Windows の場合: `<install_path>/var/webtruststore`

  バージョン 7.7.x から 8.1.2 のメディアサーバーに NetBackup `cacert.pem` ファイルがない場合は、プライマリサーバーで `nbcertcmd -getCACertificate` を実行します。このコマンドを実行した後、NetBackup CloudStore サービスコンテナを再起動してください。
  コマンドの詳細については、『NetBackup コマンドリファレンスガイド』を参照してください。

メモ: この NetBackup `cacert.pem` ファイルは NetBackup 固有のファイルです。このファイルには、NetBackup 認可サービスによって生成された CA 証明書が含まれています。

- NetBackup `cacert.pem` ファイルが、NetBackup のプライマリサーバーとメディアサーバーで同一のものである。
- バージョン 7.7.x から 8.1.2 のメディアサーバーの場合、マシンの証明書は次の場所にあります。
  - UNIX/Linux の場合: `/usr/openv/var/vxss/credentials`
  - Windows の場合: `<install_path>/var/vxss/credentials`

  セキュリティ証明書が存在しない場合は、プライマリサーバーで `bpnbaz -ProvisionCert` を実行してください。このコマンドを実行した後、プライマリサーバーおよびメディアサーバーで NetBackup CloudStore Service Container を再起動してください。
  p.88 の「ホスト名ベースの証明書の配備」を参照してください。
- バージョン 7.7.x から 8.1.2 のメディアサーバーの場合、NetBackup CloudStore Service Container はアクティブです。
  p.155 の「NetBackup CloudStore Service Container の停止と起動」を参照してください。
- メディアサーバーがバージョン 8.0 以前の場合、NetBackup プライマリサーバーで［8.0 以前のホストとの安全でない通信を有効にする (Enable insecure communication with 8.0 and earlier hosts)］オプションが選択されています。このオプションは、NetBackup Web UI の［設定 (Settings)］>［グローバルセキュリティ (Global security)］>［安全な通信 (Secure communication)］で利用できます。
- メディアサーバーでは、証明書配備のセキュリティレベルが［最高 (Very High)］に設定されている場合、自動証明書配備が無効になります。すべての新しい証明書要求に認証トークンが必要になります。したがって、証明書を配備する前に認証トークンを作成する必要があります。
  詳しい手順については、『NetBackup セキュリティおよび暗号化ガイド』の「認証トークンの作成」の項を参照してください。

クラウドストレージサーバーへのデータ転送が、SSL モードで失敗する

NetBackup は、SSL モードでのクラウドストレージとの通信時に、認証局（CA）によって署名された証明書のみをサポートします。クラウドサーバー (パブリックまたはプライベート) に CA による署名付き証明書があることを確認します。CA によって署名された証明書がない場合は、SSL モードでの NetBackup とクラウドプロバイダ間のデータ転送が失敗します。

Amazon GovCloud クラウドストレージの設定が非 SSL モードで失敗する

Amazon GovCloud クラウドプロバイダ (s3-fips-us-gov-west-1.amazonaws.com) の FIPS 領域では、セキュアモードの通信のみをサポートします。このため、FIPS 領域を持つ Amazon GovCloud クラウドストレージを設定するときに[SSL を使用する (Use SSL)]オプションを無効にすると、設定は失敗します。

SSL モードを再度有効にするには、`-us` パラメータ付きで `csconfig` コマンドを実行して、SSL の値を「2」に設定します。

コマンドの詳しい説明については、『NetBackup コマンドリファレンスガイド』を参照してください。

Google Nearline ストレージからのデータリストアは失敗する場合がある

Google Nearline ストレージからのデータリストアは、NetBackup の `READ_BUFFER_SIZE` が割り当て済み読み込みスループットより大きな値に設定されている場合、失敗する可能性があります。Google は、Google Nearline ストレージクラスに格納されているデータの総合サイズに基づいて読み取りスループットを割り当てます。

メモ: `READ_BUFFER_SIZE` のデフォルト値は 100 MB です。

Google Nearline からのデータのリストアが失敗した後、NetBackup bptm ログに次のエラーが記録されます。

```
HTTP status: 429, Retry type: RETRY_EXHAUSTED
```

Google では、場所別に Google Nearline ストレージクラスに格納される TB データ単位の読み取りスループットを 4 MB/s としています。Google が割り当てる読み取りスループットに合わせるには、NetBackup の READ_BUFFER_SIZE 値を変更する必要があります。

たとえば、Google Nearline ストレージクラスに格納したデータが 5 TB である場合、`READ_BUFFER_SIZE` 値は、割り当て済み読み取りスループットである 20 MB になるように変更する必要があります。

詳しくは、Google ガイドラインを参照してください。

https://cloud.google.com/storage/docs/nearline?hl=en

https://cloud.google.com/storage/docs/nearline?hl=en

p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。

認証バージョン V2 でのストレージリージョンのフェッチの失敗

認証バージョン V2 を使用する際にストレージリージョンのフェッチがポップアップエラー `Unable to process request (228)` で失敗する場合、次のトラブルシューティング手順を実行します。

`nbsl` および `nbwmc` サービスが起動して実行中であることを確認します。

`nblog.conf` ファイルで `nbwmc` ログを有効にし、詳細度を最高レベルに増やします。領域のフェッチを再試行します。

p.85 の「NetBackup cloudstore.conf 設定ファイル」を参照してください。

問題が解決しない場合は、`csconfig` ログで cURL エラーを検索します。cURL エラーコードにより、問題の根本原因を判断できます。

不正な構成シナリオの例を次に示します。

- cURL エラーで、無効な認証が問題の原因であると示されている場合は、identity API バージョン 2 のエンドポイント (v2.0/tokens) が認証に使われていることを確認します。
  たとえば、https://mycloud.xyz.com:5000 の代わりに http://mycloud.xyz.com.com:5000/v2.0/tokens が認証で使われている必要があります。
- cURL エラーで、CA 以外によって署名された証明書が問題の原因であると示されている場合、authentication と storage endpoint (これらが個別にホストされている場合) の `cacert.pem` に自己署名の証明書を追加します。

スナップショットの親ジョブからのバックアップが状態コード 160 で失敗する

保護計画で構成されているストレージサーバーに対応するメディアサーバーから、ポート 443 で Snapshot Manager にアクセスできるかどうかを確認します。

メディアサーバーの `/etc/hosts` ファイルに適切なエントリを追加して、ネットワークの問題を解決します。

クラウドストレージの操作上の問題のトラブルシューティング

操作上の問題のトラブルシューティングでは、次の項の情報が役に立つ場合があります。

p.147 の「NetBackup の拡張性のあるストレージのホストプロパティを利用できない」を参照してください。

p.151 の「クラウドストレージバックアップが失敗する」を参照してください。

p.156 の「nbcssc (レガシーメディアサーバー)、nbwmc、nbsl のプロセスを再起動するとすべての cloudstore.conf 設定が元に戻される」を参照してください。

p.156 の「NetBackup CloudStore Service Container の起動とシャットダウンのトラブルシューティング」を参照してください。

クラウドストレージバックアップが失敗する

次のトピックを参照してください。

- 「アクセラレータバックアップの失敗」
- 「WRITE_BUFFER_SIZE を大きくした後にバックアップが失敗する」
- 「ストレージボリュームがクラウドベンダーインターフェースによって作成された」
- 「NetBackup CloudStore Service Container が非アクティブ」
- 「[任意のメディアサーバーを使用 (Use any available media server)]オプションが選択されているとバックアップが失敗することがあります。」
- 「エラーコード 83 またはエラーコード 2106 が表示され、クラウドバックアップとリストアの操作が失敗します。」
- 「証明書の問題のため、クラウドストレージのバックアップに失敗します。」
- 「Amazon S3 対応クラウドストレージへのバックアップジョブが状態コード 41 で失敗する」

アクセラレータバックアップの失敗

次のようなメッセージがジョブの詳細に表示されます。

```
Critical bptm(pid=28291) accelerator verification failed: backupid= host_name_1373526632,

offset=3584, length=141976576, error= 2060022, error message: software error
Critical bptm(pid=28291) image write failed: error 2060022: software error
Error bptm(pid=28291) cannot write image to disk, Invalid argument end writing;
write time: 0:02:31
Info bptm(pid=28291) EXITING with status 84
Info bpbkar(pid=6044) done. status: 84: media write error media write error(84)
```

このエラーは、複数のクラウドストレージサーバーがある環境で発生します。このエラーは、あるクラウドストレージサーバーに宛てられたクライアントの NetBackup アクセラレータのバックアップがその後に別のクラウドストレージサーバーに宛てられたことを示します。

クラウドストレージへのアクセラレータバックアップに対しては、次のことを確認します。

- 各クライアントを常に同じストレージサーバーにバックアップします。他のストレージサーバーが同じクラウドストレージベンダーのストレージである場合にもそうしてください。

- クライアントのバックアップに常に同じバックアップポリシーを使用し、ポリシーのストレージ宛先を変更しないでください。

WRITE_BUFFER_SIZE を大きくした後にバックアップが失敗する

クラウドのストレージサーバーの WRITE_BUFFER_SIZE プロパティがコンピュータの総スワップ領域を超えると、バックアップが状態 84 で失敗する場合があります。

この問題を解決するために、WRITE_BUFFER_SIZE のサイズをコンピュータの総スワップ領域より小さい値に調整します。

ストレージボリュームがクラウドベンダーインターフェースによって作成された

次のようなメッセージがジョブの詳細に表示されます。

```
Info bptm(pid=xxx) start backup
Critical bptm(pid=xxxx) image open failed: error 2060029: authorization failure
Error bpbrm(pid=xxxx) from client gabby: ERR - Cannot write to STDOUT. Errno = 32:
Broken pipe
Info bptm(pid=xxxx) EXITING with status 84
```

次のようなメッセージが bptm ログファイルに表示されます。

```
Container container_name is not Cohesity container or tag data error,
fail to create image. Please make sure that the LSU is created by
means of NBU.
```

このエラーは、ボリュームがクラウドストレージベンダーのインターフェースを使って作成されたことを示します。

NetBackup Web UI を使用して、クラウドストレージにボリュームを作成します。NetBackup はボリュームに必要なパートナー ID を適用します。ベンダーのインターフェースを使ってコンテナを作成する場合、パートナー ID は適用されません。

問題を解決するには、クラウドストレージベンダーのインターフェースを使ってコンテナを削除します。NetBackupで、ディスクプールを削除し、Web UI で再作成します。

p.128 の「クラウドストレージジョブの詳細表示」を参照してください。

p.143 の「NetBackup クラウドストレージログファイル」を参照してください。

NetBackup CloudStore Service Container が非アクティブ

これは、バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ該当します。

NetBackup CloudStore Service Container が非アクティブの場合は、バックアップをクラウドストレージに送信できません。

NetBackup では、NetBackup コマンドを使って NetBackup クラウドストレージを構成するときに、CloudStore Service Container がアクティブであるかどうかが確認されません。したがって、このような状況で開始したバックアップは失敗します。

p.156 の「NetBackup CloudStore Service Container の起動とシャットダウンのトラブルシューティング」を参照してください。

[任意のメディアサーバーを使用 (Use any available media server)]オプションが選択されているとバックアップが失敗することがあります。

クラウドストレージサーバーの構成中に、メディアサーバーとプライマリサーバーが同じバージョンになっていることを確認する必要があります。

メモ: この制限は、既存のクラウドストレージサーバーには適用されません。

クラウドバックアップは、次のシナリオで失敗することがあります。

ストレージユニットの構成中に[任意のメディアサーバーを使用 (Use any available media server)]を選択し、クラウドストレージの構成中に NetBackup がプライマリサーバーのバージョンと異なるメディアサーバーのバージョンを使っている場合。

この問題を解決するには、次を実行します。

ストレージユニットの構成中に[次のメディアサーバーのみを使用 (Only use the following media servers)]を選択し、[メディアサーバー (Media Servers)]ペインで、プライマリサーバーと同じバージョンのメディアサーバーを選択します。

p.150 の「クラウドストレージの操作上の問題のトラブルシューティング」を参照してください。

エラーコード 83 またはエラーコード 2106 が表示され、クラウドバックアップとリストアの操作が失敗します。

次のいずれかの理由により、エラーコード 83 またはエラーコード 2106 が表示され、クラウドバックアップとリストアの操作が失敗する場合があります。

- メディアサーバーの日付と時刻の設定がずれています (GMT/UTC 時間と同期していません)。
- ストレージサーバーの指定されたクレデンシャルが正しくありません。

次の手順を実行します。

メディアサーバーの日付と時刻の設定を変更して、GMT/UTC 時間と同期するようにします。

ストレージサーバーのクレデンシャルを更新します。`tpconfig` コマンドを使用して、クレデンシャルを更新します。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。

証明書の問題のため、クラウドストレージのバックアップに失敗します。

証明書の問題のためにクラウドストレージのバックアップに失敗する場合、次のことを確認します。

- NetBackup `cacert.pem` ファイルが、次の場所において NetBackup のプライマリサーバー、メディアサーバーの両方に存在する。
  - UNIX/Linux の場合: `/usr/openv/var/webtruststore`
  - Windows の場合: `<install_path>/var/webtruststore`

  バージョン 7.7.x から 8.1.2 のメディアサーバーで、NetBackup `cacert.pem` ファイルがない場合は、プライマリサーバーで `nbcertcmd -getCACertificate` を実行します。このコマンドを実行した後、NetBackup CloudStore サービスコンテナを再起動してください。
  コマンドの詳細については、『NetBackup コマンドリファレンスガイド』を参照してください。

  メモ: この NetBackup `cacert.pem` ファイルは NetBackup 固有のファイルです。このファイルには、NetBackup 認可サービスによって生成された CA 証明書が含まれています。

- NetBackup `cacert.pem` ファイルが NetBackup のプライマリサーバーとメディアサーバーで同一のものである。
- バージョン 7.7.x から 8.1.2 のメディアサーバーの場合、マシンの証明書は次の場所にあります。
  - UNIX/Linux の場合: `/usr/openv/var/vxss/credentials`
  - Windows の場合: `<install_path>/var/vxss/credentials`

  セキュリティ証明書が存在しない場合は、プライマリサーバーで `bpnbaz -ProvisionCert` を実行してください。このコマンドを実行した後、プライマリサーバーおよびメディアサーバーで NetBackup CloudStore Service Container を再起動してください。
  p.88 の「ホスト名ベースの証明書の配備」を参照してください。
- バージョン 7.7.x から 8.1.2 のメディアサーバーの場合、NetBackup CloudStore Service Container はアクティブです。
  p.155 の「NetBackup CloudStore Service Container の停止と起動」を参照してください。
- メディアサーバーがバージョン 8.0 以前の場合、NetBackup プライマリサーバーで［8.0 以前のホストとの安全でない通信を有効にする (Enable insecure communication with 8.0 and earlier hosts)］オプションが選択されています。このオ

プションは、[設定 (Settings)]>[グローバルセキュリティ (Global security)]>[安全な通信 (Secure communication)]の順に選択したタブで利用できます。

- メディアサーバーでは、証明書配備のセキュリティレベルが[最高 (Very High)]に設定されている場合、自動証明書配備が無効になります。すべての新しい証明書要求に認証トークンが必要になります。したがって、証明書を配備する前に認証トークンを作成する必要があります。
  詳しい手順については、『NetBackup™ セキュリティおよび暗号化ガイド』の「認証トークンの作成」の項を参照してください。

Amazon S3 対応クラウドストレージへのバックアップジョブが状態コード 41 で失敗する

NetBackup は利用可能な最大の帯域幅を使用し、相応の要求をプッシュしますが、Amazon S3 対応クラウドが多数の要求を処理できません。

クラウドベンダーは要求の速度を低下させる 503 エラーを返し、バックアップジョブは次のエラーで失敗します。

- メディアサーバーで bptm は次のログを記録します。

```
bptm:4940:<media_server_name>: AmzResiliency:
AmzResiliency::getRetryType cURL error: 0, multi cURL error: 0,
HTTP status: 503, XML response: SlowDown, RetryType:
RETRY_EXHAUSTED
```

- メディアサーバーで bpbrm は次のログを記録します。

```
bpbrm Exit: client backup EXIT STATUS 41: network connection timed
out
```

この問題は、NetBackup とクラウドストレージ間で高帯域幅が利用可能な場合にのみ発生します。

トラブルシューティングするには、次のいずれかを実行します。

- 帯域幅の調整を構成して要求の数を減らします。
  p.106 の「NetBackup クラウドストレージサーバーの接続プロパティ」を参照してください。
- 読み取り/書き込みバッファの数を減らします。
  p.103 の「NetBackup クラウドストレージサーバー帯域幅スロットルのプロパティ」を参照してください。
- クラウドベンダーに問い合わせて並列要求の上限の数を増やします。これには追加のコストが発生する可能性があります。

NetBackup CloudStore Service Container の停止と起動

これは、バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ該当します。

NetBackup CloudStore Service Container (nbcssc) サービスを停止および起動します。

p.82 の「NetBackup CloudStore Service Container について」を参照してください。

p.156 の「NetBackup CloudStore Service Container の起動とシャットダウンのトラブルシューティング」を参照してください。

CloudStore サービスコンテナを起動または停止する方法

1. NetBackup Web UI で、[アクティビティモニター (Activity monitor)]をクリックします。
2. [デーモン (Daemons)]タブをクリックします。
3. nbcssc サービスを見つけます。
4. [処理 (Actions)]>[停止 (Stop)]または[処理 (Actions)]>[開始 (Start)]をクリックします。

nbcssc (レガシーメディアサーバー)、nbwmc、nbsl のプロセスを再起動するとすべての cloudstore.conf 設定が元に戻される

欠落エントリとコメントは、cloudstore.conf ファイルでは使用できません。cloudstore.conf ファイルの値を削除またはコメントアウトすると、メディアサーバーで nbcssc (古いメディアサーバー)、nbwmc、nbsl のプロセスを再起動した場合にすべての設定がデフォルト値に戻ります。

NetBackup CloudStore Service Container の起動とシャットダウンのトラブルシューティング

これは、バージョン 7.7.x から 8.1.2 のメディアサーバーにのみ適用されます。

次のトピックを参照してください。

- 「プロビジョニングされていないセキュリティ証明書」
- 「サービスがアクティブなときにセキュリティモードが変更された」

プロビジョニングされていないセキュリティ証明書

クラウドストレージに使う NetBackup メディアサーバーでは、プロビジョニングされたセキュリティ証明書が必要です。そうでない場合は、CloudStore Service Container は開始できません。証明書が存在することを確認します。

p.83 の「NetBackup CloudStore Service Container のセキュリティ証明書」を参照してください。

NetBackup 7.7 から 8.1.2	証明書が存在しない場合は、NetBackup プライマリサーバーから 1 つ作成します。 p.83 の「NetBackup CloudStore Service Container のセキュリティ証明書」を参照してください。

サービスがアクティブなときにセキュリティモードが変更された

サービスがアクティブの間に、NetBackup CloudStore サービスコンテナのセキュリティモードを変更しないでください。サービスがアクティブの間にセキュリティモードが変わると、サービスの起動またはシャットダウンで問題が発生する場合があります。開始時と同じモードでサービスを停止してください。

p.84 の「NetBackup CloudStore Service Container のセキュリティモード」を参照してください。

p.155 の「NetBackup CloudStore Service Container の停止と起動」を参照してください。

GLACIER リストアジョブのキャンセル後に bptm プロセスの終了に時間がかかる

GLACIER にあるイメージのリストアジョブをキャンセルした後で、UNIX メディアサーバーで Amazon GLACIER をリストアすると、bptm プロセスが終了するのに約 4 時間かかります。

回避策

プロセスを手動で強制終了する必要があります。

Amazon Glacier Vault のイメージクリーンアップエラーの処理

このトピックでは、Vault ロックポリシーが Vault に適用されているときに、Amazon Glacier Vault のイメージクリーンアップエラーを処理する方法について説明します。NetBackup ポリシーに設定されている保持期間が、Amazon Glacier Vault ストレージユニットに適用されている Vault ロックポリシーによって強制される期間よりも短い場合に、イメージクリーンアップは失敗します。

イメージのエラーをクリーンアップするには、
https://support.cohesity.com/s/article/article-100042245 を参照してください。

孤立したアーカイブの手動によるクリーンアップ

メタデータオブジェクトが存在しないために、Amazon Glacier Vault の孤立したイメージをクリーンアップできない場合があります。メタデータオブジェクトには、データオブジェクトと NetBackup イメージ間のマッピング情報が含まれています。

Amazon Glacier Vault の孤立したアーカイブを手動でクリーンアップするには、https://support.cohesity.com/s/article/article-100042314 を参照してください。

Amazon Glacier Vault からのリストアが 1 つのフラグメントで 24 時間より長くかかる

Amazon Glacier Vault に保存されたアーカイブが取得されると、その後ダウンロードできるのは 24 時間だけです。リストアジョブ (Amazon Glacier Vault に存在するイメージ用) の 1 つのフラグメントのダウンロードに 24 時間よりも長い時間がかかる場合、イメージの読み込み中にリストアジョブが失敗する可能性があります。NetBackupたとえば、フラグメントサイズが 512 GB でリストア速度が 50 Mbps 未満の場合、リストアは失敗します。

このような状況から回復するには、次のいずれかの操作を行います。

- チェックポイントリストアを使用します。
- 残りのファイルのリストアを開始します。
- フラグメントサイズを小さくして、イメージを複製します。

GLACIER_VAULT からのリストアが Oracle データベースで 24 時間より長くかかる

Oracle でのリストアジョブは、まずデータファイルがリストアされ (データファイルごとに 1 つのジョブ)、次にデータファイルに関連付けられているアーカイブログの各セット (ログのセットごとに 1 つのリストアジョブ) がリストアされるようになっています。これにより、Oracle リストアジョブでは、5 つのリストアジョブが連続して実行されることになります (1 つのリストアジョブが終了すると、次のジョブが自動的に開始される)。Amazon Glacier クラウドストレージの Vault にデータが含まれるすべての新しいリストアジョブでは、データをオンプレミスに移すためのデータ取得に最短で 4 時間が必要になります。このため、Oracle データファイルのリストアジョブの実行に、24 時間以上かかることになります。

リカバリを実行するための、2 つのオプションがあります。

NetBackup for Oracle リカバリウィザードの使用

[リストア/リカバリの並列ストリーム数 (Number of parallel streams for restore and recover)]を、必要なバックアップ要求の数まで増やします。例: 10. Oracle RMAN は必要な数のストリームのみを使うため、この数値には大きな数を設定できます。

『NetBackup for Oracle 管理者ガイド』で、NetBackup for Oracle のリストアに関する説明を参照してください。

RMAN テンプレートの使用

この手順は、前述の方法よりも長い時間がかかります。

1. リカバリ手順 (アーカイブログのリストア) に必要なログシーケンスとスレッド数を確認します。これは、Oracle を確認するか、バックアップジョブを確認するとわかります。
2. RMAN スクリプトを作成し、アーカイブログのリストアを実行するために必要なチャネル数を割り当てます。

   たとえば、8 個のチャネルが割り当てられていて、リストアされたシーケンス番号が 1373 から 1380 の「run」ブロックについて考えます。

```
RMAN> run

{ allocate channel ch00 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';

allocate channel ch01 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';

allocate channel ch02 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';

allocate channel ch03 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';

allocate channel ch04 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';

allocate channel ch05 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';

allocate channel ch06 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';

allocate channel ch07 type 'SBT_TAPE' PARMS
'SBT_LIBRARY=/bp/bin/libobk.so64';
```

   シーケンス 1373 スレッド 1 からシーケンス 1380 スレッド 1 までアーカイブログをリストアします。

```
release channel ch00;

release channel ch01;

release channel ch02;

release channel ch03;

release channel ch04;

release channel ch05;

release channel ch06;

release channel ch07;
```

```
}
```

3. NetBackup for Oracle クライアントを使用して、NetBackup のバックアップ、アーカイブ、リストアインターフェースを起動するか、別のスクリプトを作成してデータファイルをリストアします。複数のデータファイルをリストアしているときに、各データファイルが異なるイメージに含まれる場合は、ストリームの数を増やす必要があることがあります。
4. データファイルとアーカイブログのリストアを開始し、並行して実行します。
5. NetBackup のバックアップ、アーカイブ、リストアインターフェースか、別のスクリプトを使用して、データベースまたはデータファイルのリカバリを実行します。

『NetBackup for Oracle 管理者ガイド』を参照してください。

Amazon IAM アクセス権がないために発生するエラーのトラブルシューティング

NetBackup クラウド構成に指定された AWS クレデンシャルに S3 または Glacier に関連するアクセス権がない場合、構成、バックアップ、リストアのさまざまな段階でエラーが表示される場合があります。

いくつかのエラーメッセージは、説明が明確で NetBackup 管理者コンソールで識別できますが、曖昧なメッセージもあります。

Amazon では、`AccessDeniedException` のエラーメッセージが表示されます。このエラーメッセージを解読するには、ログファイルを調べて、不足しているアクセス権を確認する必要があります。

- List Vault または List Bucket のアクセス権 (`glacier:ListVaults`) がない場合。このエラーは、ストレージサーバーの作成中に発生します。CLI を使用している場合は、クレデンシャルを追加するための `tpcommand` が失敗します。

  `tpcommand` のログで、次に示すような AccessDeniedException を確認します。

  ```
  amazon: Json:
  {"code":"AccessDeniedException","type":"Client","message":"User:
  arn:aws:iam::326221795898:user/Readonly_user is not authorized to
  perform: glacier:ListVaults on resource:
  arn:aws:glacier:ap-south-1:326221795898:vaults/"} 16:17:52.139
  [7388.4424] <2> magmavm1.abc.xyz.qwe.com: AmzVaultApi:
  json_string({"code":"AccessDeniedException","type":"Client","message":"User:
  arn:aws:iam::326221795898:user/Readonly_user is not authorized to
  perform: glacier:ListVaults on resource:
  arn:aws:glacier:ap-south-1:326221795898:vaults/"}) 16:17:52.139
  [7388.4424] <16> magmavm1.abc.xyz.qwe.com:
  ```

- Create Vault または Create Bucket のアクセス権 (glicier:CreateVault または glacier:DescribeVault) がない場合。
  このエラーは、NetBackup 管理者コンソールを使用したディスクプールの作成中に発生します。CLI を使用している場合は、nbdevconfig コマンドが失敗します。
  nbrrms のログで、次に示すような AccessDeniedException を確認します。

```
amazon_raw:: AmzVaultApi: Error: server error code
AccessDeniedException, User:
arn:aws:iam::326221795898:user/Readonly_user is not authorized to
perform: glacier:CreateVault on resource:
arn:aws:glacier:ap-south-1:326221795898:vaults/fail-to-create,
httpcode [403] returning [2060037],11:STS Service,1Post Archive
or S3 Object permission missing - backup will fail in activity
monitor.
```

- アーカイブアップロードのアクセス権 (glacier:UploadArchive) がない場合。
  このエラーは、アーカイブのバックアップ中に発生します。バックアップジョブは、アクセス権のエラーで失敗します。
  詳しくは、次に示すような bptm のログを確認します。

```
"code":"AccessDeniedException","type":"Client","message":"User:
arn:aws:iam::3234415151:user/XYZ is not authorized to perform:
glacier:UploadArchive on resource: LSTR-gtwy-00076(debug).
```

- アーカイブ後にジョブを取得するアクセス権 (glacier:InitiateJob) がない場合。
  このエラーは、リストアを開始した後に発生します。
  詳しくは、次に示すような bptm のログを確認します。

```
"code":"AccessDeniedException","type":"Client","message":"User:
arn:aws:iam::3234415151:user/XYZ is not authorized to perform:
glacier:InitiateJob on resource: LSTR-gtwy-00076(debug).
```

- Retrieve Archive または Retrieve Object のアクセス権 (glacier:GetJobOutput) がない場合。
  このアクセス権がないと、ジョブをポストした後に NetBackup がアーカイブをダウンロードできない場合に、リストアジョブが未完了の状態になります。
  詳しくは、次に示すような bptm のログを確認します。

```
"code":"AccessDeniedException","type":"Client","message":"User:
arn:aws:iam::3234415151:user/XYZ is not authorized to perform:
glacier:GetJobOutput on resource: LSTR-gtwy-00076(debug).
```

- Delete Archive または Delete Object のアクセス権 (glacier:DeleteArchive) がない場合。
  このアクセス権がないと、イメージのクリーンアップまたはイメージの有効期限の処理が失敗します。
  詳しくは、次に示すような bpdm のログを確認します。

```
"code":"AccessDeniedException","type":"Client","message":"User:
arn:aws:iam::3234415151:user/XYZ is not authorized to perform:
glacier:DeleteArchive on resource: LSTR-gtwy-00076(debug).
```

リストアジョブの開始時刻がバックアップジョブの終了時刻と重なるとリストアジョブが失敗する

バックアップジョブが完了してから数秒以内にリストアジョブを開始すると、リストアジョブは次のエラーで失敗します。

```
Standard policy restore error
```

このようなシナリオでは、クラウドプロバイダがリストアの実行に必要なパラメータを更新する時間を必要とするため、リストアジョブは失敗します。したがって、リストアは、バックアップジョブが完了してから数分後に実行してください。

Azure アーカイブからのリストアの後処理が失敗する

Azure アーカイブからのリストアの後処理が失敗すると、blob はリストア後にホット層からアーカイブ層に移動されません。

ホット層からアーカイブ層に blob を移動するには、次の手順に従います。

- blob の一覧表示操作を使用して、接頭辞が REHYDRATE_PENDING の blob 一覧を取得します。REHYDRATE_PENDING/<image_name> という形式の blob 名が返されます。
- 接頭辞 <image_name>/ で blob を検索し、接頭辞の後が整数形式になっている blob 名でフィルタ処理します。
  次に例を示します。
  imagename_1544519515_C1_F1 というイメージ名があるとします
  後処理に選択される blob - imagename_1544519515_C1_F1/21
  選択されない blob - imagename_1544519515_C1_F1/imagename_1544519515/0
- 上に示す手順で返される blob のアクセス層をホットアクセス層からアーカイブアクセス層に変更するには、blob で blob 層設定操作を使用します。

  メモ: META_BLOCK_MAP_FILE と META_IMAGE_PROPERTIES、および blob はアーカイブ層に移動しないでください。

- blob をアーカイブアクセス層に正常に移動したら、blob 削除操作を使用して、接頭辞が REHYDRATE_PENDING の blob を削除します。

Amazon Snowball および Amazon Snowball Edge の問題のトラブルシューティング

ディスクプールの作成に失敗する

クラウドストレージプロパティを Amazon Snowball エンドポイントに変更すると、ディスクプールの作成が失敗します。次のエラーが発生します。

```
No Volumes found.
```

トラブルシューティングするには:

OFFLINE_TRANSFER_MODE ストレージサーバープロパティが PROVIDER_API に設定されていることを確認します。

リストアが失敗する

リストアが次のエラーで失敗します。

```
The specified key does not exist.
```

リストアするイメージが正常にクラウドにインポートされませんでした。クラウドへのイメージ複製操作を再実行し、リストアを実行します。

bpduplicate コマンドを実行します。『NetBackup コマンドリファレンスガイド』を参照してください。

クラウドへのインポートが失敗する

クラウドへのイメージ複製操作を実行します。bpduplicate コマンドを使用します。『NetBackup コマンドリファレンスガイド』を参照してください。

その他の問題については、構成が適切に行われていることを確認します。「NetBackup with Amazon Snowball and Snowball Edge Configuration Checks」テクニカルノートを参照してください。

索引

記号

インデックスマーカーを 1 つ以上追加する 72
クラウド
　ストレージユニットのプロパティ 117
クラウドストレージ
　Amazon S3 の API 形式 15
　Microsoft Azure API 形式 63
　構成 73
クラウドストレージを構成する 73
クラウドストレージサーバー
　の暗号化プロパティ 112
　［帯域幅 (Bandwidth)］プロパティ 103
クラウドプライマリホスト 98
ストレージサーバー
　について 95
ストレージサーバー (storage server)。「クラウドストレージサーバー」を参照
ストレージユニット
　クラウドのプロパティ 117
　重複排除用の構成 117
ストレージユニット名 (Storage unit name) 118
ストレージユニット形式 (Storage unit type) 118
ディスク形式 (Disk Type) 118
バックアップの失敗
　NetBackup CloudStore Service Container が非アクティブ 152
　［任意のメディアサーバーを使用 (Use any available media server)］オプション 153
プライベートクラウド
　Amazon S3 対応クラウドプロバイダ 27
プロパティ
　帯域幅 103
　暗号化 112
ホスト ID ベースの証明書
　トークンなしの配備 90
　トークンを使った配備 90
ホスト名ベースの証明書
　配備 89
仮想プライベートクラウド 29
優先設定
　スロットル調整 112
　暗号化 113
動的ホスト構成プロトコル (DHCP) 89
外部 KMS 94
帯域幅
　スロットル調整 103
拡張性のあるストレージのホストプロパティを利用できない 147
最大フラグメントサイズ (Maximum fragment size) 119
最大並列実行ジョブ数 (Maximum concurrent jobs) 119
最適化された合成バックアップ
　概要 121
構成
　ディスクプールの構成ウィザード 114
機能 8
統合ログ 137
　ファイルの形式 138
統合ログのジョブ ID 検索 141
要件 74
認証局 (CA) 90
重複排除ストレージユニット
　任意のメディアサーバーを使用 (Use any available media server) 118
　次のメディアサーバーのみ使用する (Only use the following media servers) 118
重複排除ストレージユニットの構成 117
［暗号化 (Encryption)］
　プロパティ 112

A

Amazon
　glacier vault 39～40
amazon
　仮想プライベートクラウド 29
amazon (S3)
　権限 17
Amazon Amazon S3 Intelligent Tiering
　リストア 46
Amazon GLACIER
　長期保護 32
Amazon Glacier 31
Amazon Glacier Deep Archive 31

Amazon Glacier Vault 31
Amazon IAM ロール 46
Amazon S3
クレデンシャルブローカーの詳細 26
概要 15
要件 16
Amazon S3 Intelligent Tiering
クラウド階層化 42
バックアップ 44
Amazon Snowball 51
Amazon S3 API インターフェースを使用した構成 54
Amazon Snowball クライアントの構成 53
Amazon Snowball Edge 51
S3 API インターフェースを使用した構成 59
ファイルインターフェースを使用した構成 57

B

bpstsinfoコマンド
操作上の注意事項 132

C

CloudStore Service Container
サービスがアクティブなときにセキュリティモードが変更された 157
セキュリティモード 84
CloudStore サービスコンテナ
の起動とシャットダウンのトラブルシューティング 156

F

FlashBackup ポリシー
［最大フラグメントサイズ (Maximum fragment size)］(ストレージユニット設定) 119

G

glacier vault
バックアップ 39
リストア 40

H

hotfix 89

I

IAM ロール 49

M

Microsoft Azure
概要 63
構成オプション 64
構成オプション (詳細) 66
要件 64

N

NetBackup
hotfix 89
NetBackup Service Layer (NBSL) 89
NetBackup の拡張性のあるストレージのホストプロパティを利用できない 147
NetBackup アクセラレータ
概要 121

V

VPC 29
vxlogview コマンド 138
ジョブ ID オプション 141